INFORMATION SECURITY TRAINING

SANSFIRE 2019
Washington, DC | June 15-22

The Most Trusted Source for Information Security Training, Certification, and Research

Protect your business and advance your career with more than 40 hands-on, immersion-style courses taught by real-world practitioners.

See inside for courses and GIAC certifications in:

- Cyber Defense
- Penetration Testing
- Ethical Hacking
- Digital Forensics
- Security Management
- Incident Response
- ICS/SCADA Security
- Cloud Security
- Critical Security Controls
- Legal
- SIEM
- Detection & Monitoring
- Cyber Threat Intelligence
- Secure Development

SAVE $350
Register and pay by April 24th
Use code EarlyBird19

www.sans.org/sansfire

"SANS training provides instant value! I sent my team five improvement action items driven by today’s content. Plus, I have a plan to implement network log collection that will likely save me over $100k in expenses for our current budget cycle.”

- Rob Conn, EchoStar
Courses at a Glance

For an up-to-date course list, please check the website at www.sans.org/sansfire/schedule

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Pg.</th>
<th>Available via Simulcast</th>
<th>Bundle Discounted with this course</th>
<th>Meet DoD 8540 (8570) Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC301</td>
<td>Introduction to Cyber Security</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC440</td>
<td>Critical Security Controls: Planning, Implementing, and Auditing</td>
<td>88</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC455</td>
<td>SIEM Design and Implementation</td>
<td>88</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC487</td>
<td>Open-Source Intelligence (OSINT) Gathering and Analysis</td>
<td>14</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC501</td>
<td>Advanced Security Essentials – Enterprise Defender</td>
<td>16</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC503</td>
<td>Intrusion Detection In-Depth</td>
<td>18</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC515</td>
<td>Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td>20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC525</td>
<td>Securing Windows and PowerShell Automation</td>
<td>22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC564</td>
<td>Secured Unix Security Administrator</td>
<td>24</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC567</td>
<td>Continuous Monitoring and Security Operations</td>
<td>26</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC574</td>
<td>Cloud Security &amp; Risk Fundamentals</td>
<td>28</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC580</td>
<td>Defensible Security Architecture</td>
<td>30</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC595</td>
<td>SIEM with Tactical Analytics</td>
<td>32</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC606</td>
<td>Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td>34</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC609</td>
<td>Defeating Advanced Adversaries – Purple Team Tactics &amp; Kill Chain Defenses</td>
<td>36</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC640</td>
<td>Enterprise Threat and Vulnerability Assessment</td>
<td>40</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC642</td>
<td>Web App Penetration Testing and Ethical Hacking</td>
<td>42</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC660</td>
<td>Network Penetration Testing and Ethical Hacking</td>
<td>44</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC664</td>
<td>Red Team Operations and Threat Emulation</td>
<td>46</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC673</td>
<td>Automating Information Security with Python</td>
<td>48</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC675</td>
<td>Mobile Device Security and Ethical Hacking</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC677</td>
<td>Wireless Penetration Testing and Ethical Hacking</td>
<td>52</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC680</td>
<td>Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques</td>
<td>54</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC689</td>
<td>Advanced Penetration Testing, Exploit Writing, and Ethical Hacking</td>
<td>56</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC700</td>
<td>Windows Forensic Analysis</td>
<td>58</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC708</td>
<td>Advanced Digital Forensics, Incident Response, and Threat Hunting</td>
<td>60</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC718</td>
<td>Mac and iOS Forensics and Incident Response</td>
<td>62</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC726</td>
<td>Advanced Memory Forensics &amp; Threat Detection</td>
<td>64</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC732</td>
<td>Advanced Network Forensics: Threat Hunting, Analysis &amp; Incident Response</td>
<td>66</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC739</td>
<td>Cyber Threat Intelligence</td>
<td>68</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC758</td>
<td>Smartphone Forensic Analysis In-Depth</td>
<td>70</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC761</td>
<td>Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td>
<td>72</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC765</td>
<td>SANS Training Program for CISSP® Certification</td>
<td>74</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MTG106</td>
<td>A Practical Introduction to Cyber Security Risk Management</td>
<td>76</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MTG107</td>
<td>SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program</td>
<td>78</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MTG108</td>
<td>Security Leadership Essentials for Managers</td>
<td>80</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MTG109</td>
<td>Strategic Planning, Policy, and Leadership</td>
<td>82</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L005</td>
<td>Law of Data Security and Investigations</td>
<td>84</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CV051</td>
<td>Secure I/Os and Cloud Application Security</td>
<td>86</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CS410</td>
<td>ICS/SCADA Security Essentials</td>
<td>88</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CS515</td>
<td>ICS Active Defense and Incident Response</td>
<td>90</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DFIR</td>
<td>DFIR NetWars Tournament</td>
<td>92</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber Defense NetWars Tournament</td>
<td>94</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Institute</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>The SANS Faculty</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Securing Approval &amp; Budget for Training</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Build a High-Performing Security Organization</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>SANS Training Roadmap</td>
<td></td>
<td>6-7</td>
</tr>
<tr>
<td>SANS OnDemand Bundle</td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>GIAC Certification Bundle</td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>GIAC Certifications</td>
<td></td>
<td>38</td>
</tr>
<tr>
<td>NetWars</td>
<td></td>
<td>39</td>
</tr>
<tr>
<td>Bonus Sessions</td>
<td></td>
<td>91-93</td>
</tr>
<tr>
<td>Vendor-Sponsored Events</td>
<td></td>
<td>93</td>
</tr>
<tr>
<td>SANS Simulcast</td>
<td></td>
<td>94</td>
</tr>
<tr>
<td>Future SANS Training Events</td>
<td></td>
<td>95</td>
</tr>
<tr>
<td>Hotel Information</td>
<td></td>
<td>96</td>
</tr>
<tr>
<td>Registration Information</td>
<td></td>
<td>96</td>
</tr>
<tr>
<td>SANS Simulcast Registration</td>
<td></td>
<td>96</td>
</tr>
<tr>
<td>SANS Voucher Program</td>
<td></td>
<td>97</td>
</tr>
<tr>
<td>Registration Fees</td>
<td></td>
<td>97</td>
</tr>
<tr>
<td>Free Resources</td>
<td></td>
<td>Back Cover</td>
</tr>
</tbody>
</table>
At the SANS Institute, our mission is to deliver the cutting-edge information security knowledge and skills that companies, military organizations, and governments need to protect their people and assets.

TRAINING ON THE CUTTING EDGE
SANS offers more than 65 unique courses, all designed to align with dominant security team roles, duties, and disciplines. Our courses prepare students to face today’s threats and tomorrow’s challenges.


In SANS courses, students are immersed in hands-on lab exercises designed to help them practice, hone, and perfect what they’ve learned. And we constantly update and rewrite our courses to be sure the tools and techniques we’re teaching are always current, and on the cutting edge.

LEARN FROM THE BEST
The SANS faculty is simply unmatched. All of our instructors are active security practitioners, bringing their extensive knowledge and real-world experiences directly to the classroom.

SANS instructors work for high-profile organizations as red team leaders, CISOs, technical directors, and research fellows. In addition to their respected technical credentials, they’re also expert teachers. Their passion for the topics they teach shines through, making the SANS classroom—both live and online—dynamic and effective.

GIAC SKILLS VALIDATION
GIAC certifications are designed to ensure that students can apply their knowledge and skills in a real-world setting. More than 30 certifications align with SANS training courses, validating student mastery for professional use in critical, specialized InfoSec domains and job-specific roles. See www.giac.org for more information.

A TRAINING FORMAT FOR EVERY STUDENT
SANS holds more than 300 live training events around the world each year, so you can find a convenient time and place to take your course. These events provide an engaging learning environment and multiple opportunities to network with other security professionals, SANS instructors, and staff.

SANS training is also offered online, with several convenient options to suit your learning style. All of our online courses include at least four months of access to the course material, so students can revisit and rewind content anytime, anywhere.

RECOGNIZED AS A SUPERIOR INVESTMENT
Information security professionals from every member of the Fortune 100, and from small and mid-sized firms alike, say they return to SANS training again and again because they trust their training will result in practical and high-quality capabilities. SANS training is also embedded in government and military programs in the United States and allies around the world for the same reason.

Customer feedback drives our continuous effort to maintain the quality and impact of SANS training, so that we continue to deserve your trust.

THE SANS PROMISE
At the heart of everything we do is the SANS Promise: Students will be able to use their new skills as soon as they return to work.

REGISTER FOR SANS TRAINING
Learn more about SANS courses, and register online, at www.sans.org

The SANS suite of education resources for information security professionals includes:

- SANS Training: Live & Online
- GIAC Certifications
- Graduate Degree Programs
- NETWARS Experience
- Security Awareness
- CyberTalent
At SANS, our course authors and instructors are renowned cybersecurity experts who share their knowledge through their own real-world examples and top-shelf curriculum. Industry professionals choose SANS training again and again, year after year, for access to these highly regarded experts.

There are only about 100 individuals in the world currently qualified as SANS Certified Instructors. Each is selected after proving his or her technical and teaching expertise through years of work and success. The instructors are the founders of international cybersecurity organizations, authors of best-selling books, and developers of the world’s most advanced cyber ranges and Capture-the-Flag challenges. Many are regularly called upon to share their expertise with government and commercial organizations around the world.

In addition to their impressive résumés, every member of the SANS faculty is fully committed to providing the most comprehensive training possible. Our instructors do more than just stand in front of a classroom—they’re present for their students every step of the way, with follow-ups, webcasts, mentoring, and more. Their goal is your success, and that dedication is what truly sets SANS training apart from all the rest.

Whether you train with SANS online or at one of our live events, we promise you’ll be able to apply what you learn from these top-tier instructors as soon as you return to work.

“I have attended several SANS classes over the years and I am always impressed with the level of knowledge and professionalism of the instructors.”

Ron Foupht, Sirius Computer Solutions

Meet the SANS faculty: www.sans.org/sansfire/instructors
Securing Approval and Budget for Training

Packaging matters
Write a formal request

- All organizations are different, but because training requires a significant investment of both time and money, most successful training requests are made via a written document (short memo and/or a few Powerpoint slides) that justifies the need and benefit. Most managers will respect and value the effort.
- Provide all the necessary information in one place. In addition to your request, provide all the right context by including the summary pages on Why SANS?, the Training Roadmap, the instructor bio, and additional benefits available at our live events or online.

Clearly state the benefits
Be specific

- How does the course relate to the job you need to be doing? Are you establishing baseline skills? Transitioning to a more focused role? Decision-makers need to understand the plan and context for the decision.
- Highlight specifics of what you will be able to do afterwards. Each SANS course description includes a section titled “You Will Be Able To.” Be sure to include this in your request so that you make the benefits clear. The clearer the match between the training and what you need to do at work, the better.

Set the context
Establish longer-term expectations

- Information security is a specialized career path within IT with practices that evolve as attacks change. Because of this, organizations should expect to spend 6%-10% of salaries to keep professionals current and improve their skills. Training for such a dynamic field is an annual, per-person expense—not a once-and-done item.
- Take a GIAC Certification exam to prove the training worked. Employers value the validation of skills and knowledge that a GIAC Certification provides. Exams are psychometrically designed to establish competency for related job tasks.
- Consider offering trade-offs for the investment. Many professionals build annual training expenses into their employment agreements even before joining a company. Some offer to stay for a year after they complete the training.
Build a **High-Performing Security Organization**

**Based on our global research, SANS has identified effective strategies for building an information security group:**

*Use practical organizing principles* to design your plan. Nearly all of the more complex frameworks may be reduced to a few simpler constructs, such as “Build and Maintain Defenses – Monitor and Detect Intrusion – Proactively Self-Assess – Respond to Incidents.”

| Use practical organizing principles | Prioritize your efforts within these areas, using the Center for Internet Security Critical Controls, as you mature your own organization. | Determine the number and types of professionals you need to perform the hands-on work, then launch an ongoing campaign to develop a team with the appropriate skills in mind. Cybersecurity is a specialized practice area within IT, and demands specialized training. |

The job roles and skills required in information security grow and change as the organization scales. While every professional needs a baseline of knowledge and capabilities in cyber defense and incident response, over time you will develop specialized members of your team to work together in particular areas.

Four critical job roles typically emerge:

- **Security Monitoring & Detection Professionals** – Identifying security anomalies within your environment requires an increasingly sophisticated set of skills. All too often, vendor training teaches to the tool, without explaining how the tool works or how it can be best used. To deploy detection and monitoring tools and interpret their output, you need a more robust understanding of tools, techniques, and analysis.

- **Pen Testers & Vulnerability Analysts** – A professional who can find weaknesses is often a different breed than one focused exclusively on building defenses. A basic tenet of red team/blue team deployments is that finding vulnerabilities requires a different set of tools and a different way of thinking, but it’s still essential in improving defenses.

- **Forensic Investigators & Incident Responders** – Larger organizations need specialized professionals who can move beyond first-level incident response. Whether you’re maintaining a trail of evidence or hunting for threats, you need the skills to analyze attacks and develop appropriate remediation and recovery plans.

- **Security Managers** – As their staffs of talented technologists grow, organizations require effective leaders to manage them. These managers won’t necessarily perform hands-on work, but they must understand enough about underlying technologies and frameworks to help set security strategy, develop appropriate policies, interact with their skilled practitioners, and measure outcomes.

Within (or beyond) these four areas, a high-performing security organization will develop individuals further, with some individual professionals able to cover more areas, while others go deeper into just one specialty. Along the entire spectrum from Active Defense to Cloud Defense, and from Python for InfoSec professionals to Malware Reengineering, SANS offers more than 30 courses to train for specialized roles or learn about more advanced topics, meeting the needs of security professionals at every level.
### Crucial Skills, Specialized Roles

SANS’s comprehensive career offerings enable professionals to deepen their technical skills in key practice areas. The courses also address other topics and audiences, such as security training for software developers, industrial control engineers, and non-technical personnel in management, legal, and audit.

#### Cyber Defense Operations

<table>
<thead>
<tr>
<th>Role</th>
<th>Course Title</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Specialized Defensive Area</strong></td>
<td><strong>Advanced Enterprises</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Advanced Cybersecurity Program</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Penetration Testing</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Incident Response &amp; Threat Hunting</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Continuous Monitoring and Security Operations</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Virtualized Data Centers</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Security Architecture</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Threat Defense</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Advanced Generalist</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Specialized Defensive Area</strong></td>
</tr>
<tr>
<td></td>
<td><strong>SIEM</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Cloud Security</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Intrusion Detection</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Scan Packets &amp; Networks</strong></td>
</tr>
</tbody>
</table>

#### Industrial Control Systems

<table>
<thead>
<tr>
<th>Role</th>
<th>Course Title</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ICS Security Professionals</strong></td>
<td><strong>ICS Security Essentials</strong></td>
</tr>
<tr>
<td></td>
<td><strong>RCS/SCADA Security Essentials</strong></td>
</tr>
<tr>
<td></td>
<td><strong>ICS Security Essentials</strong></td>
</tr>
<tr>
<td></td>
<td><strong>ICS/SCADA Security</strong></td>
</tr>
<tr>
<td></td>
<td><strong>ICS/SCADA Security Professionals</strong></td>
</tr>
</tbody>
</table>

#### Development & Secure Coding

<table>
<thead>
<tr>
<th>Role</th>
<th>Course Title</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Every Developer Should Know</strong></td>
<td><strong>Secure Web Apps</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Penetration Testing</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Incident Response &amp; Threat Hunting</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Continuous Monitoring and Security Operations</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Virtualized Data Centers</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Security Architecture</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Threat Defense</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Advanced Generalist</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Specialized Defensive Area</strong></td>
</tr>
<tr>
<td></td>
<td><strong>SIEM</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Cloud Security</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Intrusion Detection</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Scan Packets &amp; Networks</strong></td>
</tr>
</tbody>
</table>

---

### Focus Job Roles

1. **You are experienced in technology, but need to learn hands-on, essential security skills and techniques**

2. **You are experienced in security, preparing for a specialized job role or focus**

   - **Penetration Testing**
   - **Incident Response & Threat Hunting**

3. **You are a candidate for specialized or advanced training**

---

### New to Cyber Security

<table>
<thead>
<tr>
<th>Concepts, Terms, &amp; Skills</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline Skills</td>
</tr>
<tr>
<td>Core Techniques</td>
</tr>
<tr>
<td>Security Management</td>
</tr>
</tbody>
</table>

---

### Core Techniques

- **Prevent, Defend, Maintain**
  - **Every Security Professional Should Know**
    - **Security Essentials**
      - **SECO4 Security Essentials Bootcamp Style**
    - **SECC7 SEC506 Security Essentials Bootcamp Style**
    - **SECO5 Hacker Tools, Techniques, Exploits, and Incident Handling**
  - **Every Professional Should Know**
    - **SECO6 Security Essentials Bootcamp Style**
    - **SECO8 Hacker Tools, Techniques, Exploits, and Incident Handling**

---

### Security Management

- **Managing Technical Security Operations**
  - **Every Security Manager Should Know**
    - **SECO9 Security Management and Incident Handling**
      - **SECO9 Management and Incident Handling**
    - **SECO10 Implementing and Auditing the Security Program**
      - **SECO10 Implementing and Auditing the Security Program**

---

### Security Fundamentals

- **SECO7 Introduction to Cyber Security**
  - **SECO7 Introduction to Cyber Security**
  - **SECO8 Hacker Tools, Techniques, Exploits, and Incident Handling**

---

### Training Roadmap | Development Paths

**Key:**
- **Essentials**
- **Specialized**
- **Advanced**
- **Certification**
- **Certified**
- **Master**

---

### See in-depth course descriptions and the digital version of this roadmap at:

- [www.sans.org/roadmap](http://www.sans.org/roadmap)
- [www.sans.org/courses](http://www.sans.org/courses)

---

**To learn more about additional SANS courses,**

[www.sans.org/courses](http://www.sans.org/courses)
Extend and Validate Your Training

Add an **OnDemand Bundle** OR **GIAC Certification Attempt**
to your course within seven days of this event to get bundle pricing.*

Extend Your Training Experience with an **OnDemand Bundle**
- **Four months** of supplemental online review
- **24/7** online access to your course lectures, materials, quizzes, and labs
- Subject-matter-expert support to help you increase your retention of course material

**OnDemand Bundle price – $769**

“The course content and OnDemand delivery method have both exceeded my expectations.”
- ROBERT JONES, TEAM JONES, INC.

Get Certified with **GIAC Certifications**
- Distinguish yourself as an information security leader
- **30+ GIAC cybersecurity certifications** available
- Two practice exams included
- Four months of access to complete the attempt
- Save over $1,100 when added to your SANS training

**GIAC bundle price – $769**

“GIAC is the only certification that proves you have hands-on technical skills.”
- CHRISTINA FORD, DEPARTMENT OF COMMERCE

More Information
www.sans.org/ondemand/bundles  |  www.giac.org

*GIAC and OnDemand Bundles are only available for certain courses.
Benefits of Attending a Live SANS Training Event

This live SANS training event is just one of many held throughout North America each year. Every SANS event provides hands-on, skills-based training that can be applied immediately to your work, and you’ll learn from the best practitioners in the industry.

Our live training events take place in many popular and convenient locations and host thousands of cybersecurity professionals. SANS also schedules local events throughout the year in most major metropolitan areas, bringing our top cybersecurity courses to the professionals who need them.

SANS live training events provide you with:

- Immersion training without home or office distractions
- Access to top SANS cybersecurity instructors who are renowned experts in the field
- A variety of networking opportunities
- Hands-on experience through NetWars challenges
- Content-loaded SANS@Night bonus sessions
- Exposure to leading solution providers at Vendor Showcases, lunch and learns, industry receptions, and more

“Attending live training events puts you in the same location with a large number of security professionals. It is a fantastic opportunity to network and socialize with so many people and not just those in your same training class.”

-Scott Meyer, Fortive

“Nothing beats interacting with peers and subject-matter experts on a one-on-one basis for rapid assimilation of information in a manner that is retainable. SANS live training facilitates that superbly.”

-Tom Stogdale, Honeywell

Visit sans.org/live-training to view the 2019 live training calendar and register for your courses.
SEC301: Introduction to Cyber Security

You Will Be Able To

- Communicate with confidence regarding information security topics, terms, and concepts
- Understand and apply the Principles of Least Privilege
- Understand and apply the Confidentiality, Integrity, and Availability (CIA) Triad
- Build better passwords that are more secure while also being easier to remember and type
- Grasp basic cryptographic principles, processes, procedures, and applications
- Understand computer network basics
- Have a fundamental grasp of any number of critical technical networking acronyms, including TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS
- Utilize built-in Windows tools to see your network settings
- Recognize and be able to discuss various security technologies, including anti-malware, firewalls, and intrusion detection systems, content filters, sniffers, etc.
- Build a simple but fully functional firewall configuration
- Secure your browser using a variety of security plug-ins
- Secure a wireless access point (also known as a wireless router)
- Scan for malware, clean malware from a system, and whitelist legitimate software identified by an anti-malware scanner as “potentially unwanted”
- Access a number of websites to better understand password security, encryption, phishing, browser security, etc.

To determine if SANS SEC301: Introduction to Cyber Security is right for you, ask yourself five simple questions:

- Do you have basic computer knowledge, but are new to cybersecurity and in need of an introduction to the fundamentals?
- Are you bombarded with complex technical security terms that you don’t understand?
- Are you a non-IT security manager who lays awake at night worrying that your company will be the next mega-breach headline story on the 6 o’clock news?
- Do you need to be conversant in basic security concepts, principles, and terms, even if you don’t need “deep in the weeds” detail?
- Have you decided to make a career change to take advantage of the job opportunities in cybersecurity and need formal training and certification?

If you answer yes to any of these questions, then the SEC301: Introduction to Cyber Security training course is for you. Students with a basic knowledge of computers and technology but no prior cybersecurity experience can jump-start their security education with insight and instruction from real-world security experts in SEC301.

This completely revised and comprehensive five-day course covers a wide range of baseline topics, including terminology, the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles. The hands-on, step-by-step learning format will enable you to grasp all the information presented even if some of the topics are new to you. You’ll learn fundamentals of cybersecurity that will serve as the foundation of your security skills and knowledge for years to come.

Written by a security professional with over 30 years of experience in both the public and private sectors, SEC301 provides uncompromising real-world insight from start to finish. The course prepares you for the Global Information Security Fundamentals (GISF) certification test, as well as for the next SANS course in this progression, SEC401: Security Essentials Bootcamp Style. It also delivers on the SANS promise: You will be able to use the knowledge and skills you learn in SEC301 as soon as you return to work.

“You provided a great foundation for the topic of security, since I deal with it on a daily basis on a high level.”

- Richard Pollich, Broadridge Financial Solutions Inc.

Keith Palmgren is an IT security professional with over 30 years of experience specializing in the field. He began his career with the U.S. Air Force working with cryptographic keys and codes management. He also worked in what was at the time the newly-formed Air Force computer security department. Following the Air Force, Keith worked as an MIS director for a small company before joining AT&T/Lucent as a Senior Security Architect working on engagements with the DoD and the National Security Agency. Later, as Security Consulting Practice Manager for both Sprint and Netigy, Keith built and ran the security consulting practice. He was responsible for all security consulting worldwide and for leading dozens of security professionals on many consulting engagements across all business spectrums. For the last several years, Keith has run his own company, NetIP, Inc. He divides his time between consulting, training, and freelance writing projects. In his career, Keith has trained over 10,000 IT professionals and authored more than 20 IT security training courses including the SANS SEC301 course. Keith currently holds 10 computer security certifications (CISSP®, GSEC, GCIH, GCED, GISF, CEH, Security+, Network+, A+, CTT+).

@kpalmgren
DAY 1: Security’s Foundation
Every good security practitioner and every good security program begins with the same mantra: learn the fundamentals. SEC301 starts by instilling familiarity with core security terms and principles. By the time you leave the classroom after the first day, you will fully understand the Principle of Least Privilege and Confidentiality, Integrity, Availability (CIA), and you’ll see why those principles drive all security discussions. You will be conversant in the fundamentals of risk management, security policy, and authentication/authorization/accountability.

DAY 2: Computer Functions and Networking
This course day begins with an explanation of how computers handle numbers using decimal, binary, and hexadecimal numbering systems. It also provides an understanding of how computers encode letters using the American Standard Code for Information Interchange (ASCII). We then spend the remainder of the day on networking. All attacks or exploits have one thing in common: they take something that exists for perfectly valid reasons and misuse it in malicious ways. Always! So as security practitioners, to grasp what is invalid we must first understand what is valid – that is, how things like networks are supposed to work. Only once we have that understanding can we hope to understand the mechanics of malicious misuse of those networks – and only with that knowledge can we understand how security devices such as firewalls seek to thwart those attacks. The networking discussion begins with a non-technical explanation of how data move across a network. From there we move to fundamental terminology dealing with network types and standards. You’ll learn about common network hardware such as switches and routers, and terms like “protocol” and “encapsulation.” We’ll give a very basic introduction to network addressing and port numbers and then work our way up the Open Systems Interconnection (OSI) protocol stack, introducing more detail only as we proceed to the next layer. In other words, we explain networking starting in non-technical terms and gradually progress to more technical detail as students are ready to take the next step. By the end of our discussions, you’ll have a fundamental grasp of any number of critical technical networking acronyms that you’ve often heard but never quite understood, including TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS.

DAY 3: An Introduction to Cryptography
Cryptography is one of the most complex issues faced by security practitioners. It is not a topic you can explain in passing, so we will spend some time on it. Not to worry, we won’t take you through the math behind cryptography. Instead, we learn basic crypto terminology and processes. What is steganography? What is substitution and transposition? What is a “work factor” in cryptography and why does it matter? What do we mean by symmetric and asymmetric key cryptography and “cryptographic hash,” and why do you need to know? How are those concepts used together in the real world to create cryptographic systems?

DAY 4: Cyber Security Technologies – Part 1
Our fourth day in the classroom begins our exploration of cybersecurity technologies. We begin with wireless network security (Wi-Fi and Bluetooth), and mobile device security (i.e., cell phones). We follow that with a brief look at some common attacks. We then move into a discussion of malware and anti-malware technologies. We end the day with an examination of several data protection protocols used for email encryption, secure remote access, secure web access, secure file transfer, and Virtual Private Network (VPN) technologies.

DAY 5: Cyber Security Technologies – Part 2
The final day of our SEC301 journey continues the discussion of cybersecurity technologies. The day begins by looking at several security technologies, including compartmentalization, firewalls, Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS), sniffers, content filters, etc. We then take a good look at browser and web security, and the difficulties of securing the web environment. For example, students will understand why and how their browser connects to anywhere from 5 to 100 different Internet locations each time they load a single web page. We end the day with a look at system security to include hardening operating systems, patching, virtual machines, cloud computing, and backup.

Who Should Attend
- Anyone new to cybersecurity and in need of an introduction to the fundamentals of security
- Those who feel bombarded with complex technical security terms they don’t understand, but want to understand
- Non-IT security managers who deal with technical issues and understand them and who worry their company will be the next mega-breach headline story on the 6 o’clock news
- Professionals with basic computer and technical knowledge in all disciplines who need to be conversant in basic security concepts, principles, and terms, but who don’t need “deep in the weeds” detail
- Those who have decided to make a career change to take advantage of the job opportunities in cybersecurity and need formal training and certification

“SEC301 is a great class for the individual who wants to learn an extensive amount of material in one week.”
- Steven Chovanec,
Discover Financial Services
SEC401: Security Essentials Bootcamp Style

Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. Learn tips and tricks from the experts so that you can win the battle against the wide range of cyber adversaries that want to harm your environment.

Is SEC401: Security Essentials Bootcamp Style the right course for you?
STOP and ask yourself the following questions:

- Do you fully understand why some organizations get compromised and others do not?
- If there were compromised systems on your network, are you confident that you would be able to find them?
- Do you know the effectiveness of each security device and are you certain that they are all configured correctly?
- Are proper security metrics set up and communicated to your executives to drive security decisions?

If you do not know the answers to these questions, then SEC401 will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs. Learn to build a security roadmap that can scale today and into the future.

SEC401: Security Essentials Bootcamp Style is focused on teaching you the essential information security skills and techniques you need to protect and secure your organization’s critical information assets and business systems. Our course will show you how to prevent your organization’s security problems from being headline news in the Wall Street Journal!

Prevention is ideal but detection is a must.

With the rise in advanced persistent threats, it is almost inevitable that organizations will be targeted. Whether the attacker is successful in penetrating an organization’s network depends on the effectiveness of the organization’s defense. Defending against attacks is an ongoing challenge, with new threats emerging all of the time, including the next generation of threats. Organizations need to understand what really works in cybersecurity. What has worked, and will always work, is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cybersecurity, three questions must be answered:

- What is the risk?
- Is it the highest priority risk?
- What is the most cost-effective way to reduce the risk?

Security is all about making sure you focus on the right areas of defense. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you will need if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security instructors in the industry.

Bryan Simon is an internationally recognized expert in cybersecurity who has been working in the information technology and security field since 1991. Over the course of his career, Bryan has held various technical and managerial positions in the education, environmental, accounting, and financial services sectors. Bryan speaks on a regular basis at international conferences and with the press on matters of cybersecurity. He has instructed individuals from the FBI, NATO, and the UN in matters of cybersecurity, on two continents. Bryan has specialized expertise in defensive and offensive capabilities. He has received recognition for his work in IT security and was most recently profiled by McAfee (part of Intel Security) as an IT Hero. Bryan holds 13 GIAC Certifications including the GSEC, GCWN, GCIB, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, GCUX, GISF, and GMON. Bryan’s scholastic achievements have resulted in the honor of sitting as a current member of the SANS Institute Advisory Board and in his acceptance into the prestigious SANS Cyber Guardian program. In addition to teaching SEC401, Bryan teaches SECC501: Advanced Security Essentials — Enterprise Defender; SECS505: Securing Windows and Powershell Automaton; and SECS11: Continuous Monitoring and Security Operations.

@BryanOnSecurity
DAY 1: Network Security Essentials
A key way that attackers gain access to a company's resources is through a network connected to the Internet. A company wants to try to prevent as many attacks as possible, but in cases where it cannot prevent an attack, it must detect it in a timely manner. Therefore, an understanding and ability to create and identify the goals of building a defensible network architecture are critical. It is just as important to know and understand the architecture of the system, types of designs, communication flow and how to protect against attacks using devices such as routers and firewalls. These essentials, and more, will be covered during this first day in order to provide a firm foundation for the consecutive days of training.

Topics: Defensible Network Architecture; Virtualization and Cloud Security; Network Device Security; Networking and Protocols; Securing Wireless Networks; Securing Web Communications

DAY 2: Defense-in-Depth and Attacks
To secure an enterprise network, you must understand the general principles of network security. On this second course day, we look at threats to our systems and take a "big picture" look at how to defend against them. You will learn that protections need to be layered – a principle called defense-in-depth. We explain some principles that will serve you well in protecting your systems. You will also learn about key areas of network security.

Topics:Defense-in-Depth; Access Control and Password Management; Security Policies; Critical Controls; Malicious Code and Exploit Mitigations; Advanced Persistent Threat (APT)

DAY 3: Threat Management
Whether targeting a specific system or just searching the Internet for an easy target, an attacker uses an arsenal of tools to automate finding new systems, mapping out networks, and probing for specific, exploitable vulnerabilities. This phase of an attack is called reconnaissance, and it can be launched by an attacker any amount of time before exploiting vulnerabilities and gaining access to systems and networks. In fact, evidence of reconnaissance activity can be a clue that a targeted attack is on the horizon.

Topics:Vulnerability Scanning and Penetration Testing; Network Security Devices; Endpoint Security; SIEM/Log Management; Active Defense

DAY 4: Cryptography, Risk Management, and Response
There is no silver bullet when it comes to security. However, there is one technology that would help solve a lot of security issues, though few companies deploy it correctly. This technology is cryptography. Concealing the meaning of a message can prevent unauthorized parties from reading sensitive information. This course section looks at various aspects of encryption and how it can be used to secure a company's assets. A related area called steganography, or information hiding, is also covered.

Topics:Cryptography, Cryptography Algorithms and Deployment; Applying Cryptography; Incident Handling and Response; Contingency Planning – BCP/DRP; IT Risk Management

DAY 5: Windows Security
Remember when Windows was simple? Windows XP desktops in a little workgroup... what could be easier? A lot has changed over time. Now, we have Windows tablets, Azure, Active Directory, PowerShell, Office 365, Hyper-V, Virtual Desktop Infrastructure (VDI), and so on. Microsoft is battling Google, Apple, Amazon.com, and other cloud giants for supremacy. The trick is to do it securely, of course. Windows is the most widely-used and targeted operating system on the planet. At the same time, the complexities of Active Directory, PKI, Bitlocker, Applocker, and User Account Control represent both challenges and opportunities. This section will help you quickly master the world of Windows security while showing you the tools that can simplify and automate your work. You will complete the day with a solid grounding in Windows security by looking at automation, auditing and forensics.

Topics:Windows Security Infrastructure; Service Packs, Hot Fixes, and Backups; Windows Access Controls; Enforcing Security Policy; Securing Windows Network Services; Automation, Auditing, and Forensics

DAY 6: Linux Security
While organizations do not have as many Unix/Linux systems, those that they do have are often some of the most critical systems that need to be protected. This final course day provides step-by-step guidance to improve the security of any Linux system. The course combines practical "how to" instructions with background information for Linux beginners, as well as security advice and best practices for administrators of all levels of expertise. This module discusses the foundational items that are needed to understand how to configure and secure a Linux system. It also provides an overview of the operating system and mobile markets. To lay a foundation, it provides an overview of the different operating systems that are based on Linux.

Topics:Linux Security: Structure, Permissions and Access; Hardening and Securing Linux Services; Monitoring and Attack Detection; Security Utilities

Who Should Attend
- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks
- Administrators responsible for building and maintaining systems that are being targeted by attackers
- Forensic specialists, penetration testers, and auditors who need a solid foundation of security principles to be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

“SEC401 provided a vast library of information on developing a strong security posture, and in the course of the training, my brain shifted into a security-first gear thanks to the intense and deep exposure to the multitudinous recommendations for securing an organization's network and data.”

-Laura Farvour, University of Minnesota
Micah Hoffman has been working in the information technology field since 1998 supporting federal government, commercial, and internal customers in their efforts to discover and quantify information security weaknesses in their organizations. He leverages years of hands-on, real-world OSINT, penetration testing, and incident response experience to provide excellent solutions to his customers. Micah is the author of SEC487: Open-Source Intelligence Gathering and Analysis, and holds GIAC’s GMON, GAWN, GWAPT, and GPEN certifications as well as the CISSP®. Micah is a highly active member in the cybersecurity and OSINT communities. When not working, teaching, or learning, Micah can be found hiking on Appalachian Trail or the many park trails in Maryland. @WebBreacher

Immeasurable amounts of personal, potentially incriminating data are currently stored in the websites, apps, and social media platforms that people access and update via their devices daily. Those data can become evidence for citizens, governments, and businesses to use in solving real financial, employment, and criminal issues with the help of a professional information gatherer.

SEC487 will teach students legitimate and effective ways to find, gather, and analyze these data from the Internet. You’ll learn about reliable places to harvest data using manual and automated methods and tools. Once you have the data, we’ll show you how to ensure that those data are analyzed, sound, and useful to your investigations.

This is a foundational course in open-source intelligence (OSINT) gathering and, as such, will move quickly through many areas of the field. The course will teach you current, real-world skills, techniques, and tools that law enforcement, private investigators, cyber attackers, and defenders use to scour the massive amount of information across the Internet, analyze the results, and pivot on interesting pieces of data to find other areas for investigation. Our goal is to provide the OSINT knowledge base for students to be successful in their fields whether they are cyber defenders, threat intelligence analysts, private investigators, insurance claims investigators, intelligence analysts, law enforcement personnel, or just someone curious about OSINT.

Throughout the course week, students will participate in numerous hands-on labs using the tools and techniques that are the basis for gathering free data from the Internet. The 20 labs in this course use the live Internet and dark web to help students gain real-world confidence. You’ll leave the course knowing not just how to use search features on a website, but all of the scenario-based requirements and OSINT techniques needed to gather truly important OSINT data.

“Fantastic introduction to a wide spectrum of OSINT techniques and practices, with great interactive labs and lots of deep dives!”
-Dave Huffman, Rockwell Automation

You Will Be Able To
- Create an OSINT process
- Conduct OSINT investigations in support of a wide range of customers
- Understand the data collection life cycle
- Create a secure platform for data collection
- Analyze customer collection requirements
- Capture and record data
- Create sock puppet accounts
- Create your own OSINT process
- Harvest web data
- Perform searches for people
- Access social media data
- Assess a remote location using online cameras and maps
- Examine geolocated social media
- Research businesses
- Use government-provided data
- Collect data from the dark web
- Leverage international sites and tools

SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis NEW!

6 Day Program | 36 CPEs | Laptop Required

6 Day Program | 36 CPEs | Laptop Required

Register at www.sans.org/sansfire | 301-654-SANS (7267)
DAY 1: Foundations of OSINT

We begin with the basics and answer the questions “what is OSINT?” and “how do people use it?” This first day is about level-setting and ensuring that all students understand the background behind what we do in the OSINT field. We also establish the foundation for the rest of the week by learning how to document findings and set up an OSINT platform, and we discuss effective research habits for OSINT analysts. This day is a key component for the success of an OSINT analyst because without these concepts and processes in place, researchers can get themselves into serious trouble during assessments by inadvertently alerting their targets or improperly collecting data, making it less useful when delivered to the customer.

Topics: Understanding OSINT; Goals of OSINT Collection; Diving into Collecting; Taking Excellent Notes; Determining Your Threat Profile; Setting Up an OSINT Platform; Effective Research Habits; Creating Sock Puppets

DAY 2: Gathering, Searching, and Analyzing OSINT

OSINT data collection begins on day two after we get a glimpse of some of the fallacies that could influence our conclusions and recommendations. From this point in the class forward, we examine distinct categories of data and think about what it could mean for our investigations. Retrieving data from the Internet could mean using a web browser to view a page or, as we learn in this section, using command line tools, scripts, and helper applications.

Topics: Data Analysis Challenges; Creating Your OSINT Process; Harvesting Web Data; OSINT Frameworks; Basic Data: Street Addresses; Basic Data: Phone Numbers; Basic Data: Email Addresses; User Names; Avatars and Reverse Image Searches; Leveraging Search Engines

DAY 3: Social Media and Geolocation

Finding data on people, especially basic content such as email addresses, home addresses, and phone numbers, can be made easier using online people search engines. This is how day three kicks off, examining free and paid choices in this data aggregator area and understanding how to use the data we receive from them. The first social media site we look at from an OSINT perspective is Facebook, with its worldwide reach. Students explore Facebook profiles, groups, events, and other Facebook objects using graph searches and Facebook query techniques. We then move to detailed examinations of LinkedIn, Twitter, and Instagram, and what OSINT data can be found in each of them.

Topics: People Search Engines; Facebook Analysis; LinkedIn Data; Instagram; Twitter Data; Geolocation; Dating and Adult Websites; Registries and Wish Lists; Web and Traffic Cameras; File Metadata Analysis

DAY 4: Imagery, Networks, Government, and Business

Day four focuses on many different but related OSINT issues. We begin by looking at how various mapping sites can assist our assessments with aerial data, distance-measuring, and “street view” imagery. We then shift from OSINT about people and locations to OSINT about networks and computers, as researching IP addresses, domain names, and related content can be important aspects of our investigations. The second portion of the day has three modules. The first covers OSINT framework tool suites. The next module covers harvesting information from federal, state, and local government web pages within the United States. The public data on these sites can help us research people and businesses.

Topics: Remote Location Recon; IP Address and WHOIS; IP Address Geolocation; Domain Name System (DNS); Wireless Networks; Recon Tool Suites and Frameworks; U.S. Government Data; Researching Companies

DAY 5: The Dark Web and International Issues

The entire morning of day five focuses on understanding and using three of the most popular dark web networks for OSINT purposes. Students will learn why people use Freenet, I2P, and Tor. The first module in the afternoon examines how blue teamers (cyber defenders) can use monitoring to receive alerts when data of interest appear on the Internet. We then shift our focus to data found on “paste” sites. Considering that a big barrier to using non-English websites can be the language, students learn how to use techniques to translate content and search locally for relevant information in our international OSINT section. We leave some time at the end of the day for a massive lab, the “Solo CTF,” which helps students put together all that they have learned in a semi-guided walk-through that touches on many of the concepts taught throughout the week.

Topics: The Surface, Deep, and Dark Webs; The Dark Web; Freenet; I2P – Invisible Internet Project; Tor; Monitoring and Alerting; International Issues; Vehicle Searches

DAY 6: Capstone: Capture (and Present) the Flag

The capstone for the course is a group event that brings together everything that students learned throughout the week. This is not a “canned” Capture-the-Flag event where specific flags are planted and your team must find them. It is a competition where each team will collect specific OSINT data about a certain group of people. The output from this work will be turned in as a “deliverable” to the “client” (the instructor), and then the three teams with the most-complete work will present their research to the class for voting. This multi-hour, hands-on event will reinforce what the students practiced in the Solo CTF the day before and add the complexity of performing OSINT assessments under pressure and in a group.

Topics: Capstone Capture-the-Flag Event

Author Statement

“I have always been intrigued by the types and amount of data that are available on the Internet. From researching the best restaurants in a foreign town to watching people via video cameras, it all fascinates me. As the Internet evolved, more high-quality, real-time resources became available and every day was like a holiday, with new and wonderful tools and sites coming online and freely accessible.

“At a certain point, I was no longer in awe of the great resources on the web and, instead, transitioned to surprise that people would post images of themselves in illegal or compromising positions or that a user profile contained such explicit, detailed content. My wonder shifted to concern for these people. Didn’t they know that their profiles, images, videos, comments, etc. were publicly accessible? Didn’t they care about it? What I found was that, if you looked in the right places, you could find almost anything about a person, a network, or a company. Piecing together seemingly random pieces of data into meaningful stories became my passion and, ultimately, the reason for this course.

“I recognized that the barrier to performing excellent OSINT was not that there was no free data on the Internet. It was that there was too much data on the Internet. The challenge transitioned from ‘how do I find something’ to ‘how do I find only what I need?’ This course was born from this need to help others learn the tools and techniques to effectively gather and analyze OSINT data from the Internet.”

-Micah Hoffman
Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad reputational damage. SEC501: Advanced Security Essentials – Enterprise Defender builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

It has been said of security that “prevention is ideal, but detection is a must.” However, detection without response has little value. Network security needs to be constantly improved to prevent as many attacks as possible and to swiftly detect and respond appropriately to any breach that does occur. This PREVENT - DETECT - RESPONSE strategy must be in place both externally and internally. As data become more portable and networks continue to be porous, there needs to be an increased focus on data protection. Critical information must be secured regardless of whether it resides on a server, in a robust network architecture, or on a portable device.

Despite an organization’s best efforts to prevent network attacks and protect its critical data, some attacks will still be successful. Therefore, organizations need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks, looking for indications of an attack, and performing penetration testing and vulnerability analysis against your organization to identify problems and issues before a compromise occurs.

Finally, once an attack is detected we must react quickly and effectively and perform the forensics required. Knowledge gained by understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

**You Will Be Able To**
- Identify the threats against network infrastructures and build defensible networks that minimize the impact of attacks
- Access tools that can be used to analyze a network to prevent attacks and detect the adversary
- Decode and analyze packets using various tools to identify anomalies and improve network defenses
- Understand how the adversary compromises networks and how to respond to attacks
- Perform penetration testing against an organization to determine vulnerabilities and points of compromise
- Apply the six-step incident handling process
- Use various tools to identify and remediate malware across your organization
- Create a data classification program and deploy data loss prevention solutions at both a host and network level

**Who Should Attend**
- Incident response and penetration testers
- Security Operations Center engineers and analysts
- Network security professionals
- Anyone who seeks technical in-depth knowledge about implementing comprehensive security solutions

**“Immediate value of putting concepts into standard practice.”**
- Manny Cadiz, EMF Broadcasting

Paul Henry is one of the world’s foremost global information security and computer forensic experts, with more than 20 years of experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principal at vNet Security, LLC and a security and forensic analyst at Lumension Security. He also advises and consults on some of the world’s most challenging and high-risk information security projects, including the National Banking System in Saudi Arabia, the Reserve Bank of Australia, the U.S. Department of Defense’s Satellite Data Project, and both government as well as telecommunications projects throughout Southeast Asia. In addition, Paul regularly authors thought leadership articles on technical security issues, and is a featured and keynote speaker at seminars and conferences worldwide, delivering presentations on diverse topics including anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, firewall architectures, security architectures, and managed security services.

