Advance your career and protect your organization with cybersecurity training and GIAC Certifications. Choose from 40 hands-on, immersion-style courses taught by the most respected practitioners in the field.

Look inside for these new courses!

- SEC450: Blue Team Fundamentals: Security Operations and Analysis
- FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics
- FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response
- ICS612: ICS Cyber Security In-Depth

SAVE $300 Register and pay by Oct 16th
Use code EarlyBird19

www.sans.org/cdi

“The decision to take five days away from the office is never easy, but so rarely have I come to the end of a course and had no regrets whatsoever. This was one of the most useful weeks of my professional life.”

-Dan Trueman, Novae PLC
## Courses at a Glance

For an up-to-date course list, please check the website at [www.sans.org/cdi/schedule](http://www.sans.org/cdi/schedule)

<table>
<thead>
<tr>
<th>Course Number</th>
<th>Course Title</th>
<th>Page</th>
<th>Available via Simulcast</th>
<th>Bundle/OnDemand with this course</th>
<th>Hours DD&amp;B $440 (50%) Requirements</th>
<th>Instructor</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC401</td>
<td>Introduction to Cyber Security</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC402</td>
<td>Security Essentials Bootcamp Style</td>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC440</td>
<td>Critical Security Controls: Planning, Implementing, and Auditing</td>
<td>75</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC550</td>
<td>Blue Team Fundamentals: Security Operations and Analysis</td>
<td>NEW!</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC455</td>
<td>SIEM Design and Implementation</td>
<td>75</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC487</td>
<td>Open-Source Intelligence (OSINT) Gathering and Analysis</td>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC501</td>
<td>Advanced Security Essentials – Enterprise Defender</td>
<td>18</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC503</td>
<td>Intrusion Detection In-Depth</td>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td>22</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC505</td>
<td>Securing Windows and PowerShell Automation</td>
<td>24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC511</td>
<td>Continuous Monitoring and Security Operations</td>
<td>26</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC530</td>
<td>Defensible Security Architecture and Engineering</td>
<td>28</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC545</td>
<td>Cloud Security Architecture and Operations</td>
<td>30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC555</td>
<td>SIEM with Tactical Analytics</td>
<td>32</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC566</td>
<td>Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td>34</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC599</td>
<td>Defeating Advanced Adversaries – Purple Team Tactics &amp; Kill Chain Defenses</td>
<td>36</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC640</td>
<td>Enterprise Threat and Vulnerability Assessment</td>
<td>34</td>
<td></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>
<td></td>
</tr>
<tr>
<td>SEC650</td>
<td>Network Penetration Testing and Ethical Hacking</td>
<td>44</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC652</td>
<td>Red Team Exercises &amp; Adversary Emulation</td>
<td>76</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC673</td>
<td>Automating Information Security with Python</td>
<td>46</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC680</td>
<td>Metasploit Kung Fu for Enterprise Pen Testing</td>
<td>76</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC660</td>
<td>Advanced Penetration Testing, Exploit Writing, and Ethical Hacking</td>
<td>48</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOR500</td>
<td>Windows Forensic Analysis</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Incident Response, Threat Hunting, and Digital Forensics</td>
<td>NEW!</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOR572</td>
<td>Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response</td>
<td>52</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOR578</td>
<td>Cyber Threat Intelligence</td>
<td>56</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOR585</td>
<td>Smartphone Forensic Analysis In-Depth</td>
<td>58</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOR610</td>
<td>Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td>
<td>60</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MGT444</td>
<td>SANS Training Program for CISSP® Certification</td>
<td>62</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MGT454</td>
<td>A Practical Introduction to Cyber Security Risk Management</td>
<td>77</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MGT433</td>
<td>SANS Security Awareness: How to Build, Maintain, and Measure a Awareness</td>
<td>77</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MGT512</td>
<td>Security Leadership Essentials for Managers</td>
<td>64</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MGT514</td>
<td>Security Strategic Planning, Policy, and Leadership</td>
<td>68</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUD607</td>
<td>Auditing &amp; Monitoring Networks, Perimeters, and Systems</td>
<td>77</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC334</td>
<td>Secure DevOps: A Practical Introduction</td>
<td>77</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC340</td>
<td>Cloud Security and DevOps Automation</td>
<td>70</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC410</td>
<td>ICS/SCADA Security Essentials</td>
<td>72</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICS315</td>
<td>ICS Active Defense and Incident Response</td>
<td>73</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICS312</td>
<td>ICS Cyber Security In-Depth</td>
<td>BETA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SANS Institute</td>
<td>SANS Training Roadmap</td>
<td>6-7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The SANS Faculty</td>
<td>SANS OnDemand Bundle</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICS</td>
<td>Cyber Defense NetWars Tournament</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DRW</td>
<td>Cyber Defense NetWars Tournament</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SANS Cyber Immersion Academy</td>
<td>Free Resources</td>
<td>Back Cover</td>
<td>80</td>
<td>Hotel Information</td>
<td>84</td>
<td>Registration Fees</td>
</tr>
<tr>
<td>SANS Simulcast</td>
<td>Registration Information</td>
<td>84</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SANS Security Awareness</td>
<td>SANS Simulcast Registration</td>
<td>84</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Future SANS Training Events</td>
<td>SANS Voucher Program</td>
<td>84</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Institute</td>
<td>2</td>
</tr>
<tr>
<td>The SANS Faculty</td>
<td>3</td>
</tr>
<tr>
<td>SANS OnDemand Bundle</td>
<td>8</td>
</tr>
<tr>
<td>SANS Technology Institute</td>
<td>9</td>
</tr>
<tr>
<td>GIAC Certification Bundle</td>
<td>8</td>
</tr>
<tr>
<td>Bonus Sessions</td>
<td>78-79</td>
</tr>
<tr>
<td>Vendor-Sponsored Events</td>
<td>79</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 who bring 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 CERTIFICATION**