@phenrycissp
DAY 1: Defensive Network Architecture
This course day will focus on security in the design and configuration of various enterprise infrastructures. From a security perspective, proper design and configuration protects both the components being configured, as well as the rest of the organization that depends on that gear to defend other components from attacks. In other words, a good house needs a good foundation.

Topics: Security Benchmarks; Standards, and the Role of Audit in Defending Infrastructure; Defense Using Authentication and Authorization, and Defending Those Services; The Use of Logging and Security Information and Event Management (SIEM) in Defending an Organization from Attack; Attacking and Defending Critical Protocols; Several Man-in-the-Middle Attack Methods, and Defenses against Each; Infrastructure Defense Using IPS, Next-Generation Firewalls, and Web Application Firewalls; Defense of Critical Servers and Services; Active Defense; Defense of Private and Public Cloud Architectures

DAY 2: Penetration Testing
Security is all about understanding, mitigating, and controlling the risk to an organization’s critical assets. An organization must understand the changing threat landscape and have the capacity to compare it against its own vulnerabilities that could be exploited to compromise the environment. On day two, students will learn about the variety of tests that can be run against an organization and how to perform effective penetration tests to better understand the security posture for network services, operating systems, and applications. In addition, we’ll talk about social engineering and reconnaissance activities to better emulate increasingly prevalent threats to users.

Topics: Introduction to Penetration Testing Concepts; Penetration Testing Scoping and Rules of Engagement; Online Reconnaissance and Offensive Counterintelligence; Social Engineering; Network Mapping and Scanning Techniques; Enterprise Vulnerability Scanning; Network Exploitation Tools and Techniques; Web Application Exploitation Tools and Techniques; Post-Exploitation and Pivoting; OS and Application Exploit Mitigations; Reporting and Debriefing

DAY 3: Security Operations Foundations
“Prevention is ideal, but detection is a must” is a critical motto for network security professionals. While organizations always want to prevent as many attacks as possible, some adversaries will still sneak into the network. In cases where an attack is not successfully prevented, network security professionals need to analyze network traffic to discover attacks in progress, ideally stopping them before significant damage is done. Packet analysis and intrusion detection are at the core of such timely detection. Organizations need to not only detect attacks but also to react in a way that ensures those attacks can be prevented in the future.

Topics: Network Security Monitoring; IP, TCP, and UDP Refresher; Advanced Packet Analysis; Introduction to Network Forensics with Security Onion; Identifying Malicious Content and Streams; Extracting and Repairing Content from PCAP files; Traffic Visualization Tools; Intrusion Detection and Intrusion Prevention; Handling Encrypted Network Traffic

DAY 4: Digital Forensics and Incident Response
In this section, you will learn the core concepts of both “Digital Forensics” and “Incident Response.” We’ll explore some of the hundreds of artifacts that can give forensic investigators specific insight into what occurred during an incident. You will also learn how incident response currently operates, after years of evolving, in order to address the dynamic procedures used by attackers to conduct their operations. We’ll look at how to integrate DFIR practices into a continuous security operations program.

Topics: DFIR Core Concepts: Digital Forensics; DFIR Core Concepts: Incident Response; Modern DFIR: A Live and Continuous Process; Widening the Net; Scaling the DFIR Process and Scoping a Compromise

DAY 5: Malware Analysis
Malicious software is responsible for many incidents in almost every type of organization. Types of malware vary widely, from Ransomware and Rootkits to Crypto Currency Miners and worms. We will define each of the most popular types of malware and walk through multiple examples. The four primary phases of malware analysis will be covered: Fully Automated Analysis, Static Properties Analysis, Interactive Behavior Analysis, and Manual Code Reversing. You will complete various in-depth labs requiring you to fully dissect a live Ransomware specimen from static analysis through code analysis. You will get hands-on experience with tricking the malware through behavioral analysis techniques, as well as decrypting files encrypted by Ransomware by extracting the keys through reverse engineering. All steps are well defined and tested to ensure that the process to achieve these goals is actionable and digestible.

Topics: Introduction to Malware Analysis; The Many Types of Malware; ATM/Cash Machine Malware; Building a Lab Environment for Malware Analysis; Malware Locations and Footprints; Fully Automated Malware; Cuckoo Sandbox; Static Properties Analysis; Interactive Behavior Analysis; Manual Code Reversing; Tools such as IDA, PeStudio, ILSpy, Process Hacker, Process Monitor, NoFuserEx, etc.

DAY 6: Enterprise Defender Capstone
The concluding section of the course will serve as a real-world challenge for students by requiring them to work in teams, use the skills they have learned throughout the course, think outside the box, and solve a range of problems from simple to complex. A web server scoring system and Capture-the-Flag system will be provided to score students as they submit flags to score points. More difficult challenges will be worth more points. In this defensive exercise, challenges include packet analysis, routing protocols, scanning, malware analysis, and other challenges related to the course material.
Reports of prominent organizations being hacked and suffering irreparable reputational damage have become all too common. How can you prevent your company from becoming the next victim of a major cyber attack?

Preserving the security of your site in today’s threat environment is more challenging than ever before. The security landscape is continually changing from what was once only perimeter protection to protecting exposed and mobile systems that are almost always connected and sometimes vulnerable. Security-savvy employees who can help detect and prevent intrusions are therefore in great demand. Our goal in SEC503: Intrusion Detection In-Depth is to acquaint you with the core knowledge, tools, and techniques to defend your networks with insight and awareness. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

Mark Twain said, “It is easier to fool people than to convince them that they’ve been fooled.” Too many IDS/IPS solutions provide a simplistic red/green, good/bad assessment of traffic and too many untrained analysts accept that feedback as the absolute truth. This course emphasizes the theory that a properly trained analyst uses an IDS alert as a starting point for examination of traffic, not as a final assessment. SEC503 imparts the philosophy that the analyst must have access and the ability to examine the alerts to give them meaning and context. You will learn to investigate and reconstruct activity to deem if it is noteworthy or a false indication.

This course delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence. You will learn about the underlying theory of TCP/IP and the most used application protocols, such as DNS and HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to master different open-source tools like tcpdump, Wireshark, Snort, Bro, tshark, and SiLK. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that you can transfer knowledge to execution. Basic exercises include assistive hints while advanced options provide a more challenging experience for students who may already know the material or who have quickly mastered new material.

You Will Be Able To

- Configure and run open-source Snort and write Snort signatures
- Configure and run open-source Bro to provide a hybrid traffic analysis framework
- Understand TCP/IP component layers to identify normal and abnormal traffic
- Use open-source traffic analysis tools to identify signs of an intrusion
- Comprehend the need to employ network forensics to investigate traffic to identify and investigate a possible intrusion
- Use Wireshark to carve out suspicious file attachments
- Write tcpdump filters to selectively examine a particular traffic trait
- Craft packets with Scapy
- Use the open-source network flow tool SiLK to find network behavior anomalies
- Use your knowledge of network architecture and hardware to customize placement of IDS sensors and sniff traffic off the wire

“Everything learned can be directly applied in my work, which is great! The practical stories shared by the instructor are really eye-opening and informative.”

- Vincent Ruers, MoD

David Hoelzer is a high-scoring SANS instructor and author of more than 20 sections of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past 25 years. Recently, David was called upon to serve as an expert witness for the Federal Trade Commission for ground-breaking GLBA Privacy Rule litigation. David has been highly involved in governance at the SANS Technology Institute, serving as a member of the Curriculum Committee as well as Audit Curriculum Lead. As a SANS instructor, David has trained security professionals from organizations including the NSA, DHHS, Fortune 500 companies, various Department of Defense sites, national laboratories, and many colleges and universities. David is a research fellow at the Center for Cybermedia Research, as well as the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC). He also is an adjunct research associate for the UNLV Cybermedia Research Lab and a research fellow with the Internet Forensics Lab. David has written and contributed to more than 15 peer-reviewed books, publications, and journal articles. Currently, David serves as the principal examiner and director of research for Enclave Forensics, a New York/Las Vegas-based incident response and forensics company. He also serves as the chief information security officer for Cyber-Defense, an open-source security software solution provider.
## Course Day Descriptions

### DAY 1: Fundamentals of Traffic Analysis – Part 1
Day 1 provides a refresher or introduction, depending on your background, to TCP/IP. It describes the need to understand packet structure and content. It covers the essential foundations such as the TCP/IP communication model, and the theory of bits, bytes, binary and hexadecimal. We introduce the use of open-source Wireshark and tcpdump for analysis. We begin our exploration of the TCP/IP communication model with the study of the link layer, the IP layer, both IPv4 and IPv6 packet fragmentation in both. We describe the layers and analyze traffic not just in theory and function, but from the perspective of an attacker and defender. All traffic is discussed and displayed using the two open-source tools, Wireshark and tcpdump.

**Topics:** Concepts of TCP/IP; Introduction to Wireshark; Network Access/Link Layer: Layer 2; IP Layer: Layer 3

### DAY 2: Fundamentals of Traffic Analysis – Part 2
Day 2 continues where the previous day ended in understanding the TCP/IP model. Two essential tools, Wireshark and tcpdump, are further explored, using their advanced features to give you the skills to analyze your own traffic. The focus of these tools on Day 2 is on filtering traffic of interest in Wireshark using display filters and in tcpdump using Berkeley Packet Filters. We proceed with our exploration of the TCP/IP layers covering TCP, UDP, and ICMP. Once again, we describe the layers and analyze traffic not just in theory and function, but from the perspective of an attacker and defender.

**Topics:** Wireshark Display Filters; Writing tcpdump Filters; TCP, UDP, ICMP

### DAY 3: Application Protocols and Traffic Analysis
Day 3 introduces the versatile packet crafting tool Scapy. It is a very powerful Python-based tool that allows for the manipulation, creation, reading, and writing of packets. Scapy can be used to craft packets to test the detection capability of an IDS/IPS, especially important when a new user-created IDS rule is added, for instance for a recently announced vulnerability. The examination of TCP/IP culminates with an exploration of the application layer. The concentration is on some of the most widely used, and sometimes vulnerable, crucial application protocols: DNS, HTTP(S), SMTP, and Microsoft communications. Our focus is on protocol analysis, a key skill in intrusion detection. IDS/IPS evasion is the bane of the analyst, so the theory and possible implications of evasions at different protocol layers are examined.

**Topics:** Scapy, Advanced Wireshark; Detection Methods for Application Protocols; DNS, Microsoft Protocols; HTTP(2)/TLS; SMTP, IDS/IPS Evasion Theory

### DAY 4: Network Monitoring: Snort and Bro
The fundamental knowledge gained from the first three days provides a fluid progression into one of the most popular days of SEC503. Snort and Bro are widely deployed open-source IDS/IPS solutions that have been industry standards for many years. The day begins with a discussion on network architecture, including the features of intrusion detection and prevention devices, along with a look at options and requirements of devices that can sniff and capture the traffic for inspection. Next, the topic of the analyst’s role in the detection process is examined. Before Snort and Bro are discussed, the capabilities and limitations are considered. Snort detection flow, running Snort, and rules are explored with an emphasis on writing efficient rules. It is likely that false positives and negatives will occur and tips for dealing with them are presented. Bro’s unique capability to use its own scripting language to write code to analyze patterns of event-driven behavior is one of the most powerful detection tools available to the analyst. We discuss how this enables monitoring and correlating activity and demonstrate with examples.

**Topics:** Network Architecture; Introduction to IDS/IPS Analysis; Snort; Bro

### DAY 5: Network Traffic Forensics
The penultimate day continues the format of less instruction and more hands-on training using three separate incidents that must be analyzed. The three incident scenarios are introduced with some new material to be used in the related hands-on analysis. This material includes an introduction to network forensics analysis for the first scenario. It continues with using network flow records to assist in analysis of the traffic from the second scenario. It concludes by examining the third scenario, including Command and Control channels and managing analysis when very large packet capture files are involved.

**Topics:** Introduction to Network Forensics Analysis; Using Network Flow Records; Examining Command and Control Traffic; Analysis of Large pcaps

### DAY 6: NetWars: IDS Version
The week culminates with a fun hands-on NetWars: IDS Version challenge. Students compete on teams to answer many questions that require using tools and theory covered in the first five days. This is a great way to end the week because it reinforces what was learned by challenging the student to think analytically and strengthens confidence to employ what was learned in a real-world environment.

### Who Should Attend
- Intrusion detection (all levels), system, and security analysts
- Network engineers/administrators
- Hands-on security managers

---

**“I got a deeper understanding of key topics from SEC503. This training will help me get more data out of my investigations.”**

-Alphonse Wichrowski, Allegiant Air

---

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/sansfire/courses](http://www.sans.org/sansfire/courses)
The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection and one or two disgruntled employees (and whose does not!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth. As defenders, it is essential we understand these hacking tools and techniques.

This course enables you to turn the tables on computer attackers by helping you understand their tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan. It addresses the latest cutting-edge insidious attack vectors, the “oldie-but-goodie” attacks that are still prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course provides a time-tested, step-by-step process for responding to computer incidents, and a detailed description of how attackers undermine systems so you can prepare for, detect, and respond to them. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a hands-on workshop that focuses on scanning, exploiting, and defending systems. This course will enable you to discover the holes in your system before the bad guys do!

The course is particularly well-suited to individuals who lead or are a part of an incident handling team. General security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

**You Will Be Able To**

- Apply incident handling processes in-depth, including preparation, identification, containment, eradication, and recovery, to protect enterprise environments
- Analyze the structure of common attack techniques in order to evaluate an attacker’s spread through a system and network, anticipating and thwarting further attacker activity
- Utilize tools and evidence to determine the kind of malware used in an attack, including rootkits, backdoors, and trojan horses, choosing appropriate defenses and response tactics for each
- Use built-in command-line tools such as Windows tasklist, wmic, and reg as well as Linux netstat, ps, and ls to detect an attacker’s presence on a machine
- Analyze router and system ARP tables along with switch CAM tables to track an attacker’s activity through a network and identify a suspect
- Use memory dumps and the Volatility tool to determine an attacker’s activities on a machine, the malware installed, and other machines the attacker used as pivot points across the network
- Gain access to a target machine using Metasploit, and then detect the artifacts and impacts of exploitation through process, file, memory, and log analysis
- Analyze a system to see how attackers use the Netcat tool to move files, create backdoors, and build relays through a target environment
- Run the Nmap port scanner and Nexscan vulnerability scanner to find openings on target systems, and apply tools such as tcpdump and netstat to detect and analyze the impacts of the scanning activity

**The training offered at SANS is the best in the industry, and the SEC504 course is a must for any IT security professional – highly recommended.”**

- Michael Hoffman, Shell Oil Products US

John Strand is the lead course author of SEC504. He has also taught SEC560: Network Penetration Testing and Ethical Hacking and SEC380: Metasploit Kung Fu for Enterprise Pen Testing. When not teaching for SANS, John co-hosts Security Weekly, the world’s largest computer security podcast. He also is the owner of Black Hills Information Security, specializing in penetration testing and security architecture services. He has presented for the FBI, NASA, the NSA, and at DefCon. In his spare time he writes loud rock music and makes various futile attempts at fly fishing.

@strandjs
### Course Day Descriptions

#### DAY 1: Incident Handling Step-by-Step and Computer Crime Investigation
The first part of this section looks at the invaluable Incident Handling Step-by-Step Model, which was created through a consensus process involving experienced incident handlers from corporations, government agencies, and educational institutes, and has been proven effective in hundreds of organizations. This section is designed to provide students a complete introduction to the incident handling process, using the six steps (preparation, identification, containment, eradication, recovery, and lessons learned) necessary to prepare for and deal with a computer incident. The second part of this section examines from-the-trenches case studies to understand what does and does not work in identifying computer attackers. This section provides valuable information on the steps a systems administrator can take to improve the chances of catching and prosecuting attackers.

**Topics:** Preparation; Identification; Containment; Eradication; Recovery; Special Actions for Responding to Different Types of Incidents; Incident Record-Keeping; Incident Follow-Up

#### DAY 2: Computer and Network Hacker Exploits – Part 1
Seemingly innocuous data leaking from your network could provide the clue needed by an attacker to blow your systems wide open. This section covers the details associated with reconnaissance and scanning, the first two phases of many computer attacks.

**Topics:** Reconnaissance; Scanning; Intrusion Detection System Evasion; Hands-on Exercises for a List of Tools

#### DAY 3: Computer and Network Hacker Exploits – Part 2
Computer attackers are ripping our networks and systems apart in novel ways while constantly improving their techniques. This section covers the third phase of many hacker attacks – gaining access. Attackers employ a variety of strategies to take over systems from the network level up to the application level. This section covers the attacks in depth, from the details of buffer overflow and format string attack techniques to the latest in session hijacking of supposedly secure protocols.

**Topics:** Network-Level Attacks; Gathering and Parsing Packets; Operating System and Application-Level Attacks; Nettac: The Attacker’s Best Friend; Hands-on Exercises with a List of Tools

#### DAY 4: Computer and Network Hacker Exploits – Part 3
This section starts out by covering one of attackers’ favorite techniques for compromising systems: worms. We will analyze worm developments over the last two years and project these trends into the future to get a feel for the coming Super Worms we will face. Then the course turns to another vital area often exploited by attackers: web applications. Because most organizations’ homegrown web applications do not get the security scrutiny of commercial software, attackers exploit these targets using SQL injection, cross-site scripting, session cloning, and a variety of other mechanisms discussed in detail.

**Topics:** Password Cracking; Web Application Attacks; Denial of Service Attacks; Hands-on Exercises with a List of Tools

#### DAY 5: Computer and Network Hacker Exploits – Part 4
This section covers the fourth and fifth phases of many hacker attacks: maintaining access and covering their tracks. Computer attackers install backdoors, apply Rootkits, and sometimes even manipulate the underlying kernel itself to hide their nefarious deeds. Each of these categories of tools requires specialized defenses to protect the underlying system. In this course, we will analyze the most commonly used malicious code specimens, as well as explore future trends in malware, including BIOS-level and combo malware possibilities.

**Topics:** Maintaining Access; Covering the Tracks; Putting It All Together; Hands-on Exercises with a List of Tools

#### DAY 6: Hacker Tools Workshop
Over the years, the security industry has become smarter and more effective in stopping hackers. Unfortunately, hacker tools are becoming smarter and more complex. One of the most effective methods to stop the enemy is to actually test the environment with the same tools and tactics an attacker might use against you. This workshop lets you put what you have learned over the past week into practice.

**Topics:** Hands-on Analysis

---

### Who Should Attend
- Incident handlers
- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack

---

“I will almost always recommend SEC504 as a baseline so that everyone is speaking the same language. I want my sys-admins to take it, my network admins to take it, even my devs to take it, regardless of whether they’re going to eventually move into an incident handling role. In my opinion it is the most critical, foundational class that SANS offers.”

- Kevin Wilcox, Information Security Specialist
You Will Be Able To

- Configure mitigations against attacks such as pass-the-hash, Kerberos golden tickets, Remote Desktop Protocol (RDP) man-in-the-middle, Security Access Token abuse, and other attacks discussed in SEC504 and other SANS hacking courses.
- Execute PowerShell commands on remote systems and begin to write your own PowerShell scripts.
- Harden PowerShell itself against abuse, and enable transcription logging for your SIEM.
- Use Group Policy and PowerShell to grant administrative privileges in a way that reduces the harm if an attack succeeds (assume breach).
- Block hacker lateral movement and malware Command & Control channels using Windows Defender Firewall, IPSec, DNS sinkholes, admin credential protections, and more.
- Prevent exploitation using AppLocker and other Windows OS hardening techniques in a scalable way with PowerShell.
- Configure PowerShell remoting to use Just Enough Admin (JEA) policies to create a Windows version of Linux sudo and setuid root.
- Install and manage a full Windows Public Key Infrastructure (PKI), including smart cards, certificate auto-enrollment, Online Certificate Status Protocol (OCSP) web responders, and detection of spoofed root Certification Authorities (CAs).
- Harden must-have protocols against exploitation, such as SSL/TLS, RDP, DNS, DNSSSEC, PowerShell Remoting, and SMB.
- Use PowerShell to access the WMI service for remote command execution, searching event logs, reconnaissance, and more.

Jason Fossen
SANS Faculty Fellow

Hackers know how to use PowerShell for evil. Do you know how to use it for good? In SEC505 you will learn PowerShell and Windows security hardening at the same time. SecOps/DevOps requires automation, and Windows automation means PowerShell.

You’ve run a vulnerability scanner and applied patches – now what? A major theme of this course is defendable architecture: we have to assume that there will be a breach, so we need to build in damage control from the beginning. Whack-a-mole incident response cannot be our only defensive strategy – we’ll never win, and we’ll never get ahead of the game. By the time your monitoring system tells you a Domain Admin account has been compromised, IT’S TOO LATE.

For the assume-breach mindset, we must carefully delegate limited administrative powers so that the compromise of one administrator account is not a disaster across the board. Managing administrative privileges and credentials is a tough problem, so this course devotes an entire day to just this one critical task. Perhaps you’ve taken a hacking course at SANS and you now want to learn Windows mitigations: SEC505 is that course. SEC505 is the defense-only mirror image of SEC504 with regard to Windows and Active Directory.

Learning PowerShell is also useful for another kind of security: job security. Employers are looking for people with these skills. You don’t have to know any PowerShell to attend the course, we will learn it together. About half the labs during the week are PowerShell, while the rest use graphical security tools. Many of the PowerShell scripts written by the course author are available to download from GitHub for free.

This course is not a vendor show to convince you to buy another security appliance or to install yet another endpoint agent. The idea is to use built-in or free Windows and Active Directory security tools when we can (especially PowerShell and Group Policy) and then purchase commercial products only when absolutely necessary.

If you are an IT manager or CIO, the aim for this course is to have it pay for itself 10 times over within two years, because automation isn’t just good for SecOps/DevOps; it can save money too.

This course is designed for systems engineers, security architects, and the Security Operations (SecOps) team. The focus of the course is on how to automate the NSA Top 10 Mitigations and the CIS Critical Security Controls related to Windows, especially the ones that are difficult to implement in large environments.

SEC505 will also prepare you for the GIAC Certified Windows Security Administrator (GCWN) certification exam to prove your Windows security expertise. The GCWN certification counts towards a Master’s Degree in Information Security from the SANS Technology Institute (www.sans.edu) and satisfies the Department of Defense 8140 computing environment requirement. The GCWN is also a foundational certification for soldiers in the U.S. Army’s 255-S Information Protection Program. For DoD students, we will see how to apply the NSA/DISA Secure Host Baseline.

This is a fun course and a real eye-opener, even for Windows administrators with years of experience. We don’t cover patch management, share permissions, or other such basics – the aim is to go far beyond that. Come have fun learning PowerShell and Windows security at the same time!

Jason Fossen is a principal security consultant at Enclave Consulting LLC, a published author, and a frequent public speaker on Microsoft security issues. He is the sole author of the SANS week-long Securing Windows course (SEC505), maintains the Windows day of Security Essentials (SEC401.5), and has been involved in numerous other SANS projects since 1998. He graduated from the University of Virginia, received his master’s degree from the University of Texas at Austin, and holds a number of professional certifications. He currently lives in Dallas, Texas.

@JasonFossen
For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/sansfire/courses

This course is available via Simulcast. See page 94 for more information.

Day 1: Learn PowerShell Scripting
This course section covers what you need to know to get started using PowerShell. You don’t need to have any prior scripting or programming experience. We have PowerShell labs throughout the week, so today is not the only PowerShell material. We start with the essentials, then go more in depth as the week progresses. Don’t worry, you won’t be left behind, the PowerShell labs walk you through every step.

Topics: PowerShell Overview and Tips; What Can We Do With PowerShell?; Write Your Own Scripts

Day 2: Host Hardening and Active Directory Scripting
Running a vulnerability scanner is easy, but remediating vulnerabilities in a large enterprise is hard. Most vulnerabilities are fixed by applying patches, but this course does not talk about patch management, you’re doing that already. What about the other vulnerabilities, the ones not fixed by applying patches? These vulnerabilities are, by definition, remediated by configuration changes. That’s the hard part. We need a secure architecture designed for SecOps/DevOps.

Topics: Continuous Secure Configuration Enforcement; Group Policy Precision Targeting; Server Hardening for SecOps/DevOps; PowerShell Desired State Configuration (DSC)

Day 3: Smart Tokens and Public Key Infrastructure (PKI)
Don’t believe what you hear on the street: Public Key Infrastructure (PKI) is not that hard to manage on Windows! You’ll be pleasantly surprised at how much Group Policy, Active Directory, and PowerShell can help you manage your PKI. And we don’t really have a choice anymore: running a PKI is pretty much mandatory for Microsoft security and cloud computing. This day of the course is basically one long hands-on lab to install and configure a full Windows Server PKI. This includes a root Certification Authority (CA), Group Policy certificate auto-enrollment on endpoints, Online Certificate Status Protocol (OCSP) revocation checking, private key roaming for users, smart card certificate deployment, and, of course, more PowerShell examples.

Topics: Why Is a PKI Necessary?; How to Install the Windows PKI; How to Manage Your PKI; Deploying Smart Cards

Day 4: Protecting Admin Credentials and PowerShell JEA
Why do submarines have pressure doors to seal off compartments? Because they are designed to assume a breach will occur. In a Windows environment, a security breach will occur, so we must design the architecture with an “assume breach” mindset as well. If we assume that some day the computers and credentials of our administrators will be compromised, then how do we build damage control into the network from the beginning? This is not about detection and incident response. The challenge here is how to design for damage control when we delegate administrative privileges. We need to proactively design damage control into the architecture, not wait until after there is a breach (when it’s too late).

Topics: Secure Architecture: Admin Privileges; Compromise of Administrative Powers; PowerShell Just Enough Admin (JEA); Active Directory Permissions and Delegation

Day 5: Thwarting Hackers Inside the Network
You are already applying patches and updating anti-virus signatures. But endpoint protection is much more than that. Because most advanced malware infections start with a compromised endpoint, we want to proactively build defensibility and damage control into our systems using a “zero trust” or “assume breach” model. How? AppLocker is an application whitelisting tool built into Windows to control which executables, scripts, DLLs and installer packages users may run. If hackers or malware attempt to launch an unauthorized process post-exploitation, the aim is to block it and log it. In the lab, we’ll use PowerShell and Group Policy to manage AppLocker. Application whitelisting can be hard to manage if used too aggressively, so we’ll also talk about how to get started without making the help desk phone ring off the hook.

Topics: Anti-Exploitation; IPSec Port Permissions; Host-Based Firewalls; Pre-Forensics

Day 6: Blue Team PowerShell: WMI, DNS, RDP, and SMB
Hackers love the Windows Management Instrumentation (WMI) service, and so should we. We are the linebackers on the Blue Team and the WMI service was made to benefit us, not hackers. The WMI service is enabled by default and accessible over the network. Through WMI we can do remote command execution (without PowerShell being installed at the target), forcibly log off the user, reboot the machine, stop services, search for processes running as Administrator, kill any process, and much more. The WMI service is nearly all-powerful and it’s built for remote administration. PowerShell is tightly integrated into WMI, and we’ll look at several PowerShell examples.

Topics: PowerShell and WMI; Hardening DNS; Dangerous Protocols We Can’t Live Without

Who Should Attend
Security Operations personnel
Blue Team players who were terrified by SEC504
Windows endpoint and server administrators
Anyone who wants to learn PowerShell automation
Anyone implementing the NSA Top 10 Mitigations
Anyone implementing the CIS Critical Security Controls
DoD admins applying the NSA/DISA Secure Host Baseline
Individuals deploying or managing a PKI or smart cards
Anyone wanting a more rugged Windows architecture

“SEC505 is practical, not just conceptual. Hands-on learning is much deeper than lectures, and the labs are very realistic. As a manager, this training increases my understanding of what the threats and vulnerabilities are, what the analysts in the chair have to do to counter them, and how to explain all of that to executive management.”

-Timothy Johnsrude,
NAVSUP FLC Puget Sound
This course provides in-depth coverage of Linux and Unix security issues that includes specific configuration guidance and practical, real-world examples, tips, and tricks. We examine how to mitigate or eliminate general problems that apply to all Unix-like operating systems, including vulnerabilities in the password authentication system, file system, virtual memory system, and applications that commonly run on Linux and Unix.

The course will teach you the skills to use freely available tools to handle security issues, including SSH, AIDE, sudo, lsof, and many others. SANS’s practical approach uses hands-on exercises every day to ensure that you will be able to use these tools as soon as you return to work. We will also put these tools to work in a special section that covers simple forensic techniques for investigating compromised systems.

You Will Be Able To

- Significantly reduce the number of vulnerabilities in the average Linux/Unix system by disabling unnecessary services
- Protect your systems from buffer overflows, denial-of-service, and physical access attacks by leveraging OS configuration settings
- Configure host-based firewalls to block attacks from outside
- Deploy SSH to protect administrative sessions, and leverage SSH functionality to securely automate routine administrative tasks
- Use sudo to control and monitor administrative access
- Create a centralized logging infrastructure with Syslog-NG, and deploy log monitoring tools to scan for significant events
- Use SELinux to effectively isolate compromised applications from harming other system services
- Securely configure common Internet-facing applications such as Apache and BIND
- Investigate compromised Unix/Linux systems with the Sleuthkit, lsof, and other open-source tools
- Understand attacker rootkits and how to detect them with AIDE and rkhunter/chkrootkit

Topics

- Memory Attacks, Buffer Overflows
- File System Attacks, Race Conditions
- Trojan Horse Programs and Rootkits
- Monitoring and Alerting Tools
- Unix Logging and Kernel-Level Auditing
- Building a Centralized Logging Infrastructure
- Network Security Tools
- SSH for Secure Administration
- Server Lockdown for Linux and Unix
- Controlling Root Access with sudo
- SELinux and chroot() for Application Security
- DNSSEC Deployment and Automation
- mod_security and Web Application Firewalls
- Secure Configuration of BIND, Sendmail, and Apache
- Forensic Investigation of Linux Systems

“Linux security courses are a rare commodity and a valuable resource to the security professional.”

- Trevor Sellers, IDA Center for Communications Research

Hal Pomeranz is an independent digital forensic investigator who has consulted on cases ranging from intellectual property theft to employee sabotage, organized cybercrime, and malicious software infrastructures. He has worked with law enforcement agencies in the United States and Europe and with global corporations. Equally at home in the Windows or Mac environment, Hal is recognized as an expert in the analysis of Linux and Unix systems. His research on EXT4 file system forensics provided a basis for the development of open-source forensic support for this file system. His EXT3 file recovery tools are used by investigators worldwide. Hal is a SANS Lethal Forensicator, and is the creator of the SANS Linux/Unix Security track (GCUX). He holds the GCFA and GREM certifications and teaches the related courses in the SANS Forensics curriculum. He is a respected author and speaker at industry gatherings worldwide. Hal is a regular contributor to the SANS Computer Forensics blog and co-author of the Command Line Kung Fu blog.

@hal_pomeranz
Course Day Descriptions

Mon, Jun 17 - Sat, Jun 22
9:00am - 5:00pm
Hands-on labs

DAY 1: Hardening Linux/Unix Systems – Part 1
This course day tackles some of the most important techniques for protecting your Linux/Unix systems from external attacks, and it also covers what those attacks are so that you know what you’re defending against. This is a full-disclosure course with in-class demos of actual exploits and hands-on exercises to experiment with various examples of malicious software, as well as different techniques for protecting Linux/Unix systems.

Topics: Memory Attacks and Overflows; Vulnerability Minimization; Boot-Time Configuration; Encrypted Access; Host-Based Firewalls

DAY 2: Hardening Linux/Unix Systems – Part 2
Continuing our exploration of Linux/Unix security issues, this course day focuses on local exploits and access control issues. What do attackers do once they gain access to your systems? How can you detect their presence? How do you protect against attackers with physical access to your systems? What can you do to protect against mistakes (or malicious activity) by your own users?

Topics: Rootkits and Malicious Software; File Integrity Assessment; Physical Attacks and Defenses; User Access Controls; Root Access Control with sudo; Warning Banners; Kernel Tuning for Security

DAY 3: Hardening Linux/Unix Systems – Part 3
Monitoring your systems is critical for maintaining a secure environment. This course day digs into the different logging and monitoring tools available in Linux/Unix, and looks at additional tools for creating a centralized monitoring infrastructure such as Syslog-NG. Along the way, the course introduces a number of useful SSH tips and tricks for automating tasks and tunneling different network protocols in a secure fashion.

Topics: Automating Tasks With SSH; AIDE via SSH; Linux/Unix Logging Overview; SSH Tunneling; Centralized Logging with Syslog-NG

DAY 4: Linux Application Security – Part 1
This course day examines common application security tools and techniques. The SCP-Only Shell will be presented as an example of using an application under chroot() restriction, and as a more secure alternative to file-sharing protocols like anonymous FTP. The SELinux application whitelisting mechanism will be examined in-depth. Tips for troubleshooting common SELinux problems will be covered and students will learn how to craft new SELinux policies from scratch for new and locally developed applications. Significant hands-on time will be provided for students to practice these concepts.

Topics: chroot() for Application Security; The SCP-Only Shell; SELinux Basics; SELinux and the Reference Policy

DAY 5: Linux Application Security – Part 2
This course section is a full day of in-depth analysis on how to manage some of the most popular application-level services securely on a Linux/Unix platform. We will tackle the practical issues involved with securing three of the most commonly used Internet servers on Linux and Unix: BIND, Sendmail, and Apache. Beyond basic security configuration information, we will take an in-depth look at topics like DNSSec and Web Application Firewalls with mod_security and the Core Rules.

Topics: BIND; DNSSec; Apache; Web Application Firewalls with mod_security

DAY 6: Digital Forensics for Linux/Unix
This hands-on course day is designed to be an information-rich introduction to basic forensic principles and techniques for investigating compromised Linux and Unix systems. At a high level, it introduces the critical forensic concepts and tools that every administrator should know and provides a real-world compromise for students to investigate using the tools and strategies discussed in class.

Topics: Tools Throughout; Forensic Preparation and Best Practices; Incident Response and Evidence Acquisition; Media Analysis; Incident Reporting

Who Should Attend
- Security professionals looking to learn the basics of securing Unix operating systems
- Experienced administrators looking for in-depth descriptions of attacks on Unix systems and how they can be prevented
- Administrators needing information on how to secure common Internet applications on the Unix platform
- Auditors, incident responders, and InfoSec analysts who need greater insight into Linux and Unix security tools, procedures, and best practices

“This course gave me a better understanding of Linux internals and specific threat hunting ideas that I will use in my environment.”
-Shelby Peterson, Adobe

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/sansfire/courses
SEC511: Continuous Monitoring and Security Operations

You Will Be Able To

- Analyze a security architecture for deficiencies
- Apply the principles learned in the course to design a defensible security architecture
- Understand the importance of a detection-dominant security architecture and a Security Operations Center (SOC)
- Identify the key components of Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Monitoring (CM)
- Determine appropriate security monitoring needs for organizations of all sizes
- Implement robust Network Security Monitoring/Continuous Security Monitoring (NSM/CSM)
- Utilize tools to support implementation of Continuous Monitoring per NIST SP 800-137 guidelines
- Determine requisite monitoring capabilities for a SOC environment
- Determine capabilities required to support continuous monitoring of key Critical Security Controls

We continue to underestimate the tenacity of our adversaries! Organizations are investing significant time and financial and human resources to combat cyber threats and prevent cyber attacks, but despite this tremendous effort, organizations are still getting compromised. The traditional perimeter-focused, prevention-dominant approach to security architecture has failed to prevent intrusions. No network is impenetrable, which is a reality that business executives and security professionals alike have to accept. Prevention is crucial, and we can’t lose sight of it as the primary goal. However, a new proactive approach to security is needed to enhance the capabilities of organizations to detect threats that will inevitably slip through their defenses.

The underlying challenge for organizations victimized by an attack is timely incident detection. Industry data suggest that most security breaches typically go undiscovered for an average of seven months. Attackers simply have to find one way into most organizations, because they know that the lack of visibility and internal security controls will then allow them to methodically carry out their mission and achieve their goals.

The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM) taught in this course will best position your organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach will be early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and this course will greatly increase your understanding and enhance your skills in implementing CM utilizing the NIST framework.

SEC511 will take you on quite a journey. We start by exploring traditional security architecture to assess its current state and the attacks against it. Next, we discuss and discover modern security design that represents a new proactive approach to such architecture that can be easily understood and defended. We then transition to how to actually build the network and endpoint security, and then carefully navigate our way through automation, NSM/CDM/CSM. For timely detection of potential intrusions, the network and systems must be proactively and continuously monitored for any changes in the security posture that might increase the likelihood that attackers will succeed.

Your SEC511 journey will conclude with one last hill to climb! The final day (Day 6) features a Capture-the-Flag competition that challenges you to apply the skills and techniques learned in the course to detect and defend the modern security architecture that has been designed. Course authors Eric Conrad and Seth Misenar have designed the Capture-the-Flag competition to be fun, engaging, comprehensive, and challenging. You will not be disappointed!

Seth Misenar
SANS Faculty Fellow

Seth Misenar is the founder of and lead consultant for Context Security, a Jackson, Mississippi-based company that provides information security thought leadership, independent research, and security training. Seth’s background includes network and web application penetration testing, vulnerability assessment, regulatory compliance efforts, security architecture design, and general security consulting. He has previously served as both a physical and network security consultant for Fortune 100 companies, as well as the Health Insurance Portability and Accountability Act, and as information security officer for a state government agency. Prior to becoming a security geek, Seth received a bachelor’s degree in philosophy from Millsaps College, where he was twice selected for a Ford Teaching Fellowship. Also, Seth is no stranger to certifications and thus far has achieved credentials that include the CISSP®, GPEN, GWAPT, GSEC, GCIA, GCICH, GCWN, GCFA, and MCSE. @sethmisenar
### Course Day Descriptions

**DAY 1: Current State Assessment, SOCs, and Security Architecture**
We begin with the end in mind by defining the key techniques and principles that will allow us to get there. An effective modern Security Operations Center (SOC) or security architecture must enable an organization’s ability to rapidly find intrusions to facilitate containment and response. Both significant knowledge and a commitment to continuous monitoring are required to achieve this goal.

**Topics:** Current State Assessment, SOCs, and Security Architecture; Modern Security Architecture Principles; Frameworks and Enterprise Security Architecture; Security Architecture – Key Techniques/Practices; Security Operations Center

**DAY 2: Network Security Architecture**
Understanding the problems with the current environment and realizing where we need to get to is far from sufficient; we need a detailed roadmap to bridge the gap between the current and desired state. Day 2 introduces and details the components of our infrastructure that become part of a defensible network security architecture and SOC. We are long past the days when a perimeter firewall and ubiquitous antivirus were sufficient security. There are many pieces and moving parts that make up a modern defensible security architecture.

**Topics:** SOCs/Security Architecture – Key Infrastructure Devices; Segmented Internal Networks; Defensible Network Security Architecture Principles Applied

**DAY 3: Network Security Monitoring**
Designing a SOC or security architecture that enhances visibility and detective capabilities represents a paradigm shift for most organizations. However, the design is simply the beginning. The most important element of a modern security architecture is the emphasis on detection. The network security architecture presented in days one and two emphasized baking visibility and detective capabilities into the design. Now we must figure out how to look at the data and continuously monitor the enterprise for evidence of compromise or changes that increase the likelihood of compromise.

**Topics:** Continuous Monitoring Overview; Network Security Monitoring (NSM); Practical NSM Issues; Cornerstone NSM

**DAY 4: Endpoint Security Architecture**
One of the hallmarks of modern attacks is an emphasis on client-side exploitation. The days of breaking into networks via direct frontal assaults on unpatched mail, web, or DNS servers are largely behind us. We must focus on mitigating the risk of compromise of clients. Day four details ways in which endpoint systems can be both more resilient to attack and also enhance detective capabilities.

**Topics:** Security Architecture – Endpoint Protection; Dangerous Endpoint Applications; Patching

**DAY 5: Automation and Continuous Security Monitoring**
Network Security Monitoring (NSM) is the beginning; we need to not only detect active intrusions and unauthorized actions, but also to know when our systems, networks, and applications are at an increased likelihood for compromise. A strong way to achieve this is through Continuous Security Monitoring (CSM) or Continuous Diagnostics and Mitigation (CDM). Rather than waiting for the results of a quarterly scan or an annual penetration test to determine what needs to be addressed, continuous monitoring proactively and repeatedly assesses and reassesses the current security posture for potential weaknesses that need to be addressed.

**Topics:** CSM Overview, Industry Best Practices; Winning CSM Techniques; Maintaining Situational Awareness; Host, Port and Service Discovery; Vulnerability Scanning; Monitoring Patching; Monitoring Applications; Monitoring Service Logs; Monitoring Change to Devices and Appliances; Leveraging Proxy and Firewall Data; Configuring Centralized Windows Event Log Collection; Monitoring Critical Windows Events; Scripting and Automation

**DAY 6: Capstone: Design, Detect, Defend**
The course culminates in a team-based design, detect, and defend the flag competition that is a full day of hands-on work applying the principles taught throughout the week.

**Topics:** Security Architecture; Assessing Provided Architecture; Continuous Security Monitoring; Using Tools/Scripts Assessing the Initial State; Quickly/Thoroughly Find All Changes Made

---

**Who Should Attend**
- Security architects
- Senior security engineers
- Technical security managers
- Security Operations Center (SOC) analysts, engineers, and managers
- CND analysts
- Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)

---

**For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/sansfire/courses**

---

“*The information and networking at this event were amazing. I’m ready to share what I learned with my organization.*

- Calvin Harris, Exelon
SEC530: Defensible Security Architecture

SEC530: Defensible Security Architecture is designed to help students build and maintain a truly defensible security architecture. “The perimeter is dead” is a favorite saying in this age of mobile, cloud, and the Internet of Things, and we are indeed living in a new world of “de-perimeterization” where the old boundaries of “inside” and “outside” or “trusted” and “untrusted” no longer apply.

This changing landscape requires a change in mindset, as well as a repurposing of many devices. Where does it leave our classic perimeter devices such as firewalls? What are the ramifications of the “encrypt everything” mindset for devices such as Network Intrusion Detection Systems?

In this course, students will learn the fundamentals of up-to-date defensible security architecture. There will be a heavy focus on leveraging current infrastructure (and investment), including switches, routers, and firewalls. Students will learn how to reconfigure these devices to better address the threat landscape they face today. The course will also suggest newer technologies that will aid in building a robust security infrastructure.

While this is not a monitoring course, it will dovetail nicely with continuous security monitoring, ensuring that security architecture not only supports prevention, but also provides the critical logs that can be fed into a Security Information and Event Management (SIEM) system in a Security Operations Center.

Hands-on labs will reinforce key points in the course and provide actionable skills that students will be able to leverage as soon as they return to work.

You Will Be Able To
- Analyze a security architecture for deficiencies
- Apply the principles learned in the course to design a defensible security architecture
- Determine appropriate security monitoring needs for organizations of all sizes
- Maximize existing investment in security architecture by reconfiguring existing assets
- Determine capabilities required to support continuous monitoring of key Critical Security Controls
- Configure appropriate logging and monitoring to support a Security Operations Center and continuous monitoring program

Who Should Attend
- Security architects
- Network engineers
- Network architects
- Security analysts
- Senior security engineers
- System administrators
- Technical security managers
- CND analysts
- Security monitoring specialists
- Cyber threat investigators

“As a systems programmer working on the development of security tools, the architectural content provided has been highly informative and extremely valuable.”
-Merv Hammer, Workday Inc.

“SEC530 provided an excellent understanding of application attacks and how to protect against them.”
-Shayne Douglass, AMEWAS Inc.

Ismael Valenzuela
SANS Certified Instructor

Ismael Valenzuela founded one of the first IT security consultancies in Spain and has participated as a security professional in numerous projects across the globe over the past 17 years. As a top cybersecurity expert with a strong technical background and deep knowledge of penetration testing, security architectures, intrusion detection and computer forensics, Ismael has provided security consultancy, advice and guidance to large government and private organizations, including major EU Institutions and U.S. government agencies. Prior to his current role as Principal Engineer at McAfee, where he leads research on threat hunting using machine-learning and expert-system-driven investigations, Ismael led the delivery of Security Operations Center, incident response and forensics services for the Foundstone Services team within Intel globally. Previously, Ismael worked as Global IT Security Manager for iSOFT Group Ltd, one of the world’s largest providers of healthcare IT solutions, managing its security operations in more than 40 countries. He holds a bachelor’s degree in computer science from the University of Malaga (Spain), has a certificate in business administration, and holds many professional certifications, including the highly regarded GIAC Security Expert (GSE #132) in addition to the GREM, GCFA, GCIA, GCIH, GPEN, GCUX, GCWN, GWAPT, GSNA, GMON, CISSP®, ITIL, CISM, and IRCA 27001 Lead Auditor from Bureau Veritas UK.

@aboutsecurity
Course Day Descriptions

**DAY 1: Defensible Security Architecture**
Day 1 of the course describes hardening systems and networks at every layer, from layer one (physical) to layer seven (applications and data). To quote Richard Bejtlich’s *The Tao of Network Security Monitoring*, defensible networks "encourage, rather than frustrate, digital self-defense." The section begins with an overview of traditional network and security architectures and their common weaknesses. The defensible security mindset is "build it once, build it right." All networks must perform their operational functions effectively, and security can be complementary to this goal. It is much more efficient to bake security in at the outset than to retrofit it later. The discussion will then turn to layer one (physical) and layer two (data link). Best practices, including many “ripped from the headlines” tips the co-authors have successfully deployed in the trenches to harden the infrastructure in order to prevent and detect modern attacks. Examples include the use of private VLANs, which effectively kills the malicious client-to-client pivot, and 802.1X and NAC, which mitigate rogue devices. Specific Cisco IOS syntax examples are provided to harden switches.

**Topics:** Traditional Security Architecture Deficiencies, Defensible Security Architecture, Threat, Vulnerability, and Data Flow Analysis; Layer 1 Best Practices; Layer 2 Best Practices

**DAY 2: Network Security Architecture**
Day 2 continues hardening the infrastructure and moves on to layer three routing. Actionable examples are provided for hardening routers, with specific Cisco IOS commands to perform each step. The section then continues with a deep dive on IPv6, which currently accounts for 23% of Internet backbone traffic, according to Google, while simultaneously being used and ignored by most organizations. This section will provide deep background on IPv6, discuss common mistakes (such as applying an IPv4 mindset to IPv6), and provide actionable solutions for securing the protocol. The section wraps up with a discussion of VPN and stateful layer three/four firewalls.

**Topics:** Layer 3: Router Best Practices; Layer 3 Attacks and Mitigation; Layer 2 and 3 Benchmarks and Auditing Tools; Securing SNMP; Securing NTP; Bogon Filtering, Blackholes, and Darknets; IPv6, Securing IPv6, VPN; Layer 3/4 Stateful Firewalls; NetFlow

**DAY 3: Network-Centric Application Security Architecture**
Organizations own or have access to many network-based security technologies ranging from Next-Generation Firewalls to web proxies and malware sandboxes. Yet the effectiveness of these technologies is directly affected by their implementation. Too much reliance on built-in capabilities like application control, antivirus, intrusion prevention, data loss prevention, or other automatic evil-finding deep packet inspection engines leads to a highly preventative-focused implementation, with huge gaps in both prevention and detection. Day 3 focuses on using application layer security solutions that an organization already owns with a modern mindset. By thinking outside the box, even old controls like a spam appliance can be used to catch modern attacks such as phishing via cousin domains and other spoofing techniques. And again, by engineering defenses for modern attacks, both prevention and detection capabilities gain significantly.

**Topics:** Proxy; NGFW; NIDS/NIPS, Network Security Monitoring, Sandboxing; Encryption; Secure Remote Access; Distributed Denial-of-Service (DDoS)

**DAY 4: Data-Centric Application Security Architecture**
Organizations cannot protect something they do not know exists. The problem is that critical and sensitive data exist all over. Complicating this even more is that data are often controlled by a full application stack involving multiple services that may be hosted on-premise or in the cloud. Day 4 focuses on identifying core data where they reside and how to protect those data. Protection includes the use of data governance solutions and full application stack security measures such as web application firewalls and database activity monitoring, as well as keeping a sharp focus on securing the systems hosting core services such as on-premise hypervisors, cloud computing platforms, and container services such as Docker. The data-centric security approach focuses on what is core to an organization and prioritizes security controls around it. Why spend copious amounts of time and money securing everything when controls can be optimized and focused on securing what matters? Let’s face it: Some systems are more critical than others.

**Topics:** Application (Reverse) Proxies; Full Stack Security Design; Web Application Firewalls; Database Firewalls/Database Activity Monitoring; File Classification; Data Loss Prevention (DLP); Data Governance; Mobile Device Management (MDM) and Mobile Application Management (MAM); Private Cloud Security; Public Cloud Security; Container Security

**DAY 5: Zero Trust Architecture: Addressing the Adversaries Already in Our Networks**
Today, a common security mantra is "trust but verify." But this is a broken concept. Computers are capable of calculating trust on the fly, so rather than thinking in terms of "trust but verify" organizations should be implementing "verify then trust." By doing so, access can be constrained to appropriate levels at the same time that access can become more fluid. This section focuses on implementing a zero trust architecture where trust is no longer implied but must be proven. By doing so, a model of variable trust must become a reality. By doing so, a model of variable trust must become a reality. This, in turn, allows for implementing fewer or more security controls as necessary given a user’s and a device’s trust maintained over time. The focus is on implementing zero trust with existing security technologies to maximize their value and impact for an organization’s security posture. During this section encryption and authentication will be used to create a hardened network, whether external or internal. Also, advanced defensive techniques will be implemented to stop modern attack tools in their tracks while leaving services fully functional for authorized assets.

**Topics:** Zero Trust Architecture; Credential Rotation; Compromised Internal Assets; Securing the Network; Tripwire and Red Herring Defenses; Patching; Deputizing Endpoints as Hardened Security Sensors; Scaling Endpoint Log Collection/Storage/Analysis

**DAY 6: Hands-On Secure-the-Flag Challenge**
The course culminates in a team-based Design-and-Secure-the-Flag competition. Powered by NetWars, day six provides a full day of hands-on work applying the principles taught throughout the week. Your team will progress through multiple levels and missions designed to ensure mastery of the modern cyber defense techniques promoted throughout this course. Teams will assess, design, and secure a variety of computer systems and devices, leveraging all seven layers of the OSI model.

**Topics:** Capstone – Design/Detect/Defend
SEC545: Cloud Security Architecture and Operations

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Revise and build internal policies to ensure cloud security is properly addressed
- Understand all major facets of cloud risk, including threats, vulnerabilities, and impact
- Articulate the key security topics and risks associated with SaaS, PaaS, and IaaS cloud deployment models
- Evaluate Cloud Access Security Brokers (CASBs) to better protect and monitor SaaS deployments
- Build security for all layers of a hybrid cloud environment, starting with hypervisors and working to application layer controls
- Evaluate basic virtualization hypervisor security controls
- Design and implement network security access controls and monitoring capabilities in a public cloud environment
- Design a hybrid cloud network architecture that includes IPSec tunnels
- Integrate cloud identity and access management (IAM) into security architecture
- Evaluate and implement various cloud encryption types and formats
- Develop multi-tier cloud architectures in a Virtual Private Cloud (VPC), using subnets, availability zones, gateways, and NAT
- Integrate security into DevOps teams, effectively creating a DevSecOps team structure
- Build automated deployment workflows using Amazon Web Services and native tools
- Incorporate vulnerability management, scanning, and penetration testing into cloud environments

As more organizations move data and infrastructure to the cloud, security is becoming a major priority. Operations and development teams are finding new uses for cloud services, and executives are eager to save money and gain new capabilities and operational efficiency by using these services. But will information security prove to be an Achilles’ heel? Many cloud providers do not provide detailed control information about their internal environments, and quite a few common security controls used internally may not translate directly to the public cloud.

SEC545: Cloud Security Architecture and Operations will tackle these issues one by one. We’ll start with a brief introduction to cloud security fundamentals, then cover the critical concepts of cloud policy and governance for security professionals. For the rest of day one and all of day two, we’ll move into technical security principles and controls for all major cloud types (SaaS, PaaS, and IaaS). We’ll learn about the Cloud Security Alliance framework for cloud control areas, then delve into assessing risk for cloud services, looking specifically at technical areas that need to be addressed.

The course then moves into cloud architecture and security design, both for building new architectures and for adapting tried-and-true security tools and processes to the cloud. This will be a comprehensive discussion that encompasses network security (firewalls and network access controls, intrusion detection, and more), as well as all the other layers of the cloud security stack. We’ll visit each layer and the components therein, including building secure instances, data security, identity and account security, and much more. We’ll devote an entire day to adapting our offense and defense focal areas to the cloud. This will involve looking at vulnerability management and pen testing, as well as covering the latest and greatest cloud security research. On the defense side, we’ll delve into incident handling, forensics, event management, and application security.

We wrap up the course by taking a deep dive into SecDevOps and automation, investigating methods of embedding security into orchestration, and every facet of the cloud life cycle. We’ll explore tools and tactics that work, and even walk through several cutting-edge use cases where security can be automated entirely in both deployment and incident detection-and-response scenarios using APIs and scripting.

“The training is excellent for cloud security understanding and overviews. I would definitely recommend this course for people looking at building a cloud security program.”

- Justin Pyle, Chan Zuckerberg Initiative

Dave Shackleford is the owner and principal consultant of Voodoo Security and a SANS analyst and course author. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering and is a VMware VExpert with extensive experience designing and configuring secure virtualized infrastructures. He has previously worked as CSO for ConfigureSoft, CTO for the Center for Internet Security, and as a security architect, analyst, and manager for several Fortune 500 companies. Dave is the author of the Sybex book Virtualization Security: Protecting Virtualized Environments, as well as the co-author of Hands-On Information Security from Course Technology. Recently Dave co-authored the first published course on virtualization security for the SANS Institute. Dave currently serves on the Board of Directors at the SANS Technology Institute and helps lead the Atlanta chapter of the Cloud Security Alliance.

@daveshackleford

Who Should Attend

- Security analysts
- Security architects
- Senior security engineers
- Technical security managers
- Security monitoring analysts
- Cloud security architects
- DevOps and DevSecOps engineers
- System administrators
- Cloud administrators

Register at www.sans.org/sansfire | 301-654-SANS (7267)
DAY 1: Cloud Security Foundations
The first day of the course starts out with an introduction to the cloud, including terminology, taxonomy, and basic technical premises. We also examine what is happening in the cloud today, and cover the spectrum of guidance available from the Cloud Security Alliance, including the Cloud Controls Matrix, the 14 major themes of cloud security, and other research available. Next we spend time on cloud policy and planning, delving into the changes an organization needs to make for security and IT policy to properly embrace the cloud. After all the legwork is done, we’ll start talking about some of the main technical considerations for the different cloud models. We’ll start by breaking down Software-as-a-Service (SaaS) and some of the main types of security controls available. A specialized type of Security-as-a-Service (SecaaS) known as Cloud Access Security Brokers (CASBs) will also be explained, with examples of what to look for in such a service. We’ll wrap up with an introduction to Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) controls, which will set the stage for the rest of the course.
Topics: Introduction to the Cloud and Cloud Security Basics; Cloud Security Alliance Guidance; Cloud Policy and Planning; SaaS Security; Cloud Access Security Brokers; Intro to PaaS and IaaS Security Controls

DAY 2: Core Security Controls for Cloud Computing
The second day of SEC545 compares traditional in-house controls with those in the cloud today. Some controls are similar and mostly compatible, but not all of them. Since most cloud environments are built on virtualization technology, we walk through a short virtualization security primer, which can help teams building hybrid clouds that integrate with internal virtualized assets, and also help teams properly evaluate the controls cloud providers offer in this area. We’ll then break down cloud network security controls and tradeoffs, since this is an area that is very different from what we’ve traditionally run in-house. For PaaS and IaaS environments, it’s critical to secure virtual machines (instances) and the images we deploy them from, so we cover this next. At a high level, we’ll also touch on identity and access management for cloud environments to help control and monitor who is accessing the cloud infrastructure, as well as what they’re doing there. We also cover data security controls and types, including encryption, tokenization, and more. Specific things to look for in application security are laid out as the final category of overall controls. We then pull it all together to demonstrate how you can properly evaluate a cloud provider’s controls and security posture.

DAY 3: Cloud Security Architecture and Design
Instead of focusing on individual layers of our cloud stack, we start day three by building the core security components. We’ll break down cloud security architecture best practices and principles that most high-performing teams prioritize when building or adding cloud security controls and processes to their environments. We start with infrastructure and core component security – in other words, we need to look at properly locking down all the pieces and parts we covered on day two! This then leads to a focus on major areas of architecture and security design. The first is building various models of access control and compartmentalization. This involves breaking things down into two categories: identity and access management (IAM) and network security. We delve into these in significant depth, as they can form the backbone of a sound cloud security strategy. We then look at architecture and design for data security, touching on encryption technologies, key management, and what the different options are today. We wrap up our third day with another crucial topic: availability. Redundant and available design is as important as ever, but we need to use cloud provider tools and geography to our advantage. At the same time, we need to make sure we evaluate the cloud provider’s disaster recovery and continuity, and so this is covered as well.
Topics: Cloud Security Architecture Overview; Cloud Architecture and Security Principles; Infrastructure and Core Component Security; Access Controls and Compartmentalization; Confidentiality and Data Protection; Availability

DAY 4: Cloud Security – Offense and Defense
There are many threats to our cloud assets, so the fourth day of the course begins with an in-depth breakdown of the types of threats out there. We’ll look at numerous examples. The class also shows students how to design a proper threat model focused on the cloud by using several well-known methods such as STRIDE and attack trees and libraries. Scanning and pen testing the cloud used to be challenging due to restrictions put in place by the cloud providers themselves. But today it is easier than ever. There are some important points to consider when planning a vulnerability management strategy in the cloud, and this class touches on how to best scan your cloud assets and which tools are available to get the job done. Pen testing naturally follows this discussion, and we talk about how to work with the cloud providers to coordinate tests, as well as how to perform testing yourself. On the defensive side, we start with network-based and host-based intrusion detection, and how to monitor and automate our processes to better carry out this detection. This is an area that has definitely changed from what we’re used to in-house, so security professionals need to know what their best options are and how to get this done. Our final topics on day four include incident response and forensics (also topics that have changed significantly in the cloud). The tools and processes are different, so we need to focus on automation and event-driven defenses more than ever.
Topics: Threats to Cloud Computing; Vulnerability Management in the Cloud; Cloud Pen Testing; Intrusion Detection in the Cloud; Cloud IR and Event Management; Cloud Forensics

DAY 5: Cloud Security Automation and Orchestration
On our final day, we’ll focus explicitly on how to automate security in the cloud, both with and without scripting techniques. We will use tools like the AWS CLI and AWS Lambda to illustrate the premises of automation, then turn our attention toward SecDevOps principles. We begin by explaining what that really means, and how security teams can best integrate into DevOps and cloud development and deployment practices. We’ll cover automation and orchestration tools like Ansible and Chef, as well as how we can develop better and more efficient workflows with AWS CloudFormation and other tools. Continuing some of the topics from day four, we will look at event-driven detection and event management, as well as response and defense strategies that work. While we won’t automate everything, some actions and scenarios really lend themselves to monitoring tools like CloudWatch, tagging assets for identification in security processes, and initiating automated response and remediation to varying degrees. We wrap up the class with a few more tools and tactics, followed by a sampling of real-world use cases.
Topics: Scripting and Automation in the Cloud; SecDevOps Principles; Creating Secure Cloud Workflows; Building Automated Event Management; Building Automated Defensive Strategies; Tools and Tactics; Real-World Use Cases; Class Wrap-Up
Many organizations have logging capabilities but lack the people and processes to analyze them. In addition, logging systems collect vast amounts of data from a variety of data sources that require an understanding of those sources for proper analysis. This class is designed to provide students with the training, methods, and processes to enhance existing logging solutions. This class will also help you understand the when, what, and why behind the logs. This is a lab-heavy course that utilizes SOF-ELK, a SANS-sponsored free Security Information and Event Management (SIEM) solution, to provide hands-on experience and the mindset for large-scale data analysis.

Today, security operations do not suffer from a “Big Data” problem but rather a “Data Analysis” problem. Let’s face it, there are multiple ways to store and process large amounts of data without any real emphasis on gaining insight into the information collected. Added to that is the daunting idea of an infinite list of systems from which one could collect logs. It is easy to get lost in the perils of data saturation. This class moves away from the typical churn-and-burn log systems and moves instead towards achieving actionable intelligence and developing a tactical Security Operations Center (SOC).

This course is designed to demystify the SIEM architecture and process by navigating the student through the steps of tailoring and deploying a SIEM to full SOC integration. The material will cover many bases in the “appropriate” use of a SIEM platform to enrich readily available log data in enterprise environments and extract actionable intelligence. Once the information is collected, the student will be shown how to present the gathered input into usable formats to aid in eventual correlation. Students will then iterate through the log data and events to analyze key components that will allow them to learn how rich this information is, how to correlate the data, how to start investigating based on the aggregate data, and finally, how to go hunting with this newly gained knowledge. They will also learn how to deploy internal post-exploitation tripwires and breach canaries to nimbly detect sophisticated intrusions. Throughout the course, the text and labs will not only show how to manually perform these actions, but also how to automate many of the processes mentioned so students can employ these tasks the day they return to the office.

The underlying theme is to actively apply Continuous Monitoring and analysis techniques by utilizing modern cyber threat attacks. Labs will involve replaying captured attack data to provide real-world results and visualizations.

“"This course uses real-world events and hands-on training to allow me to immediately improve my organization's security stance. Day one back in the office I was implementing what I learned.”

-Frank Giachino, Bechtel
DAY 1: SIEM Architecture and SOF-ELK
This section will introduce free logging and analysis tools and focus on techniques to make sense of and augment traditional logs. It also covers how to handle the big data problem of handling billions of logs and how advances in free tools are starting to give commercial solutions a run for their money. Day one is designed to bring all students up to speed on SIEM concepts and to bring all students to a base level to carry them through the rest of the class. It is designed to also cover SIEM best practices. During day one we will be introducing Elasticsearch, Logstash, and Kibana within SOF-ELK and immediately go into labs to get students comfortable with ingesting, manipulating, and reporting on log data.
Topics: State of the SOC/SIEM; Log Monitoring; Logging Architecture; SIEM Platforms; Planning a SIEM; SIEM Architecture; Ingestion Techniques and Nodes; Data Queuing and Resiliency; Storage and Speed; Analytical Reporting

DAY 2: Service Profiling with SIEM
This section covers how to collect and handle this massive amount of data. Methods for collecting these logs through service logs such as from DNS servers will be covered, as will be passive ways of pulling the same data from the network itself. Techniques will be demonstrated to augment and add valuable context to the data as they are collected. Finally, analytical principles will be covered for finding the needles in the stack of needles. We will cover how, even if we have the problem of searching through billions of logs, we can surface only meaningful items of interest. Active dashboards will be designed to quickly find the logs of interest and to provide analysts with additional context for what to do next.
Topics: Detection Methods and Relevance to Log Analysis; Analyzing Common Application Logs that Generate Tremendous Amounts of Data; Apply Threat Intelligence to Generic Network Logs; Active Dashboards and Visualizations

DAY 3: Advanced Endpoint Analytics
The value in endpoint logs provides tremendous visibility in detecting attacks. In particular, with regard to finding post-compromise activity, endpoint logs can quickly become second to none. However, logs even on a single desktop can range in the tens if not hundreds of thousands of events per day. Multiply this by the number of systems in your environment and it is no surprise that organizations get overwhelmed. This section will cover the how and more importantly the why behind collecting system logs. Various collection strategies and tools will be used to gain hands-on experience and to provide simplification with handling and filtering the seemingly infinite amount of data generated by both servers and workstations. Workstation log strategies will be covered in depth due to their value in today’s modern attack vectors. After all, modern-day attacks typically start and then spread from workstations.
Topics: Endpoint Logs

DAY 4: Baselining and User Behavior Monitoring
This section focuses on applying techniques to automatically maintain a list of assets and their configurations as well as methods to distinguish if they are authorized or unauthorized. Key locations to provide high-fidelity data will be covered and techniques to correlate and combine multiple sources of data together will be demonstrated to build a master inventory list. Other forms of knowing thyself will be introduced such as gaining hands-on experience in applying network and system baselining techniques. We will monitor network flows and identify abnormal activity such as C2 beaconing as well as look for unusual user activity. Finally, we will apply large data analysis techniques to sift through massive amounts of endpoint data. This will be used to find things such as unwanted persistence mechanisms, dual-homed devices, and more.
Topics: Identify Authorized and Unauthorized Assets; Identify Authorized and Unauthorized Software; Baseline Data

DAY 5: Tactical SIEM Detection and Post-Mortem Analysis
This section focuses on combining multiple security logs for central analysis. More importantly, we will cover methods for combining multiple sources to provide improved context to analysts. We will also show how providing context with asset data can help prioritize analyst time, saving money and addressing risks that matter. After covering ways to optimize traditional security alerts, we will jump into new methods to utilize logging technology to implement virtual tripwires. While it would be ideal to prevent attackers from gaining access to your network, it is given that at some point you will be compromised. However, preventing compromise is the beginning, not the end goal. Adversaries will crawl your systems and network to achieve their own ends. Knowing this, we will implement logging-based tripwires—and if a single one is stepped on, we can quickly detect it and respond to the adversary.
Topics: Centralize NIDS and HIDS Alerts; Analyze Endpoint Security Logs; Augment Intrusion Detection Alerts; Analyze Vulnerability Information; Correlate Malware Sandbox Logs with Other Systems to Identify Victims Across the Enterprise; Monitor Firewall Activity; SIEM Tripwires; Post Mortem Analysis

DAY 6: Capstone: Design, Detect, Defend
The course culminates in a team-based design, detect, and defend the flag competition. Powered by NetWars, day six provides a full day of hands-on work applying the principles taught throughout the week. Your team will progress through multiple levels and missions designed to ensure mastery of the modern cyber defense techniques promoted all week long. From building a logging architecture to augmenting logs, analyzing network logs, analyzing system logs, and developing dashboards to find attacks, this challenging exercise will reinforce key principles in a fun, hands-on, team-based challenge.
Topics: Defend-the-Flag Challenge – Hands-on Experience

Who Should Attend
- Security analysts
- Security architects
- Senior security engineers
- Technical security managers
- Security Operations Center analysts, engineers, and managers
- CND analysts
- Security monitoring specialists
- System administrators
- Cyber threat investigators
- Individuals working to implement Continuous Security Monitoring
- Individuals working in a hunt team capacity

“This course is as practical and real-world as it gets. SEC555 provides numerous quick wins and really stimulates thinking about the relative value of numerous ways to defend your organization.”
-Mikhail Vitebsky, Lexington Partners
Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches? This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS).

As threats evolve, an organization’s security should too. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course that teaches students the Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle. The British government’s Center for the Protection of National Infrastructure describes the Controls as the “baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence.”

SANS’s in-depth, hands-on training will teach you how to master the specific techniques and tools needed to implement and audit the Critical Controls. It will help security practitioners understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats.

The course shows security professionals how to implement the Controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.

“SEC566 provides great tools, explanation, and insight!”

- Ryan LeVan, Trex Company, Inc.
DAY 1: Introduction and Overview of the 20 Critical Controls

Day 1 will introduce you to all of the Critical Controls, laying the foundation for the rest of the class. For each Control, we will follow the same outline covering the following information:

• Overview of the Control
• How It Is Compromised
• Defensive Goals
• Quick Wins
• Visibility & Attribution
• Configuration & Hygiene
• Advanced
• Overview of Evaluating the Control
• Core Evaluation Test(s)
• Testing/Reporting Metrics
• Steps for Root Cause Analysis of Failures
• Audit/Evaluation Methodologies
• Evaluation Tools
• Exercise to Illustrate Implementation or Steps for Auditing a Control

In addition, Critical Controls 1 and 2 will be covered in depth.

Topics: Critical Control 1: Inventory of Authorized and Unauthorized Devices; Critical Control 2: Inventory of Authorized and Unauthorized Software

DAY 2: Critical Controls 3, 4, 5, and 6

Topics: Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers; Critical Control 4: Continuous Vulnerability Assessment and Remediation; Critical Control 5: Controlled Use of Administrative Privileges; Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs

DAY 3: Critical Controls 7, 8, 9, 10, and 11

Topics: Critical Control 7: Email and Web Browser Protections; Critical Control 8: Malware Defenses; Critical Control 9: Limitation and Control of Network Ports, Protocols, and Services; Critical Control 10: Data Recovery Capability (validated manually); Critical Control 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

DAY 4: Critical Controls 12, 13, 14, and 15

Topics: Critical Control 12: Boundary Defense; Critical Control 13: Data Protection; Critical Control 14: Controlled Access Based on the Need to Know; Critical Control 15: Wireless Device Control

DAY 5: Critical Controls 16, 17, 18, 19, and 20

Topics: Critical Control 16: Account Monitoring and Control; Critical Control 17: Security Skills Assessment and Appropriate Training to Fill Gaps (validated manually); Critical Control 18: Application Software Security; Critical Control 19: Incident Response and Management (validated manually); Critical Control 20: Penetration Tests and Red Team Exercises (validated manually)

“This course is providing me with the necessary context to understand the Critical Security Controls in depth, and further helping me understand how to present recommendations to our business owners.”

- Chris Harper, Centrus Energy
SEC599: Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses

You Will Be Able To

▌ Understand how red and blue teams can effectively work together to form a true purple team
▌ Understand how recent high-profile attacks were delivered and how they could have been stopped
▌ Implement security controls throughout the different phases in the APT attack cycle to prevent, detect, and respond to attacks. We will define the following stages in the APT attack cycle:
  - Reconnaissance
  - Weaponization
  - Delivery
  - Exploitation
  - Installation
  - Command and control
  - Action on objectives
▌ Carry out a series of practical exercises:
  - Comprise a virtual organization to understand how attackers operate
  - Build your own mail sandbox solution to detect spear phishing
  - Develop effective group policies to prevent script execution and stop malicious code execution
  - Stop 0-day exploits using exploit mitigation techniques and application whitelisting
  - Detect and avoid malware persistence using host-based IDS techniques
  - Detect and prevent lateral movement through Sysmon, Windows event monitoring, and group policies
  - Block and detect command and control through network analysis
  - Manage, share, and operationalize threat intelligence using MISP, a threat-information-sharing platform

Erik Van Buggenhout
SANS Certified Instructor

You just got hired to help our virtual organization “SyncTechLabs” build out a cybersecurity capability. On your first day, your manager tells you: “We looked at some recent cybersecurity trend reports and we feel like we’ve lost the plot. Advanced persistent threats, ransomware, denial of service...We’re not even sure where to start!”

Cyber threats are on the rise: ransomware is affecting small, medium and large enterprises alike, while state-sponsored adversaries are attempting to obtain access to your most precious crown jewels. SEC599: Defeating Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses will provide an in-depth understanding of how current adversaries operate and arm you with the knowledge and expertise you need to detect and respond to today’s threats.

SEC599 aims to leverage the purple team concept by bringing together red and blue teams for maximum effect. Recognizing that a prevent-only strategy is not sufficient, the course focuses on current attack strategies and how they can be effectively mitigated and detected using a Kill Chain structure. Throughout the course, the purple team principle will be maintained, where attack techniques are first explained in-depth, after which effective security controls are introduced and implemented.

Course authors Erik Van Buggenhout and Stephen Sims (both certified as GIAC Security Experts) are hands-on practitioners who have achieved a deep understanding of how cyber attacks work through penetration testing and incident response. While teaching penetration testing courses, they were often asked “But how do I prevent this type of attack?” With more than 20 labs plus a full-day Defend-the-Flag exercise during which students attempt to defend our virtual organization from different waves of attacks against its environment, SEC599 gives students real-world examples of how to prevent attacks.

Our six-day journey will start with an analysis of recent attacks through in-depth case studies. We will explain what types of attacks are occurring and introduce the Advanced Persistent Threat (APT) Attack Cycle as a structured approach to describing attacks. In order to understand how attacks work, you will also compromise our virtual organization “SyncTechLabs” in our Day 1 exercises.

Throughout days 2 through 5 we will discuss how effective security controls can be implemented to prevent, detect, and respond to cyber attacks. Some of the topics we will address include:

▌ How red and blue teams can improve collaboration, forming a true purple team
▌ How current advanced adversaries are breaching our defenses
▌ Security controls structured around the Kill Chain

In designing the course and its exercises, the authors went the extra mile to ensure that attendees “build” something that can be used later on. For this reason, the different technologies illustrated throughout the course (e.g., IDS systems, web proxies, sandboxes, visualization dashboards, etc.) will be provided as usable virtual machines on the course USB.

SEC599 will finish with a bang. During the Defend-the-Flag challenge on the final course day, you will be pitted against advanced adversaries in an attempt to keep your network secure. Can you protect the environment against the different waves of attacks? The adversaries aren’t slowing down, so what are you waiting for?

Erik Van Buggenhout is the lead author of SEC599: Defeating Advanced Adversaries. In addition, Erik teaches SEC560: Network Penetration Testing and Ethical Hacking and SEC542: Web Application Penetration Testing and Ethical Hacking. He has been involved with SANS since 2009, starting as a Mentor, working his way to Community Instructor in 2012, and finally becoming a Certified Instructor in 2016. Erik loves explaining deeply technical concepts by using war stories, adding a few funny anecdotes here and there. As testimony to his technical expertise, he has obtained the GSE, GCIA, GNFA, OPEN, GWAPT, GCID, and GSEC certifications. Erik is the co-founder of the Belgian firm NVISO, which focuses on high-end cybersecurity services, specializing in government, defense and the financial sector. Together with his team of 20+ technical experts, Erik delivers a wide array of technical security services, including penetration testing, security monitoring and incident response. Prior to NVISO, Erik spent five years at a Big 4 firm, starting as a junior penetration tester and evolving into a subject-matter expert for the EMEA region. Erik is a self-confessed speed walker, so if you see him rushing around at a conference, feel free to stop him and say “Hi” @ErikVaBu
### Course Day Descriptions

**DAY 1: Knowing the Adversary, Knowing Yourself**

Our six-day journey will start with an introduction on the purple team concept. What is it all about? Should you form another dedicated cybersecurity team? We will focus on how red and blue teams can be encouraged to form a strong feedback loop for maximum effect. We will explain how recent attacks operate through in-depth case studies and introduce the APT attack cycle as a structured approach to describing attacks. In order to understand how attacks work, you will also compromise our virtual organization “SyncTechLabs” during the day’s exercises. Once we understand how adversaries are operating, we will flip over to the blue side and explain how defenders can better understand their own environments, set up a fundamental detection capability, and understand their own “soft spots.”

**Topics:** Course Outline and Lab Set-up, Current Threat and Attack Landscape, Introducing the APT Attack Cycle, A Defensible Architecture and Environment, Preparation – Knowing Yourself

**DAY 2: Averting Payload Delivery**

Day 2 will cover how attackers take their first steps. How do they deliver their initial payload and what can defenders do about it? We will cover the most frequently used payload delivery mechanisms:

- Delivery through (spear-)phishing
- Delivery through removable media
- Delivery through the network (e.g., Server Message Block relays, Responder, etc.)
- Delivery through HTTP or HTTPS

As always, students will first learn how the adversaries are operating by simulating the attacks in our lab environment, after which they will implement security controls to prevent and detect these attacks. The courseware will cover technical controls, but will also touch upon “soft topics” such as security awareness.

**Topics:** End-User Security Awareness, Leveraging Suricata IDS/IPS, Stopping Delivery Through Removable Media; Stopping Delivery Through the Network; Stopping Delivery Through Email; Stopping Delivery Through HTTP(S)

**DAY 3: Preventing Exploitation**

On Day 3 we will explain how exploitation can be prevented. Attendees will gain an in-depth understanding of current exploitation tactics. We will introduce effective security controls to stop exploitation attempts dead in their tracks. Discussions will include:

- Operating system hardening
- Payload execution control (including application whitelisting and script control)
- Securing applications from the ground up by doing threat modeling and implementing compile-time controls
- Securing vulnerable applications by implementing exploit mitigating techniques

**Topics:** Operating System Hardening; Preventing Execution of Payloads; Securing Applications

**DAY 4: Avoiding Installation, Foiling Command and Control, and Thwarting Lateral Movement**

On Day 4 we will continue our journey in the Kill Chain, with a key focus on how malicious adversary persistence can be avoided, how command and control channels can be detected, and how lateral movement can be stopped. Topics to be discussed include:

- Principle of least privilege to prevent malware persistence
- Detecting malware persistence in user land
- Network monitoring to detect command and control
- Hardening Windows to prevent lateral movement
- Analyzing Windows event logs to detect ongoing lateral movement

**Topics:** Avoiding Installation; Foiling Command and Control; Thwarting Lateral Movement

**DAY 5: Thwarting Exfiltration, Cyber Deception, and Incident Response**

Day 5 focuses on stopping the adversary during the final stages of the attack:

- How can data exfiltration be detected and stopped?
- How can cyber deception be used to slow down and stop advanced adversaries?
- How can threat intelligence aid defenders in the APT Attack Cycle?
- How can defenders perform effective incident response?

As always, theoretical concepts will be illustrated during the different exercises performed throughout the day.

**Topics:** Data Exfiltration; Cyber Deception Strategies; Patrolling Your Neighborhood; Leveraging Threat Intelligence; Incident Response

**DAY 6: Advanced Persistent Threat Defender Capstone**

The course culminates in a team-based Defend-the-Flag competition. Day six provides a full day of hands-on work applying the principles taught throughout the week. Your team will progress through multiple levels and missions designed to ensure mastery of the modern cybersecurity controls studied all week long. This challenging exercise will reinforce key principles in a fun, hands-on, team-based challenge.

**Topics:** Applying Previously Covered Security Controls In-depth, Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, Action on Objectives

---

**Who Should Attend**

- Security architects
- Security engineers
- Technical security managers
- Security Operations Center analysts, engineers, and managers
- IT administrators
- Penetration testers who want to better understand how defensive controls work
- IT administrators
- Individuals looking to better understand how persistent cyber adversaries operate and how the IT environment can be improved to better prevent, detect, and respond to incidents

---

“The course handles a lot of important aspects (of the entire Kill Chain). It gives good insight into potential attacks and mitigation.”

—Kevin Giesekam, Dutch Police
Job-Specific, Specialized Focus

Today’s cyber attacks are highly sophisticated and exploit specific vulnerabilities. Broad and general InfoSec certifications are no longer enough. Professionals need the specific skills and specialized knowledge required to meet multiple and varied threats. That’s why GIAC has more than 30 certifications, each focused on specific job skills and each requiring unmatched and distinct knowledge.

Deep, Real-World Knowledge

Theoretical knowledge is the ultimate security risk. Deep, real-world knowledge and hands-on skills are the only reliable means to reduce security risk. Nothing comes close to a GIAC certification to ensure that this level of real-world knowledge and skill has been mastered.

Most Trusted Certification Design

The design of a certification exam impacts the quality and integrity of a certification. GIAC exam content and question design are developed through a rigorous process led by GIAC’s on-staff psychometrician and reviewed by experts in each area. More than 78,000 certifications have been issued since 1999. GIAC certifications meet ANSI standards.

“GIAC made the testing process much better than other organizations. The material is spot on with what I do at work, daily.”
– Jason Pfister, EWEB, GIAC Continuous Monitoring (GMON)

“I think the exam was both fair and practical. These are the kind of real-world problems I expect to see in the field.”
– Carl Hallberg, Wells Fargo, GIAC Reverse Engineering Malware (GREM)
Experience NetWars at SANSFIRE 2019
Thu, June 20 & Fri, June 21

Play solo or on a team of up to five players

“NetWars takes the concepts in the class and gives you an opportunity to put them into action. Highly recommended!”
— Kyle McDaniel, Lenovo

Choose from:
Core NetWars | DFIR NetWars | Cyber Defense NetWars

Develop skills in:
• Cyber Defense
• Penetration Testing
• Digital Forensics & Incident Response

Participation in NetWars is free for students taking 4-, 5-, or 6-day courses.
NetWars takes place in the evening, after class, and gives you an immediate opportunity to apply what you’ve learned in a fun, competitive, hands-on, and educational environment!
Seating is limited, so add NetWars when you register for your course.
SEC460: Enterprise Threat and Vulnerability Assessment

You Will Be Able To

- Perform end-to-end vulnerability assessments
- Develop customized vulnerability discovery, management, and remediation plans
- Conduct threat intelligence gathering and analysis to create a tailored cybersecurity plan that integrates various attack and vulnerability modeling frameworks
- Implement a proven testing methodology using industry-leading tactics and techniques
- Adapt information security approaches to target real-world enterprise challenges
- Configure and manage vulnerability assessment tools to limit risk added to the environment by the tester
- Operate enumeration tools like Nmap, Masscan, Recon-ng, and WMI to identify network nodes, services, configurations, and vulnerabilities that an attacker could use as an opportunity for exploitation
- Conduct infrastructure vulnerability enumeration at scale across numerous network segments, in spite of divergent network infrastructure and nonstandard configurations
- Conduct web application vulnerability enumeration in enterprise environments while solving complex challenges resulting from scale
- Perform manual discovery and validation of cybersecurity vulnerabilities that can be extended to custom and unique applications and systems
- Manage large vulnerability datasets and perform risk calculation and scoring against organization-specific risks
- Implement vulnerability triage and prioritize mitigation

Matthew Toussain
SANS Certified Instructor

Computer exploitation is on the rise. As advanced adversaries become more numerous, more capable, and much more destructive, organizations must become more effective at mitigating their information security risks at the enterprise scale. SEC460 is the premier course focused on building technical vulnerability assessment skills and techniques, while highlighting time-tested practical approaches to ensure true value across the enterprise. The course covers threat management, introduces the core components of comprehensive vulnerability assessment, and provides the hands-on instruction necessary to produce a vigorous defensive strategy from day one. The course is focused on equipping information security personnel from mid-sized to large organizations charged with effectively and efficiently securing 10,000 or more systems.

SEC460 begins with an introduction to information security vulnerability assessment fundamentals, followed by in-depth coverage of the Vulnerability Assessment Framework. It then moves into the structural components of a dynamic and iterative information security program. Through a detailed, practical analysis of threat intelligence, modeling, and automation, students will learn the skills necessary to not only use the tools of the trade, but also to implement a transformational security vulnerability assessment program.

SEC460 will teach you how to use real industry-standard security tools for vulnerability assessment, management, and mitigation. It is the only course that teaches a holistic vulnerability assessment methodology while focusing on challenges faced in a large enterprise. You will learn on a full-scale enterprise range chock full of target machines representative of an enterprise environment, leveraging production-ready tools and a proven testing methodology.

SEC460 takes you beyond the checklist, giving you a tour of the attackers’ perspective that is crucial to discovering where they will strike. Operators are more than the scanner they employ. SEC460 emphasizes this personnel-centric approach by examining the shortfalls of many vulnerability assessment programs in order to provide you with the tactics and techniques required to secure networks against even the most advanced intrusions.

We wrap up the first five days of instruction with a discussion of triage, remediation, and reporting before putting your skills to the test on the final day against an enterprise-grade cyber range with numerous target systems for you to analyze and explore. The cyber range is a large environment of servers, end-users, and networking gear that represents many of the systems and topologies used by enterprises. By adopting an end-to-end approach to vulnerability assessment, you can be confident that your skills will provide much-needed value in securing your organization.

“SEC460 has provided me the knowledge to build a great Vulnerability Management/Vulnerability Assessment Program that vendor courses couldn’t provide.”

-Eric Osmus, ConocoPhillips Company

Matthew Toussain is the founder of Open Security and a penetration tester with Black Hills Information Security. As an avid information security researcher, Matthew regularly hunts for vulnerabilities in computer systems and releases tools to demonstrate the effectiveness of attacks and countermeasures. He has been a guest speaker at many conference venues, including DEFCON, the largest security conference in the world. Matthew is an author of SEC460: Enterprise Threat and Vulnerability Assessment. After graduating from the U.S. Air Force Academy, where he architected and instructed the summer cyber course that now trains over 400 cadets per year, Matthew served as the Senior Cyber Tactics Development Lead for the U.S. Air Force. He directed the teams responsible for developing innovative tactics, techniques, and procedures for offensive operations as well as for cyber protection teams (CPT). Later, as a member of the 688th Cyber Warfare Wing he managed the Air Force’s transition of all 18 CPTS to fully operational capability. He earned his master’s degree in information security engineering as one of the first graduates of the SANS Technology Institute and supports many national and international cyber competitions including the CCDC, Netwars, and the National Security Agency’s Cyber Defense Exercise as a red team member and instructor.

@0sm0s1z
DAY 1: Methodology, Planning, and Threat Modeling
In this section of the course, students will develop the skills needed to conduct high-value vulnerability assessments with measurable impact. We will explore the elemental components of successful vulnerability assessment programs, deconstruct the logistical prerequisites to value-added operations, and integrate adversarial threat modeling and intelligence.

Topics: Maximizing Value from Vulnerability Assessments and Programs; Setting Up for Success at Scale: Enterprise Architecture and Strategy; Developing Transformational Vulnerability Assessment Strategies; Performing Enterprise Threat Modeling; Generating Compounding Interest from Threat Intelligence and Avoiding Information Overload; The Vulnerability Assessment Framework; Overview of Comprehensive Network Scanning; Compliance Standards and Information Security

DAY 2: Discovery
Having mastered the structural foundations of vulnerability management, we pivot to the realm of direct, tactical application. Comprehensive reconnaissance, enumeration, and discovery techniques are the prime elements of successful vulnerability assessment. While gaining additional familiarity with hands-on enterprise operations, you will systematically probe the environment in order to discover the relevant host, service, version, and configuration details that will drive the remainder of the assessment system.

Topics: Active and Passive Reconnaissance; Identification and Enumeration with DNS, DNS Zone Speculation and Diction-Enabled Discovery; Port Scanning with Nmap and Zenmap; Scanning Large-Scale Environments; Commonplace Services; Scanning the Network Perimeter and Engaging the DMZ; The Windows Domain: Exchange, SharePoint, and Active Directory; Recruiting Disparate Data Sources. Patches, Hotfixes, and Configurations; Trade-offs: Speed, Efficiency, Accuracy, and Thoroughness; Introduction to PowerShell

DAY 3: Enhanced Vulnerability Scanning and Automation
We begin day three by delving into the next phase of the Vulnerability Assessment Framework and charging into the most exciting topic in security testing: automation to handle scale. We start by breaking vulnerability scanning into its elemental components and gaining an understanding of vulnerability measurement that can be applied to task automation. This focus will direct us to the quantitative facets underlying cybersecurity vulnerabilities and drive our discussion of impact, risk, and triage. Each topic discussed will focus on identifying, observing, inciting, or assessing the entry points that threats leverage during network attacks. Later in the day, we will apply our understanding of the vulnerability concept to evolve our PowerShell skills and take action on an enterprise scale.

Topics: Enhanced Vulnerability Scanning; Risk Assessment Matrices and Rating Systems; Quantitative Analysis Techniques Applied to Vulnerability Scoring; Performing Tailored Risk Calculation to Drive Triage; General Purpose vs. Application Specific Vulnerability Scanning; Tuning the Scanner to the Task, the Enterprise, and Tremendous Scale; Scan Policies and Compliance Auditing; Performing Vulnerability Discovery with Open-Source and Commercial Appliances; Nmap Scripting Engine and OpenVAS; Testing for Insecure Cryptographic Implementations Including SSL; Assessing VQIP Environments; Discovering Vulnerabilities in the Enterprise Backbone: Active Directory, Exchange, and SharePoint; Evaluating Vulnerability Risk in Custom and Unique Systems including Web Applications; Minimizing Supplemental Risk while Conducting Authenticated Scanning through Purposeful Application of Least Privilege; Probing for Data Link Liability to Identify Hazards in Wireless Infrastructure, Switches, and VLANs; Manual Vulnerability Discovery Automated to Attain Maximal Efficacy

DAY 4: Vulnerability Validation, Triage, and Data Management
Over the course of this day we will tackle the next phase of our overarching testing methodology, vulnerability validation, while simultaneously confronting the biggest headaches common to a vulnerability assessment at scale. At large scale, vulnerability data can be overwhelming and possibly even contradictory. We will cover the specific techniques needed to wade through and better focus those data. Next, we will examine techniques for collaboration and data management with the Acheron tool for analyzing vulnerability data across an organization.