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](http://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 and with 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](http://www.sans.org)
At SANS, our course authors and instructors are renowned cybersecurity experts who share their knowledge by drawing on their own real-world experiences 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.

Meet the SANS faculty: www.sans.org/cdi/instructors

“SANS instructors are the best in the game. Their technical knowledge combined with presentation skills and real-world examples make for an unparalleled training experience. SANS rocks!”

-Chris Gergen, Bank of North Dakota
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.
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 purposefully develop its personnel to either be generalists who can engage in multiple tactics or specialists who deep dive into a critical niche. 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.
### Baseline Skills

#### New to Cyber Security
- **Concepts, Terms, and Skills**
  - **Security Fundamentals**: SEC501 Introduction to Cyber Security | GISP
  - **Hacker Techniques**: SEC502 Hacker Tools, Techniques, Exploits, and Incident Handling | GCIH

All professionals entrusted with hands-on cybersecurity work should be trained to possess a common set of capabilities enabling them to secure systems, practice defense-in-depth, understand how attacks work, and manage incidents when they occur. To be secure, you should set a high bar for the baseline set of skills in your security organization.

#### Core Techniques
- **Prevent, Detect, Maintain**
  - **Security Essentials**: SEC280 Security Essentials Bootcamp Style | GCED
  - **Hacker Tools**: SEC502 Hacker Tools, Techniques, Exploits, and Incident Handling | GCIH

#### Security Management
- **Managing Technical Security Operations**
  - **Every Security Manager Should Know**
    - **Leadership Essentials**: MGT414 Security Leadership Essentials for Managers | GSEC
    - **Critical Controls**: SEC505 Cloud Security Architecture and Operations | GMON

With an increasing number of failure technologies, organizations require effective leaders to manage their teams and processes. While managers will not necessarily perform hands-on work, they must have enough about the underlying technologies and frameworks to help set strategy, develop appropriate policies, interact with skilled practitioners, and oversee outcomes.

### Focus Job Roles

#### Monitoring & Detection
- **Intelligence-Detection, Monitoring Over Time**
  - **Intrusion Detection**: SEC303 Intrusion Detection in-depth | GSIAT
  - **Monitoring & Operations**: SEC513 Continuous Monitoring and Security Operations | GCWN

The detection of what is happening in your environment requires an increasingly sophisticated set of skills and capabilities. Identifying security anomalies requires increased depth of understanding to develop detection and monitoring tools and interpret their output.

#### Penetration Testing
- **Vulnerability Analysis, Ethical Hacking**
  - **Every Pen Tester Should Know**
    - **Networks**: SEC550 Network Penetration Testing and Ethical Hacking | GSEC
    - **Web Apps**: SEC542 Web App Penetration Testing and Ethical Hacking | GCWN

The professional who can find weaknesses is often a different breed than one focused exclusively on building defenses. A basic level of core蓝队 team deployments is in finding vulnerabilities requires a different type of thinking, and different tools, but it is essential for defense specialists to improve their defenses.

#### Incident Response & Threat Hunting
- **Host and Network Forensics**
  - **Endpoint Forensics**: FOR555 Windows Forensics | GIAC
  - **Network Forensics**: FOR554 Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response | GIAC

Whether you’re working to maintain a trail of evidence on host or network systems, or hunting for threats using similar techniques, larger organizations need specialized professionals who can move beyond their response incident handling in order to analyze an attack and develop an appropriate remediation and recovery plan.