Topics: Recruiting Disparate Data Sources: Patches, Hotfixes, and Configurations; Manual Vulnerability Validation Targeting Enterprise Infrastructure; Converting Disparate Datasets into a Central, Normalized, and Relational Knowledge Base; Managing Large Repositories of Vulnerability Data; Querying the Vulnerability Knowledge Base; Evaluating Vulnerability Risk in Custom and Unique Systems, including Web Applications; Triage: Assessing the Relative Importance of Vulnerabilities Against Strategic Risk

DAY 5: Remediation and Reporting
Many well-intentioned vulnerability assessment programs begin with zeal and vitality, but after the discovery of vulnerabilities there is often a tendency to ignore the risk reality and shift back to the status quo. Over the previous course modules we focused on knowing the target environment and uncovering its weak points. Now it’s time for decision and action based on an understanding of the risks the organization faces. Developing an actionable vulnerability remediation plan with time-based success targets sets the stage for continuous improvement, and that's exactly what we cover in this section of the course. Developing this plan in conjunction with the Vulnerability Assessment Report is an opportunity to galvanize the team, while enhancing the vulnerability assessment value proposition.

Topics: Team Operations and Collaboration; Security Operations Project Management Essentials; Transforming Triage Listing into the Vulnerability Remediation Plan; Developing the Cybersecurity Risk Sight Picture; Connecting Related Datasets and Framing the Narrative; Developing a Network and Host Affiliations, Modeling Account Relationships on Active Directory Forests, Creating Effective Vulnerability Assessment Reports; Curbing the Vulnerability Lifecycle and Aspiring to Zero Hour; Closure: Be a Positive Influence in the Context of the Global Information Security Crisis

DAY 6: Vulnerability Assessment Foundry Hands-on Challenge
In celebration of your diligence, curiosity, and mad new vulnerability skills, we welcome you to your final hands-on challenge to hammer home your capabilities. The guided scenario on this final course day is designed to test your mettle through trial and detailed work in a fun Capture-the-Flag-style environment. The challenge is the canvas upon which you can hone your skills and measure your maturing talents. Armed for the fight, you will doubtless rise to the challenge...and triumph! The scenario: An organization called “The Foundry” has engaged you to perform a vulnerability assessment of its environment. The organization is very aware of your particular set of vulnerability assessment skills, and treasures the insights it is certain you will provide to help secure the organization against its formidable adversaries, including nefarious cybercrime cartels and jealous nation-state actors. Teams will work together to help squash issues that would lead to a compromise of The Foundry’s precious assets.

Topics: Tactical Employment of the Vulnerability Assessment Framework, Threat Modeling, Discovery, Vulnerability Scanning, Validation, Data Management and Triage
You Will Be Able To

- Apply a detailed, four-step methodology to your web application penetration tests: reconnaissance, mapping, discovery, and exploitation
- Analyze the results from automated web testing tools to validate findings, determine their business impact, and eliminate false positives
- Manually discover key web application flaws
- Use Python to create testing and exploitation scripts during a penetration test
- Discover and exploit SQL injection flaws to determine true risk to the victim organization
- Create configurations and test payloads within other web attacks
- Fuzz potential inputs for injection attacks
- Explain the impact of exploitation of web application flaws
- Analyze traffic between the client and the server application using tools such as the Zed Attack Proxy and Burp Suite to find security issues within the client-side application code
- Manually discover and exploit Cross-Site Request Forgery (CSRF) attacks
- Use the Browser Exploitation Framework (BeEF) to hook victim browsers, attack client software and the network, and evaluate the potential impact that XSS flaws have within an application
- Perform a complete web penetration test during the Capture-the-Flag exercise to bring techniques and tools together into a comprehensive test

SEC542: Web App Penetration Testing and Ethical Hacking

Web applications play a vital role in every modern organization. However, if your organization doesn’t properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

SEC542 helps students move beyond push-button scanning to professional, thorough, and high-value web application penetration testing.

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organization. Unfortunately, there is no “patch Tuesday” for custom web applications, and major industry studies find that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but effective web application penetration testing requires something deeper.

SEC542 enables students to assess a web application’s security posture and convincingly demonstrate the impact of inadequate security that plagues most organizations.

In this course, students will come to understand major web application flaws and their exploitation. Most importantly, they’ll learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organizations. Even technically gifted security geeks often struggle with helping organizations understand risk in terms relatable to business. Much of the art of penetration testing has less to do with learning how adversaries are breaking in than it does with convincing an organization to take the risk seriously and employ appropriate countermeasures. The goal of SEC542 is to better secure organizations through penetration testing, and not just show off hacking skills. This course will help you demonstrate the true impact of web application flaws through exploitation.

In addition to high-quality course content, SEC542 focuses heavily on in-depth, hands-on labs to ensure that students can immediately apply all they learn.

In addition to having more than 30 formal hands-on labs, the course culminates in a web application pen test tournament, powered by the SANS NetWars Cyber Range. This Capture-the-Flag event on the final day brings students into teams to apply their newly acquired command of web application penetration testing techniques in a fun way that hammers home lessons learned.

Moses Frost is a seasoned security professional with over 15 years in the IT industry. He has held positions as a network engineer, network architect, security architect, platform engineer, site reliability engineer, and consulting sales engineer. He has a background in complex network systems, systems administration, forensics, penetration testing, and development. He has worked with some of the largest companies in the nation as well as fast-growing, bootstrap startups. Moses has developed information security regimens safeguarding some of the most sensitive personal data in the nation. He creates custom security software to find and mitigate unknown threats, and works on continually evolving his penetration testing skills. He enjoys building software, networks, systems, and working with business-minded individuals. Moses’s current passions include offensive forensics, building secure systems, finance, economics, history, and music.

@mosesrenegade
DAY 1: Introduction and Information Gathering
Understanding the attacker’s perspective is key to successful web application penetration testing. The course begins by thoroughly examining web technology, including protocols, languages, clients and server architectures, from the attacker’s perspective. We will also examine different authentication systems, including Basic, Digest, Forms and Windows Integrated authentication, and discuss how servers use them and attackers abuse them.

Topics: Overview of the Web from a Penetration Tester’s Perspective; Exploring the Various Servers and Clients; Discussion of the Various Web Architectures; Discovering How Session State Works; Discussion of the Different Types of Vulnerabilities; Defining a Web Application Test Scope and Process; Defining Types of Penetration Testing; Heartbleed Exploitation; Utilizing the Burp Suite in Web App Penetration Testing

DAY 2: Configuration, Identity, and Authentication Testing
The second day starts the actual penetration testing process, beginning with the reconnaissance and mapping phases. Reconnaissance includes gathering publicly available information regarding the target application and organization, identifying the machines that support our target application, and building a profile of each server, including the operating system, specific software and configuration. The discussion is underscored through several practical, hands-on labs in which we conduct reconnaissance against in-class targets.

Topics: Discovering the Infrastructure Within the Application; Identifying the Machines and Operating Systems; Secure Sockets Layer (SSL) Configurations and Weaknesses; Exploring Virtual Hosting and Its Impact on Testing; Learning Methods to Identify Load Balancers; Software Configuration Discovery; Exploring External Information Sources; Learning Tools to Spider a Website; Scripting to Automate Web Requests and Spidering; Brute Forcing Unlinked Files and Directories; Discovering and Exploiting Shellshock

DAY 3: Injection
This section continues to explore our methodology with the discovery phase. We will build on the information started the previous day, exploring methods to find and verify vulnerabilities within the application. Students will also begin to explore the interactions between the various vulnerabilities.

Topics: Python for Web App Penetration Testing; Web App Vulnerabilities and Manual Verification Techniques; Reflection: Proxies, Zed Attack Proxy (ZAP), Burp Suite; Information Leakage and Directory Browsing; Username Harvesting; Command Injection; Directory Traversal; SQL Injection, Blind SQL Injection, Local File Inclusion (LFI), Remote-File Inclusion (RFI); JavaScript for the Attacker

DAY 4: XXE and XSS
On day four, students continue exploring the discovery phase of the methodology. We cover methods to discover key vulnerabilities within web applications, such as Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF/XSRF). Manual discovery methods are employed during hands-on labs.

Topics: XML External Entity (XXE); Cross-Site Scripting (XSS); Browser Exploitation Framework (BeEF); AJAX, XML and JSON; Document Object Model (DOM); Logic Attacks; API Attacks; Data Attacks

DAY 5: CSRF, Logic Flaws, and Advanced Tools
On the fifth day, we launch actual exploits against real-world applications, building on the previous three steps, expanding our foothold within the application, and extending it to the network on which it resides. As penetration testers, we specifically focus on ways to leverage previously discovered vulnerabilities to gain further access, highlighting the cyclical nature of the four-step attack methodology.

Topics: Metasploit for Web Penetration Testing; The sqlmap Tool; Exploring Methods to Zombify Browsers; Browser Exploitation Framework (BeEF); Walking Through an Entire Attack Scenario; Leveraging Attacks to Gain Access to the System; How to Pivot Our Attacks Through a Web Application; Understanding Methods of Interacting with a Server Through SQL Injection; Exploiting Applications to Steal Cookies; Executing Commands Through Web Application Vulnerabilities

DAY 6: Capture-the-Flag Challenge
On day six, students form teams and compete in a web application penetration testing tournament. This NetWars-powered Capture-the-Flag Challenge provides students an opportunity to wield their newly developed or further-honed skills to answer questions, complete missions, and exfiltrate data, applying skills gained throughout the course. The style of challenge and integrated-hint system allows students of various skill levels to both enjoy a game environment and solidify the skills learned in class.

Who Should Attend
- General security practitioners
- Penetration testers
- Ethical hackers
- Web application developers
- Website designers and architects

“SEC542 shows a hands-on way of doing web app penetration testing – not just how to use this tool or that tool.”
-Christopher J. Stover, Infogressive Inc.
SEC560: Network Penetration Testing and Ethical Hacking

You Will Be Able To

- Develop tailored scoping and rules of engagement for penetration testing projects to ensure the work is focused, well defined, and conducted in a safe manner.
- Conduct detailed reconnaissance using document metadata, search engines, and other publicly available information sources to build a technical and organizational understanding of the target environment.
- Utilize a scanning tool such as Nmap to conduct comprehensive network sweeps, port scans, OS fingerprinting, and version scanning to develop a map of target environments.
- Choose and properly execute Nmap Scripting Engine scripts to extract detailed information from target systems.
- Configure and launch a vulnerability scanner such as Nessus so that it safely discovers vulnerabilities through both authenticated and unauthenticated scans, and customize the output from such tools to represent the business risk to the organization.
- Analyze the output of scanning tools to eliminate false positive reduction with tools including Netcat and Scapy.
- Utilize the Windows PowerShell and Linux bash command lines during post-exploitation to plunder target systems for vital information that can further overall penetration test progress, establish pivots for deeper compromise, and help determine business risks.
- Configure an exploitation tool such as Metasploit to scan, exploit, and then pivot through a target environment.

As a cybersecurity professional, you have a unique responsibility to find and understand your organization’s vulnerabilities, and to work diligently to mitigate them before the bad guys pounce. Are you ready? SANS SEC560, our flagship course for penetration testing, fully arms you to address this task head-on.

SEC560 IS THE MUST-HAVE COURSE FOR EVERY WELL-ROUNDED SECURITY PROFESSIONAL

With comprehensive coverage of tools, techniques, and methodologies for network penetration testing, SEC560 truly prepares you to conduct high-value penetration testing projects step by step and end to end. Every organization needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specially designed to get you ready for that role. The course starts with proper planning, scouting and recon, then dives deep into scanning, target exploitation, password attacks, and web app manipulation, with over 30 detailed hands-on labs throughout. The course is chock full of practical, real-world tips from some of the world’s best penetration testers to help you do your job safely, efficiently, and with great skill.

LEARN THE BEST WAYS TO TEST YOUR OWN SYSTEMS BEFORE THE BAD GUYS ATTACK

You’ll learn how to perform detailed reconnaissance, studying a target’s infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won’t just cover run-of-the-mill options and configurations, we’ll also go over the lesser-known but super-useful capabilities of the best pen test toolsets available today. After scanning, you’ll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You’ll dive deep into post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth.

EQUIPPING SECURITY ORGANIZATIONS WITH COMPREHENSIVE PENETRATION TESTING AND ETHICAL HACKING KNOW-HOW

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test and at the end of the course you’ll do just that. After building your skills in comprehensive and challenging labs, the course culminates with a final real-world penetration test scenario. You’ll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization, demonstrating the skills you’ve gained in this course.

“SEC560 provides practical, how-to material that I can use daily in my penetration testing activities – not only technically, but also from a business perspective.”

-Steve Nolan, General Dynamics

Ed Skoudis is the founder of Counter Hack, an innovative organization that designs, builds, and operates popular InfoSec challenges and simulations including CyberCity, NetWars, Cyber Quests, and Cyber Foundations. As director of the CyberCity project, Ed oversees the development of missions that help train cyber warriors to defend the kinetic assets of a physical, miniaturized city. Ed’s expertise includes hacker attacks and defenses, incident response, and malware analysis, with over 15 years of experience in information security. Ed authored and regularly teaches the SANS courses on network penetration testing (SEC560) and incident response (SEC504), helping over 3,000 information security professionals each year improve their skills and abilities to defend their networks. He has performed numerous security assessments; conducted exhaustive anti-virus, anti-spyware, Virtual Machine, and IPS research; and responded to computer attacks for clients in government, military, financial, high technology, healthcare, and other industries. Previously, Ed served as a security consultant with InGuardians, International Network Services (INS), Global Integrity, Predictive Systems, SAIC, and Bell Communications Research (Bellcore). Ed also blogs about command line tips and penetration testing. @edskoudis
Course Day Descriptions

**Day 1: Comprehensive Pen Test Planning, Scoping, and Recon**

In this course section, you’ll develop the skills needed to conduct a best-of-breed, high-value penetration test. We’ll go in-depth on how to build a penetration testing infrastructure that includes all the hardware, software, network infrastructure, and tools you will need to conduct great penetration tests, with specific low-cost recommendations for your arsenal. We’ll then cover formulating a pen test scope and rules of engagement that will set you up for success, including a role-play exercise. We’ll also dig deep into the reconnaissance portion of a penetration test, covering the latest tools and techniques, including hands-on document metadata analysis to pull sensitive information about a target environment, as well as a lab using Recon-ng to plunder a target’s DNS infrastructure for information such as which anti-virus tools the target organization uses.

**Topics:** The Mindset of the Professional Pen Tester; Building a World-Class Pen Test Infrastructure; Creating Effective Pen Test Scopes and Rules of Engagement; Detailed Recon Using the Latest Tools; Effective Pen Test Reporting to Maximize Impact; Mining Search Engine Results; Document Metadata Extraction and Analysis; Interrogating DNS for Juicy Information

**Day 2: In-Depth Scanning**

This course section focuses on the vital task of mapping the target environment’s attack surface by creating a comprehensive inventory of machines, accounts, and potential vulnerabilities. We look at some of the most useful scanning tools freely available today and run them in numerous hands-on labs to help hammer home the most effective way to use each tool. We also conduct a deep dive into some of the most useful tools available to pen testers today for formulating packets: Scapy and Netcat. We finish the module covering vital techniques for false-positive reduction, so you can focus your findings on meaningful results and avoid the sting of a false positive. And we examine the best ways to conduct your scans safely and efficiently.

**Topics:** Tips for Awesome Scanning; Tcpdump for the Pen Tester; Nmap In-Depth: The Nmap Scripting Engine; Version Scanning with Nmap, Vulnerability Scanning with Nessus, False-Positive Reduction; Packet Manipulation with Scapy, Enumerating Users; Nmap, Netcat for the Pen Tester; Monitoring Services during a Scan

**Day 3: Exploitation**

In this section, we look at the many kinds of exploits that penetration testers use to compromise target machines, including client-side exploits, service-side exploits, and local privilege escalation. We’ll see how these exploits are packaged in frameworks like Metasploit and its mighty Meterpreter. You’ll learn in-depth how to leverage Metasploit and the Meterpreter to compromise target environments. We’ll also analyze the topic of anti-virus evasion to bypass the target organization’s security measures, as well as methods for pivoting through target environments, all with a focus on determining the true business risk of the target organization.

**Topics:** Comprehensive Metasploit Coverage with Exploits, Stagers, and Stages; Strategies and Tactics for Anti-Virus Evasion; In-Depth Meterpreter Analysis, Hands-On; Implementing Port Forwarding Relays for Merciless Pivots; How to Leverage PowerShell Empire to Plunder a Target Environment

**Day 4: Post-Exploitation and Merciless Pivoting**

Once you’ve successfully exploited a target environment, penetration testing gets extra exciting as you perform post-exploitation, gathering information from compromised machines and pivoting to other systems in your scope. This course section zooms in on pillaging target environments and building formidable hands-on command line skills. We’ll cover Windows command line skills in-depth, including PowerShell’s awesome abilities for post-exploitation. We’ll see how we can leverage malicious services and the incredible WMI toolset to access and pivot through a target organization. We’ll then turn our attention to password guessing attacks, discussing how to avoid account lockout, as well as numerous options for plundering password hashes from target machines including the great Mimikatz Kiwi tool. Finally, we’ll look at Metasploit’s fantastic features for pivoting, including the msfconsole route command. We’ll see how we can leverage malicious services and the incredible WMI toolset to access and pivot through a target organization. We’ll then turn our attention to password guessing attacks, discussing how to avoid account lockout, as well as numerous options for plundering password hashes from target machines including the great Mimikatz Kiwi tool.

**Topics:** Windows Command Line Kung Fu for Penetration Testers; PowerShell’s Amazing Post-Exploitation Capabilities; Password Attack Tips; Account Lockout and Strategies for Avoiding It; Automated Password Guessing with THC-Hydra; Retrieving and Manipulating Hashes from Windows, Linux, and Other Systems; Pivoting through Target Environments; Extracting Hashes and Passwords from Memory with Mimikatz Kiwi

**Day 5: In-Depth Password Attacks and Web App Pen Testing**

In this course section, we’ll go even deeper in exploiting one of the weakest aspects of most computing environments: passwords. You’ll custom-compile John the Ripper to optimize its performance in cracking passwords. You’ll look at the amazingly full-featured Cain tool, running it to crack sniffed Windows authentication messages. We’ll use the incredible Hashcat tool for increased speed in cracking passwords, all hands-on. And we’ll cover powerful “pass-the-hash” attacks, leveraging Metasploit, the Meterpreter, and more. We then turn our attention to web application pen testing, covering the most powerful and common web app attack techniques, with hands-on labs for every topic we address. We’ll cover finding and exploiting cross-site scripting (XSS), cross-site request forgery (XSRF), command injection, and SQL injection flaws in applications such as online banking, blog sites, and more.

**Topics:** Password Cracking with John the Ripper; Sniffing and Cracking Windows Authentication Exchanges Using Cain; Using Hashcat for Maximum Effectiveness; Pass-the-Hash Attacks with Metasploit and More; Finding and Exploiting Cross-Site Scripting; Utilizing Cross-Site Request Forgery Flaws; Data Plundering with SQL Injection; Leveraging SQL Injection to Perform Command Injection; Maximizing Effectiveness of Command Injection Testing

**Day 6: Penetration Test and Capture-the-Flag Challenge**

This lively session represents the culmination of the network penetration testing and ethical hacking course. You’ll apply all of the skills mastered in the course in a comprehensive, hands-on workshop during which you’ll conduct an actual penetration test of a sample target environment. We’ll provide the scope and rules of engagement, and you’ll work to achieve your goal of finding out whether the target organization’s Personally Identifiable Information (PII) is at risk. As a final step in preparing you for conducting penetration tests, you’ll make recommendations about remediating the risks you identify.

**Topics:** Applying Penetration Testing and Ethical Hacking Practices End-to-End; Detailed Scanning to Find Vulnerabilities and Avenues to Entry, Exploitation to Gain Control of Target Systems, Post-Exploitation to Determine Business Risk; Merciless Pivoting; Analyzing Results to Understand Business Risk and Devise Corrective Actions

Who Should Attend

- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Defenders who want to better understand offensive methodologies, tools, and techniques
- Auditors who need to build deeper technical skills
- Red and blue team members
- Forensics specialists who want to better understand offensive tactics

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/sansfire/courses](http://www.sans.org/sansfire/courses)
Python is a simple, user-friendly language that is designed to make automating the tasks that security professionals perform quick and easy. Whether you are new to coding or have been coding for years, SANS SEC573: Automating Information Security with Python will have you creating programs that make your job easier and your work more efficient. This self-paced course starts from the very beginning, assuming you have no prior experience or knowledge of programming. We cover all of the essentials of the language up front. If you already know the essentials, you will find that the pyWars lab environment allows advanced developers to quickly accelerate to more advanced material in the course.

All security professionals, including Penetration Testers, Forensics Analysts, Network Defenders, Security Administrators, and Incident Responders, have one thing in common: CHANGE. Change is constant. Technology, threats, and tools are constantly evolving. If we don’t evolve with them, we’ll become ineffective and irrelevant, unable to provide the vital defenses our organizations increasingly require.

Maybe your chosen Operating System has a new feature that creates interesting forensics artifacts that would be invaluable for your investigation, if only you had a tool to access it. Often for new features and forensics artifacts, no such tool has yet been released. You could try moving your case forward without that evidence or hope that someone creates a tool before the case goes cold...or you can write a tool yourself.

Or perhaps an attacker bypassed your defenses and owned your network months ago. If existing tools were able to find the attack, you wouldn’t be in this situation. You are bleeding sensitive data and the time-consuming manual process of finding and eradicating the attacker is costing you money and hurting your organization big time. The answer is simple if you have the skills: Write a tool to automate your defenses.

Or, as a penetration tester, you need to evolve as quickly as the threats you are paid to emulate. What do you do when “off-the-shelf” tools and exploits fall short? If you’re good, you write your own tool.

SEC573 is designed to give you the skills you need for tweaking, customizing, or outright developing your own tools. We put you on the path of creating your own tools, empowering you to better automate the daily routine of today’s information security professional and to achieve more value in less time. Again and again, organizations serious about security emphasize their need for skilled tool builders. There is a huge demand for people who can understand a problem and then rapidly develop prototype code to attack or defend against it. Join us and learn Python in-depth and fully weaponized.

---

**You Will Be Able To**

- Modify existing open-source tools to customize them to meet the needs of your organization
- Manipulate log file formats to make them compatible with various log collectors
- Write new tools to analyze log files and network packets to identify attackers in your environment
- Develop tools that extract otherwise inaccessible forensics artifacts from computer systems of all types
- Automate the collection of intelligence information to augment your security from online resources
- Automate the extraction of signs of compromise and other forensics data from the Windows Registry and other databases
- Write a backdoor that uses exception handling, sockets, process execution, and encryption to provide you with your initial foothold in a target environment. The backdoor will include features such as a port scanner to find an open outbound port, techniques for evading antivirus software and network monitoring, and the ability to embed payload from tools such as Metasploit.

---

Mark Baggett
SANS Senior Instructor

Mark Baggett is the owner of Indepth Defense, an independent consulting firm that offers incident response and penetration testing services. Mark has more than 28 years of commercial and government experience ranging from software developer to chief information security officer. He is the author of the SEC573: Automating Information Security with Python course. Mark has a master’s degree in information security engineering and many industry certifications, including being the 15th person in the world to receive the prestigious GIAC Security Expert certification (GSE). Mark is very active in the information security community. He is the founding president of The Greater Augusta ISSA (Information Systems Security Association) chapter, which has been extremely successful in bringing networking and educational opportunities to Augusta Information Technology workers. Since January 2011, Mark has served as the SANS Technical Advisor to the DoD, where he assists various entities in the development of information security capabilities.

@MarkBaggett
Course Day Descriptions

**DAY 1: Essentials Workshop with pyWars**
The course begins with a brief introduction to Python and the pyWars Capture-the-Flag game. We set the stage for students to learn at their own pace in the 100% hands-on pyWars lab environment. As more advanced students take on Python-based Capture-the-Flag challenges, students who are new to programming will start from the very beginning with Python essentials.

**Topics:** Syntax; Variables; Math Operators; Strings; Functions; Modules; Control Statements; Introspection

**DAY 2: Essentials Workshop with MORE pyWars**
You will never learn to program by staring at PowerPoint slides. The second day continues the hands-on, lab-centric approach established on day one. This section covers data structures and more detailed programming concepts. Next, we focus on invaluable tips and tricks to make you a better Python programmer and on how to debug your code.

**Topics:** Lists; Loops; Tuples; Dictionaries; The Python Debugger; Coding Tips, Tricks, and Shortcuts; System Arguments; ArgParser Module

**DAY 3: Defensive Python**
In this section we take on the role of a network defender with more logs to examine than there is time in the day. Attackers have penetrated the network and you will have to analyze the logs and packet captures to find them. We will discuss how to analyze network logs and packets to discover where the attackers are coming from and what they are doing. We will build scripts to empower continuous monitoring and disrupt the attackers before they exfiltrate your data. Forensicators and offensive security professionals won’t be left out because reading and writing files and parsing data are also important skills that will apply to their craft.

**Topics:** File Operations; Python Sets; Regular Expressions; Log Parsing; Data Analysis Tools and Techniques; Long Tail/Short Tail Analysis; Geolocation Acquisition; Blacklists and Whitelists; Packet Analysis; Packet Reassembly; Payload Extraction

**DAY 4: Forensics Python**
On day four we will play the role of a forensics analyst who has to carve evidence from artifacts when no tool exists to do so. Even if you don’t do forensics you will find that these skills covered on day four are foundational to every security role. We will discuss the process required to carve binary images, find appropriate data of interest in them, and extract those data. Once you have the artifact isolated, there is more analysis to be done. You will learn how to extract metadata from image files. Then we will discuss techniques for finding artifacts in other locations such as SQL databases and interacting with web pages.

**Topics:** Acquiring Images from Disk, Memory, and the Network; File Carving; The STRUCT Module; Raw Network Sockets and Protocols; Image Forensics and PII; SQL Queries; HTTP Communications with Python Built-In Libraries; Web Communications with the Requests Module

**DAY 5: Offensive Python**
On day five we play the role of penetration testers whose normal tricks have failed. Their attempts to establish a foothold have been stopped by modern defenses. To bypass these defenses, you will build an agent to give you access to a remote system. Similar agents can be used for incident response or systems administration, but our focus will be on offensive operations.

**Topics:** Network Socket Operations; Exception Handling; Process Execution; Blocking and Non-blocking Sockets; Asynchronous Operations; The Select Module; Python Objects; Argument Packing and Unpacking

**DAY 6: Capture-the-Flag Challenge**
In this final section, you will be placed on a team with other students. You will apply the skills you have mastered in a series of programming challenges. Participants will exercise the new skills and the code they have developed throughout the course in a series of challenges. You will solve programming challenges, exploit vulnerable systems, analyze packets, parse logs, and automate code execution on remote systems. Test your skills! Prove your might!

“SEC573 is excellent. I went from having almost no Python coding ability to being able to write functional and useful programs.”

- Caleb Jaren, Microsoft
Imagine an attack surface that is spread across your organization and in the hands of every user. It moves from place to place regularly, stores highly sensitive and critical data, and sports numerous different wireless technologies all ripe for attack. Such a surface already exists today: mobile devices. These devices are the biggest attack surface in most organizations, yet these same organizations often don’t have the skills needed to assess them.

SEC575 NOW COVERS ANDROID PIE AND iOS 12

SEC575: Mobile Device Security and Ethical Hacking is designed to give you the skills you need to understand the security strengths and weaknesses in Apple iOS and Android devices. Mobile devices are no longer a convenience technology; they are an essential tool carried or worn by users worldwide, often displacing conventional computers for everyday enterprise data needs. You can see this trend in corporations, hospitals, banks, schools, and retail stores throughout the world. Users rely on mobile devices more today than ever before – we know it, and the bad guys do too. The SEC575 course examines the full gamut of these devices.

LEARN HOW TO PEN TEST THE BIGGEST ATTACK SURFACE IN YOUR ENTIRE ORGANIZATION

With the skills you learn in SEC575, you will be able to evaluate the security weaknesses of built-in and third-party applications. You’ll learn how to bypass platform encryption and how to manipulate apps to circumvent client-side security techniques. You’ll leverage automated and manual mobile application analysis tools to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels. You’ll safely work with mobile malware samples to understand the data exposure and access threats affecting Android and iOS, and you’ll bypass lock screen to exploit lost or stolen devices.

TAKE A DEEP DIVE INTO EVALUATING MOBILE APPS, OPERATING SYSTEMS, AND THEIR ASSOCIATED INFRASTRUCTURES

Understanding and identifying vulnerabilities and threats to mobile devices is a valuable skill, but it must be paired with the ability to communicate the associated risks. Throughout the course, you’ll review ways to effectively communicate threats to key stakeholders. You’ll leverage tools, including Mobile App Report Cards, to characterize threats for managers and decision-makers, while also identifying sample code and libraries that developers can use to address risks for in-house applications.

YOUR MOBILE DEVICES ARE GOING TO COME UNDER ATTACK – HELP YOUR ORGANIZATION PREPARE FOR THE ONSLAUGHT!

In employing your newly learned skills, you’ll apply a step-by-step mobile device deployment penetration test. Starting with gaining access to wireless networks to implement man-in-the-middle attacks and finishing with mobile device exploits and data harvesting, you’ll examine each step of the test with hands-on exercises, detailed instructions, and tips and tricks learned from hundreds of successful penetration tests. By building these skills, you’ll return to work prepared to conduct your own test, or better informed on what to look for and how to review an outsourced penetration test.

Mobile device deployments introduce new threats to organizations, including advanced malware, data leakage, and the disclosure to attackers of enterprise secrets, intellectual property, and personally identifiable information assets. Further complicating matters, there simply are not enough people with the security skills needed to identify and manage secure mobile phone and tablet deployments. By completing this course, you’ll be able to differentiate yourself as having prepared to evaluate the security of mobile devices, effectively assess and identify flaws in mobile applications, and conduct a mobile device penetration test – all critical skills to protect and defend mobile device deployments.

Joshua Wright is a senior technical analyst with Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through his experiences as a penetration tester, Josh has worked with hundreds of organizations on attacking and defending mobile devices and wireless systems, ethically disclosing significant product and protocol security weaknesses to well-known organizations. As an open-source software advocate, Josh has conducted cutting-edge research resulting in several software tools that are commonly used to evaluate the security of widely deployed technology targeting WiFi, Bluetooth, and ZigBee wireless systems, smart grid deployments, and the Android and Apple iOS mobile device platforms. As the technical lead of the innovative CyberCity, Josh also oversees and manages the development of critical training and educational missions for cyber warriors in the U.S. military, government agencies, and critical infrastructure providers.

@joswr1ght
DAY 1: Device Architecture and Common Mobile Threats
The first module of SEC575 quickly looks at the significant threats affecting mobile device deployments, highlighted by a hands-on exercise evaluating network traffic from a vulnerable mobile banking application. As a critical component of a secure deployment, we will examine the architectural and implementation differences and similarities between Android Pie and iOS 12, and the Apple Watch and Google Wear platforms. We will also look at the specific implementation details of popular platform features such as iBeacon, AirDrop, App Verification, and more. Hands-on exercises will be used to interact with mobile devices running in a virtualized environment, including low-level access to installed application services and application data. We’ll examine the tools used to evaluate mobile devices as part of establishing a lab environment for mobile device assessments, including the analysis of mobile malware affecting Android and non-jailbroken iOS devices. Finally, we will address the threats of lost and stolen devices (and opportunities for a pen tester), including techniques to bypass mobile device lock screens.

Topics: Mobile Problems and Opportunities; Mobile Device Platform Analysis; Wearable Platforms; Mobile Device Lab Analysis Tools; Mobile Device Malware Threats

DAY 2: Mobile Platform Access and Application Analysis
With an understanding of the threats, architectural components and desired security methods, we dig deeper into iOS and Android mobile platforms focusing on sandboxing and data isolation models, and on the evaluation of mobile applications. This module is designed to help build skills in analyzing mobile device data and applications through rooting and jailbreaking Android and iOS devices and using that access to evaluate file system artifacts. We will also start to evaluate the security of mobile applications, using network capture analysis tools to identify weak network protocol use and sensitive data disclosure over the network. Finally, we’ll wrap up the module with an introduction to reverse engineering of iOS and Android applications using.decompilers, disassemblers, and manual analysis techniques.

Topics: Unlocking, Rooting, and Jailbreaking Mobile Devices; Mobile Phone Data Storage and File System Architecture; Network Activity Monitoring; Static Application Analysis

DAY 3: Mobile Application Reverse Engineering
One of the core skills you need as a mobile security analyst is the ability to evaluate the risks and threats a mobile app introduces to your organization. Through lecture and hands-on exercises in this module, with some analysis skills, you will be able to evaluate critical mobile applications to determine the type of access threats and information disclosure threats they represent. In this module we will use automated and manual application assessment tools to evaluate iOS and Android apps. We’ll build upon the static application analysis skills covered in Module 2 to manipulate application components, including Android Intents and iOS URL extensions. We’ll also learn and practice techniques for manipulating iOS and Android applications, such as method swizzling on iOS, and disassembly, modification, and reassembly of Android apps. The module ends with a look at a consistent system for evaluating and grading the security of mobile applications using the Application Report Card Project.

Topics: Automated Application Analysis Systems; Reverse Engineering Obfuscated Applications; Application Report Cards

DAY 4: Penetration Testing Mobile Devices – Part 1
An essential component of developing a secure mobile device deployment is to perform or outsource a penetration test. Through ethical hacking and penetration testing, we examine the mobile devices and infrastructure from the perspective of an attacker, identifying and exploiting flaws that deliver unauthorized access to data or supporting networks. By identifying these flaws we can evaluate the mobile phone deployment risk to the organization with practical and useful risk metrics. Whether your role is to implement the penetration test, or to source and evaluate the penetration tests of others, understanding these techniques will help your organization identify and resolve vulnerabilities before they become incidents.

Topics: Manipulating Application Behavior; Using Mobile Device Remote Access Trojans; Wireless Network Probe Mapping; Weak Wireless Attacks; Enterprise Wireless Security Attacks

DAY 5: Penetration Testing Mobile Devices – Part 2
Continuing our look at ethical hacking and penetration testing, we turn our focus to exploiting weaknesses on iOS and Android devices. We will also examine platform-specific application weaknesses and look at the growing use of web framework attacks in mobile application exploitation. Hands-on exercises are used throughout the module to practice these attacks, exploiting both vulnerable mobile applications and the supporting back-end servers.

Topics: Network Manipulation Attacks; Sidejacking Attacks; SSL/TLS Attacks; Client-Side Injection Attacks; Web Framework Attacks; Back-end Application Support Attacks

DAY 6: Capture-the-Flag Event
In the final module of SEC575 we will pull together all the concepts and technology covered during the week in a comprehensive Capture-the-Flag event. In this hands-on exercise, you will have the option to participate in multiple roles, including designing a secure infrastructure for the deployment of mobile phones, monitoring network activity to identify attacks against mobile devices, extracting sensitive data from a compromised iPad, and attacking a variety of mobile phones and related network infrastructure components. During this mobile security event you will put into practice the skills you have learned in order to evaluate systems and defend against attackers, simulating the realistic environment you will be prepared to protect when you get back to the office.

Who Should Attend
- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing, deploying or securing mobile phones and tablets
- Network and system administrators supporting mobile phones and tablets

“SEC575 provides an incredible amount of information, and the hands-on labs are awesome. It is a must-have for mobile penetration testers.”

-Richard Takacs, Integrity360

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/sansfire/courses

Course Day Descriptions
Mon, Jun 17 - Sat, Jun 22
9:00am - 5:00pm
Hands-on labs
SEC617: Wireless Penetration Testing and Ethical Hacking

You Will Be Able To

- Identify and locate malicious rogue access points using free and low-cost tools
- Conduct a penetration test against low-power wireless devices to identify control system and related wireless vulnerabilities
- Identify vulnerabilities and bypass authentication mechanisms in Bluetooth networks
- Utilize wireless capture tools to extract audio conversations and network traffic from DECT wireless phones
- Implement a WPA2 Enterprise penetration test to exploit vulnerable wireless client systems for credential harvesting
- Utilize Scapy to force custom packets to manipulate wireless networks in new ways, quickly building custom attack tools to meet specific penetration test requirements
- Identify WiFi attacks using network packet captures traces and freely available analysis tools
- Identify and exploit shortcomings in the security of proximity key card systems
- Decode proprietary radio signals using Software-Defined Radio
- Mount a penetration test against numerous standards-based or proprietary wireless technologies

Larry Pesce
SANS Certified Instructor

This course is designed for professionals seeking a comprehensive technical ability to understand, analyze, and defend the various wireless technologies that have become ubiquitous in our environments and, increasingly, key entrance points for attackers.

The authors of SEC617, as penetration testers themselves, know that many organizations overlook wireless security as an attack surface, and therefore fail to establish required defenses and monitoring, even though wireless technologies are now commonplace in executive suites, financial departments, government offices, manufacturing production lines, retail networks, medical devices, and air traffic control systems. Given the known risks of insecure wireless technologies and the attacks used against them, SEC617 was designed to help people build the vital skills needed to identify, evaluate, assess, and defend against these threats. These skills are "must-haves" for any high-performing security organization.

For many analysts, "wireless" was once synonymous with "WiFi," the ever-present networking technology, and many organizations deployed complex security systems to protect these networks. Today, wireless takes on a much broader meaning— not only encompassing the security of WiFi systems, but also the security of Bluetooth, ZigBee, Z-Wave, DECT, RFID, NFC, contactless smart cards, and even proprietary wireless systems. To effectively evaluate the security of wireless systems, your skillset needs to expand to include many different types of wireless technologies.

SEC617 will give you the skills you need to understand the security strengths and weaknesses of wireless systems. You will learn how to evaluate the ever-present cacophony of WiFi networks and identify the WiFi access points (APs) and client devices that threaten your organization. You will learn how to assess, attack, and exploit deficiencies in modern WiFi deployments using WPA2 technology, including sophisticated WPA2 Enterprise networks. You will gain a strong, practical understanding of the many weaknesses in WiFi protocols and how to apply that understanding to modern wireless systems. Along with identifying and attacking WiFi access points, you will learn to identify and exploit the behavioral differences in how client devices scan for, identify, and select APs, with deep insight into the behavior of the Windows 10, macOS, Apple iOS, and Android WiFi stacks.

A significant portion of the course focuses on Bluetooth and Bluetooth Low Energy (BLE) attacks, targeting a variety of devices, including wireless keyboards, smart light bulbs, mobile devices, audio streaming devices, and more. You will learn to assess a target Bluetooth device, identify the present (or absent) security controls, and apply a solid checklist to certify a device’s security for use within your organization.

Beyond analyzing WiFi and Bluetooth security threats, analysts must also understand many other wireless technologies that are widely utilized in complex systems. SEC617 provides insight and hands-on training to help analysts identify and assess the use of ZigBee and Z-Wave wireless systems used for automation, control, and smart home systems. The course also investigates the security of cordless telephony systems in the worldwide Digital Enhanced Cordless Telephony (DECT) standard, including audio eavesdropping and recording attacks.

Radio frequency identification (RFID), near field communication (NFC), and contactless smart card systems are more popular than ever in countless applications such as point of sale systems and data center access control systems. You will learn how to assess and evaluate these deployments using hands-on exercises to exploit the same kinds of flaws discovered in mass transit smart card systems, hotel guest room access systems, and more.

In addition to standards-based wireless systems, we also dig deeper into the radio spectrum using software-defined radio (SDR) systems to scour for signals. Using SDR, you will gain new insight into how widely pervasive wireless systems are deployed. With your skills in identifying, decoding, and evaluating the data these systems transmit, you will be able to spot vulnerabilities even in custom wireless infrastructures.

Larry is a Senior Security Analyst with InGuardians after a long stint in security and disaster recovery in healthcare, performing penetration testing, wireless assessments, and hardware hacking. He also diverts a significant portion of his attention to co-hosting the Security Weekly podcast and likes to tinker with all things electronic and wireless, much to the disappointment of his family, friends, warranties, and his second Leatherman Multi-tool. Larry co-authored Linksys WRT54G Ultimate Hacking and Using Wireshark and Ethereal from Syngress. Larry is an Extra Class Amateur Radio operator (KBITNF) and enjoys developing hardware and real-world challenges for the Mid-Atlantic Collegiate Cyber Defense Challenge.

@haxorthematrix
DAY 1: WiFi Data Collection and Analysis
The first section of the course quickly looks at wireless threats and attack surfaces and analyzes where you will likely see non-WiFi systems deployed in modern networks. We start off with a look at fundamental analysis techniques for evaluating WiFi networks, including the identification and analysis of rogue devices, and finish with a dive into remote penetration testing techniques using compromised Windows 10 and macOS devices to pivot.
Topics: Characterize the Wireless Threat; Sniffing WiFi; Rogue Access Point (AP) Analysis

DAY 2: WiFi Attack and Exploitation Techniques
After developing skills needed to capture and evaluate WiFi activity, we start our look at exploiting WiFi, targeting AP and client devices. We cover techniques that apply to any WiFi products, from consumer to enterprise-class devices, focusing on understanding protocol-level deficiencies that will continue to be applied throughout the course on non-WiFi wireless systems as well.
Topics: Exploiting WiFi Hotspots; WiFi Client Attacks; Exploiting WEP; Denial of Service (DoS) Attacks; WiFi Fuzzing for Bug Discovery

DAY 3: Enterprise WiFi, DECT, and ZigBee Attacks
We finish our look at WiFi attack techniques with a detailed look at assessing and exploiting WPA2 networks. Starting with WPA2 consumer networks, we investigate the flaws associated with pre-shared key networks and WiFi Protected Setup (WPS) deployments, continuing with a look at exploiting WPA2 Enterprise networks using various Extensible Authentication Protocol (EAP) methods. We continue to investigate the security of wireless networks on day 3, switching to non-WiFi analysis with a look at exploiting the worldwide Digital Enhanced Cordless Telephony (DECT) standard to capture and export audio conversations from cordless headsets and phones. We also investigate the security of ZigBee and IEEE 802.15.4 networks, looking at cryptographic flaws, key management failures, and hardware attacks.
Topics: Attacking WPA2 Pre-Shared Key Networks; Attacking WPA2 Enterprise Networks; Attacking Digital Enhanced Cordless Telephony Deployments; Attacking ZigBee Deployments

DAY 4: Bluetooth and Software Defined Radio Attacks
Bluetooth technology is nearly as pervasive as WiFi, with widespread adoption in smart phones, fitness trackers, wireless keyboard, smart watches, and more. In this module, we dig into the Bluetooth Classic, Enhanced Data Rate, and Low Energy protocols, including tools and techniques to evaluate target devices for vulnerabilities. Immediately following our look at Bluetooth technology, we jump into the practical application of Software Defined Radio (SDR) technology to identify, decode, and assess proprietary wireless systems. We investigate the hardware and software available for SDR systems, and look at the tools and techniques to start exploring this exciting area of wireless security assessment.
Topics: Bluetooth Introduction and Attack Techniques; Bluetooth Low Energy Introduction and Attack Techniques; Practical Application of Software-Defined Radio (SDR)

DAY 5: RFID, Smart Cards, and NFC Hacking
On day 5, we evaluate RFID technology in its multiple forms to identify the risks associated with privacy loss and tracking, while also building an understanding of both low-frequency and high-frequency RFID systems and NFC. We examine the security associated with contactless Point of Sale (PoS) terminals, including Apple Pay and Google Wallet, and proximity lock access systems from HID and other vendors. We also examine generalized techniques for attacking smart card systems, including critical data analysis skills needed to bypass the intended security of smart card systems used for mass transit systems, concert venues, bike rentals, and more.
Topics: RFID Overview; RFID Tracking and Privacy Attacks; Low-Frequency RFID Attacks; Exploiting Contactless RFID Smart Cards; Attacking NFC

DAY 6: Capture-the-Flag Challenge
On the last day of class, we will pull together all the concepts and technology we have covered during the week in a comprehensive Capture-the-Flag challenge. In this hands-on exercise, you will have the option to participate in multiple roles: identifying unauthorized/rogue WiFi access points, attacking live and recorded WiFi networks, decoding proprietary wireless signals, exploiting smart card deficiencies, and more. During this wireless security event you will put into practice the skills you have learned in order to evaluate systems and defend against attackers, simulating the realistic environment you will be prepared to protect when you get back to the office.

Who Should Attend
- Ethical hackers and penetration testers
- Network security staff
- Network and system administrators
- Incident response teams
- Information security policy decision-makers
- Technical auditors
- Information security consultants
- Wireless system engineers
- Embedded wireless system developers

“For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/sansfire/courses

“SEC617 is great for someone looking for a top-to-bottom rundown in wireless attacks.”
—Garret Picchioni, Salesforce
Adrien de Beaupre works as an independent consultant in beautiful Ottawa, Ontario. His work experience includes technical instruction, vulnerability assessment, penetration testing, intrusion detection, incident response and forensic analysis. He is a member of the SANS Internet Storm Center (isc.sans.edu). He is the lead course author of SANS SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques and SEC460: Enterprise Threat and Vulnerability Assessment. He is actively involved with the information security community, and has been working with SANS since 2000. Adrien holds a variety of certifications including the GXPN, GPEN, GWAPT, GCIC, GCIH, GSEC, CISSP®, OPST, and OPSA. When not geeking out he can be found with his family, or at the dojo.

@adriendb

SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques

You Will Be Able To

- Perform advanced Local File Include (LFI)/Remote File Include (RFI), Blind SQL injection (SQI), and Cross-Site Scripting (XSS) combined with Cross-Site Request Forger (XSRF) discovery and exploitation
- Exploit advanced vulnerabilities common to most backend language like Mass Assignments, Type Juggling, and Object Serialization
- Perform JavaScript-based injection against ExpressJS, Node.js, and NoSQL
- Understand the special testing methods for content management systems such as SharePoint and WordPress
- Identify and exploit encryption implementations within web applications and frameworks
- Discover XML Entity and XPath vulnerabilities in SOAP or REST web services and other datastores
- Use tools and techniques to work with and exploit HTTP/2 and WebSockets
- Identify and bypass Web Application Firewalls and application filtering techniques to exploit the system

Who Should Attend

- Web and network penetration testers
- Red team members
- Vulnerability assessment personnel
- Security consultants
- Developers and QA testers
- System administrators and IT managers
- System architects

Can your web apps withstand the onslaught of modern advanced attack techniques? Modern web applications are growing more sophisticated and complex as they utilize exciting new technologies and support ever more critical operations. Long gone are the days of basic HTML requests and responses. Even in the age of Web 2.0 and AJAX, the complexity of HTTP and modern web applications is progressing at breathtaking speed. With the demands of highly available web clusters and cloud deployments, web applications are looking to deliver more functionality in smaller packets, with a decreased strain on backend infrastructure. Welcome to an era that includes tricked-out cryptography, WebSockets, HTTP/2, and a whole lot more. Are your web application assessment and penetration testing skills ready to evaluate these impressive new technologies and make them more secure?

“SEC642 is the perfect course for someone who has a background in web app pen testing, but wants to really gain advanced skills.”

-Matthew Sullivan, Webfilings
DAY 1: Advanced Attacks
As applications and their vulnerabilities become more complex, penetration testers have to be able to handle advanced targets. We’ll start the course with a warm-up pen test of a small application. After our review of this exercise, we will explore some of the more advanced techniques for LFI/RFI and SQLi server-based flaws. We will then take a stab at combined XSS and XSRF attacks, where we leverage the two vulnerabilities together for even greater effect. After discovering the flaws, we will then work through various ways to exploit these flaws beyond the typical means exhibited today. These advanced techniques will help penetration testers find ways to demonstrate these vulnerabilities to their organization through advanced and custom exploitation.

Topics: Review of the Testing Methodology; Using Burp Suite in a Web Penetration Test; Exploiting Local and Remote File Inclusions; Exploring Advanced Discovery Techniques for SQL Injection and Other Server-Based Flaws; Exploring Advanced Exploitation of XSS and XSRF in a Combined Attack; Learning Advanced Exploitation Techniques

DAY 2: Web Frameworks
We’ll continue exploring advanced discovery and exploitation techniques for today’s complex web applications. We’ll look at vulnerabilities that could affect web applications written in any backend language, then examine how logic flaws in applications, especially in Mass Object Assignments, can have devastating effects on security. We’ll also dig into assumptions made by core development teams of backend programming languages and learn how even something as simple as handling the data types in variables can be leveraged through the web with Type Juggling and Object Serialization. Next we’ll explore various popular applications and frameworks and how they change the discovery techniques within a web penetration test. Part of this discussion will lead us to cutting-edge technologies like the MEAN stack, where JavaScript is leveraged from the browser, web server, and backend NoSQL storage. The final section of the class examines applications in content management systems such as SharePoint and WordPress, which have unique needs and features that make testing them both more complex and more fruitful for the tester.

Topics: Web Architectures; Web Design Patterns; Languages and Frameworks; Java and Struts; PHP-Type Juggling; Logic Flaws; Attacking Object Serialization; The MEAN Stack; Content Management Systems; SharePoint; WordPress

DAY 3: Web Cryptography
Cryptographic weaknesses are common, yet few penetration testers have the skill to investigate, attack and exploit these flaws. When we investigate web application crypto attacks, we typically target the implementation and use of cryptography in modern web applications. Many popular web programming languages or development frameworks make encryption services available to the developer, but do not inherently protect encrypted data from being attacked, or only permit the developer to use cryptography in a weak manner. These implementation mistakes are going to be our focus in this section, as opposed to the exploitation of deficiencies in the cryptographic algorithms themselves. We will also explore the various ways applications use encryption and hashing insecurely. Students will learn techniques ranging from identifying what the encryption technique is to exploiting various flaws within the encryption or hashing.

Topics: Identifying the Cryptography Used in the Web Application; Analyzing and Attacking the Encryption Keys; Exploiting Stream Cipher IV Solisisons; Exploiting Electronic Codebook (ECB) Mode Ciphers with Block Shuffling; Exploiting Cipher Block Chaining (CBC) Mode with Bit Flipping; Vulnerabilities in PKCS#7 Padding Implementations

DAY 4: Alternative Web Interfaces
Web applications are no longer limited to the traditional HTML-based interfaces. Web services and mobile applications have become more common and are regularly being used to attack clients and organizations. As such, it has become very important that penetration testers understand how to evaluate the security of these systems. We will examine Flash, Java, Active X, and Silverlight flaws. We will explore various techniques to discover flaws within the applications and backend systems. These techniques will make use of tools such as Burp Suite and other automated toolsets. We’ll use lab exercises to explore the newer protocols of HTTP/2 and WebSockets, exploiting flaws exposed within each of them.

Topics: Intercepting Traffic to Web Services and from Mobile Applications; Flash, Java, ActiveX, and Silverlight Vulnerabilities; SOAP and REST Web Services; Penetration Testing of Web Services; WebSocket Protocol Issues and Vulnerabilities; New HTTP/2 Protocol Issues and Penetration Testing

DAY 5: Web Application Firewall and Filter Bypass
Applications today are using more security controls to help prevent attacks. These controls, such as Web Application Firewalls and filtering techniques, make it more difficult for penetration testers during their testing. The controls block many of the automated tools and simple techniques used to discover flaws. On this day we’ll explore techniques used to map the control and how that control is configured to block attacks. You’ll be able to map out the rule sets and determine the specifics of how the Web Application Firewall detects attacks. This mapping will then be used to determine attacks that will bypass the control. You’ll use HTML5, UNICODE, and other encodings that will enable your discovery techniques to work within the protected application.

Topics: Understanding of Web Application Firewalling and Filtering Techniques; Determining the Rule Sets Protecting the Application; Fingerprinting the Defense Techniques Used; Learning How HTML5 Injections Work; Using UNICODE, CSRF, and Data URIs to Bypass Restrictions; Bypassing a Web Application Firewall’s Best-Defended Vulnerabilities; XSS and SQLi

DAY 6: Capture-the-Flag Challenge
On this final course day you will be placed on a network and given the opportunity to complete an entire penetration test. The goal of this exercise is for you to explore the techniques, tools, and methodology you will have learned over the last five days. You’ll be able to use these skills against a realistic extranet and intranet. At the end of the day, you will provide a verbal report of the findings and methodology you followed to complete the test. Students will be provided with a virtual machine that contains the Samurai Web Testing Framework (SamuraiWTF). You will be able to use this both in the class and after leaving and returning to your jobs.
SEC660: **Advanced Penetration Testing, Exploit Writing, and Ethical Hacking**

This course is designed as a logical progression point for those who have completed SEC560: Network Penetration Testing and Ethical Hacking, or for those with existing penetration testing experience. Students with the prerequisite knowledge to take this course will walk through dozens of real-world attacks used by the most seasoned penetration testers. The methodology of a given attack is discussed, followed by exercises in a real-world lab environment to solidify advanced concepts and allow for the immediate application of techniques in the workplace. Each day includes a two-hour evening bootcamp to allow for additional mastery of the techniques discussed and even more hands-on exercises. A sample of topics covered includes weaponizing Python for penetration testers, attacks against network access control (NAC) and VLAN manipulation, network device exploitation, breaking out of Linux and Windows restricted environments, IPv6, Linux privilege escalation and exploit-writing, testing cryptographic implementations, fuzzing, defeating modern OS controls such as ASLR and DEP, return-oriented programming (ROP), Windows exploit-writing, and much more!

Attackers are becoming more clever and their attacks more complex. In order to keep up with the latest attack methods, you need a strong desire to learn, the support of others, and the opportunity to practice and build experience. SEC660 provides attendees with in-depth knowledge of the most prominent and powerful attack vectors and an environment to perform these attacks in numerous hands-on scenarios. This course goes far beyond simple scanning for low-hanging fruit, and shows penetration testers how to model the abilities of an advanced attacker to find significant flaws in a target environment and demonstrate the business risk associated with these flaws.

SEC660 starts off by introducing the advanced penetration concept, and provides an overview to help prepare students for what lies ahead. The focus of day one is on network attacks, an area often left untouched by testers. Topics include accessing, manipulating, and exploiting the network. Attacks are performed against NAC, VLANs, OSPF, 802.1X, CDP, IPv6, VOIP, SSL, ARP, SNMP, and others. Day two starts off with a technical module on performing penetration testing against various cryptographic implementations. The rest of the day is spent on network booting attacks, escaping Linux restricted environments such as chroot, and escaping Windows restricted desktop environments. Day three jumps into an introduction of Python for penetration testing, Scapy for packet crafting, product security testing, network and application fuzzing, and code coverage techniques. Days four and five are spent exploiting programs on the Linux and Windows operating systems. You will learn to identify privileged programs, redirect the execution of code, reverse-engineer programs to locate vulnerable code, obtain code execution for administrative shell access, and defeat modern operating system controls such as ASLR, canaries, and DEP using ROP and other techniques. Local and remote exploits, as well as client-side exploitation techniques, are covered. The final course day is dedicated to numerous penetration testing challenges requiring you to solve complex problems and capture flags.

**Who Should Attend**
- Network and systems penetration testers
- Incident handlers
- Application developers
- IDS engineers

**You Will Be Able To**
- Perform fuzz testing to enhance your company’s SDL process
- Exploit network devices and assess network application protocols
- Escape from restricted environments on Linux and Windows
- Test cryptographic implementations
- Model the techniques used by attackers to perform 0-day vulnerability discovery and exploit development
- Develop more accurate quantitative and qualitative risk assessments through validation
- Demonstrate the needs and effects of leveraging modern exploit mitigation controls
- Reverse-engineer vulnerable code to write custom exploits

**Tim Medin**
SANS Principal Instructor

Tim Medin is the founder and Principal Consultant at Red Siege, a company focused on adversary emulation and penetration testing. Tim is also the SANS MSiSE Program Director and a course author. Throughout the course of his career, Tim has performed penetration tests on a wide range of organizations and technologies. He gained information security experience in a variety of industries including previous positions in control systems, higher education, financial services, and manufacturing. Tim is an experienced international speaker, having presented at organizations around the world. Tim is also the creator of Kerberoasting, a technique to extract kerberos tickets in order to offline attack the password of enterprise service accounts. Tim earned his MBA at the University of Texas.

@timmedin

Register at [www.sans.org/sansfire](http://www.sans.org/sansfire) | 301-654-SANS (7267)
DAY 1: Network Attacks for Penetration Testers
Day one serves as an advanced network attack module, building on knowledge gained from SEC660. The focus will be on obtaining access to the network; manipulating the network to gain an attacker position for eavesdropping and attacks, and for exploiting network devices; leveraging weaknesses in network infrastructure; and taking advantage of client frailty.

Topics: Bypassing Network Admission Control; Impersonating Devices with Admission Control Policy Exceptions; Exploiting EAP-MD5 Authentication; Custom Network Protocol Manipulation with Ettercap and Custom Filters; Multiple Techniques for Gaining Man-in-the-Middle Network Access; Exploiting OSPF Authentication to inject Malicious Routing Updates; Using Evtlograce to Attack Software Updates; Overcoming SSL Transport Encryption Security with Sslstrip; Remote Cisco Router Configuration File Retrieval; IPv6 for Penetration Testers

DAY 2: Crypto and Post-Exploitation
Day two starts by taking a tactical look at techniques penetration testers can use to investigate and exploit common cryptography mistakes. We finish the module with lab exercises that allow you to practice your new-found crypto attack skill set against reproduced real-world application vulnerabilities.

Topics: Pen Testing Cryptographic Implementations; Exploiting CBC Bit Flipping Vulnerabilities; Exploiting Hash Length Extension Vulnerabilities; Delivering Malicious Operating Systems to Devices Using Network Booting and PXE; PowerShell Essentials; Enterprise PowerShell; Post-Exploitation with PowerShell and Metasploit; Escaping Software Restrictions; Two-hour Evening Capture-the-Flag Exercise Using PXE, Network Attacks, and Local Privilege Escalation

DAY 3: Python, Scapy, and Fuzzing
Day three starts with a focus on how to leverage Python as a penetration tester. It is designed to help people unfamiliar with Python start modifying scripts to add to their own functionality while helping seasoned Python scripters improve their skills. Once we leverage the Python skills in creative lab exercises, we move on to leveraging Scapy for custom network targeting and protocol manipulation. Using Scapy, we examine techniques for transmitting and receiving network traffic beyond what canned tools can accomplish, including IPv6.

Topics: Becoming familiar with Python Types; Leveraging Python Modules for Real-World Pen Tester Tasks; Manipulating Stateful Protocols with Scapy; Using Scapy to Create a Custom Wireless Data Leakage Tool; Product Security Testing; Using Taof for Quick Protocol Mutation Fuzzing; Optimizing Your Fuzzing Time with Smart Target Selection; Automating Target Monitoring While Fuzzing with Sulley; Leveraging Microsoft Word Macros for Fuzzing .doc files; Block-Based Code Coverage Techniques Using Paimei

DAY 4: Exploiting Linux for Penetration Testers
Day four begins by walking through memory from an exploitation perspective as well as introducing x86 assembler and linking and loading. Processor registers are directly manipulated by testers and must be intimately understood. Disassembly is a critical piece of testing and will be used throughout the remainder of the course. We will take a look at the Linux OS from an exploitation perspective and discuss the topic of privilege escalation.

Topics: Stack and Dynamic Memory Management and Allocation on the Linux OS; Disassembling a Binary and Analyzing x86 Assembly Code; Performing Symbol Resolution on the Linux OS; Identifying Vulnerable Programs; Code Execution Redirection and Memory Leaks; Return-Oriented Programming (ROP); Identifying and Analyzing Stack-Based Overflows on the Linux OS; Performing Return-to-libc (ret2libc) Attacks on the Stack; Defeating Stack Protection on the Linux OS; Defeating ASLR on the Linux OS

DAY 5: Exploiting Windows for Penetration Testers
On day five we start with covering the OS security features (ASLR, DEP, etc.) added to the Windows OS over the years, as well as Windows-specific constructs, such as the process environment block (PEB), structured exception handling (SEH), thread information block (TIB), and the Windows API. Differences between Linux and Windows will be covered. These topics are critical in assessing Windows-based applications. We then focus on stack-based attacks against programs running on the Windows OS.

Topics: The State of Windows OS Protections on Windows 7, 8, 10, Server 2008 and 2012; Understanding Common Windows Constructs: Stack Exploitation on Windows; Defeating OS Protections Added to Windows; Creating a Metasploit Module; Advanced Stack-Smashing on Windows; Using ROP; Building ROP Chains to Defeat DEP and Bypass ASLR; Windows 7 and 8, Porting Metasploit Modules; Client-side Exploitation; Windows Shellcode

DAY 6: Capture-the-Flag Challenge
This day will serve as a real-world challenge for students by requiring them to utilize skills they have learned throughout the course, think outside the box, and solve a range of problems from simple to complex. A web server scoring system will be provided to score students as they capture flags. More difficult challenges will be worth more points. This day will serve as a real-world challenge for students by requiring them to utilize skills they have learned throughout the course, think outside the box, and solve a range of problems from simple to complex. A web server scoring system will be provided to score students as they capture flags. More difficult challenges will be worth more points. In this offensive exercise, challenges range from local privilege escalation to remote exploitation on both Linux and Windows systems, as well as networking attacks and other challenges related to the course material.

“SEC660 is the right balance between theory and practice; it’s hands-on, not too hard, but also not too easy.”
-Anton Ebertzeder, Siemens AG

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/sansfire/courses
Vulnerabilities in modern operating systems such as Microsoft Windows 7/8/10, Server 2012, and the latest Linux distributions are often very complex and subtle. Yet these vulnerabilities could expose organizations to significant attacks, undermining their defenses when attacked by very skilled adversaries. Few security professionals have the skillset to discover let alone even understand at a fundamental level why the vulnerability exists and how to write an exploit to compromise it. Conversely, attackers must maintain this skillset regardless of the increased complexity. SEC760: Advanced Exploit Development for Penetration Testers, the SANS Institute’s only 700-level course, teaches the skills required to reverse-engineer 32- and 64-bit applications, perform remote user application and kernel debugging, analyze patches for one-day exploits, and write complex exploits, such as use-after-free attacks, against modern software and operating systems.

Some of the skills you will learn in SEC760 include:

- How to write modern exploits against the Windows 7/8/10 operating systems
- How to perform complex attacks such as use-after-free, Kernel exploit techniques, one-day exploitation through patch analysis, and other advanced topics
- The importance of utilizing a Security Development Lifecycle (SDL) or Secure SDLC, along with Threat Modeling
- How to effectively utilize various debuggers and plug-ins to improve vulnerability research and speed
- How to deal with modern exploit mitigation controls aimed at thwarting success and defeating determination

“SEC760 is a kind of training we could not get anywhere else. It is not a theory, we got to implement and to exploit everything we learned.”

-Jenny Kitaichit, Intel

Stephen Sims is an industry expert with over 15 years of experience in information technology and security. Stephen currently works out of San Francisco as a consultant performing reverse engineering, exploit development, threat modeling, and penetration testing. Stephen has a MS in information assurance from Norwich University. He is the author of SANS’ only 700-level course, SEC760: Advanced Exploit Development for Penetration Testers, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author of SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking. He holds the GIAC Security Expert (GSE) certification as well as the CISSP®, CISA, Immunity NOP, and many other certifications. In his spare time Stephen enjoys snowboarding and writing music.

@Steph3nSims
**Course Day Descriptions**

**DAY 1: Threat Modeling, Reversing and Debugging with IDA** 
Many penetration testers, incident handlers, developers, and other related professionals lack reverse-engineering and debugging skills. These are different skills than reverse-engineering malicious software. As part of the Security Development Lifecycle (SDL) and Secure-SDLC, developers and exploit writers should have experience using IDA Pro to debug and reverse their code when finding bugs or when identifying potential risks after static code analysis or fuzzing.

**Topics:** Security Development Lifecycle; Threat Modeling; Why IDA is the #1 Tool for Reverse Engineering; IDA Navigation; IDA Python and the IDA IDB; IDA Plug-ins and Extensibility; Local Application Debugging with IDA; Remote Application Debugging with IDA.

**DAY 2: Advanced Linux Exploitation** 
The ability to progress into more advanced reversing and exploitation requires an expert-level understanding of basic software vulnerabilities, such as those covered in SEC660. Heap overflows serve as a rite of passage into modern exploitation techniques. This day is aimed at bridging this gap of knowledge in order to inspire thinking in a more abstract manner, necessary for continuing further with the course. Linux can sometimes be an easier operating system to learn these techniques, serving as a productive gateway into Windows.

**Topics:** Linux Heap Management, Constructs, and Environment; Navigating the Heap; Abusing Macros such as unlink() and fcntl(); Function Pointer Overwrites; Format String Exploitation; Abusing Custom Doubly-Linked Lists; Defeating Linux Exploit Mitigation Controls; Using IDA for Linux Application Exploitation; Using Format String Bugs for ASLR Bypass.

**DAY 3: Patch Diffing, One-Day Exploits, and Return-Oriented Shellcode** 
Attackers often download patches as soon as they are distributed by vendors such as Microsoft in order to find newly patched vulnerabilities. Vulnerabilities are usually disclosed privately, or even discovered in-house, allowing the vendor to more silently patch the vulnerability. This also allows the vendor to release limited or even no details at all about a patched vulnerability. Attackers are well aware of this and quickly work to find the patched vulnerability in order to take control of unpatched systems. This technique is also performed by incident handlers, IDS administrators and vendors, vulnerability and penetration testing framework companies, government entities, and others. You will use the material covered in this day to identify bugs patched by vendors and take them through to exploitation.

**Topics:** The Microsoft Patch Management Process and Patch Tuesday; Obtaining Patches and Patch Extraction; Binary Diffing with BinDiff, patchdiff2, turbodiff, and DarunGrimg; Visualizing Code Changes and Identifying Fixes; Reversing 32-bit and 64-bit Applications and Modules; Triggering Patched Vulnerabilities; Writing One-Day Exploits; Handling Modern Exploit Mitigation Controls; UsingROP to Compiled Shellcode on the Fly (Return-Oriented Shellcode).

**DAY 4: Windows Kernel Debugging and Exploitation** 
The Windows Kernel is very complex and intimidating. This course day aims to help you understand the Windows Kernel and the various exploit mitigations added into recent versions. You will perform Kernel debugging on various versions of the Windows OS, such as Windows 7 and 8, and learn to deal with its inherent complexities. Exercises will be performed to analyze vulnerabilities, look at exploitation techniques, and get a working exploit.

**Topics:** Understanding the Windows Kernel; Navigating the Windows Kernel; Modern Kernel Protections; Debugging the Windows 7/8 Kernels and Drivers; WinDbg; Analyzing Kernel Vulnerabilities and Kernel Vulnerability Types; Kernel Exploitation Techniques; Token Stealing and HAL Dispatch Table Overwrites.

**DAY 5: Windows Heap Overflows and Client-Side Exploitation** 
The focus of this section is primarily on Windows browser and client-side exploitation. You will learn to analyze C++ vtable overflows, one of the most common mechanisms used to compromise a modern Windows system. Many of these vulnerabilities are discovered in the browser, so browser techniques will also be taught, including modern heap spraying to deal with Internet Explorer 8/9/10 and other browsers such as Firefox and Chrome. You will work towards writing exploits in the Use-After-Free/Dangling Pointer vulnerability class.

**Topics:** Windows Heap Management, Constructs, and Environment; Understanding the Low Fragmentation Heap (LFH); Browser-based and Client-side Exploitation; Remedial Heap Spraying; Understanding C++ vtable/vtable Behavior; Modern Heap Spraying to Determine Address Predictability; Use-after-free Attacks and Dangling Pointers; Using Custom Flash Objects to Bypass ASLR; Defeating ASLR, DEP, and Other Common Exploit Mitigation Controls.

**DAY 6: Capture-the-Flag Challenge** 
Day 6 will feature a Capture-the-Flag event with different types of challenges taken from material taught throughout the week.

---

**Who Should Attend**
- Senior network and system penetration testers
- Secure application developers (C and C++)
- Reverse-engineering professionals
- Senior incident handlers
- Senior threat analysts
- Vulnerability researchers
- Security researchers

**Course Author Statement**
“SEC760 is the challenge I am looking for. It will be overwhelming, but well worth it.”

-Stephen Sims

---

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/sansfire/courses](http://www.sans.org/sansfire/courses)

---

[57]
FOR500: Windows Forensic Analysis

You Will Be Able To

- Perform proper Windows forensic analysis by applying key techniques focusing on Windows 7/8/10
- Use full-scale forensic tools and analysis methods to detail nearly every action a suspect accomplished on a Windows system, including who placed an artifact on the system and how, program execution, file/folder opening, geo-location, browser history, profile USB device usage, and more
- Uncover the exact time that a specific user last executed a program through Registry and Windows artifact analysis, and understand how this information can be used to prove intent in cases such as intellectual property theft, hacker-breached systems, and traditional crimes
- Determine the number of times files have been opened by a suspect through browser forensics, shortcut file analysis (LNK), e-mail analysis, and Windows Registry parsing
- Identify keywords searched by a specific user on a Windows system in order to pinpoint the files and information the suspect was interested in finding and accomplish detailed damage assessments
- Use Windows shellbags analysis tools to articulate every folder and directory that a user opened up while browsing local, removable, and network drives
- Determine each time a unique and specific USB device was attached to the Windows system, the files and folders that were accessed on it, and who plugged it in by parsing key Windows artifacts such as the Registry and log files
- Use event log analysis techniques to determine when and how users logged into a Windows system, whether via a remote session, at the keyboard, or simply by unlocking a screensaver

Ovie Carroll
SANS Principal Instructor

MASTERS WINDOWS FORENSICS – YOU CAN'T PROTECT WHAT YOU DON'T KNOW ABOUT

FOR500: Windows Forensic Analysis will teach you to:

- Identify artifact and evidence locations to answer critical questions, including application execution, file access, data theft, external device usage, cloud services, geolocation, file download, anti-forensics, and detailed system usage
- Focus your capabilities on analysis instead of on how to use a particular tool
- Extract critical answers and build an in-house forensic capability via a variety of free, open-source, and commercial tools provided within the SANS Windows SIFT Workstation

All organizations must prepare for cyber-crime occurring on their computer systems and within their networks. Demand has never been greater for analysts who can investigate crimes such as fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover vital intelligence from Windows systems. To help solve these cases, SANS is training a new cadre of the world’s best digital forensic professionals, incident responders, and media exploitation experts capable of piecing together what happened on computer systems second by second.

FOR500: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of Microsoft Windows operating systems. You can’t protect what you don’t know about, and understanding forensic capabilities and artifacts is a core component of information security. You will learn how to recover, analyze, and authenticate forensic data on Windows systems, track particular user activity on your network, and organize findings for use in incident response, internal investigations, and civil/criminal litigation. You will be able to use your new skills to validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies. Whether you know it or not, Windows is silently recording an unbelievable amount of data about you and your users.

FOR500 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR500 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7, Windows 8/8.1, Windows 10, Office and Office365, Cloud Storage, SharePoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows 7 systems to just-discovered Windows 10 artifacts.

“I have gained so much insight taking this course and can’t wait to apply these skills!”

-Dylan Ong, Stroz Friedberg

Ovie Carroll has 31 years of law enforcement experience and over 20 years of cyber investigative experience. He is the Director of the Cybercrime Lab of the Computer Crime and Intellectual Property Section (CCIPS) at the Department of Justice (DOJ). The lab provides advanced computer forensics, cybercrime investigation, and other technical assistance to DOJ prosecutors to support implementation of the department’s national strategies for digital evidence and to combat electronic penetration, data theft, and cyberattacks on critical information systems.

At SANS Ovie teaches FOR500: Windows Forensic Analysis, a course he also co-authored. Prior to joining the DOJ, Ovie was a special agent in charge of overseeing the Technical Crimes Unit of the Postal Inspector General’s Office, where he was responsible for all computer intrusion investigations within the postal service network infrastructure and for providing all digital forensic analysis in support of criminal investigations and audits. He also served as a special agent in the U.S. Air Force Office of Special Investigations, investigating computer intrusions and working both general crimes and counterintelligence as well as conducting investigations into offenses including murder, rape, fraud, bribery, theft, and gangs and narcotics.

@ovie
Course Day Descriptions

**DAY 1: Windows Digital Forensics and Advanced Data Triage**
The Windows forensics course starts with an examination of digital forensics in today’s interconnected environments and discusses challenges associated with mobile devices, tablets, cloud storage, and modern Windows operating systems. We will discuss how modern hard drives, such as Solid State Devices (SSD), can affect the digital forensics acquisition process and how analysts need to adapt to overcome the introduction of these new technologies.

**Topics:** Windows Operating System Components; Core Forensic Principles; Live Response and Triage-Based Acquisition Techniques; Acquisition Review with Write Blocker; Advanced Acquisition Challenges; Windows Image Mounting and Examination; NTFS File System Overview; Document and File Metadata; File Carving; Custom Carving Signatures; Memory, Pagefile, and Unallocated Space Analysis

---

**DAY 2: Core Windows Forensics Part 1 – Windows Registry Forensics and Analysis**
Our journey continues with the Windows Registry, where the digital forensic investigator will learn how to discover critical user and system information pertinent to almost any investigation. Each examiner will learn how to navigate and examine the Registry to obtain user-profile data and system data. The course teaches forensic investigators how to prove that a specific user performed key word searches, ran specific programs, opened and saved files, perused folders, and used removable devices. Throughout the section, investigators will use their skills in a real hands-on case, exploring the evidence and analyzing evidence.

**Topics:** Registry Basics; Profile Users and Groups; Core System Information; User Forensic Data; Tools Utilized

---

**DAY 3: Core Windows Forensics Part 2 – USB Devices and Shell Items**
Being able to show the first and last time a file or folder was opened is a critical analysis skill. Utilizing shortcut (LNK), jump list, and Shellbag databases through the examination of SHELL ITEMS, we can quickly pinpoint which file or folder was opened and when. The knowledge obtained by examining SHELL ITEMS is crucial in tracking user activity in intellectual property theft cases internally or in tracking hackers. Removable storage device investigations are often an essential part of performing digital forensics. We will show you how to perform in-depth USB device examinations on Windows 7, 8/8.1, and 10. You will learn how to determine when a storage device was first and last plugged in, its vendor/make/model, and even the unique serial number of the device used.

**Topics:** Shell Item Forensics; USB and Bring Your Own Device (BYOD) Forensic Examinations

---

**DAY 4: Core Windows Forensics Part 3 – Email, Key Additional Artifacts, and Event Logs**
Depending on the type of investigation and authorization, a wealth of evidence can be unearthed through the analysis of email files. Recovered email can bring excellent corroborating information to an investigation, and its informality often provides very incriminating evidence. It is common for users to have an email that exists locally on their workstation, on their company email server, in a private cloud, and in multiple webmail accounts. Windows event log analysis has solved more cases than possibly any other type of analysis. Understanding the locations and content of these files is crucial to the success of any investigator. Many researchers overlook these records because they do not have adequate knowledge or tools to get the job done efficiently. This section arms each investigator with the core knowledge and capability to maintain this crucial skill for many years to come.

**Topics:** Email Forensics; Forensicating Additional Windows OS Artifacts; Windows Event Log Analysis

---

**DAY 5: Core Windows Forensics Part 4 – Web Browser Forensics: Firefox, Internet Explorer, and Chrome**
With the increasing use of the web and the shift toward web-based applications and cloud computing, browser forensic analysis is a critical skill. During this section, the investigator will comprehensively explore web browser evidence created during the use of Internet Explorer, Edge, Firefox, and Google Chrome. The analyst will learn how to examine every significant artifact stored by the browser and how to analyze some of the more obscure (and powerful) browser artifacts, such as session restore, tracking cookies, zoom levels, predictive site prefetching, and private browsing remnants.

**Topics:** Browser Forensics; History, Cache, Searches, Downloads, Understanding of Browser Timestamps, Internet Explorer; Firefox; Chrome; Examination of Browser Artifacts; Tools Used

---

**DAY 6: Windows Forensic Challenge**
This complex case will involve an investigation into one of the most recent versions of the Windows Operating System. The evidence is real and provides the most realistic training opportunity currently available. Solving the case will require that students use all of the skills gained from each of the previous sections.

**Topics:** Digital Forensic Case; Windows 7 Forensic Challenge

---

**Who Should Attend**
- Information security professionals
- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Anyone interested in a deep understanding of Windows forensics

---

“SANS training is, by far, the best I’ve ever seen. The DFIR is the best of SANS in my opinion. The teaching and content are unmatched. You come in thinking you’re learning forensics but it’s much more. You gain tremendous understanding of concepts and methods.”

-Gary Sanders, LWCC

---

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/sansfire/courses
FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting

You Will Be Able To
- Learn and master the tools, techniques, and procedures necessary to effectively hunt, detect, and contain a variety of adversaries and to remediate incidents
- Detect and hunt unknown live, dormant, and custom malware in memory across multiple Windows systems in an enterprise environment
- Hunt through and perform incident response across hundreds of unique systems simultaneously using F-Response Enterprise and the SIFT Workstation
- Identify and track malware beaconing outbound to its command and control (C2) channel via memory forensics, registry analysis, and network connection residue
- Determine how the breach occurred by identifying the beachhead and spear phishing attack mechanisms
- Target advanced adversary anti-forensics techniques like hidden and time-stopped malware, along with utility-ware used to move in the network and maintain an attacker’s presence
- Use memory analysis, incident response, and threat hunting tools in the SIFT Workstation to detect hidden processes, malware, attacker command lines, rootkits, network connections, and more
- Track user and attacker activity second-by-second on the system you are analyzing through in-depth timeline and super-timeline analysis
- Recover data cleared using anti-forensics techniques via Volume Shadow Copy and Restore Point analysis
- Identify lateral movement and pivots within your enterprise, showing how attackers transition from system to system without detection

FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting will help you to:
- Detect how and when a breach occurred
- Identify compromised and affected systems
- Determine what attackers took or changed
- Contain and remediate incidents
- Develop key sources of threat intelligence
- Hunt down additional breaches using knowledge of the adversary

DAY 0: A 3-letter government agency contacts you to say an advanced threat group is targeting organizations like yours, and that your organization is likely a target. They won’t tell how they know, but they suspect that there are already several breached systems within your enterprise. An advanced persistent threat, aka an APT, is likely involved. This is the most sophisticated threat that you are likely to face in your efforts to defend your systems and data, and these adversaries may have been actively rummaging through your network undetected for months or even years.

This is a hypothetical situation, but the chances are very high that hidden threats already exist inside your organization’s networks. Organizations can’t afford to believe that their security measures are perfect and impenetrable, no matter how thorough their security precautions might be. Prevention systems alone are insufficient to counter focused human adversaries who know how to get around most security and monitoring tools.

Threat hunting and Incident response tactics and procedures have evolved rapidly over the past several years. Your team can no longer afford to use antiquated incident response and threat hunting techniques that fail to properly identify compromised systems, provide ineffective containment of the breach, and ultimately fail to rapidly remediate the incident. Incident response and threat hunting teams are the keys to identifying and observing malware indicators and patterns of activity in order to generate accurate threat intelligence that can be used to detect current and future intrusions.

This in-depth incident response and threat hunting course provides responders and threat hunting teams with advanced skills to hunt down, identify, counter, and recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, organized crime syndicates, and activism. Constantly updated, FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting addresses today’s incidents by providing hands-on incident response and threat hunting tactics and techniques that elite responders and hunters are successfully using to detect, counter, and respond to real-world breach cases.

GATHER YOUR INCIDENT RESPONSE TEAM – IT’S TIME TO GO HUNTING!

“This class arms you with the information and skills that are relevant and immediately usable and it helps you stay current.”

-Stephen McVey, Macys

Rob Lee is an entrepreneur and consultant in the Washington, DC area and currently the Curriculum Lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 15 years’ experience in computer forensics, vulnerability and exploit development, intrusion detection/prevention, and incident response. Rob graduated from the U.S. Air Force Academy and earned his MBA from Georgetown University. He served in the U.S. Air Force as a member of the 609th Information Warfare Squadron (IWS), the first U.S. military operational unit focused on information warfare. Later, he was a member of the Air Force Office of Special Investigations (AFOSI), where he led crime investigations and an incident response team. Over the next seven years, he worked directly with a variety of government agencies in the law enforcement, U.S. Department of Defense, and intelligence communities as the technical lead for vulnerability discovery and exploit development teams, lead for a cyber-forensics branch, and lead for a computer forensic and security software development team. Most recently, Rob was a Director for MANDIANT, a commercial firm focusing on responding to advanced adversaries such as the APT. Rob co-authored the book Know Your Enemy, 2nd Edition. Rob is also co-author of the MANDIANT threat intelligence report “M-Trends: The Advanced Persistent Threat.”

@roblee

Rob Lee
SANS Faculty Fellow

60 Day Program | 36 CPES | Laptop Required

Register at www.sans.org/sansfire | 301-654-SANS (7267)

www.giac.org/gcfa

GCFA
Forensic Analyst
www.giac.org/gcfa
Course Day Descriptions

**DAY 1: Advanced Incident Response and Threat Hunting**

Incident responders and threat hunters should be armed with the latest tools, memory analysis techniques, and enterprise methodologies to identify, track, and contain advanced adversaries and to remediate incidents. Incident response and threat hunting analysts must be able to scale their analysis across thousands of systems in their enterprise. This section examines the six-step incident response methodology as it applies to incident response for advanced threat groups. We will show the importance of developing cyber threat intelligence to impact the adversaries’ “kill chain” and demonstrate live response techniques and tactics that can be applied to a single system and across the entire enterprise.

**Topics:** Real Incident Response Tactics; Threat Hunting; Cyber Threat Intelligence; Threat Hunting in the Enterprise; Malware Persistence Identification; Remote and Enterprise Incident Response

---

**DAY 2: Memory Forensics in Incident Response and Threat Hunting**

Now a critical component of many incident response and threat hunting teams that detect advanced threats in their organization, memory forensics has come a long way in just a few years. Memory forensics can be extraordinarily effective at finding evidence of worms, rootkits, and advanced malware used by an APT group of attackers. Traditionally, memory analysis was solely the domain of Windows internals experts, but the recent development of new tools makes it accessible today to anyone, especially incident responders and threat hunters. Better tools, interfaces and detection heuristics have greatly leveled the playing field. Understanding attack patterns in memory is a core analyst skill applicable across a wide range of endpoint detection and response products. This extremely popular section will introduce some of the most capable tools available and provide you with a solid basis to add foundational and advanced memory forensic skills to your incident response and forensics capabilities.

**Topics:** Memory Acquisition; Memory Forensics Analysis Process for Response and Hunting; Memory Forensics Examinations; Memory Analysis Tools

---

**DAY 3: Intrusion Forensics**

Cyber defenders have a wide variety of tools and artifacts available to identify, hunt, and track adversary activity in a network. Each attacker’s action leaves a corresponding artifact, and understanding what is left behind as footprints can be critical to both red and blue team members. Attacks follow a predictable pattern, and we focus our detective efforts on immutable portions of that pattern. In this section, we cover common attacker tradecraft and discuss the various data sources and forensic tools you can use to identify malicious activity in the enterprise.

**Topics:** Advanced Evidence of Execution Detection; Window Shadow Volume Copy Analysis; Lateral Movement Adversary Tactics, Techniques, and Procedures (TTPs); Event Log Analysis for Incident Responders and Hunters

---

**DAY 4: Timeline Analysis**

Learn advanced incident response and hunting techniques uncovered via timeline analysis directly from the authors who pioneered timeline analysis tradecraft. This section will step you through the two primary methods of building and analyzing timelines created during advanced incident response, threat hunting, and forensic cases. Exercises will show analysts how to create a timeline and also how to introduce the key methods to help you use those timelines effectively in your cases.

**Topics:** Timeline Analysis Overview; Memory Analysis Timeline Creation; Filesystem Timeline Creation & Analysis; Super Timeline Creation and Analysis

---

**DAY 5: Incident Response and Hunting Across the Enterprise – Advanced Adversary and Anti-Forensics Detection**

Over the years, we have observed that many incident responders and threat hunters have a challenging time finding threats without pre-built indicators of compromise or threat intelligence gathered before a breach. This is especially true in APT adversary intrusions. This advanced session will demonstrate techniques used by first responders to identify malware or forensic artifacts when very little information exists about their capabilities or hidden locations. We will discuss techniques to help funnel possibilities down to the candidates most likely to be evil malware trying to hide on the system.

**Topics:** Evolution of Incident Response Scripting; Malware and Anti-Forensic Detection; Anti-Forensic Detection Methodologies; Identifying Compromised Hosts without Active Malware

---

**DAY 6: The APT Incident Response Challenge**

This incredibly rich and realistic enterprise intrusion exercise is based on a real-world advanced persistent threat (APT) group. It brings together techniques learned earlier in the week and tests your newly acquired skills in a case that simulates an attack by an advanced adversary. The challenge brings it all together using a real intrusion into a complete Windows enterprise environment. You will be asked to uncover how the systems were compromised in the initial intrusion, find other systems the adversary moved laterally, and identify intellectual property stolen via data exfiltration. You will walk out of the course with hands-on experience investigating realistic attacks, curated by a cadre of instructors with decades of experience fighting advanced threats from attackers ranging from nation-states to financial crime syndicates and hacktivist groups.

**Topics:** Identification and Scoping; Containment and Threat Intelligence Gathering; Remediation and Recovery

---

**Who Should Attend**

- Incident response team members
- Threat hunters
- Experienced digital forensic analysts
- Information security professionals
- Federal agents and law enforcement personnel
- Red team members, penetration testers, and exploit developers
- SANS FOR500 and SEC504 graduates

---

“Extremely useful module! Lots of technical information was covered that I can implement immediately!”

-Jon Bentley, Leidos

---

“In one day I have learned more about running an incident investigation than I have in many months of independent study.”

-Ryan Jones, Baker Hughes GE
Digital forensic investigators have traditionally dealt with Windows machines, but what if they find themselves in front of a new Apple Mac or iDevice? The increasing popularity of Apple devices can be seen everywhere, from coffee shops to corporate boardrooms, yet most investigators are familiar with Windows-only machines.

Times and trends change and forensic investigators and analysts need to change with them. The new FOR518: Mac Forensic Analysis course provides the tools and techniques necessary to take on any Mac case without hesitation. The intense, hands-on forensic analysis skills taught in the course will enable Windows-based investigators to broaden their analysis capabilities and have the confidence and knowledge to comfortably analyze any Mac or iOS system.

This course will teach you:

- Mac and iOS Fundamentals: How to analyze and parse the Hierarchical File System (HFS+) by hand and recognize the specific domains of the logical file system and Mac-specific file types.
- User Activity: How to understand and profile users through their data files and preference configurations.
- Advanced Analysis and Correlation: How to determine how a system has been used or compromised by using the system and user data files in correlation with system log files.
- Apple Technologies: How to understand and analyze many Mac and iOS specific technologies, including Time Machine, Spotlight, iCloud, Document Versions, FileVault, Continuity, and FaceTime.

FOR518: Mac Forensic Analysis aims to form a well-rounded investigator by introducing Mac and iOS forensics into a Windows-based forensics world. This course focuses on topics such as the HFS+ file system, Mac-specific data files, tracking of user activity, system configuration, analysis and correlation of Mac logs, Mac applications, and Mac-exclusive technologies. A computer forensic analyst who successfully completes the course will have the skills needed to take on a Mac or iOS forensics case.

FORENSICATE DIFFERENTLY!

“[FOR518] is valuable in providing me with foundational knowledge of the file system and artifacts.”
- Kevin Neely, Pure Storage

Sarah Edwards
SANS Certified Instructor

A self-described Mac nerd, Sarah Edwards is a forensic analyst, author, speaker, and both author and instructor of SANS FOR518: Mac Forensic Analysis. She has been a devoted user of Apple devices for many years and has worked specifically in Mac forensics since 2004, carving out a niche for herself when this area of forensics was still new. Although Sarah appreciates digital forensics in all platforms, she has a passion for working within Apple environments and is well known for her work with cutting-edge Mac OS X and iOS, and for her forensic file system expertise. Sarah has more than 12 years of experience in digital forensics, and her passion for teaching is fueled by the ever-increasing presence of Mac devices in today’s digital forensic investigations. Sarah has worked with federal law enforcement agencies on a variety of high-profile investigations in such areas as computer intrusions, criminal cases, counter-intelligence, counter-narcotics, and counter-terrorism. Her research and analytical interests include Mac forensics, mobile device forensics, digital profiling, and malware reverse engineering.
Course Day Descriptions

**DAY 1: Mac and iOS Essentials**
This section introduces the student to Mac and iOS essentials such as acquisition, timestamps, logical file system, and disk structure. Acquisition fundamentals are the same with Mac and iOS devices, but there are a few tips and tricks that can be used to successfully and easily collect Mac and iOS systems for analysis. Students comfortable with Windows forensic analysis can easily learn the slight differences on a Mac system – the data are the same, only the format differs.
**Topics:** Apple Essentials; Mac Essentials and Acquisition; Disks & Partitions; iOS Essentials; iOS Acquisition; iOS Backups

**DAY 2: File Systems & System Triage**
The building blocks of Mac and iOS forensics start with a thorough understanding of the HFS+. Utilizing a hex editor, students will learn the basic principles of the primary file system implemented on Mac OS X systems. The students will then use that information to look at a variety of great artifacts that use the file system and that are different from other operating systems students have seen in the past. Rounding out the day, students will review Mac and iOS triage data.
**Topics:** HFS+ File System; Extended Attributes; File System Events Store Database; Spotlight; Portable Artifacts; Mac and iOS Triage; Most Recently Used (MRU)

**DAY 3: User Data, System Configuration, and Log Analysis**
This section contains a wide area of information that can be used to profile and understand how individuals use their computers. The logical Mac file system is made up of four domains: User, Local, System, and Network. The User Domain contains most of the user-related items of forensic interest. This domain consists of user preferences and configurations. The System and Local Domains contain system-specific information such as application installation, system settings and preferences, and system logs. This section details basic system information, GUI preferences, and system application data. A basic analysis of system logs can give a good understanding of how a system was used or abused. Timeline analysis tells the story of how the system was used. Each entry in a log file has a specific meaning and may be able to tell how the user interacted with the computer. The log entries can be correlated with other data found on the system to create an in-depth timeline that can be used to solve cases quickly and efficiently. Analysis tools and techniques will be used to correlate the data and help the student put the story back together in a coherent and meaningful way.
**Topics:** User Data and System Configuration; Log Parsing and Analysis; Timeline Analysis and Data Correlation

**DAY 4: Application Data Analysis**
In addition to all the configuration and preference information found in the User Domain, the user can interact with a variety of native Apple applications, including the Internet, email, communication, photos, locational data, etc. These data can provide analysts with the who, what, where, why, and how for any investigation. This section will explore the various databases and other files where data are being stored. The student will be able to parse this information by hand without the help of a commercial tool parser.
**Topics:** Application Permissions; Native Application Fundamentals; Safari Browser; Apple Mail; Communication; Calendar and Reminders; Contacts; Notes; Photos; Maps; Location Data; Random Apps; Apple Watch; Third-Party Apps

**DAY 5: Advanced Analysis Topics**
Mac systems implement some technologies that are available only to those with Mac and iOS devices. These include data backup with Time Machine, Document Versions, and iCloud, and disk encryption with FileVault. Other advanced topics include data hidden in encrypted containers, live response, Mac intrusion and malware analysis, and Mac memory analysis.
**Topics:** Live Response; Time Machine; OS X Malware and Intrusion Analysis; iCloud; Versions; Memory Acquisitions and Analysis; Password Cracking and Encrypted Containers

**DAY 6: Mac Forensics & Incident Response Challenge**
Students will put their new Mac forensics skills to the test by running through a real-life scenario with team members.
**Topics:** In-Depth HFS+ File System Examination; File System Timeline Analysis; Advanced Computer Forensics Methodology; Mac Memory Analysis; File System Data Analysis; Metadata Analysis; Recovering Key Mac Files; Volume and Disk Image Analysis; Analysis of Mac Technologies including Time Machine, Spotlight, and FileVault; Advanced Log Analysis and Correlation; iDevice Analysis and iOS Artifacts

---
**Who Should Attend**
- Experienced digital forensic analysts who want to solidify and expand their understanding of file system forensics and advanced Mac analysis
- Law enforcement officers, federal agents, and detectives who want to master advanced computer forensics and expand their investigative skill set
- Media exploitation analysts who need to know where to find the critical data they need from a Mac system
- Incident response team members who are responding to complex security incidents and/or intrusions from sophisticated adversaries and need to know what to do when examining a compromised system
- Information security professionals who want to become knowledgeable with Mac OS X and iOS system internals
- SANS FOR500, FOR508, FOR526, FOR585, and FOR610 alumni looking to round out their forensic skills

---
**“This course provides good, clear training on Mac OS/iOS and how they relate/differ in several aspects and is a must for anyone carrying out forensic analysis today.”**

- Ian Spence, MOD

---
For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/sansfire/courses](http://www.sans.org/sansfire/courses)
FOR526: Advanced Memory Forensics & Threat Detection

What You Will Receive

- SIFT Workstation 3
- Windows 8.1 Workstation with license
- 32 GB Course USB 3.0
- SANS Memory Forensics Exercise Workbook
- MP3 audio files of the complete course lecture

FOR526: Memory Forensics In-Depth will teach you:

- Proper Memory Acquisition: Demonstrate targeted memory capture ensuring data integrity and overcoming obstacles to acquisition/anti-acquisition behaviors
- How to Find Evil in Memory: Detect rogue, hidden, and injected processes, kernel-level rootkits, Dynamic Link Libraries (DLL) hijacking, process hollowing, and sophisticated persistence mechanisms
- Effective Step-by-Step Memory Analysis Techniques: Use process timelining, high-low level analysis, and walking the Virtual Address Descriptors (VAD) tree to spot anomalous behavior
- Best Practice Techniques: Learn when to implement triage, live system analysis, and alternative acquisition techniques and how to devise custom parsing scripts for targeted memory analysis

MALWARE CAN HIDE, BUT IT MUST RUN

Digital Forensics and Incident Response (DFIR) professionals need Windows memory forensics training to be at the top of their game. Investigators who do not look at volatile memory are leaving evidence at the crime scene. RAM content holds evidence of user actions, as well as evil processes and furtive behaviors implemented by malicious code. It is this evidence that often proves to be the smoking gun that unravels the story of what happened on a system.

FOR526: Memory Forensics In-Depth provides the critical skills necessary for digital forensics examiners and incident responders to successfully perform live system memory triage and analyze captured memory images. The course uses the most effective freeware and open-source tools in the industry today and provides an in-depth understanding of how these tools work. FOR526 is a critical course for any serious DFIR investigator who wants to tackle advanced forensics, trusted insider, and incident response cases.

In today’s forensics cases, it is just as critical to understand memory structures as it is to understand disk and registry structures. Having in-depth knowledge of Windows memory internals allows the examiner to access target data specific to the needs of the case at hand. For those investigating platforms other than Windows, this course also introduces OSX and Linux memory forensics acquisition and analysis using hands-on lab exercises.

There is an arms race between analysts and attackers. Modern malware and post-exploitation modules increasingly employ self-defense techniques that include more sophisticated rootkit and anti-memory analysis mechanisms that destroy or subvert volatile data. Examiners must have a deeper understanding of memory internals in order to discern the intentions of attackers or rogue trusted insiders. FOR526 draws on best practices and recommendations from experts in the field to guide DFIR professionals through acquisition, validation, and memory analysis with real-world and malware-laden memory images.

FOR526: Memory Forensics In-Depth provides the critical skills necessary for digital forensics examiners and incident responders to successfully perform live system memory triage and analyze captured memory images. The course uses the most effective freeware and open-source tools in the industry today and provides an in-depth understanding of how these tools work. FOR526 is a critical course for any serious DFIR investigator who wants to tackle advanced forensics, trusted insider, and incident response cases.

FOR526: Memory Forensics In-Depth will teach you:

- Proper Memory Acquisition: Demonstrate targeted memory capture ensuring data integrity and overcoming obstacles to acquisition/anti-acquisition behaviors
- How to Find Evil in Memory: Detect rogue, hidden, and injected processes, kernel-level rootkits, Dynamic Link Libraries (DLL) hijacking, process hollowing, and sophisticated persistence mechanisms
- Effective Step-by-Step Memory Analysis Techniques: Use process timelining, high-low level analysis, and walking the Virtual Address Descriptors (VAD) tree to spot anomalous behavior
- Best Practice Techniques: Learn when to implement triage, live system analysis, and alternative acquisition techniques and how to devise custom parsing scripts for targeted memory analysis

MALWARE CAN HIDE, BUT IT MUST RUN

Alissa Torres
SANS Principal Instructor

Alissa has more than 15 years of experience in computer and network security spanning government, academic, and corporate environments. She has the deep experience and technical savvy to take on even the most difficult computer forensics challenges that come her way. Her current role as an incident response advisor at Cargill provides daily challenges “in the trenches” and demands constant technical growth. Alissa is also founder of her own firm, Sibertor Forensics, and has taught internationally in more than 10 countries. Alissa has a B.S. from the University of Virginia and a M.S. in information technology from the University of Maryland. She is a GIAC Certified Forensic Analyst (GCFA), and holds the GCFE, GCIH, GSEC, CISSP®, and EnCE certifications. Alissa has served as a member of the GIAC Advisory Board since 2013 and was recognized by SC Magazine as one of its “2016 Women to Watch.”

@sibertor
### Course Day Descriptions

<table>
<thead>
<tr>
<th>Day</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DAY 1: Foundations in Memory Analysis and Acquisition</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Simply put, memory analysis has become a required skill for all incident responders and digital forensics examiners. Regardless of the type of investigation, system memory and its contents often expose the first piece of the evidential thread that, when pulled, unravels the whole picture of what happened on the target system. Where is the malware? How did the machine get infected? Where did the attacker move laterally? Or what did the disgruntled employee do on the system? What lies in physical memory can provide answers to all of these questions and more.</td>
</tr>
<tr>
<td></td>
<td><strong>Topics:</strong> Why Memory Forensics?; Investigative Methodologies; The Ubuntu SIFT and Windows 8.1 Workstations; The Volatility Framework; System Architectures; Triage versus Full Memory Acquisition; Physical Memory Acquisition</td>
</tr>
<tr>
<td><strong>DAY 2: Unstructured Analysis and Process Exploration</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Structured memory analysis using tools that identify and interpret operating system structures is certainly powerful. However, many remnants of previously allocated memory remain available for analysis, and they cannot be parsed through structure identification. What tools are best for processing fragmented data? Unstructured analysis tools! They neither know nor care about operating system structures. Instead, they examine data, extracting findings using pattern matching. You will learn how to use Bulk Extractor to parse memory images and extract investigative leads such as email addresses, network packets, and more.</td>
</tr>
<tr>
<td></td>
<td><strong>Topics:</strong> Unstructured Memory Analysis; Page File Analysis; Exploring Process Structures; List Walking and Scanning; Pool Memory; Exploring Process Relationships; Exploring DLLs; Kernel Objects</td>
</tr>
<tr>
<td><strong>DAY 3: Investigating the User via Memory Artifacts</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>An incident responder (IR) is often asked to triage a system because of a network intrusion detection system alert. The Security Operations Center makes the call and requires more information due to outbound network traffic from an endpoint and the IR team is asked to respond. In this section, we cover how to enumerate active and terminated TCP connections – selecting the right plugin for the job based on the OS version.</td>
</tr>
<tr>
<td></td>
<td><strong>Topics:</strong> Network Connections; Virtual Address Descriptors; Detecting Injected Code; Analyzing the Registry via Memory Analysis; User Artifacts in Memory</td>
</tr>
<tr>
<td><strong>DAY 4: Internal Memory Structures</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Day 4 focuses on introducing some internal memory structures (such as drivers), Windows memory table structures, and extraction techniques for portable executables. As we come to the final steps in our investigative methodology, &quot;Spotting Rootkit Behaviors&quot; and &quot;Extracting Suspicious Binaries,&quot; it is important to emphasize again the rootkit paradox. The more malicious code attempts to hide itself, the more abnormal and seemingly suspicious it appears. We will use this concept to evaluate some of the most common structures in Windows memory for hooking, the IDTs and SSDTs.</td>
</tr>
<tr>
<td></td>
<td><strong>Topics:</strong> Interrupt Descriptor Tables; System Service Descriptor Tables; Drivers; Direct Kernel Object Manipulation; Module Extraction; Hibernation Files; Crash Dump Files</td>
</tr>
<tr>
<td><strong>DAY 5: Memory Analysis on Platforms Other than Windows</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows systems may be the most prevalent platform encountered by forensic examiners today, but most enterprises are not homogeneous. Forensic examiners and incident responders are best served by having the skills to analyze the memory of multiple platforms, including Linux and Mac—that is, platforms other than Windows.</td>
</tr>
<tr>
<td></td>
<td><strong>Topics:</strong> Linux Memory Acquisition and Analysis, Mac Memory Acquisition and Analysis</td>
</tr>
<tr>
<td><strong>DAY 6: Memory Analysis Challenge</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This final course section provides students with a direct memory forensics challenge that makes use of the SANS NetWars Tournament platform. Your memory analysis skills are put to the test with a variety of hands-on scenarios involving hibernation files, Crash Dump files, and raw memory images, reinforcing techniques covered in the first five sections of the course. These challenges strengthen students’ ability to respond to typical and atypical memory forensics challenges from all types of cases, from investigating the user to isolating the malware. By applying the techniques learned earlier in the course, students consolidate their knowledge and can shore up skill areas where they feel they need additional practice.</td>
</tr>
<tr>
<td></td>
<td><strong>Topics:</strong> Malware and Rootkit Behavior Detection; Persistence Mechanism Identification; Code Injection Analysis; User Activity Reconstruction; Linux Memory Image Parsing; Mac OSX Memory Image Parsing; Windows Hibernation File Conversion and Analysis; Windows Crash Dump Analysis (Using Windows Debugger)</td>
</tr>
</tbody>
</table>

**Who Should Attend**

- Incident response team members
- Experienced digital forensic analysts
- Red team members, penetration testers, and exploit developers
- Law enforcement officers, federal agents, and detectives
- SANS FOR508 and SEC504 graduates
- Forensics investigators

---

**“The training opened my eyes to the need to collect memory images, as well as physical images for single computer analysis, such as theft of IP or other employee investigations.”**

- Greg Caouette, Kroll

---

**“This training is a must to cover the foundations of memory forensics and be efficient at it. Very recommended.”**

- Hugo Gabignon, Amazon.com

---

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/sansfire/courses](http://www.sans.org/sansfire/courses)

---

**NEW! Evening bootcamp sessions; hands-on labs**
FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

You Will Be Able To
- Extract files from network packet captures and proxy cache files, allowing for follow-on malware analysis or definitive data loss determination
- Use historical NetFlow data to identify relevant past network occurrences, allowing for accurate incident scoping
- Reverse-engineer custom network protocols to identify an attacker’s command-and-control abilities and actions
- Decrypt captured SSL traffic to identify attackers’ actions and what data they extracted from the victim
- Use data from typical network protocols to increase the fidelity of the investigation’s findings
- Identify opportunities to collect additional evidence based on the existing systems and platforms within a network architecture
- Examine traffic using common network protocols to identify patterns of activity or specific actions that warrant further investigation
- Incorporate log data into a comprehensive analytic process, filling knowledge gaps that may be far in the past
- Learn how attackers leverage man-in-the-middle tools to intercept seemingly secure communications
- Examine proprietary network protocols to determine what actions occurred on the endpoint systems
- Analyze wireless network traffic to find evidence of malicious activity
- Learn how to modify configuration on typical network devices such as firewalls and intrusion detection systems to increase the intelligence value of their logs and alerts during an investigation

Philip Hagen
SANS Senior Instructor

FIGHT CRIME. UNRAVEL INCIDENTS...ONE BYTE (OR PACKET) AT A TIME.

Take your system-based forensic knowledge onto the wire. Incorporate network evidence into your investigations, provide better findings, and get the job done faster.

It is exceedingly rare to work any forensic investigation that doesn’t have a network component. Endpoint forensics will always be a critical and foundational skill for this career, but overlooking their network communications is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, employee misuse scenario, or are engaged in proactive adversary discovery, the network often provides an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, uncover attackers that have been active for months or longer, or even prove useful in definitively proving a crime actually occurred.

FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response was built from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. We focus on the knowledge necessary to expand the forensic mindset from residual data on the storage media from a system or device to the transient communications that occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero. Put another way: Bad guys are talking – we’ll teach you to listen.

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will cover the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap exploration, ancillary network log examination, and more. We cover how to leverage existing infrastructure devices that may contain months or years of valuable evidence as well as how to place new collection platforms while an incident is already under way.

Whether you are a consultant responding to a client’s site, a law enforcement professional assisting victims of cybercrime and seeking prosecution of those responsible, an on-staff forensic practitioner, or a member of the growing ranks of “threat hunters,” this course offers hands-on experience with real-world scenarios that will help take your work to the next level.

The hands-on labs in this class cover a wide range of tools and platforms, including the venerable tcpdump and Wireshark for packet capture and analysis; NetworkMiner for artifact extraction; and open-source tools including nfdump, tcpxtract, tcpflow, and more. Newly added tools in the course include the SOF-ELK platform, a VMware appliance pre-configured with the ELK stack. This “big data” platform includes the Elasticsearch storage and search database, the Logstash ingest and parse utility, and the Kibana graphical dashboard interface. Together with the custom SOF-ELK configuration files, the platform gives forensicators a ready-to-use platform for log and NetFlow analysis. For full-packet analysis and hunting at scale, the Moloch platform is also used. Through all of the in-class labs, your shell scripting abilities will also be used to make easy work of ripping through hundreds and thousands of data records.

Phil Hagen began his studies at the U.S. Air Force Academy’s Computer Science Department, where he focused on network security and was an inaugural member of the computer security extracurricular group. He served in the Air Force as a communications officer at Beale AFB and the Pentagon. Today, Phil’s career has spanned the full attack life cycle – tool development, deployment, operations, and the investigative aftermath – giving him rare and deep insight into the artifacts left behind. Phil has covered deep technical tasks, managed an entire computer forensic services portfolio, and handled executive responsibilities. He’s supported systems that demanded 24x7x365 functionality, managed a team of 85 computer forensic professionals in the national security sector, and provided forensic consulting services for law enforcement, government, and commercial clients. All of that brings Phil to his role today as the DFIR strategist at Red Canary, where he supports the firm’s managed threat detection service. Phil also spends time developing and maintaining the SOF-ELK distribution, a virtual appliance free for the DFIR Community.

@PhilHagen
For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/sansfire/courses

Course Day Descriptions

**Day 1: Off the Disk and Onto the Wire**
Network data can be preserved, but only if captured directly from the wire. Whether tactical or strategic, packet capture methods are quite basic. You will re-acquaint yourself with tcpdump and Wireshark, the most common tools used to capture and analyze network packets, respectively. However, since long-term full-packet capture is still uncommon in most environments, many artifacts that can tell us about what happened on the wire in the past come from devices that manage network functions. You will learn about what kinds of devices can provide valuable evidence and at what level of granularity. We will walk through collecting evidence from one of the most common sources of network evidence—a web proxy server—then go hands-on to find and extract stolen data from the proxy yourself.

**Topics:** Web Proxy Server Examination; Foundational Network Forensics Tools: tcpdump and Wireshark; Network Evidence Acquisition; Network Architectural Challenges and Opportunities

**Day 2: Core Protocols & Log Aggregation/Analysis**
There are thousands of protocols that may be in use within a production network environment. We will cover several of these that are most likely to benefit the forensicator in typical casework, as well as several that help demonstrate analysis methods useful when facing new, undocumented, or proprietary protocols. By learning the “typical” behaviors of these protocols, we can more readily identify anomalies that may suggest an adversary is misusing that protocol for nefarious purposes. These protocol artifacts and anomalies can be profiled through direct traffic analysis as well as through the log evidence created by systems that have control or purview of that traffic. While this affords the investigator with vast opportunities to analyze the network traffic, efficient analysis of large quantities of source data generally requires tools and methods designed to scale.

**Topics:** Hypertext Transfer Protocol (HTTP): Protocol and Logs; Domain Name Service (DNS): Protocol and Logs; Firewalls, Intrusion Detection System, and Network Security Monitoring Logs; Logging Protocol and Aggregation; ELK Stack and the SOF-ELK Platform

**Day 3: NetFlow and File Access Protocols**
Network connection logging, commonly called NetFlow, may be the single most valuable source of evidence in network investigations. Many organizations have extensive archives of flow data due to its minimal storage requirements. Since NetFlow does not capture any content of the transmission, many legal issues with long-term retention are mitigated. Even without content, NetFlow provides an excellent means of guiding an investigation and characterizing an adversary’s activities from pre-attack through operations. Whether within a victim’s environment or for data exfiltration, adversaries must move their quarry around through the use of various file access protocols. By knowing some of the more common file access and transfer protocols, a forensicator can quickly identify an attacker’s theft actions.

**Topics:** NetFlow Collection and Analysis; Open-Source Flow Tools; File Transfer Protocol (FTP); Microsoft Protocols

**Day 4: Commercial Tools, Wireless, and Full-Packet Hunting**
Commercial tools are a mainstay in the network forensicator’s toolkit. We’ll explore the various roles that commercial tools generally fill, as well as how they can be best integrated into an investigative workflow. With the runaway adoption of wireless networking, investigators must also be prepared to address the unique challenges this technology brings to the table. However, regardless of the protocol being examined or budget used to perform the analysis, having a means of exploring full-packet capture is a necessity, and having a toolkit to perform this at scale is critical.

**Topics:** Simple Mail Transfer Protocol (SMTP); Commercial Network Forensics; Wireless Network Forensics; Automated Tools and Libraries; Full-Packet Hunting with Moloch

**Day 5: Encryption, Protocol Reversing, OPSEC, and Intel**
Advancements in common technology have made it easier to be a bad guy and harder for us to track them. Strong encryption methods are readily available and custom protocols are easy to develop and deploy. Despite this, there are still weaknesses even in the most advanced adversaries’ methods. As we learn what the attackers have deliberately hidden from us, we must operate carefully to avoid tipping our hats regarding the investigative progress—or the attacker can quickly pivot, nullifying our progress.

**Topics:** Encoding, Encryption, and SSL; Man in the Middle; Network Protocol Reverse Engineering; Investigation OPSEC and Threat Intel

**Day 6: Network Forensics Capstone Challenge**
This section will combine all of what you have learned prior to and during this week. In groups, you will examine network evidence from a real-world compromise by an advanced attacker. Each group will independently analyze data, form and develop hypotheses, and present findings. No evidence from endpoint systems is available—only the network and its infrastructure.

**Topics:** Network Forensic Case

---

“**The advanced network forensics course provides a great deal of valuable training in an important field.**”

- Paul Lee, Cisco

“**Good perspective of finding malicious behavior on a network— all around great content.**”

- Trent Bennett, Adobe
FOR578: Cyber Threat Intelligence

Security practitioners should attend FOR578: Cyber Threat Intelligence because it is unlike any other technical training. It focuses on structured analysis in order to establish a solid foundation for any security skillset and to amplify existing skills. The course will help practitioners from across the security spectrum to:

- Develop analysis skills to better comprehend, synthesize, and leverage complex scenarios
- Identify and create intelligence requirements through practices such as threat modeling
- Understand and develop skills in tactical, operational, and strategic-level threat intelligence
- Generate threat intelligence to detect, respond to, and defeat focused and targeted threats
- Learn about the different sources from which to collect adversary data and how to exploit and pivot off of those data
- Validate information received externally to minimize the costs of bad intelligence
- Create Indicators of Compromise (IOCs) in formats such as YARA, OpenIOC, and STIX
- Move security maturity past IOCs into understanding and countering the behavioral tradecraft of threats
- Establish structured analytical techniques to be successful in any security role

It is common for security practitioners to call themselves analysts. But how many of us have taken structured analysis training instead of simply attending technical training? Both are important, but very rarely do analysts focus on training on analytical ways of thinking. This course exposes analysts to new mindsets, methodologies, and techniques that will complement their existing knowledge as well as establish new best practices for their security teams. Proper analysis skills are key to the complex world that defenders are exposed to on a daily basis.

The analysis of an adversary’s intent, opportunity, and capability to do harm is known as cyber threat intelligence. Intelligence is not a data feed, nor is it something that comes from a tool. Intelligence is actionable information that answers a key knowledge gap, pain point, or requirement of an organization. This collection, classification, and exploitation of knowledge about adversaries gives defenders an upper hand against adversaries and forces defenders to learn and evolve with each subsequent intrusion they face.

Cyber threat intelligence thus represents a force multiplier for organizations looking to establish or update their response and detection programs to deal with increasingly sophisticated threats. Malware is an adversary’s tool, but the real threat is the human one, and cyber threat intelligence focuses on countering those flexible and persistent human threats with empowered and trained human defenders.

Knowledge about the adversary is core to all security teams. The red team needs to understand adversaries’ methods in order to emulate their tradecraft. The Security Operations Center needs to know how to prioritize intrusions and quickly deal with those that need immediate attention. The incident response team needs actionable information on how to quickly scope and respond to targeted intrusions. The vulnerability management group needs to understand which vulnerabilities matter most for prioritization and the risk that each one presents. The threat hunting team needs to understand adversary behaviors to search out new threats.

In other words, cyber threat intelligence informs all security practices that deal with adversaries. FOR578: Cyber Threat Intelligence will equip you, your security team, and your organization with the tactical, operational, and strategic-level cyber threat intelligence skills and tradecraft required to better understand the evolving threat landscape and to accurately and effectively counter those threats.

Robert M. Lee
SANS Certified Instructor

“Excellent course. Great stepping stone into the field of cyber threat intelligence.”
-Abdulrahman Alsuhaimi, Saudi Aramco

Robert is the CEO and founder of his own company, Dragos, Inc., which provides cybersecurity solutions for industrial control system networks. Robert got his start in information security making small control systems (ICS) for humanitarian missions. He joined the U.S. Air Force and became a cyberspace warfare operations officer in the U.S. intelligence community. In that role, he created and led a mission examining nation–states targeting ICS, the first mission of its kind in the U.S. intelligence community. When the Ukraine power grid went down due to a cyber attack in 2015, Robert helped form a specialized team to analyze the event, then passed the information on to the impacted parties as well as the U.S. government and private sector. He and his team also analyzed malware from the 2016 cyber-attack on Ukraine’s Kiev substation and dubbed it CRASHOVERRIDE as the first ever malware tailored to specifically disrupt electricity grid operations. Robert has a master’s degree in cybersecurity and computer forensics from Utica College as well as cyber and warfare training through the U.S. Air Force, and he’s pursuing his doctorate in war studies from King’s College London. He was named one of Forbes’ 30 under 30 in Enterprise Technology in 2016, awarded EnergySec’s 2015 Cyber Security Professional of the Year, and named one of Passcode’s “Influencers.”

@RobertMLee

Who Should Attend
- Security practitioners
- Incident response team members
- Threat hunters
- Security Operations Center personnel and information security practitioners
- Digital forensic analysts and malware analysts
- Federal agents and law enforcement officials
- Technical managers
- SANS alumni looking to take their analytical skills to the next level

FOR578: Cyber Threat Intelligence

5 Day Program
30 CPEs
Laptop Required

EnergySec’s 2015 Cyber Security Professional of the Year, and named one of Passcode’s “Influencers.”

Register at www.sans.org/sansfire | 301-654-SANS (7267)

Robert is the CEO and founder of his own company, Dragos, Inc., which provides cybersecurity solutions for industrial control system networks. Robert got his start in information security making small control systems (ICS) for humanitarian missions. He joined the U.S. Air Force and became a cyberspace warfare operations officer in the U.S. intelligence community. In that role, he created and led a mission examining nation–states targeting ICS, the first mission of its kind in the U.S. intelligence community. When the Ukraine power grid went down due to a cyber attack in 2015, Robert helped form a specialized team to analyze the event, then passed the information on to the impacted parties as well as the U.S. government and private sector. He and his team also analyzed malware from the 2016 cyber-attack on Ukraine’s Kiev substation and dubbed it CRASHOVERRIDE as the first ever malware tailored to specifically disrupt electricity grid operations. Robert has a master’s degree in cybersecurity and computer forensics from Utica College as well as cyber and warfare training through the U.S. Air Force, and he’s pursuing his doctorate in war studies from King’s College London. He was named one of Forbes’ 30 under 30 in Enterprise Technology in 2016, awarded EnergySec’s 2015 Cyber Security Professional of the Year, and named one of Passcode’s “Influencers.”

@RobertMLee

Register at www.sans.org/sansfire | 301-654-SANS (7267)
DAY 1: Cyber Threat Intelligence and Requirements
Cyber threat intelligence is a rapidly growing field. However, intelligence was a profession long before the word “cyber” entered the lexicon. Understanding the key points regarding intelligence terminology, tradecraft, and impact is vital to understanding and using cyber threat intelligence. This section introduces students to the most important concepts of intelligence, analysis tradecraft, and levels of threat intelligence, and the value they can add to organizations. It also focuses on getting your intelligence program off to the right start with planning, direction, and the generation of intelligence requirements. As with all sections, the day includes immersive hands-on labs to ensure that students have the ability to turn theory into practice.

Topics: Case Study: Carbanak, The Great Bank Robbery; Understanding Intelligence; Understanding Cyber Threat Intelligence; Threat Intelligence Consumption; Positioning the Team to Generate Intelligence; Planning and Direction (Developing Requirements)

DAY 2: The Fundamental Skillset: Intrusion Analysis
Intrusion analysis is at the heart of threat intelligence. It is a fundamental skillset for any security practitioner who wants to use a more complete approach to addressing security. Two of the most commonly used models for assessing adversary intrusions are the “kill chain” and the “Diamond Model.” These models serve as a framework and structured scheme for analyzing intrusions and extracting patterns such as adversary behaviors and malicious indicators. In this section students will participate in and be walked through multi-phase intrusions from initial notification of adversary activity to the completion of analysis of the event. The section also highlights the importance of this process in terms of structuring and defining adversary campaigns.

Topics: Primary Collection Source: Intrusion Analysis; Kill Chain Courses of Action; Kill Chain Deep Dive; Handling Multiple Kill Chains; Collection Source: Malware

DAY 3: Collection Sources
Cyber threat intelligence analysts must be able to interrogate and fully understand their collection sources. Analysts do not have to be malware reverse engineers, as an example, but they must at least understand that work and know what data can be sought. This section continues from the previous one in identifying key collection sources for analysts. There is also a lot of available information on what is commonly referred to as open-source intelligence (OSINT). In this course section students will learn to seek and exploit information from Domains, External Datasets, Transport Layer Security/Secure Sockets Layer (TLS/SSL) Certificates, and more while also structuring the data to be exploited for purposes of sharing internally and externally.

Topics: Case Study: Axiom; Collection Source: Domains; Case Study: GlassRAT; Collection Source: External Datasets; Collection Source: TLS Certificates; Case Study: Trickbots; Exploitation: Storing and Structuring Data

DAY 4: Analysis and Dissemination of Intelligence
Many organizations seek to share intelligence but often fail to understand its value, its limitations, and the right formats to choose for each audience. Additionally, indicators and information shared without analysis are not intelligence. Structured analytical techniques such as the Analysis of Competing Hypotheses can help add considerable value to intelligence before it is disseminated. This section will focus on identifying both open-source and professional tools that are available for students as well as on sharing standards for each level of cyber threat intelligence both internally and externally. Students will learn about YARA and generate YARA rules to help incident responders, security operations personnel, and malware analysts. Students will gain hands-on experience with STIX and understand the Cybox and TAXII frameworks for sharing information between organizations. Finally, the section will focus on building the singular intrusions into campaigns and being able to communicate about those campaigns.

Topics: Analysis: Exploring Hypotheses; Analysis: Building Campaigns; Dissemination: Tactical; Case Study: Sony Attack; Dissemination: Operational

DAY 5: Higher-Order Analysis and Attribution
A core component of intelligence analysis at any level is the ability to defeat biases and analyze information. The skills required to think critically are exceptionally important and can have an organization-wide or national-level impact. In this section students will learn about logical fallacies and cognitive biases as well as how to defeat them. They will also learn about nation-state attribution, including when it can be of value and when it is merely a distraction. Students will also learn about nation-state-level attribution from previously identified campaigns and take away a more holistic view of the cyber threat intelligence industry to date. The class will finish with a discussion on consuming threat intelligence and actionable takeaways for students to make significant changes in their organizations once they complete the course.

Topics: Logical Fallacies and Cognitive Biases; Dissemination Strategies; Case Study: Stuxnet; Fine-Tuning Analysis; Case Study: Sofacy; Attribution

“The course invoked discussion from all on real-life use cases, which enriched the course content well.”

-Ryan H., MOD

“Great value focusing on collection of data and modeling and how to use frameworks to build out capabilities.”

-Aaron Bostwick, GA
FOR585: Smartphone Forensic Analysis In-Depth

You Will Be Able To

- Select the most effective forensic tools, techniques, and procedures for critical analysis of smartphone data
- Reconstruct events surrounding a crime using information from smartphones, including manual timeline development and link analysis (e.g., who communicated with whom, where, and when) without relying on a tool
- Understand how smartphone file systems store data, how they differ, and how the evidence will be stored on each device
- Interpret file systems on smartphones and locate information that is not generally accessible to users
- Identify how the evidence got onto the mobile device – we’ll teach you how to know if the user created the data, which will help you avoid the critical mistake of reporting false evidence obtained from tools
- Incorporate manual decoding techniques to recover deleted data stored on smartphones and mobile devices
- Tie a user to a smartphone at a specific date/time and at various locations
- Recover hidden or obfuscated communication from applications on smartphones
- Decrypt or decode application data that are not parsed by your forensic tools
- Detect smartphones compromised by malware and spyware using forensic methods
- Decompile and analyze mobile malware using open-source tools
- Handle encryption on smartphones and bypass, crack, and/or decode lock codes manually recovered from smartphones, including cracking iOS backup files that were encrypted with iTunes

Heather Mahalik
SANS Senior Instructor

FOR585: Smartphone Forensic Analysis In-Depth will help you understand:

- Where key evidence is located on a smartphone
- How the data got onto the smartphone
- How to recover deleted mobile device data that forensic tools miss
- How to decode evidence stored in third-party applications
- How to detect, decompile, and analyze mobile malware and spyware
- Advanced acquisition terminology and free techniques to gain access to data on smartphones
- How to handle locked or encrypted devices, applications, and containers

SMARTPHONES HAVE MINDS OF THEIR OWN. DON’T MAKE THE MISTAKE OF REPORTING SYSTEM EVIDENCE, SUGGESTIONS, OR APPLICATION ASSOCIATIONS AS USER ACTIVITY. IT’S TIME TO GET SMARTER!

A smartphone lands on your desk and you are tasked with determining if the user was at a specific location at a specific date and time. You rely on your forensic tools to dump and parse the data. The tools show location information tying the device to the place of interest. Are you ready to prove the user was at that location? Do you know how to take this further to place the subject at the location of interest at that specific date and time? Tread carefully, because the user may not have done what the tools are showing!

Mobile devices are often a key factor in criminal cases, intrusions, IP theft, security threats, accident reconstruction, and more. Understanding how to leverage the data from the device in a correct manner can make or break your case and your future as an expert. FOR585: Smartphone Forensic Analysis In-Depth will teach you those skills.

Every time the smartphone thinks or makes a suggestion, the data are saved. It’s easy to get mixed up in what the forensic tools are reporting. Smartphone forensics is more than just pressing the find evidence button and getting answers. Your team cannot afford to rely solely on the tools in your lab. You have to understand how to use them correctly to guide your investigation, instead of just letting the tool report what it believes happened on the device. It is impossible for commercial tools to parse everything from smartphones and understand how the data were put on the device. Examination and interpretation of the data is your job and this course will provide you and your organization with the capability to find and extract the correct evidence from smartphones with confidence.

This in-depth smartphone forensic course provides examiners and investigators with advanced skills to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. The course features 27 hands-on labs, a forensic challenge, and a bonus take-home case that allow students to analyze different datasets from smart devices and leverage the best forensic tools, methods, and custom scripts to learn how smartphone data hide and can be easily misinterpreted by forensic tools. Each lab is designed to teach you a lesson that can be applied to other smartphones. You will gain experience with the different data formats on multiple platforms and learn how the data are stored and encoded on each type of smart device. The labs will open your eyes to what you are missing by relying 100% on your forensic tools.

Smartphone technologies are constantly changing, and most forensic professionals are unfamiliar with the data formats for each technology. Take your skills to the next level: it’s time for the good guys to get smarter and for the bad guys to know that their smartphone activity can and will be used against them!

SMARTPHONE DATA CAN’T HIDE FOREVER – IT’S TIME TO OUTSMART THE MOBILE DEVICE!

Heather has worked on high-stress and high-profile cases, investigating everything from child exploitation to Osama Bin Laden’s media. She has helped law enforcement, eDiscovery firms, and the federal government extract and manually decode artifacts used in solving investigations around the world. All told she has more than 34 years of experience in digital forensics, including eight years focused on mobile forensics—there’s hardly a device or platform she hasn’t researched or examined or a commercial tool she hasn’t used. These days Heather is the Director of Forensic Engineering at ManTech CARD. Heather previously led the mobile device team for Basis Technology, where she focused on mobile device exploitation in support of the federal government. She also worked as a forensic examiner at Stroz Friedberg and the U.S. State Department Computer Investigations and Forensics Lab, where she handled a number of high-profile cases. She has also developed and implemented forensic training programs and standard operating procedures.

@HeatherMahalik

Heather Mahalik
SANS Senior Instructor
**Course Day Descriptions**

**DAY 1: Malware Forensics, Smartphone Overview, and SQLite Introduction**

Although smartphone forensic concepts are similar to those of digital forensics, smartphone file system structures differ and require specialized decoding skills to correctly interpret the data acquired from the device. On this first course day, students will apply what they know to smartphone forensic handling, device capabilities, acquisition methods, and SQLite database examination and query development. Students will also become familiar with the forensic tools required to complete comprehensive examinations of smartphone data structures. Malware affects a plethora of smartphone devices. This course section will examine various types of malware, how it exists on smartphones, and how to identify and analyze it. Most commercial smartphone tools help you identify malware, but none of them will allow you to tear down the malware to the level we cover in class. Up to five labs will be conducted on this first day alone!

**Topics:** The SIFT Workstation, Malware and Spyware Forensics; Introduction to Smartphones; Smartphone Handling; Forensic Acquisition Concepts of Smartphones; Smartphone Forensics Tool Overview; JTAG Forensics; Smartphone Components; Introduction to SQLite

**DAY 3: Android Backups and iOS Device Forensics**

Android backups can be created for forensic analysis or by a user. Smartphone examiners need to understand the file structures and how to parse these data. Apple iOS devices contain substantial amounts of data (including deleted records) that can be decoded and interpreted into useful information. Proper handling and parsing skills are needed for bypassing locked iOS devices and correctly interpreting the data. Without iOS instruction, you will be unprepared to deal with the iOS device that will likely be a major component in a forensic investigation.

**Topics:** Android Backup Files; iOS Forensics Overview and Acquisition; iOS File System Structures; iOS Evidentiary Locations; Handling Locked iOS Devices; Traces of User Activity on iOS Devices

**DAY 5: Third-Party Application and Knock-Off Forensics**

This day starts with third-party applications across all smartphones and is designed to teach students how to leverage third-party application data and preference files to support an investigation. The rest of the day focuses heavily on secure chat applications, recovering deleted application data and attachments, mobile browser artifacts, and knock-off phone forensics. The skills learned in this section will provide you with advanced methods for decoding data stored in third-party applications across all smartphones. We will show you what the commercial tools miss and teach you how to recover these artifacts yourself.

**Topics:** Third-Party Applications Overview; Third-Party Application Artifacts; Messaging Applications and Recovering Attachments; Secure Chat Applications; Mobile Browsers; Knock-Off Phone Forensics

**DAY 2: Android Forensics**

Android devices are among the most widely used smartphones in the world, which means they will surely be part of an investigation that will come across your desk. Android devices contain substantial amounts of data that can be decoded and interpreted into useful information. However, without honing the appropriate skills for bypassing locked Androids and correctly interpreting the data stored on them, you will be unprepared for the rapidly evolving world of smartphone forensics.

**Topics:** Android Forensics Overview; Handling Locked Android Devices; Android File System Structures; Android Evidentiary Locations; Traces of User Activity on Android Devices

**DAY 4: iOS Backups, Windows, and BlackBerry 10 Forensics**

iOS backups are extremely common and are found in the cloud and on hard drives. Not only do users create backups, we often find that our best data can be derived from creating an iOS backup for forensic investigation. We realize that not everyone examines BlackBerry and Windows Phone devices, which is why we are focusing primarily on BlackBerry 10, Windows Phone 8 and 10 and application usage. Both the Windows Phone and BlackBerry 10 sections highlight pieces of evidence that can be found on multiple smartphones. BlackBerry smartphones are designed to protect user privacy, but techniques taught on this course day will enable the investigator to go beyond what the tools decode and manually recover data residing in database files of BlackBerry device file systems. The day ends with the students challenging themselves using tools and methods learned throughout the week to recover user data from a wiped Windows Phone before embarking on a BlackBerry 10 lab that covers tying SIM cards and application usage to a device.

**Topics:** iOS Backup File Forensics; Windows Phone/Mobile Forensics; BlackBerry 10 Forensic Overview; BlackBerry 10 File System, Evidentiary Locations, and Forensic Analysis

**DAY 6: Smartphone Forensics Capstone Exercise**

This final course day will test all that you have learned during the course. Working in small groups, students will examine three smartphone devices and solve a scenario relating to a real-world smartphone forensic investigation. Each group will independently analyze the three smartphones, manually decode data, answer specific questions, form an investigation hypothesis, develop a report, and present findings.

---

**Who Should Attend**

- Experienced digital forensic analysts
- Media exploitation analysts
- Information security professionals
- Incident response teams
- Law enforcement officers, federal agents, and detectives
- Accident reconstruction investigators
- IT auditors
- Graduates of SANS SEC575, SEC563, FOR500, FOR508, FOR572, FOR526, FOR610, or FOR518 who want to take their skills to the next level

“With so many security measures put in place by O/S devs and app devs, the analysis techniques taught in this course are an absolute necessity. If the good guys want to stay ahead of the bad guys, this course is a must.”

-Luis Martinez, Westchester District Attorney’s Office

“Really useful to know the differences in the tools used and how to explore and analyze the data in a safe environment.”

-Nageen Mirza, Deloitte
Learn to turn malware inside out! This popular course explores malware analysis tools and techniques in depth. FOR610 training has helped forensic investigators, incident responders, security engineers, and IT administrators acquire the practical skills to examine malicious programs that target and infect Windows systems.

Understanding the capabilities of malware is critical to an organization’s ability to derive threat intelligence, respond to information security incidents, and fortify defenses. This course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and many other freely available tools.

The course begins by establishing the foundation for analyzing malware in a way that dramatically expands upon the findings of automated analysis tools. You will learn how to set up a flexible laboratory to examine the inner workings of malicious software, and how to use the lab to uncover characteristics of real-world malware samples. You will also learn how to redirect and intercept network traffic in the lab to explore the specimen’s capabilities by interacting with the malicious program.

Malware is often obfuscated to hinder analysis efforts, so the course will equip you with the skills to unpack executable files. You will learn how to dump such programs from memory with the help of a debugger and additional specialized tools, and how to rebuild the files’ structure to bypass the packer’s protection. You will also learn how to examine malware that exhibits rootkit functionality to conceal its presence on the system, employing code analysis and memory forensics approaches to examining these characteristics.

FOR610 malware analysis training also teaches how to handle malicious software that attempts to safeguard itself from analysis. You will learn how to recognize and bypass common self-defense measures, including code injection, sandbox evasion, flow misdIRECTION, and other measures.

Hands-on workshop exercises are a critical aspect of this course. They enable you to apply malware analysis techniques by examining malicious software in a controlled and systematic manner. When performing the exercises, you will study the supplied specimens’ behavioral patterns and examine key portions of their code. To support these activities, you will receive pre-built Windows and Linux virtual machines that include tools for examining and interacting with malware.

Who Should Attend

’experienced individuals who have informal experience with and want to learn how to understand key aspects of malicious programs’
‘Technologists who have informally experimented with aspects of malware analysis prior to the course and are looking to formalize and expand their expertise in this area’
‘Forensic investigators and IT practitioners looking to expand their skillsets and learn how to play a pivotal role in the incident response process’

Lenny Zeltser
SANS Senior Instructor

Aptly called the “Yoda” of malware analysis by his students, Lenny Zeltser keeps his eye on the big picture and focuses on the sum of events rather than individual occurrences. He lives by that philosophy and brings it to his job and classroom. A seasoned business and technology leader with extensive information security expertise, Lenny started his professional journey in a variety of technical InfoSec roles before serving as the national lead of the U.S. security consulting practice at a major cloud services provider. Later in his career he oversaw a portfolio of security services at a Fortune 500 technology company. Today, as VP of Products at Minerva Labs, Lenny designs and builds creative anti-malware products. Lenny also developed the Linux toolkit REMnux to make it easier to use a variety of freely available malware analysis tools, many of which run well on Linux but can be difficult to find and install. Lenny earned the prestigious GIAC Security Expert professional designation, and he currently serves on the Board of Directors of the SANS Technology Institute. Lenny holds a bachelor’s degree in computer science from the University of Pennsylvania and a master’s in business administration from MIT Sloan. He is the co-author of four books on malware, network security, and digital forensics.

@lennyzeltser
DAY 1: Malware Analysis Fundamentals
Section one lays the groundwork for malware analysis by presenting the key tools and techniques useful for examining malicious programs. You will learn how to save time by exploring Windows malware in two phases. Behavioral analysis focuses on the program’s interactions with its environment, such as the registry, the network, and the file system. Code analysis focuses on the specimen’s code and makes use of a disassembler and debugger tools such as IDA Pro and OllyDbg. You will learn how to set up a flexible laboratory to perform such analysis in a controlled manner, and set up such a lab on your laptop using the supplied Windows and Linux (REnux) virtual machines. You will then learn how to use the key analysis tools by examining a malware sample in your lab—with guidance and explanations from the instructor—to reinforce the concepts discussed throughout the day.

Topics: Assembling a Toolkit for Effective Malware Analysis; Examining Static Properties of Suspicious Programs; Performing Behavioral Analysis of Malicious Windows Executables; Performing Static and Dynamic Code Analysis of Malicious Windows Executables; Interacting with Malware in a Lab to Derive Additional Behavioral Characteristics

DAY 2: Reversing Malicious Code
Section two focuses on examining malicious Windows executables at the assembly level. You will discover approaches for studying inner workings of a specimen by looking at it through a disassembler and, at times, with the help of a debugger. The section begins with an overview of key code-reversing concepts and presents a primer on essential x86 intel assembly concepts, such as instructions, function calls, variables, and jumps. You will also learn how to examine common assembly constructs, such as functions, loops, and conditional statements. The material will then build on this foundation and expand your understanding to incorporate 64-bit malware, given its growing popularity. Throughout the discussion, you will learn to recognize common characteristics at a code level, including HTTP command and control, keylogging, and command execution.

Topics: Understanding Core x86 Assembly Concepts to Perform Malicious Code Analysis; Identifying Key Assembly Logic Structures with a Disassembler; Following Program Control Flow to Understand Decision Points During Execution; Recognizing Common Malware Characteristics at the Windows API Level (Registry Manipulation, Keylogging, HTTP Communications, Droppers); Extending Assembly Knowledge to Include x64 Code Analysis

DAY 3: Malicious Web and Document Files
Section three focuses on examining malicious web pages and documents, which adversaries can use to directly perform malicious actions on the infected system and launch attacks that lead to the installation of malicious executable files. The section begins by discussing how to examine suspicious websites that might host client-side exploits. Next, you will learn how to de-obfuscate malicious scripts with the help of script debuggers and interpreters, examine Microsoft Office macros, and assess the threats associated with PDF and RTF files using several techniques.

Topics: Interacting with Malicious Websites to Assess the Nature of Their Threats; De-obfuscating Malicious JavaScript Using Debuggers and Interpreters; Analyzing Suspicious PDF Files; Examining Malicious Microsoft Office Documents, Including Files with Macros; Analyzing Malicious RTF Document Files

DAY 4: In-Depth Malware Analysis
Section four builds on the approaches to behavioral and code analysis introduced earlier in the course, exploring techniques for uncovering additional aspects of the functionality of malicious programs. The section begins by discussing how to handle packed malware. We will examine ways to identify packers and strip away their protection with the help of a debugger and other utilities. We will also walk through the analysis of malware that employs multiple technologies to conceal its true nature, including the use of registry, obfuscated JavaScript and PowerShell scripts, and shellcode. Finally, we will learn how malware implements Usermode rootkit functionality to perform code injection and API hooking, examining this functionality from both code and memory forensics perspectives.

Topics: Recognizing Packed Malware; Getting Started with Unpacking; Using Debuggers for Dumping Packed Malware from Memory; Analyzing Multi-Technology and Fileless Malware; Code Injection and API Hooking; Using Memory Forensics for Malware Analysis

DAY 5: Examining Self-Defending Malware
Section five takes a close look at the techniques malware authors commonly employ to protect malicious software from being examined. You will learn how to recognize and bypass anti-analysis measures designed to slow you down or misdirect you. In the process, you will gain more experience performing static and dynamic analysis of malware that is able to unpack or inject itself into other processes. You will also expand your understanding of how malware authors safeguard the data that they embed inside malicious executables. As with the other topics covered throughout the course, you will be able to experiment with such techniques during hands-on exercises.

Topics: Analyzing Malicious Microsoft Office (Word, Excel, PowerPoint) Documents; Analyzing Malicious Adobe PDF Documents; Analyzing Memory to Assess Malware Characteristics and Reconstruct Infection Artifacts; Using Memory Forensics to Analyze Rootkit Infections

DAY 6: Malware Analysis Tournament
Section six assigns students to the role of a malware analyst working as a member of an incident response or forensics team. Students are presented with a variety of hands-on challenges involving real-world malware in the context of a fun tournament. These challenges further a student’s ability to respond to typical malware-reversing tasks in an instructor-led lab environment and offer additional learning opportunities. Moreover, the challenges are designed to reinforce skills covered in the first five sections of the course, making use of the hugely popular SANS NetWars tournament platform. By applying the techniques learned earlier in the course, students solidify their knowledge and can shore up skill areas where they feel they need additional practice. Students who score the highest in the malware analysis challenge will be awarded the coveted SANS Lethal Forensicator coin.

Topics: Behavioral Malware Analysis; Dynamic Malware Analysis (Using a Debugger); Static Malware Analysis (Using a Disassembler); JavaScript Deobfuscation, PDF Document Analysis; Office Document Analysis, Memory Analysis

“The theory of this course in combination with the labs is a great introduction for the possibilities and approaches one can take when fighting malware.”

-Max de Bruijn, Fox-IT

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/sansfire/courses

73
MGT414: SANS Training Program for CISSP® Certification

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that is specifically designed to prepare students to successfully pass the CISSP® exam. MGT414 focuses solely on the eight domains of knowledge as determined by (ISC)² that form a critical part of the CISSP® exam. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

You Will Be Able To

- Understand the eight domains of knowledge that are covered on the CISSP® exam
- Analyze questions on the exam and be able to select the correct answer
- Apply the knowledge and testing skills learned in class to pass the CISSP® exam
- Understand and explain all of the concepts covered in the eight domains of knowledge
- Apply the skills learned across the eight domains to solve security problems when you return to work

After completing the course students will have:

- Detailed coverage of the eight domains of knowledge
- The analytical skills required to pass the CISSP® exam
- The technical skills required to understand each question
- The foundational information needed to become a Certified Information Systems Security Professional (CISSP®)

External Product Notice:
The CISSP® exam itself is not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam. Please note as well that the GISP exam offered by GIAC is NOT the same as the CISSP® exam offered by (ISC)².

“You [course] really pulls a lot together for me and it has been hugely valuable. I know parts of this are going to impact my approach to my work from the first day back.”
- Merewyn Boak, Apple

Eric Conrad is the lead author of the book The CISSP® Study Guide. Eric’s career began in 1991 as a UNIX systems administrator for a small oceanographic communications company. He gained information security experience in a variety of industries, including research, education, power, Internet, and healthcare. He is now president of Backshore Communications, a company focusing on intrusion detection, incident handling, information warfare, and penetration testing. He is a graduate of the SANS Technology Institute with a master of science degree in information security engineering. In addition to the CISSP®, he holds the prestigious GIAC Security Expert (GSE) certification as well as the GPEN, GCIH, GCIA, GCFA, GAWN, and GSEC certifications. Eric also blogs about information security at ericconrad.com.

@eric_conrad
Course Day Descriptions

**DAY 1: Introduction; Security and Risk Management**

On the first day of training for the CISSP® exam, MGT414 introduces the specific requirements needed to obtain certification. The exam update will be discussed in detail. We will cover the general security principles needed to understand the eight domains of knowledge, with specific examples for each domain. The first of the eight domains, Security and Risk Management, is discussed using real-world scenarios to illustrate the critical points.

**Topics:** Overview of CISSP® Certification; Introductory Material; Overview of the Eight Domains; Domain 1: Security and Risk Management

---

**DAY 2: Asset Security and Security Engineering – Part 1**

Understanding asset security is critical to building a solid information security program. The Asset Security domain, the initial focus of today’s course section, describes data classification programs, including those used by both governments and the military as well as the private sector. We will also discuss ownership ranging from business/mission owners to data and system owners. We will examine data retention and destruction in detail, including secure methods for purging data from electronic media. We then turn to the first part of the Security Engineering domain, including new topics for the 2019 exam such as the Internet of Things, Trusted Platform Modules, Cloud Security, and much more.

**Topics:** Domain 2: Asset Security; Domain 3: Security Engineering (Part 1)

---

**DAY 3: Security Engineering – Part 2; Communication and Network Security**

This course section continues the discussion of the Security Engineering domain, including a deep dive into cryptography. The focus is on real-world implementation of core cryptographic concepts, including the three types of cryptography: symmetric, asymmetric, and hashing. Salts are discussed, as well as rainbow tables. We will round out Domain 3 with a look at physical security before turning to Domain 4, Communication and Network Security. The discussion will cover a range of protocols and technologies, from the Open Systems Interconnection (OSI) model to storage area networks.

**Topics:** Domain 3: Security Engineering (Part 2); Domain 4: Communication and Network Security

---

**DAY 4: Identity and Access Management**

Controlling access to data and systems is one of the primary objectives of information security. Domain 5, Identity and Access Management, strikes at the heart of access control by focusing on identification, authentication, and authorization of accounts. Password-based authentication represents a continued weakness, so Domain 5 stresses multi-factor authentication, biometrics, and secure credential management. The CISSP® exam underscores the increased role of external users and service providers, and mastery of Domain 5 requires an understanding of federated identity, SSO, SAML, and third-party identity and authorization services like OAuth and OpenID.

**Topics:** Domain 5: Identity and Access Management

---

**DAY 5: Security Assessment and Testing; Security Operations**

This course section covers Domain 6 (Security Assessment) and Domain 7 (Security Operations). Security Assessment covers types of security tests, testing strategies, and security processes. Security Operations covers investigatory issues, including eDiscovery, logging and monitoring, and provisioning. We will discuss cutting-edge technologies such as the cloud, and we’ll wrap up day five with a deep dive into disaster recovery.

**Topics:** Domain 6: Security Assessment; Domain 7: Security Operations

---

**DAY 6: Software Development Security**

Domain 8 (Software Development Security) describes the requirements for secure software. Security should be “baked in” as part of network design from day one, since it is always less effective when it is added later to a poor design. We will discuss classic development models, including waterfall and spiral methodologies. We will then turn to more modern models, including agile software development methodologies. New content for the CISSP® exam update will be discussed, including DevOps. We will wrap up this course section by discussing security vulnerabilities, secure coding strategies, and testing methodologies.

**Topics:** Domain 8: Software Development Security

---

**Who Should Attend**

- Security professionals who are interested in understanding the concepts covered on the CISSP® exam as determined by (ISC)²
- Managers who want to understand the critical areas of information security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® eight domains
- Security professionals and managers looking for practical ways the eight domains of knowledge can be applied to their current job

“Great discussions and examples that provide a clear understanding and relate material to examples.”

-Kelley O’Neil, Wells Fargo
G. Mark Hardy is founder and president of National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for over 35 years, and is an internationally recognized expert and keynote speaker who has presented at over 250 events world-wide. He provides consulting services as a virtual CISO, expert witness testimony, and domain expertise in blockchain and cryptocurrency.

G. Mark serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. He is a retired U.S. Navy captain who was entrusted with nine command assignments, including responsibility for leadership training for 70,000 sailors. A graduate of Northwestern University, he holds a B.S. in computer science, a B.A. in mathematics, a master’s degree in business administration, and a master’s degree in strategic studies, and holds the GSLC, CISSP®, CISM and CISA certifications.

G. Mark Hardy
SANS Principal Instructor

You Will Be Able To
- Become an effective information security manager
- Get up to speed quickly on information security issues and terminology
- Establish a minimum standard of security knowledge, skills, and abilities
- Speak the same language as technical security professionals

Security managers need both technical knowledge and management skills to gain the respect of technical team members, understand what technical staff are actually doing, and appropriately plan and manage security projects and initiatives. This is a big and important job that requires an understanding of a wide array of security topics.

This approach prepares you to:
- Make sense of different cybersecurity frameworks
- Understand and analyze risk
- Understand the pros and cons of different reporting relationships
- Manage technical personnel
- Build a vulnerability management program
- Inject security into modern DevOps workflows
- Strategically leverage a SIEM
- Change behavior and build a security-aware culture
- Effectively manage security projects
- Enable modern security architectures and the cloud

MGT512 uses case studies, group discussions, team-based exercises, and in-class games to help students absorb both technical and management topics.

You Will Be Able To
- Become an effective information security manager
- Get up to speed quickly on information security issues and terminology
- Establish a minimum standard of security knowledge, skills, and abilities
- Speak the same language as technical security professionals

“SANS prepared me for the [GSLC] certification and provided valuable information that I can use on the job immediately. Networking with peers and SANS@NIght provided extra value that’s not normally available at other training sessions.”

-Rick Derks, FCS Financial

G. Mark Hardy is founder and president of National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for over 35 years, and is an internationally recognized expert and keynote speaker who has presented at over 250 events world-wide. He provides consulting services as a virtual CISO, expert witness testimony, and domain expertise in blockchain and cryptocurrency.

G. Mark serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. He is a retired U.S. Navy captain who was entrusted with nine command assignments, including responsibility for leadership training for 70,000 sailors. A graduate of Northwestern University, he holds a B.S. in computer science, a B.A. in mathematics, a master’s degree in business administration, and a master’s degree in strategic studies, and holds the GSLC, CISSP®, CISM and CISA certifications.

@g_mark
Day 1: Building Your Program
The course starts with a tour of the information and topics that effective security managers and leaders must know to function in the modern security environment. This includes an understanding of the different types of cybersecurity frameworks available to structure your security team and program. Risk is central to effective information security management, and key risk concepts are discussed to lay the foundation for effective risk assessment and management. Security policy is a key tool that security managers use to manage risk. We’ll cover approaches to policy to help you plan and manage your policy process. Finally, security functions, reporting relationships, and roles and responsibilities are discussed to give the advancing manager a view into effective security team and program structure.

Topics: Security Frameworks, Understanding Risk; Security Policy, Program Structure

Day 2: Protecting Data and Networks
Day 2 provides foundational knowledge to protect data and networks. This includes building an understanding of cryptography concepts, encryption algorithms, and applications of cryptography. Since encrypting data alone is not sufficient, the distinction between privacy and security is discussed to give managers a primer on key privacy concepts. Finally, a thorough discussion of network security is modeled around the various layers of the network stack. This allows managers to gain a deeper understanding of what their teams are talking about, what vendors are selling, and where various issues and protections lay within the seven layers of the network model.

Topics: Data Protection, Privacy Primer, Network Security

Day 3: Protecting and Patching Systems
Day 3 is focused on protecting and patching systems. This includes coverage of host security that encompasses endpoint and server security along with malware and attack examples. Modern infrastructure as code approaches and tools are also discussed as ways to automate consistent deployment of standard configurations. Managers must also be knowledgeable about software development processes, issues, and application vulnerabilities. Coverage includes an overview of the secure SDLC, OWASP Top Ten, and leading-edge development processes built on DevOps. Managers must also understand physical security controls that, when not implemented appropriately, can cause technical security controls to fail or be bypassed. All of these issues and corresponding vulnerabilities must be appropriately managed. This leads to a discussion on building a vulnerability management program and the associated process for successfully finding and fixing vulnerabilities.

Topics: Host Security; Application Security; Physical Security; Vulnerability Management

Day 4: Leading Modern Security Initiatives
Day 4 covers what managers need to know about leading modern security initiatives. Security awareness is a huge component of any security program that is focused on driving activities that lead to changes in human behavior and creating a more risk-aware and security-aware culture. For any project or initiative, security leaders must also be able to drive effective project execution. Having a well-grounded understanding of the project management process makes it easier to move these projects forward. The cloud is a major initiative that many organizations are either tackling now or planning to undertake. To get ready for these initiatives, an overview of Amazon Web Services (AWS) is provided to serve as a reference, along with a discussion of key cloud security issues based on the Cloud Security Alliance guidance. The cloud, the rise of mobile devices, and other factors are highlighting weaknesses in traditional, perimeter-oriented security architectures. This leads to a discussion of the Zero Trust Model. To execute such new initiatives security leaders must also develop negotiation skills and the ability to manage highly technical team members.

Topics: Security Awareness; Project Management; Cloud Security; Modern Security Architecture; Management Methods

Day 5: Detecting and Responding to Attacks
Day 5 is focused on detection and response capabilities. This includes gaining appropriate visibility via logging, monitoring, and thinking strategically about a Security Information and Event Management (SIEM) system. These logs are a core component of any Security Operations Center (SOC). The key functions of a SOC are discussed along with how to design, build, operate, and mature security operations for your organization. The incident response process is discussed in relation to identifying, containing, eradicating, and recovering from security incidents. This leads into a discussion of longer-term disaster recovery and business continuity planning. Finally, the course ends with a war game that simulates an actual incident. This tabletop simulation contains a number of injects or points at which students are presented with additional information to which they can respond. After dealing with the incident itself, the simulation concludes with a game focused on choosing appropriate security controls to mitigate future incidents.

Topics: Logging and Monitoring; Security Operations Center; Incident Response; Contingency Planning; War Game

Who Should Attend
- Security Managers
  - Newly appointed information security officers
  - Recently promoted security leaders who want to build a security foundation for leading and building teams
- Security Professionals
  - Technically skilled security administrators who have recently been given leadership responsibilities
- Managers
  - Managers who want to understand what technical people are telling them
  - Managers who need an understanding of security from a management perspective

Course Author Statement
“I have found that technical professionals who are taking on management responsibility need to learn how to convey security concepts in ways that non-technical people can understand. At the same time, managers who are new to security need to learn more about the different domains of cybersecurity. In both cases, there is a need to learn about the work of managing security. That is why this course focuses on the big picture of securing the enterprise, from governance all the way to the technical security topics that serve as the foundation for any security manager. Ultimately, the goal of the course is to ensure that you, the advancing manager, can make informed choices to improve security at your organization.”

-Frank Kim

“This course was very relevant to my new role as Director of IT.”

-Brian Harris, Jackson EMC
As security professionals we have seen the landscape change. Cybersecurity is now more vital and relevant to the growth of your organization than ever before. As a result, information security teams have more visibility, more budget, and more opportunity. However, with this increased responsibility comes more scrutiny.

This course teaches security professionals how to do three things:

▐ Develop Strategic Plans
Strategic planning is hard for people in IT and IT security because we spend so much time responding and reacting. We almost never get to practice until we get promoted to a senior position and then we are not equipped with the skills we need to run with the pack. Learn how to develop strategic plans that resonate with other IT and business leaders.

▐ Create Effective Information Security Policy
Policy is a manager’s opportunity to express expectations for the workforce, set the boundaries of acceptable behavior, and empower people to do what they ought to be doing. It is easy to get wrong. Have you ever seen a policy and your response was, “No way, I am not going to do that!”? Policy must be aligned with an organization’s culture. We will break down the steps to policy development so that you have the ability to develop and assess policy to successfully guide your organization.

▐ Develop Management and Leadership Skills
Leadership is a capability that must be learned, exercised and developed to better ensure organizational success. Strong leadership is brought about primarily through selfless devotion to the organization and staff, tireless effort in setting the example, and the vision to see and effectively use available resources toward the end goal. Effective leadership entails persuading team members to accomplish their objectives while removing obstacles and maintaining the well-being of the team in support of the organization’s mission. Learn to utilize management tools and frameworks to better lead, inspire, and motivate your teams.

Using case studies from Harvard Business School, team-based exercises, and discussions that put students in real-world scenarios, students will participate in activities that they can then carry out with their own team members when they return to work.

The next generation of security leadership must bridge the gap between security staff and senior leadership by strategically planning how to build and run effective security programs. After taking this course you will have the fundamental skills to create strategic plans that protect your company, enable key innovations, and work effectively with your business partners.

You Will Be Able To

▐ Develop security strategic plans that incorporate business and organizational drivers
▐ Develop and assess information security policy
▐ Use management and leadership techniques to motivate and inspire your teams

“...The knowledge gained in class will directly translate to an increased maturity in my organization’s security policy as topics and principles discussed are implemented.”

-Mike Parkin, Chapters Health System

Frank Kim
SANS Senior Instructor

Frank is the founder of ThinkSec, a security consulting and CISO advisory firm. Previously, as CISO at the SANS Institute, Frank led the information risk function for the most trusted source of computer security training and certification in the world. Frank continues to lead the management and software security curricula at SANS, helping to develop the next generation of security leaders. Frank was also executive director of cybersecurity at Kaiser Permanente, where he built an innovative security program to meet the unique needs of the nation’s largest not-for-profit health plan and integrated health care provider with annual revenue of $60 billion, 10 million members, and 175,000 employees. Frank holds degrees from the University of California at Berkeley and is the author and instructor of popular courses on strategic planning, leadership, application security, and DevOps.

@fykim
**Course Day Descriptions**

**Mon, Jun 17 - Fri, Jun 21**

**9:00am - 5:00pm**

---

**DAY 1: Strategic Planning Foundations**

On this first day we will introduce the key elements of strategic security plans and lay the groundwork for the rest of the course. Creating strategic plans for security requires a fundamental understanding of the business and a deep understanding of the threat landscape.

**Topics:** Vision and Mission Statements; Stakeholder Management; PEST Analysis; Porter’s Five Forces; Threat Actors; Asset Analysis; Threat Analysis

---

**DAY 2: Strategic Roadmap Development**

With a firm understanding of business drivers as well as the threats facing the organization, you will develop a plan to analyze the current situation, identify the target situation, perform gap analysis, and develop a prioritized roadmap. In other words, you will be able to determine (1) what you do today, (2) what you should be doing in the future, (3) what you don’t do, and (4) what you should do first. With this plan in place you will learn how to build and execute your plan by developing a business case, defining metrics for success, and effectively marketing your security program.

**Topics:** Historical Analysis; Values and Culture; SWOT Analysis; Vision and Innovation; Security Framework; Gap Analysis; Roadmap Development; Business Case Development; Metrics and Dashboards; Marketing and Executive Communications

---

**DAY 3: Security Policy Development and Assessment**

Policy is one of the key tools that security leaders have to influence and guide the organization. Security managers must understand how to review, write, assess, and support security policy and procedure. Using an instructional delivery methodology that balances lecture, exercises, and in-class discussion, this course section will teach techniques to create successful policy that users will read and follow and business leaders will accept. Learn key elements of policy, including positive and negative tone, consistency of policy bullets, how to balance the level of specificity to the problem at hand, the role of policy, awareness and training, and the SMART approach to policy development and assessment.

**Topics:** Purpose of Policy; Policy Gap Analysis; Policy Development; Policy Review; Awareness and Training

---

**DAY 4: Leadership and Management Competencies**

Learn the critical skills you need to lead, motivate, and inspire your teams to achieve the goal. By establishing a minimum standard for the knowledge, skills, and abilities required to develop leadership you will understand how to motivate employees and develop from a manager into a leader.

**Topics:** Leadership Building Blocks; Creating and Developing Teams; Coaching and Mentoring; Customer Service Focus; Conflict Resolution; Effective Communication; Leading Through Change; Relationship Building; Motivation and Self-Direction; Teamwork; Leadership Development

---

**DAY 5: Strategic Planning Workshop**

Using the case study method, students will work through real-world scenarios by applying the skills and knowledge learned throughout the course. Case studies are taken directly from Harvard Business School, the pioneer of the case-study method, and focus specifically on information security management and leadership competencies. The Strategic Planning Workshop serves as a capstone exercise for the course, allowing students to synthesize and apply concepts, management tools, and methodologies learned in class.

**Topics:** Creating a Security Plan for the CEO; Understanding Business Priorities; Enabling Business Innovation; Working with BYOD; Effective Communication; Stakeholder Management

---

**Who Should Attend**

- CISOs
- Information security officers
- Security directors
- Security managers
- Aspiring security leaders
- Other security personnel who have team lead or management responsibilities

---

“This training is valuable because it shines a light on the many business aspects of security, while also providing excellent guidance for applying learnings in real life.”

- Alyssa DeVita, Marriott

---

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/sansfire/courses](http://www.sans.org/sansfire/courses)
LEG523: Law of Data Security and Investigations

LEG523 is constantly updated to address changing trends and current events. Here’s a sampling of what’s new:

- Sample contract clauses requiring cybersecurity for the Danish government, consistent with the General Data Protection Regulation (GDPR)
- Court decision showing how to improve an official investigation using artificial intelligence
- Unique and indispensable training for GDPR Data Protection Officers
- Form contract for inviting outside incident responders – including police, contractors, National Guard, or civil defense agencies anywhere in the world – to help with a cyber crisis
- The European Union’s new GDPR and its impact around the world

New law on privacy, e-discovery and data security is creating an urgent need for professionals who can bridge the gap between the legal department and the IT department. SANS LEG523 provides this unique professional training, including skills in the analysis and use of contracts, policies, and records management procedures.

This course covers the law of fraud, crime, policy, contracts, liability, IT security and active defense—all with a focus on electronically stored and transmitted records. It also teaches investigators how to prepare credible, defensible reports, whether for cyber crimes, forensics, incident response, human resource issues or other investigations.

Each successive day of this five-day course builds upon lessons from the earlier days in order to comprehensively strengthen your ability to help your enterprise (public or private sector) cope with illegal hackers, botnets, malware, phishing, unruly vendors, data leakage, industrial spies, rogue or uncooperative employees, or bad publicity connected with IT security.

Recent updates to the course address hot topics such as legal tips on confiscating and interrogating mobile devices, the retention of business records connected with cloud computing and social networks like Facebook and Twitter, and analysis and response to the risks and opportunities surrounding open-source intelligence gathering.

Over the years this course has adopted an increasingly global perspective. Non-U.S. professionals attend LEG523 because there is no training like it anywhere else in the world. For example, a lawyer from the national tax authority in an African country took the course because electronic filings, evidence and investigations have become so important to her work. International students help the instructor, U.S. attorney Benjamin Wright, constantly revise the course and include more content that crosses borders.

Who Should Attend

- Investigators
- Security and IT professionals
- Lawyers
- Paralegals
- Auditors
- Accountants
- Technology managers
- Vendors
- Compliance officers
- Law enforcement personnel
- Privacy officers
- Penetration testers
- Cyber incident and emergency responders around the world (including private sector, law enforcement, national guard, civil defense and the like)

Benjamin Wright is the author of several technology law books, including Business Law and Computer Security, published by the SANS Institute. With 26 years in private law practice, he has advised many organizations, large and small, on privacy, e-commerce, computer security, and e-mail discovery and has been quoted in publications around the globe, from the Wall Street Journal to the Sydney Morning Herald. He is known for spotting and evaluating trends, such as the rise of whistleblowers wielding small video cameras. In 2010, Russian banking authorities tapped him for experience and advice on the law of cyber investigations and electronic payments.

@benjaminwright
DAY 1: Fundamentals of Data Security Law and Policy

The first day is an introduction to law and IT that serves as the foundation for discussions during the rest of the course. We survey the general legal issues that must be addressed in establishing best information security practices, then canvas the many new laws on data security and evaluate information security as a field of growing legal controversy. We will cover computer crime and intellectual property laws where applicable, as well as emerging topics such as honeypots. We will look at the impact of future technologies on law and investigations in order to help students factor in legal concerns when they draft enterprise IT security policies. For example, students will debate what the words of an enterprise policy would mean in a courtroom. The course also dives deep into the legal question of what constitutes a “breach of data security” for purposes of notifying others about it or for other purposes. The course includes a case study on the drafting of policy to comply with the Payment Card Industry Data Security Standard (PCI). Students learn how to choose words more carefully and accurately when responding to cybersecurity questionnaires from regulators, cyber insurers and corporate customers.

DAY 2: E-Records, E-Discovery and Business Law

IT professionals can advance their careers by upgrading their expertise in the hot fields of e-discovery and cyber investigations. Critical facets of those fields come forward in course day two. We will focus on the use of computer records in disputes and litigation, with a view to teaching students how to manage requests to turn over e-records to adversaries (i.e., e-discovery), manage implementation of a “legal hold” over some records to prevent their destruction, and coordinate with legal counsel to develop workable strategies to legal challenges. Transactions that used to be conducted on paper are now done electronically, so commercial law now applies to computer security. The IT function within an enterprise has become the custodian of an enterprise’s business records. You will learn how to craft sound policy for the retention and destruction of electronic records like email, text messages, and social networking interactions. We will provide methods for balancing the competing interests in electronic records management, including costs, risks, security, regulations and user cooperation. Law and technology are changing quickly, and it is impossible for professionals to comprehend all the laws that apply to their work. But they can comprehend overarching trends in law, and they can possess a mindset for finding solutions to legal problems. A key goal of this course day is to equip students with the analytical skills and tools to address technology law issues as they arise, both in the United States and around the world. Special attention is devoted to European data protection laws (see the white paper by Mr. Wright on the European Union’s new General Data Protection Regulation). The course is chock full of actual court case studies dealing with privacy, computer records, digital evidence, electronic contracts, regulatory investigations, and liability for shortfalls in security. The purpose of the case studies is to draw practical lessons that students can take back to their jobs.

DAY 3: Contracting for Data Security and Other Technology

Day three focuses on the essentials of contract law sensitive to the current legislative requirements for security. Compliance with many of the new data security laws requires contracts. Because IT pulls together the products and services of many vendors, consultants, and outsourcees, enterprises need appropriate contracts to comply with Gramm-Leach-Bliley, HIPAA, GDRR, PCI-DSS, data breach notice laws and other regulations. The section provides practical steps and tools that students can apply to their enterprises and includes a lab on writing contract-related documents relevant to the students’ professional responsibilities. (The lab is an optional, informal “office hours” discussion with the instructor at the end of the day when the course is delivered live.) You will learn the language of common technology contract clauses and the issues surrounding those clauses, and become familiar with specific legal cases that show how different disputes have been resolved in litigation. Recognizing that enterprises today operate increasingly on a global basis, the course teaches cases and contract drafting styles applicable to a multinational setting. Contracts covered include agreements for software, consulting, nondisclosure, outsourced services, penetration testing, and private investigation services (such as cyber incident response). Special emphasis is applied to cloud computing issues. Students will also learn how to exploit the surprising power of informal contract records and communications, including cybersecurity questionnaires and requests for InfoSec assurances.

DAY 4: The Law of Data Compliance: How to Conduct Investigations

Information security professionals and cyber investigators operate in a world of ambiguity, rapid change, and legal uncertainty. To address these challenges, this course day presents methods to analyze a situation and then act in a way that is ethical and defensible and reduces risk. Lessons will be invaluable to the effective and credible execution of any kind of investigation, be it internal, government, consultant, security incident, or any other. The lessons also include methods and justifications for maintaining the confidentiality of an investigation. The course surveys white-collar fraud and other misbehaviors with an emphasis on the role of technology in the commission and prevention of that fraud. It teaches IT managers practical and case-study-driven lessons about the monitoring of employees and employee privacy. IT is often expected to “comply” with many mandates, whether stated in regulations, contracts, internal policies or industry standards (such as PCI-DSS). This course teaches many broadly applicable techniques to help technical professionals establish that they and their organizations are in fact in compliance, or to reduce risk if they are not in perfect compliance. The course draws lessons from models such as the Sarbanes-Oxley Act. As IT security professionals take on more responsibility for controls throughout an enterprise, it is natural that they worry about fraud, which becomes a new part of their domain. This day covers what fraud is, where it occurs, what the law says about it and how it can be avoided and remedied. Indeed, the primary objective of Sarbanes-Oxley is not to keep hackers out; it is to snuff out fraud inside the enterprise. Scattered through the course are numerous descriptions of actual fraud cases involving technology. The purpose is to acquaint the student with the range of modern business crimes, whether committed by executives, employees, suppliers or whole companies. More importantly, the course draws on the law of fraud and corporate misconduct to teach larger and broader lessons about legal compliance, ethical hacking and proper professional conduct in difficult case scenarios. Further, the course teaches how to conduct forensics investigations involving social, mobile and other electronic media. Students learn how to improve the assessment and interpretation of digital evidence, such as evidence of a breach or other cyber event.

DAY 5: Applying Law to Emerging Dangers: Cyber Defense

Knowing some rules of law is not the same as knowing how to deal strategically with real-world legal problems. This day is organized around extended case studies in security law: break-ins, investigations, piracy, extortion, rootkits, phishing, botnets, espionage and defamation. The studies lay out the chronology of events and critique what the good guys did right and what they did wrong. The goal is to learn to apply principles and skills to address incidents in your day-to-day work. The course includes an in-depth review of legal responses to the major security breaches at TIA, Target, and Home Depot, and looks at how to develop a Bring Your Own Device (BYOD) policy for an enterprise and its employees. The skills learned are a form of crisis management, with a focus on how your enterprise will be judged in a courtroom, by a regulatory agency, or in a contract relationship. Emphasis will be on how to present your side of a story to others, such as law enforcement, Internet gatekeepers, or the public at large, so that a security incident does not turn into a legal fiasco. In addition to case studies, the core material will include tutorials on relevant legislation and judicial decisions in such areas as privacy, negligence, contracts, e-investigations, computer crime and offensive countermeasures. LEG523 is increasingly global in its coverage, so although this course day centers around U.S. law, non-U.S. law and the roles of government authorities outside the United States will be examined, as well. At the end of this course section, the instructor will discuss a few sample questions to help students prepare for the GIAC exam associated with this course (GLEG).
DEV540: Secure DevOps and Cloud Application Security

This course covers how developers and security professionals can build and deliver secure software using DevOps and cloud services, specifically Amazon Web Services (AWS). It explains how principles, practices, and tools in DevOps and AWS can be leveraged to improve the reliability, integrity, and security of applications.

The first two days of the course cover how Secure DevOps can be implemented using lessons from successful DevOps security programs. Students build a secure DevOps Continuous Integration/Continuous Delivery (CI/CD) toolchain and understand how code is automatically built, tested, and deployed using popular open-source tools such as git, Puppet, Jenkins, and Docker. In a series of labs you learn to inject security into your CI/CD toolchain using various security tools, patterns, and techniques.

The final three days of the course cover how developers and security professionals can utilize AWS services to build secure software in the cloud. Students leverage the CI/CD toolchain to push application code directly to the cloud instead of to local servers on their class virtual machines. Students analyze and fix applications hosted in the cloud using AWS services and features such as API Gateway, IAM, signed cookies, Security Token Service, autoscaling, KMS, encryption, WAF, and Lambda for Serverless computing.

The course makes extensive use of open-source materials and tooling for automated configuration management (“Infrastructure as Code”), Continuous Integration, Continuous Delivery, Containerization, micro-segmentation, automated compliance (“Compliance as Code”), and Continuous Monitoring.

This course also makes extensive use of AWS and associated developer tools such as CloudFormation, CodeCommit, CodeBuild, CodePipeline, and other cloud application services so students can experience how these services can be utilized in their applications.

You Will Be Able To
- Understand the core principles and patterns behind DevOps
- Map out and implement a Continuous Delivery/Deployment pipeline
- Map out where security controls and checks can be added in Continuous Delivery and Continuous Deployment
- Integrate security into production operations
- Create a plan for introducing – or improving – security in a DevOps environment
- Move your DevOps workflows to the cloud
- Consume cloud services to secure cloud applications

“"The training was a valuable centralized collection of resources to the ever-evolving DevSecOps world.""

-Almahdi Sahad, CoStar

You Will Be Able To

Eric Johnson is a Principal Security Consultant at Cypress Data Defense, where he leads secure software development lifecycle consulting, web and mobile application penetration testing, secure code review assessments, static source code analysis, security research, and security tools development. He also founded the Puma Scan static analysis open-source project, which allows software engineers to run security-focused .NET static analysis rules during development and in continuous integration pipelines. At the SANS Institute, Eric authors application security courses on DevOps, cloud security, secure coding, and defending mobile apps. He serves on the advisory board for the SANS Securing The Human Developer awareness training program, delivers security training around the world, and has presented his security research at conferences including BlackHat, OWASP BSides, JavaOne, UberConf, and ISSA. Eric completed a bachelor of science degree in computer engineering and a master of science degree in information assurance at Iowa State University, and currently holds the CISSP®, GWAPT, GSSP-.NET, and GSSP-Java certifications. He is based in West Des Moines, Iowa and outside the office enjoys spending time with his family, attending Iowa State athletic events, and playing golf.

@emjohn20
**DAY 1: Introduction to Secure DevOps**
The first day is an introduction to DevOps practices, principles and tooling, how DevOps works, and how work is done in DevOps. We’ll look at the importance of culture, collaboration, and automation in DevOps. Using case studies of DevOps “Unicorns” – the Internet tech leaders who have created the DNA for DevOps – we’ll show you how and why they succeeded. This includes the keys to their DevOps security programs. Then you’ll learn Continuous Delivery – the automation engine in DevOps – and how to build up a Continuous Delivery or Continuous Deployment pipeline. This includes how security controls can be folded into or wired into the CD pipeline, and how to automate security checks and tests in CD.

**Topics:** Introduction to DevOps; Case Studies on DevOps Unicorns; DevOps Principles; Working in DevOps; From Continuous Integration to Continuous Delivery; Building a CD Pipeline; Deployment Kata; Secure Continuous Delivery: Challenges and Issues; Introducing Security into CD; Static Analysis in CD; Pen Testing and Manual Assessments – How Do They Fit in DevOps?; Vulnerability Management in CD; Securing Your Software Supply Chain; Automated Security Testing and Scanning in CI/CD

---

**DAY 2: Moving to Production**
Building on the ideas and frameworks developed in the first course section, you will learn how secure Infrastructure as code, using modern automated configuration management tools like Puppet, Chef and Ansible, allows you to quickly and consistently deploy new infrastructure and manage configurations.

**Topics:** Securing Your CD Pipeline; Threat Modeling and Locking Down Your Build and Deployment Environment; Runtime Checks and Monitoring – Monkeys and Smart Checks; Run-Time Defense: RASP, IAST and Other Run-Time Security Solutions; Security in Monitoring: Using Production Metrics and Insight to Drive Improvements in Your Security Program; Red Teaming, Bug Bounties and Blameless Postmortems; Secure Infrastructure as Code – Building Security Policies into Infrastructure Code; Security with Puppet Lab; Managing Secrets: The Problem of Secrets in an Automated Environment; Patterns – and Anti-Patterns – for Managing Secrets; Container Security – Introduction to Containers, Docker, and Docker Security Risks and Tools; Compliance as Code: How to Satisfy Compliance Requirements Using Continuous Delivery and Continuous Deployment; Going Forward: Introducing Security into DevOps – and DevOps into Security: Quick Wins and Long-Term Investments Needed to Succeed

---

**DAY 3: Moving to the Cloud**
Utilizing DevOps principles you will learn how to move your CI/CD toolchain into the cloud. This section provides an overview of Amazon Web Services (AWS) and introduces the foundational tools and practices needed to securely deploy your applications in the cloud.

**Topics:** Introduction to the Cloud; Introduction to Amazon Web Services; Cloud Infrastructure as Code; Cloud CI/CD; Cloud Container Orchestration

---

**DAY 4: Cloud Application Security**
In this course section, we will examine how to leverage cloud application security services to ensure that applications have appropriate authentication and access control functionality while maintaining availability even while patching critical security defects.

**Topics:** Authentication and Access Control; API Gateway; Availability; Patch Management

---

**DAY 5: Cloud Security Automation**
Expanding on the foundation of the previous sections, we’ll now focus on leveraging cloud services to automate security tasks such as deploying application patches to blue/green environments, deploying and configuring cloud web application firewalls, enabling cloud security monitoring, and automating cloud compliance scanning.

**Topics:** Encryption; Security Monitoring; Security Automation; Serverless Security

---

**Who Should Attend**
- Anyone working in the DevOps environment or transitioning to a DevOps environment
- Anyone who wants to understand where to add security checks, testing, and other controls to DevOps and Continuous Delivery
- Anyone interested in learning how to migrate DevOps workflows to the cloud, specifically Amazon Web Services (AWS)
- Anyone interested in learning how to leverage cloud application security services provided by AWS
- Developers
- Software architects
- Operations engineers
- System administrators
- Security analysts
- Security engineers
- Auditors
- Risk managers
- Security consultants

---

“Extremely relevant to our DevOps and CI/CD journey.”

– Devon D., USAA

---

“DEV540 opened my eyes to a new way of thinking about operations and security unlike anything since SEC401: Security Essentials.”

– Todd Anderson, OBE

---

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/sansfire/courses](http://www.sans.org/sansfire/courses)
ICS410: ICS/SCADA Security Essentials

You Will Be Able To

- Better understand various industrial control systems and their purpose, application, function, and dependencies on network IP and industrial communications
- Work with control network infrastructure design (network architecture concepts, including topology, protocols, and components) and their relation to IEC 62443 and the Purdue Model.
- Run Windows command line tools to analyze the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat, etc) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Work with operating systems (system administration concepts for Unix/Linux and/or Windows operating systems)
- Better understand the systems' security lifecycle
- Better understand information assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)
- Use your skills in computer network defense to detect host and network-based intrusions via intrusion detection technologies
- Implement incident response and handling methodologies
- Map different ICS technologies, attacks, and defenses to various cybersecurity standards including NIST Cyber Security Framework, ISA/IEC 62443, ISO/IEC 27001, NIST SP 800-53, the Center for Internet Security Critical Security Controls, and COBIT 5

Justin Searle
SANS Senior Instructor

SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. ICS410: ICS/SCADA Security Essentials provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems (ICS) is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

The course will provide you with:

- An understanding of ICS components, purposes, deployments, significant drivers, and constraints
- Hands-on lab learning experiences to control system attack surfaces, methods, and tools
- Control system approaches to system and network defense architectures and techniques
- Incident-response skills in a control system environment
- Governance models and resources for industrial cybersecurity professionals

When examining the greatest risks and needs in critical infrastructure sectors, the course authors looked carefully at the core security principles necessary for the range of tasks involved in supporting control systems on a daily basis. While other courses are available for higher-level security practitioners who need to develop specific skills such as ICS penetration testing, vulnerability analysis, malware analysis, forensics, secure coding, and red team training, most of these courses do not focus on the people who operate, manage, design, implement, monitor, and integrate critical infrastructure production control systems.

With the dynamic nature of ICS, many engineers do not fully understand the features and risks of many devices. For their part, IT support personnel who provide the communications paths and network defenses do not always grasp the systems’ operational drivers and constraints. This course is designed to help traditional IT personnel fully understand the design principles underlying control systems and how to support those systems in a manner that ensures availability and integrity. In parallel, the course addresses the need for control system system engineers and operators to better understand the important role they play in cybersecurity. This starts by ensuring that a control system is designed and engineered with cybersecurity built into it, and that cybersecurity has the same level of focus as system reliability throughout the system lifecycle.

When these different groups of professionals complete this course, they will have developed an appreciation, understanding, and common language that will enable them to work together to secure their ICS environments. The course will help develop cyber-secure-aware engineering practices and real-time control system IT/OT support carried out by professionals who understand the physical effects of actions in the cyber world.

Justin Searle is a Managing Partner of UtiliSec, specializing in Smart Grid security architecture design and penetration testing. Justin led the Smart Grid Security Architecture group in the creation of NIST Interagency Report 7628 and played key roles in the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG). He currently leads the testing group at the National Electric Sector Cybersecurity Organization Resource (NESCOR). Justin has taught courses in hacking techniques, forensics, networking, and intrusion detection for multiple universities, corporations, and security conferences. In addition to electric power industry conferences, Justin frequently presents at top international security conferences such as Black Hat, DEFCON, OWASP, Nullcon, and AusCERT. Justin co-leads prominent open-source projects including the Samurai Web Testing Framework (SamuraiWTF), the Samurai Security Testing Framework for Utilities (SamuraiSTFU), Middler, Yokoso!, and Laudanum. Justin has an MBA in international technology and is a CISSP® and SANS GIAC certified Incident Handler (GCHI), Intrusion Analyst (GCIA), and Web Application Penetration Tester (GWAPT).

@meeas
Course Day Descriptions

**DAY 1: ICS Overview**

Students will develop and reinforce a common language and understanding of industrial control system (ICS) cybersecurity as well as the important considerations that come with cyber-to-physical operations within these environments. Each student will receive programmable logic controller (PLC) hardware to keep. The PLC contains physical inputs and outputs that will be programmed in class and mapped to an operator interface, or HMI, also created in class. This improved hardware-enabled approach provides the necessary cyber-to-physical knowledge that allows students to better understand ICS operational drivers and constraints that require specific safety protection, communications needs, system management approaches, and cybersecurity implementations. Essential terms, architectures, methodologies, and devices are all covered to build a common language for students from a variety of different roles.

**Topics:** Global Industrial Cybersecurity Professional (GICSP) Overview; Overview of ICS; Purdue Levels 0 and 1; Purdue Levels 2 and 3; DCS and SCADA; IT & ICS Differences; Physical and Cyber Security; Secure ICS Network Architectures

**DAY 2: Field Devices and Controllers**

If you know the adversary’s approaches to attacking an ICS environment, you will be better prepared to defend that environment. Numerous attack vectors exist within an ICS environment. Some are similar to traditional IT systems, while others are more specific to ICS. During day 2, students will develop a better understanding of where these specific attack vectors exist and how to block them, starting at the lowest levels of the control network. Students will look at different technologies and communications used in Purdue Levels 0 and 1, the levels that are the most different from an IT network. Students will capture fieldbus traffic from the PLCs they programmed in day 1 and look at what other fieldbus protocols used in the industry. Later in the day, students will analyze network captures containing other control protocols that traverse Ethernet-only networks and TCP/IP networks, set up a simulated controller, and interact with it through a control protocol.

**Topics:** ICS Attack Surface; Purdue Levels 0 and 1; Ethernet and TCP/IP

**DAY 3: Supervisory Systems**

Day 3 will take students through the middle layers of control networks. Students will learn about different methods to segment and control the flow of traffic through the control network. Students will explore cryptographic concepts and how they can be applied to communications protocols and on devices that store sensitive data. Students will learn about the risks of using wireless communications in control networks, which wireless technologies are commonly used, and available defenses for each. After a hands-on network forensics exercise where students follow an attacker from phishing campaign to HMI breach, students will look at HMI, historian, and user interface technologies used in the middle to upper levels of the control network, namely Purdue Levels 2 and 3, while performing attacks on HMI web technologies and interfaces susceptible to password brute force attacks.

**Topics:** Enforcement Zone Devices; Understanding Basic Cryptography; Wireless Technologies; Wireless Attacks and Defenses; Exercise: Network Forensics of an Attack; Purdue Level 2 and 3 Attacks

**DAY 4: Workstations and Servers**

Students will learn essential ICS-related server and workstation operating system capabilities, implementation approaches, and system management practices. Students will receive and work with both Windows- and Linux-based virtual machines in order to understand how to monitor and harden these hosts from attack. Students will examine concepts that benefit ICS systems such as system hardening, log management, monitoring, alerting, and audit approaches, then look at some of the more common applications and databases used in ICS environments across multiple industries. Finally, students will explore attacks and defenses on remote access for control systems.

**Topics:** Patching ICS Systems; Defending Microsoft Windows; Defending Unix and Linux; Endpoint Security Software; Event Logging and Analysis; Remote Access Attacks

**DAY 5: ICS Security Governance**

Students will learn about the various models, methodologies, and industry-specific regulations that are used to govern what must be done to protect critical ICS systems. Key business processes that consider risk assessments, disaster recovery, business impact analysis, and contingency planning will be examined from the perspective of ICS environments. On this final course day, students will work together on an incident response exercise that places them squarely in an ICS environment that is under attack. This exercise ties together key aspects of what has been learned throughout the course and presents students with a scenario to review with their peers. Specific incident-response roles and responsibilities are considered, and actions available to defenders throughout the incident response cycle are explored. Students will leave with a variety of resources for multiple industries and will be well prepared to pursue the GICSP, an important ICS-focused professional certification.

**Topics:** Building an ICS Cybersecurity Program; Creating ICS Cybersecurity Policy; Disaster Recovery; Measuring Cybersecurity Risk; Incident Response; Exercise: Incident Response Tabletop Exercise; Final Thoughts and Next Steps

Who Should Attend

The course is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:

- IT (includes operational technology support)
- IT security (includes operational technology security)
- Engineering
- Corporate, industry, and professional standards

“Good comprehensive content with dynamic instructor really made this course good. This is the best training course I’ve taken in 25+ years.”

-Curt Imanse, Accenture
ICS515: ICS Active Defense and Incident Response

You Will Be Able To

- Perform industrial control system (ICS) incident response focusing on security operations and prioritizing the safety and reliability of operations
- Determine how ICS threat intelligence is generated and how to use what is available in the community to support ICS environments. The analysis skills you learn will enable you to critically analyze and apply information from ICS threat intelligence reports on a regular basis
- Identify ICS assets and their network topologies and how to monitor ICS hotspots for abnormalities and threats. Methodologies such as ICS network security monitoring and approaches to reducing the control system threat landscape will be introduced and reinforced
- Analyze ICS malware and extract the most important information needed to understand the nature of the threat
- Operate through an attack and gain the information necessary to instruct teams and decision-makers on when operations must shut down, or if it is safe to respond to the threat and continue operations
- Use multiple security disciplines in conjunction with each other to leverage an active defense and safeguard the ICS, all reinforced with hands-on labs and technical concepts

ICS515: ICS Active Defense and Incident Response will help you deconstruct industrial control system (ICS) cyber attacks, leverage an active defense to identify and counter threats in your ICS, and use incident response procedures to maintain the safety and reliability of operations.

This course will empower students to understand their networked ICS environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security. This process of monitoring, responding to, and learning from threats internal to the network is known as active defense. An active defense is the approach needed to counter advanced adversaries targeting an ICS, as has been seen with malware such as Stuxnet, Havex, and BlackEnergy2. Students can expect to come out of this course with the ability to deconstruct targeted ICS attacks and fight these adversaries and others. The course uses a hands-on approach and real-world malware to break down cyber attacks on ICS from start to finish. Students will gain a practical and technical understanding of leveraging active defense concepts such as using threat intelligence, performing network security monitoring, and utilizing malware analysis and incident response to ensure the safety and reliability of operations. The strategy and technical skills presented in this course serve as a basis for ICS organizations looking to show that defense is do-able.

This course will prepare you to:

- Examine ICS networks and identify the assets and their data flows in order to understand the network baseline information needed to identify advanced threats
- Use active defense concepts such as threat intelligence consumption, network security monitoring, malware analysis, and incident response to safeguard the ICS
- Build your own Programmable Logic Controller using a CYBATIworks Kit and keep it after the class ends
- Gain hands-on experience with samples of Havex, BlackEnergy2, and Stuxnet by participating in labs and de-constructing these threats and others
- Leverage technical tools such as Shodan, Security Onion, TCPDump, NetworkMiner, Foremost, Wireshark, Snort, Bro, SGUilla, ELSA, Volatility, Redline, FTK Imager, PDF analyzers, malware sandboxes, and more
- Create indicators of compromise (IoCs) in OpenIOC and YARA while understanding sharing standards such as STIX and TAXII
- Take advantage of models such as the Sliding Scale of Cybersecurity, the Active Cyber Defense Cycle, and the ICS Cyber Kill Chain to extract information from threats and use it to encourage the long-term success of ICS network security.

Mark Bristow was born to work in information security, as he found his first bug in an ICS system at the age of 10. As a teen he had a passion for technology and spent a lot of time exploring the possibilities on his computer. Once he realized he could make a career out of this passion, he jumped at the opportunity and earned a computer engineering degree from Penn State. Mark loves the ever-changing landscape of security and views it as a puzzle that must be solved. He especially loves the challenges in ICS security, as it means defending the systems where cyber meets physical in order to make them safe and effective. Currently, Mark is the Chief of ICS-CERT Incident Response at the U.S. Department of Homeland Security, where he leverages his expertise in incident response, industrial control systems, network monitoring and defense to support national security interests. In Mark’s 12-year security career, he has also worked for SRA and Securicon, where he supported a variety of private and public sector clients. Mark’s experience has led him to the path of sharing his knowledge and helping others learn to protect critical infrastructure.

@kodefupanda

Mark Bristow
SANS Certified Instructor
Day 1: Threat Intelligence
Industrial control system (ICS) security professionals must be able to leverage internal and external threat intelligence to critically analyze threats, extract indicators of compromise (IOCs), and guide security teams to find threats in the environment. Today you will learn how threat intelligence is generated, how to critically analyze reports, and the basic tenets of active defense functions. Students will become better analysts and critical thinkers by learning skills useful in day-to-day operations, regardless of their jobs and roles. This day features four hands-on labs that include building a Programmable Logic Controller (PLC), identifying information available about assets online through Shodan, completing an analysis of competing hypotheses, and ingesting threat intelligence reports. This will guide the practices of students during the rest of the labs in the course.
Topics: Case Study: Haver, Introduction to ICS Active Defense and Incident Response; Intelligence Life Cycle and Threat Intelligence; ICS Information Attack Surface; External ICS Threat Intelligence; Internal ICS Threat Intelligence; Sharing and Consuming ICS Threat Intelligence.

Day 2: Asset Identification and Network Security Monitoring
Understanding the networked environment is the only way to fully defend it: you cannot defend what you do not know. This course section will teach students to use tools such as Wireshark, TCPdump, SGUIL, ELSA, CyberLens, Bro, NetworkMiner, and Snort to map their ICS network, collect data, detect threats, and analyze threats to drive incident response procedures. During this section, students will be introduced to the lab network and an advanced persistent threat (APT) that is present on it. Drawing on threat intelligence from the previous course section, students will have to discover, identify, and analyze the threat using their new active defense skills to guide incident responders to the affected Human Machine Interface (HMI).

Day 3: Incident Response
The ability to prepare for and perform ICS incident response is vital to the safety and reliability of control systems. ICS incident response is a core concept in an ICS active defense and requires that analysts safely acquire digital evidence while scopeing the environment for threats and their impact on operations. ICS incident response is a young field with many challenges, but students in this section will learn effective tactics and tools to collect and preserve forensic-quality data. Students will then use these data to perform timely forensic analysis and create IOCs. In the previous section’s labs, APT malware was identified in the network. In this section, the labs will focus on identifying which system is impacted and gathering a sample of the threat that can be analyzed.
Topics: Case Study: Stuxnet; Incident Response and Digital Forensics Overview; Preparing an ICS Incident Response Team; Evidence Acquisition; Sources of Forensic Data in ICS Networks; Time-Critical Analysis; Maintaining and Restoring Operations.

Day 4: Threat and Environment Manipulation
Understanding the threat is key to discovering its capabilities and its potential to affect the ICS. The information extracted from threats through processes such as malware analysis is also critical to being able to make the necessary changes to the environment to reduce the effectiveness of the threat. The information obtained is vital to an ICS active defense, which requires internal data collection to create and share threat intelligence. In this section, students will learn how to analyze initial attack vectors such as spearphishing emails, perform timely malware analysis techniques, analyze memory images, and create Indicators of Compromise in YARA. The previous section’s labs identified the infected HMI and gathered a sample of the APT malware. In this section’s labs, students will analyze the malware, extract information, and develop YARA rules to complete the active defense model introduced in the class and maintain operations.
Topics: Case Study: German Steelworks; ICS Threat and Environment Manipulation Goals and Considerations; Establishing a Safe Working Environment; Analyzing Acquired Evidence; Memory Forensics; Malware Analysis Methodologies; Case Study: BlackEnergy2 Automated Analysis; Indicators of Compromise; Environment Manipulation.

Day 5: Active Defense and Incident Response Challenge
This section focuses on reinforcing the strategy, methodologies, skillsets, and tools introduced in the first four sections of the course. This entirely hands-on section will present students with two different scenarios. The first involves data collected from an intrusion into SANS Cyber City. The second involves data collected from a Distributed Control System (DCS) infected with malware. This section will truly challenge students to utilize their ICS active defense and incident response skills and test themselves.
Topics: Scenario One: Identify the Assets and Map the ICS Networks; Perform ICS Network Security Monitoring to Identify the Abnormalities; Execute ICS Incident Response Procedures Into the SANS Cyber City Data Files; Analyze the Malicious Capability and Determine if the Threat is an Insider Threat or a Targeted External Threat.

Who Should Attend
- ICS incident response team leads and members
- ICS and operations technology security personnel
- IT security professionals
- Security Operations Center team leads and analysts
- ICS red team and penetration testers
- Active defenders

“ICS515 integrated the OT/ICS side of security into the course well, not like other courses I’ve taken that taught general IT security with OT added as an afterthought.”
Josh Tanski, Morton Salt
Cyber Defense | 2-Day Courses

SEC440: Critical Security Controls: Planning, Implementing, and Auditing

This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS). These Critical Security Controls are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all serious and sensitive organizations. These controls were selected and defined by the U.S. military and other government agencies (including the NSA, DHS, GAO, and many others) and private organizations that are the most respected experts on how attacks actually work and what can be done to stop them. They defined these controls as their consensus for the best way to block known attacks and find and mitigate damage from the attacks that get through. For security professionals, the course will enable you to see how to put the controls in place in your existing network through widespread use of cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the controls are effectively implemented. SEC440 does not contain any labs. Students looking for hands-on labs involving the Critical Controls should take SEC566.

One of the best features of the course is that it uses offense to inform defense. In other words, you will learn about the actual attacks that you’ll be stopping or mitigating. That makes the defenses very real, and it makes you a better security professional.

You will find the full document describing the Critical Security Controls posted at the Center for Internet Security (www.cisecurity.org/controls).

SEC455: SIEM Design and Implementation

Security Information and Event Management (SIEM) can be an extraordinary benefit to an organization’s security posture, but understanding and maintaining it can be difficult. Many solutions require complex infrastructure and software that necessitate professional services for installation. The use of professional services can leave security teams feeling as if they do not truly own or understand how their SIEM operates. Combine this situation of complicated solutions with a shortage of available skills, a lack of simple documentation, and the high costs of software and labor, and it is not surprising that deployments often fail to meet expectations. A SIEM can be the most powerful tool a cyber defense team can wield, but only when it is used to its fullest potential. This course is designed to address this problem by demystifying SIEMs and simplifying the process of implementing a solution that is usable, scalable, and simple to maintain.

The goal of this course is to teach students how to build a SIEM from the ground up using the Elastic Stack. Throughout the course, students will learn about the required stages of log collection. We will cover endpoint agent selection, logging formats, parsing, enrichment, storage, and alerting, and we will combine these components to make a flexible, high-performance SIEM solution. Using this approach empowers SIEM engineers and analysts to understand the complete system, make the best use of technology purchases, and supplement current underperforming deployments. This process allows organizations to save money on professional services, increase the efficiency of internal labor, and develop a nimbler solution than many existing deployments. For example, many organizations pay thousands of dollars in consulting fees when a unique log source needs a custom parser. This course will train students how to easily parse any log source without requiring consulting services, saving their organizations both time and money, and facilitating faster collection and use of new log sources.

“SEC455 has made me rethink how I do event log monitoring and what I can do to improve.”

-Roger Christopher, Bureau of Land Management
Cyber Defense | 2-Day Course

SEC524: Cloud Security & Risk Fundamentals
SEC524: Cloud Security and Risk Fundamentals teaches you how to properly evaluate cloud providers and perform risk assessment. The course starts with a detailed introduction to the various cloud computing delivery models, ranging from Software as a Service (SaaS) to Infrastructure as a Service (IaaS) and everything in between. Each of these delivery models represents an entirely separate set of security conditions to consider, especially when coupled with various cloud types, including public, private, and hybrid.

Policy and governance within cloud environments will also be covered, including recommendations for both internal policies and contract provisions. This will lead us to a discussion of compliance and legal concerns. We’ll also conduct a mock exercise to review a cloud provider’s stated security capabilities and evaluate a simple risk score.

Day one of this two-day course will feature architecture and infrastructure fundamentals, plus a wide range of topics such as patch and configuration management, virtualization security, application security, and change management. As we walk through these fundamental cloud standards, you will learn how to immediately improve the ways in which your own team is deploying assets in the cloud.

Day two starts with an examination of disaster recovery and business continuity planning using cloud models and architecture. Cloud data storage has become common, so we’ll discuss how to protect those data, utilizing many tactics including identity and access management protocols. New approaches for data encryption, network encryption, key management, and data lifecycle concerns will be covered in detail. This will be followed by a discussion on intrusion detection and incident response in cloud environments, along with how to best manage these critical security processes and the technologies that support them, given that most controls are managed by the Cloud Service Provider (CSP). We’ll wrap up with a final risk assessment for your own projects potentially moving into cloud.

Penetration Testing | 2-Day Course

SEC564: Red Team Operations and Threat Emulation
Red Teaming is the process of using tactics, techniques, and procedures (TTPs) to emulate real-world threats in order to train and measure the effectiveness of the people, processes, and technology used to defend environments. Built on the fundamentals of penetration testing, Red Teaming uses a comprehensive approach to gain insight into an organization’s overall security in order to test its ability to detect, respond to, and recover from an attack. When properly conducted, Red Team activities significantly improve an organization’s security controls, hone its defensive capabilities, and measure the effectiveness of its security operations.

The Red Team concept requires a different approach from a typical security test and relies heavily on well-defined TTPs, which are critical to successfully emulate a realistic threat or adversary. Red Team results exceed a typical list of penetration test vulnerabilities, provide a deeper understanding of how an organization would perform against an actual threat, and identify where security strengths and weaknesses exist.

Whether you support a defensive or offensive role in security, understanding how Red Teams can be used to improve security is extremely valuable. Organizations spend a great deal of time and money on the security of their systems, and it is critical to have professionals who can effectively and efficiently operate those systems. SEC564 will provide you with the skills to manage and operate a Red Team, conduct Red Team engagements, and understand the role of a Red Team and its importance in security testing. This two-day course will explore Red Team concepts in-depth, provide the fundamentals of threat emulation, and help you reinforce your organization’s security posture.
Management | 2-Day Courses

MGT415: A Practical Introduction to Cyber Security Risk Management

In this course students will learn the practical skills necessary to perform regular risk assessments for their organizations. The ability to perform risk management is crucial for organizations hoping to defend their systems. There are simply too many threats, too many potential vulnerabilities that could exist, and not enough resources to create an impregnable security infrastructure. Therefore all organizations, whether they do so in an organized manner or not, will make priority decisions on how to best defend their valuable data assets. Risk management should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.

You Will Learn:

- How to perform a risk assessment step by step
- How to map an organization’s business requirements to implemented security controls
- The elements of risk assessment and the data necessary for performing an effective risk assessment
- About the in-depth risk-management models that exist to implement a deeper risk-management program in an organization

MGT433: SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program

Organizations have invested a tremendous amount of money and resources into securing technology, but little if anything into securing their workforce. As a result, people, not technology, have become the most common target for cyber attackers. The most effective way to secure the human element is to establish a mature security awareness program that goes beyond just compliance, changes peoples’ behaviors and ultimately creates a secure culture. This intense two-day course will teach you the key concepts and skills needed to do just that, and is designed for those establishing a new program or wanting to improve an existing one. Course content is based on lessons learned from hundreds of security awareness programs from around the world. In addition, you will learn not only from your instructor, but from extensive interaction with your peers. Finally, through a series of labs and exercises, you will develop your own custom security awareness plan that you can implement as soon as you return to your organization.

You Will Learn:

- The Security Awareness Maturity Model and how to leverage it as the roadmap for your awareness program
- How to gain and maintain leadership support for your program
- Key models for learning theory, behavioral change and cultural analysis
- How to identify different target groups and deploy role-based training
- How to effectively engage and communicate to your workforce, including addressing the challenges of different roles, generations and nationalities
- How to sustain your security awareness program over the long term, including advanced programs such as gamification and ambassador programs
- How to measure the impact of your awareness program, track reduction in human risk, and communicate the program’s value to leadership

“‘Our company is creating a formal cyber risk and controls assessment program. This class was a perfect introduction to the topic.’
- Jim Schleske, Ball Aerospace

“‘This course is a must for enhancing the overall security posture for any organization.’
- Pranav Teli, Saudi Aramco
Bonus Sessions

Enrich your SANS training experience! Evening talks led by our instructors and selected subject-matter experts help you broaden your knowledge, hear from the voices that matter in computer security, and get the most for your training dollar.

General Session – Welcome to SANS
Dr. Johannes Ullrich
Join us for a 30-minute overview to help you get the most out of your SANS training experience. You will receive event information and learn about programs and resources offered by SANS. This brief session will answer many questions and get your training experience off to a great start. This session will be valuable to all attendees but is highly recommended for first-time attendees.

KEYNOTE: State of the Internet Panel Discussion
Dr. Johannes Ullrich, ISC Director; Marcus Sachs; and Internet Storm Center Handlers
SANSFIRE offers the greatest opportunity to meet Internet Storm Center (ISC) handlers from around the world, and our most popular bonus session is their “State of the Internet” panel discussion. During this session, you will have the chance to hear from our handlers and ask their opinions and insights on current threats. This is a unique opportunity you will only have at SANSFIRE – a dozen of the industry’s brightest minds at your disposal for two intriguing hours!

Industrial Internet of Things Panel
Join us at SANSFIRE for the Industrial Internet of Things (IIoT) panel, where our subject-matter experts will address topics including:
• Use cases for IIoT, including smart factories and production, logistics and supply chain optimization, and safety and security
• What makes a contemporary IIoT architecture
• How does securing IIoT differ from other systems
• Important considerations for IIoT

Securing All the Things: CIS Benchmarks for the Win!
Rob Vandenbrink
A security benchmark is a great starting point to securing any platform, especially if you are not an expert on that platform. Even if you are an expert, a well-written benchmark document will make sure that things don't get missed. Or who knows, you might find a few things in that benchmark that you knew but forgot. In this session we’ll discuss the Center for Internet Security (CIS), and in particular the security benchmarks that are produced by the CIS. CIS benchmarks are vendor-agnostic, written and maintained by teams of volunteers. They cover soup-to-nuts security on more operating systems, applications or platforms than you’ll ever find in any one place. We’ll of course discuss how to use these benchmarks to secure any given platform. More importantly, we’ll talk about how to get involved: How to volunteer, how to budget time to see a benchmark through to successful completion, what the time commitment looks like, and how creating these documents as a team works.

Moving Past Just Googling It: Harvesting and Using OSINT
Micah Hoffman
Every single day we search for things on the Internet. Defenders research a domain or IP that contains malware. Attackers look for email addresses for an upcoming phishing campaign. DFIR people examine locations and usernames that they acquired from a subject's computer. Policy and compliance people examine the risk that employees in their organizations might bring to work. Recruiters scour the Internet looking for candidates. And normal people shop, date, geolocate, post, tweet, and otherwise send a huge amount of data to the public Internet.
Come join Micah Hoffman as we examine how Open-Source Intelligence (OSINT) can reveal interesting content about your work and personal lives.

Modern Information Security: Forget Cyber, It’s All About AppSec
Adrien de Beaupre
This discussion will focus on how modern information security has evolved and what we will need to move into the 21st century. We need a new paradigm in security with a workforce that understands application security: the new frontier.

Staying Offensive: The Changing Landscape of Offense
Tim Medin
Defense is changing and offense has to adapt accordingly. In this talk, Tim will discuss the changes in the landscape he has seen during his decade of experience in offense and what you can do to be more offensive. The goal of offense is to emulate real-world attackers so the defenders can test the technology and better respond to attacks. The aim is to help the blue team by being more offensive.

SANS State of OT/ICS Survey Findings
Doug Wylie and Jason Dely

Come to the Dark Side: Python’s Sinister Secrets
Mark Baggett
Python is in an incredible programming language that grants security super powers to those who know how to wield its might. But it has a sinister side that gives evil attackers the ability to conquer the unwitting developer. Come to this talk to learn about Python’s history of vulnerabilities and quirks that make attackers do their happy dance.
Oh, You Got This? Practical Attacks on Modern Infrastructure
Moses Frost

Have you ever been on a Web Assessment, Bug Bounty, Pen Test, or Red Team and encountered a component that is using the latest frameworks, languages, or libraries, or that is on the infrastructure? This presentation will provide a practical guide to approach these types of scenarios. Many of these technologies are strikingly new, and probably visually stunning, but are they entirely secure? This talk will explore concepts like Modernized Languages, Exposed In-Memory Databases, Proxies, Breaking Microservices, and more. We will show demos of how to abuse the latest architectures and frameworks. Follow Moses Frost as he breaks down the stuff that everyone else is just riding by, or discovering by accident. Let’s go attack the cloud people! This talk walks through the land of the cloud in a fun and storybook way. Let’s also figure out along the way how to break, attack, and pillage, for good.

A BEAST and a POODLE celebrating SWEET32
Bojan Zdrnja

In the last couple of years, we have witnessed many SSL/TLS vulnerabilities with various acronyms: POODLE, BEAST, BREACH, CRIME, DROWN, FREAK, and SWEET32 to name a few. Almost every time, a snazzy logo and a lot of panic around the vulnerability made us believe that this is the end of secure communication on the Internet. However, we are yet to see any real hacks that actually exploited one of the above-mentioned vulnerabilities. This presentation will explain how these vulnerabilities work and will comment on their viability for web, mobile, and fat client applications. We will try to identify the SSL/TLS vulnerabilities that cried wolf so we can concentrate on those that pose a serious threat (if such a threat exists, that is).

Let’s Go Hunting Bad Guys
John Strand

In this presentation John will share custom free tools to help you hunt bad guys inside and outside of your network...with awesomeness and math. But mostly math.

Building and Operating an OT/ICS Security Operations Center
Robert M. Lee

Security operations is an important aspect of countering targeted cyber threats. As organizations look at their industrial networks, such as the operations technology (OT) and industrial control systems (ICS), the discussion naturally comes up as to whether to include them in the IT SOC or establish an OT SOC. This presentation will walk through that decision process, right-sizing security for your organization as it relates to OT/ICS. We’ll also look at how to build and operate the OT SOC (whether it’s a dedicated entity or integrated).

Coffee and Donuts with the Graduate Students

Get the inside scoop on what it’s like to pursue a graduate degree in cybersecurity from SANS from like-minded information security professionals currently enrolled in SANS graduate programs. SANS regionally accredited graduate program, the SANS Technology Institute, combines SANS technical training and certifications with leadership and management curriculum specifically designed for the unique needs of aspiring leaders. Find out how the class you’re taking this week may be applied towards a master’s degree or graduate certificate program. Visit www.sans.edu for complete information on curriculum, admissions, and funding options.

Cutting the Wrong Wire: How a Clumsy Attacker Revealed a Global Cryptojacking Campaign
Renato Marinho

In 2018, we saw a massive spike in malicious crypto mining campaigns doing whatever it takes for the chance to have their victim’s Central Processing Unit. The shorter and shorter time window between vulnerability disclosure and cryptojacking opportunistic attacks taking advantage of them may help us to understand how profitable those attacks are, to the point of warranting priority over ransomware attacks. This presentation walks through a remarkable incident caused by an eager and clumsy attacker that ended up revealing multiple cryptojacking campaigns targeting large organizations across the world in early 2018. We’ll also look at the current panorama with the drop in the value of cryptocurrencies.

“Wide variety of excellent courses. The SANS@Night talks and NetWars make this an excellent training opportunity.”
-Lee Neely, LLNL
Adventures of the 100Gb Bloodhound
Tom Webb
Network speeds continue to grow, and incident response teams are getting overwhelmed sifting through it. What would you do if you were told that you are going to have a 100Gb Internet connection you need to monitor? When you have a major network upgrade, it’s a great time to evaluate what you are watching and why. In this session, we will discuss strategies for the reduction of monitored data, integration of client-side decryption, server-side decryption, tool deployment options and more.

Threat Hunting with OSSEC
Xavier Mertens
Open Source HIDS SECurity (OSSEC) is sometimes described as a low-cost log management solution, but it has many interesting features that, when combined with external sources of information, may help in hunting for suspicious activity occurring on your servers and end-points. During this presentation, Xavier will demonstrate how to use OSSEC to perform threat hunting. Then he will demonstrate how to deploy specific rules to catch suspicious activities and integrate the alerts with third-party tools.

Pcap or It Didn’t Happen: Sanitizing Pcap Files to Share With the Community
Brad Duncan
Sharing pcap files involves a certain amount of risk, because outside parties can gain insight into the environment of the packet capture. MAC addresses, internal (non-routable) IP address space, and other information that could reveal information about your environment are best kept private. For this reason, people are often advised not to share pcaps of malicious or suspicious activity outside of their organization. However, much of this sensitive information can be edited to mask characteristics of your network environment. In this presentation, Brad Duncan reviews how he edits pcap files before posting the information on his malware-traffic-analysis.net blog. With careful use of a hex editor and the tcperture command line tool, most pcap files can be sanitized to share with the general public. This talk details various types of commodity malware infections and the best way to mask sensitive data from the associated network traffic.

“SANS training is well-organized, and the extra speaking topics presented in the evening were good. I appreciate these extra lectures, as they are beneficial.”
-Andrew Crouse, Epiq

Vendor-Sponsored Events

Vendor Showcase
Wed, June 19  |  12:00pm - 1:30pm  |  5:15pm - 6:15pm
All attendees are invited to meet with established and emerging solution providers as they reveal the latest tools and technologies critical to information security. See the product offerings from key technology providers in the commercial tools and services market. Vendors arrive prepared to interact with a technically savvy audience. You’ll find product demos and partner information that feature all the best that the security industry has to offer!

Vendor-Sponsored Lunch & Learns
Since SANS course material is product neutral, these presentations provide the opportunity to evaluate vendor tools in an interactive environment to increase your effectiveness, productivity, and knowledge gained from the conference. These sessions feature a light meal or refreshments provided by the sponsor.
SANS Simulcast

You can attend SANSFIRE 2019 remotely with Simulcast

Simulcast is a great way to attend SANS cybersecurity courses remotely, with content streamed directly from the classroom to you. Additionally, Simulcast offers four months of access to revisit recorded lectures and labs and includes subject-matter-expert support.

Here are some benefits of taking your SANS training on the Simulcast platform:

- Dedicated, pre-event setup support so you are ready for class on day 1
- You can complete your course in one week through live, scheduled daytime sessions with SANS Certified Instructors
- In-class moderators who actively convey your questions to the instructor and ensure an interactive experience
- Teaching assistants available to support complex content and lab questions during your training sessions
- No travel, which extends training dollars and saves time
- The same instruction and learning outcomes as live training, with an additional four months of online access to recordings and virtual labs to absorb the course content

Simulcast Courses | SANSFIRE 2019

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Instructor</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
<td>Bryan Simon</td>
<td>Jun 17 - 22</td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td>John Strand</td>
<td>Jun 17 - 22</td>
</tr>
<tr>
<td>SEC505</td>
<td>Securing Windows and PowerShell Automation</td>
<td>Jason Fossen</td>
<td>Jun 17 - 22</td>
</tr>
<tr>
<td>SEC511</td>
<td>Continuous Monitoring and Security Operations</td>
<td>Seth Misenar</td>
<td>Jun 17 - 22</td>
</tr>
<tr>
<td>SEC530</td>
<td>Defensible Security Architecture</td>
<td>Ismael Valenzuela</td>
<td>Jun 17 - 22</td>
</tr>
<tr>
<td>SEC555</td>
<td>SIEM with Tactical Analytics</td>
<td>Justin Henderson</td>
<td>Jun 17 - 22</td>
</tr>
<tr>
<td>SEC566</td>
<td>Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td>James Tarala</td>
<td>Jun 17 - 21</td>
</tr>
<tr>
<td>DEV540</td>
<td>Secure DevOps and Cloud Application Security</td>
<td>Eric Johnson</td>
<td>Jun 17 - 21</td>
</tr>
</tbody>
</table>

Register now at www.sans.org/sansfire/attend-remotely

“I’m at home taking the online Simulcast class but I feel like I’m there in the room. I don’t feel isolated at all. I just have access to my comforts while taking the class.”

– Deona Vastine, State of California
Future SANS Training Events

Norfolk ...................................................... Norfolk, VA .......................... Mar 18-23

SANS 2019 Orlando, FL Apr 1-8

Boston Spring .............................................. Boston, MA .......................... Apr 14-19
Seattle Spring .............................................. Seattle, WA .......................... Apr 14-19
Northern VA – Alexandria .......................... Alexandria, VA ........................ Apr 23-28
Pen Test Austin ............................................. Austin, TX ............................. Apr 29 - May 4

Security West San Diego, CA May 9-16

Northern VA Spring – Reston ...................... Reston, VA ............................. May 19-24
New Orleans .............................................. New Orleans, LA ........................ May 19-24
Atlanta .................................................. Atlanta, GA ............................. May 28 - Jun 2
San Antonio .............................................. San Antonio, TX ........................ May 28 - Jun 2
Kansas City ............................................... Kansas City, MO ........................ Jun 10-15

SANSFIRE Washington, DC Jun 15-22

Charlotte .................................................. Charlotte, NC ........................ Jul 8-13
Pittsburgh .................................................. Pittsburgh, PA ........................ Jul 8-13
Columbia ................................................... Columbia, MD ........................ Jul 15-20

Future SANS Summit Events

ICS Security ................................................ Orlando, FL ............................ Mar 18-25
Blue Team .................................................. Louisville, KY ........................ Apr 11-18
Cloud Security .......................................... San Jose, CA ............................ Apr 29 - May 6
Security Operations ..................................... New Orleans, LA ........................ Jun 24 - Jul 1

Future Community SANS Events

Local, single-course events are also offered throughout the year via SANS Community. Visit www.sans.org/community for up-to-date Community course information.

Take SANS Training Anytime, Anywhere with OnDemand
More than 30 of the most popular SANS courses are available in our online training format OnDemand with no travel required. All OnDemand courses include:
• Four months of online access to your course
• Subject-matter-expert support
• Training with SANS top instructors
• All printed books and materials
• Labs and quizzes to reinforce your learning

Visit www.sans.org/ondemand to learn more about your OnDemand training options.
Marriott Wardman Park Hotel
2660 Woodley Road NW
Washington, DC  20008
202-328-2000
www.sans.org/sansfire/location

When you arrive at the Washington Marriott Wardman Park, you’ll find a charming neighborhood in the heart of Washington, DC filled with amazing restaurants and quaint shops. With a Metro stop just outside the doors and area airports close by, it’s a premier city destination just two Metro stops from everything DC has to offer.

Special Hotel Rates Available
A special discounted rate of $219 S/D plus applicable taxes will be honored based on space availability.

The SANSFIRE 2019 group rate is less than the posted government per diem rate in Washington, D.C. for June 2019. These rates include high-speed Internet in your room and are only available through May 16, 2019.

Top three reasons to stay at the Washington Marriott Wardman Park
1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Washington Marriott Wardman Park, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
3. SANS schedules morning and evening events at the Washington Marriott Wardman Park that you won’t want to miss!

Registration Information
Register online at www.sans.org/sansfire
We recommend you register early to ensure you get your first choice of courses.

Select your course and indicate whether you plan to test for GIAC certification. If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone. An email confirmation will be sent to you when once the registration form has been completed. If you have not received this email confirmation within two business days of registering, please call 301-654-7267 or contact registration@sans.org for assistance.

Pay Early and Save*

<table>
<thead>
<tr>
<th>DATE</th>
<th>DISCOUNT</th>
<th>DATE</th>
<th>DISCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr 24</td>
<td>$350</td>
<td>May 15</td>
<td>$200</td>
</tr>
</tbody>
</table>

*Some restrictions apply. Early bird discounts do not apply to Hosted courses.

SANS SIMULCAST
Nothing beats the SANS live training experience, but if you are unable to attend, learn how you can register for a SANSFIRE 2019 Simulcast course. Visit www.sans.org/sansfire/attend-remotely

SANS Voucher Program
Expand your training budget!
For organizations with multiple employees taking SANS training courses, the SANS Voucher Program is an easy-to-use, flexible training management solution. Based on the number of anticipated students and investment, you may be eligible to receive bonus funds from SANS. Your investment and bonus funds can be used for classroom and online training, and can also be used to pay for GIAC certification exams. Contact SANS for more detailed information about our Voucher Program. www.sans.org/vouchers

Cancellation & Access Policy
If an attendee must cancel, a substitute may attend instead. Substitution requests can be made at any time prior to the event start date. Processing fees will apply. All substitution requests must be submitted by email to registration@sans.org. If an attendee must cancel and no substitute is available, a refund can be issued for any payments received by May 22, 2019. A credit memo can be requested up to the event start date. All cancellation requests must be submitted in writing by mail or fax and received by the stated deadlines. Payments will be refunded by the method that they were submitted. Processing fees will apply.
## Registration Fees

Register online at [www.sans.org/sansfire](http://www.sans.org/sansfire)

If you don’t wish to register online, please call [301-654-SANS (7267)](tel:301-654-7267) 9:00am-8:00pm (Mon-Fri) EST and we will fax or mail you an order form.

### Courses – 4–6 Days

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Course fee if taking a 4-6 day course</th>
<th>Course fee</th>
<th>Add GIAC Cert</th>
<th>Add OnDemand</th>
<th>Add NetWars Continuous</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC301</td>
<td>Introduction to Cyber Security</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>SEC660</td>
<td>Enterprise Threat and Vulnerability Assessment</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>SEC687</td>
<td>Open-Source Intelligence (OSINT) Gathering and Analysis <strong>NEW!</strong></td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>SEC501</td>
<td>Advanced Security Essentials – Enterprise Defender</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>SEC503</td>
<td>Intrusion Detection In-Depth</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>SEC505</td>
<td>Securing Windows and PowerShell Automation</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>SEC506</td>
<td>Securing Linux/Unix</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>SEC511</td>
<td>Continuous Monitoring and Security Operations</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>SEC530</td>
<td>Defensible Security Architecture <strong>NEW!</strong></td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>SEC542</td>
<td>Web App Penetration Testing and Ethical Hacking</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>SEC545</td>
<td>Cloud Security Architecture and Operations</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>SEC555</td>
<td>SIEM with Tactical Analytics</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>SEC560</td>
<td>Network Penetration Testing and Ethical Hacking</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>SEC566</td>
<td>Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>SEC573</td>
<td>Automating Information Security with Python</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>SEC575</td>
<td>Mobile Device Security and Ethical Hacking</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>SEC599</td>
<td>Defeating Advanced Adversaries – Purple Team Tactics &amp; Kill Chain Defenses</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>SEC617</td>
<td>Wireless Penetration Testing and Ethical Hacking</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>SEC642</td>
<td>Advanced Web App Penetration Testing, Ethical Hacking &amp; Exploitation Techniques</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>SEC660</td>
<td>Advanced Penetration Testing, Exploit Writing, and Ethical Hacking</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>SEC760</td>
<td>Advanced Exploit Development for Penetration Testers</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>FOR500</td>
<td>Windows Forensic Analysis</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Digital Forensics, Incident Response, and Threat Hunting</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>FOR518</td>
<td>Mac and iOS Forensic Analysis and Incident Response</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>FOR526</td>
<td>Advanced Memory Forensics &amp; Threat Detection</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>FOR572</td>
<td>Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>FOR578</td>
<td>Cyber Threat Intelligence</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>FOR585</td>
<td>Smartphone Forensic Analysis In-Depth</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>FOR610</td>
<td>Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>MGT414</td>
<td>SANS Training Program for CISSP® Certification</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>MGT512</td>
<td>Security Leadership Essentials for Managers <strong>NEW!</strong></td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>MGT514</td>
<td>Security Strategic Planning, Policy, and Leadership</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>LEG523</td>
<td>Law of Data Security and Investigations</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>DEV540</td>
<td>Secure DevOps and Cloud Application Security</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>ICS410</td>
<td>ICS/SCADA Security Essentials</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
<tr>
<td>ICS515</td>
<td>ICS Active Defense and Incident Response</td>
<td>$769</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
<td></td>
</tr>
</tbody>
</table>

### Skill-Based Short Courses

- **SEC440** Critical Security Controls: Planning, Implementing, and Auditing
  - Course fee if taking a 4-6 day course: $1,980
  - Add GIAC Cert: $2,640
  - Add OnDemand: $299

- **SEC455** SIEM Design & Implementation
  - Course fee if taking a 4-6 day course: $1,980
  - Add GIAC Cert: $2,640
  - Add OnDemand: $299

- **SEC524** Cloud Security & Risk Fundamentals
  - Course fee if taking a 4-6 day course: $1,980
  - Add GIAC Cert: $2,640
  - Add OnDemand: $299

- **SEC564** Red Team Operations and Threat Emulation
  - Course fee if taking a 4-6 day course: $1,980
  - Add GIAC Cert: $2,640
  - Add OnDemand: $299

- **MG5415** A Practical Introduction to Cyber Security Risk Management
  - Course fee if taking a 4-6 day course: $1,980
  - Add GIAC Cert: $2,640
  - Add OnDemand: $299

- **MG5433** SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program
  - Course fee if taking a 4-6 day course: $1,980
  - Add GIAC Cert: $2,640
  - Add OnDemand: $299

- **SPECIAL** Core NetWars Experience – Tournament Entrance Fee
  - Payment: FREE

- **SPECIAL** DFIR NetWars Tournament – Tournament Entrance Fee
  - Payment: FREE

- **SPECIAL** Cyber Defense NetWars Tournament – Tournament Entrance Fee
  - Payment: $1,695

### Early Bird Discounts

- Pay for any long course using the code **EarlyBird19** at checkout by
  - **April 24th** to get $350 OFF or by **May 15th** to get $200 OFF*

*Some restrictions apply. Early bird discounts do not apply to Hosted courses.*
Join the SANS.org community today to enjoy these free resources at www.sans.org/join

Newsletters

NewsBites
Twice-weekly, high-level executive summary of the most important news relevant to cybersecurity professionals.

OUCH!
The world’s leading monthly free security awareness newsletter designed for the common computer user.

Webcasts

Ask the Experts Webcasts
SANS experts bring current and timely information on relevant topics in IT Security.

Analyst Webcasts
A follow-on to the SANS Analyst Program, Analyst Webcasts provide key information from our whitepapers and surveys.

Other Free Resources (SANS.org account not required)

• InfoSec Reading Room
• Top 25 Software Errors
• 20 Critical Controls
• Security Policies
• Intrusion Detection FAQs
• Tip of the Day

@RISK: The Consensus Security Alert
A reliable weekly summary of newly discovered attack vectors, vulnerabilities with active new exploits, how recent attacks worked, and other valuable data.

WhatWorks Webcasts
The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT Security issues.

Tool Talks
Tool Talks are designed to give you a solid understanding of a problem, and how a vendor’s commercial tool can be used to solve or mitigate that problem.

SAVE $350
Register and pay by April 24th
Use code EarlyBird19

www.sans.org/sansfire

To be removed from future mailings, please contact unsubscribe@sans.org or 301-654-SANS (7267). Please include name and complete address.

NALT-BRO-SANSFIRE2019