### Crucial Skills, Specialized Roles

#### Cyber Defense Operations
- **Hardened Specific Defenses**
  - **Specialized Defense Area**
    - **GSAF**: SEC451 Open Source Intelligence (OSINT) Gathering and Analysis
    - **Advanced Forensics**: SEC501 Advanced Forensics - Enterprise Defender | GSEC
    - **Cloud Security**: SEC505 Cloud Security Architecture and Operations
    - **Windows/Powershell**: SEC505 Securing Windows and PowerShell Automation | GCWN
    - **Linux/Unix Defense**: SEC505 Securing Linux/Unix | GSEC
    - **SIEM**: SEC505 SIEM with Tactical Analytics | GCDA
    - **Security Architecture**: SEC510 Defensible Security Architecture and Engineering | GEDA
    - **Threat Defense**: SEC519 Defending Advanced Adversaries - Purple Team Tactics and Full-Scale Defenses | GIAT

#### Specialized Penetration Testing
- **Focused Techniques and Areas**
  - **In-Depth Coverage**
    - **Vulnerability Assessment**: SEC280 Enterprise Threat and Vulnerability Assessment | GIAT
    - **Networks**: SEC500 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking | GISP
    - **Web Apps**: SEC542 Advanced Web-App Penetration Testing, Ethical Hacking, and Exploitation Techniques
    - **Mobile**: SEC571 Mobile Device Security and Ethical Hacking | GCWN
    - **Windows**: SEC515 Windows Penetration Testing and Ethical Hacking | GISP
    - **Python Coding**: SEC571 Automating Information Security with Python | GCPC

#### Digital Forensics, Malware Analysis, & Threat Intel
- **Specialized Investigation Skills**
  - **Malware Analysis**: SEC555 Reverse Engineering Malware: Malware Analysis Tools and Techniques | GIAT
  - **Threat Intelligence**: SEC571 Digital Forensics and malware Analysis | GCDC
  - **Cyber Threat Intelligence**: SEC571 Cyber Threat Intelligence | GIAT
  - **Digital Forensics & Malware Exploitation**
    - **Smartphones**: SEC555 Smartphone Forensics: Analysis in Depth | GIAT
    - **Memory Forensics**: SEC555 Advanced Memory Forensics & Threat Detection
  - **IoT Forensics**: SEC555 Internet of Things Forensics Analysis and Incident Response

#### Advanced Management
- **Advanced Leadership, Audit, Legal**
  - **Management Skills**
    - **Planning, Policy, Leadership**: SEC501 Security Planning, Policy, and Leadership | GIAT

### Industrial Control Systems
- **ICS Security Professionals Need**
  - **Essentials**: SEC730 ICS/SCADA Security Essentials | GCSP
  - **ICS Defense & Response**: SEC731 ICS Active Defense and Incident Response | GIAT
  - **MIRE Protection**: SEC745 MIRE Security Essentials | GCSP
  - **NERC Essentials**: SEC730 ICS/SCADA Security Essentials | GCSP

### Development and Secure Coding
- **Every Developer Should Know**
  - **Secure Web Apps**: DEV502 Defending Web Applications Security Essentials | GICSP
  - **Secure Development**: DEV501 Cloud Security and Development Automation

#### Language-Specific Courses
- **JAVA/BE**: DEV514 Secure Coding in Java/Beta Developing Defensible Applications
- **NET**: DEV518 Secure Coding in .NET Developing Defensible Applications

### Advanced Penetration Testing, Exploit Writing, and Exploitation Techniques
- **Focused Techniques and Areas**
  - **In-Depth Coverage**
    - **Vulnerability Assessment**: SEC280 Enterprise Threat and Vulnerability Assessment | GIAT
    - **Networks**: SEC500 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking | GISP
    - **Web Apps**: SEC542 Advanced Web-App Penetration Testing, Ethical Hacking, and Exploitation Techniques
    - **Mobile**: SEC571 Mobile Device Security and Ethical Hacking | GCWN
    - **Windows**: SEC515 Windows Penetration Testing and Ethical Hacking | GISP
    - **Python Coding**: SEC571 Automating Information Security with Python | GCPC

### See in-depth course descriptions and the digital version of this roadmap at: www.sans.org/roadmap

To learn more about additional SANS courses, go to: 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

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

“The course content and OnDemand delivery method have both exceeded my expectations.”

-ROBERT JONES, TEAM JONES, INC.

“GIAC is the only certification that proves you have hands-on technical skills.”

-CHRISTINA FORD, DEPARTMENT OF COMMERCE

Special Pricing

*GIAC and OnDemand Bundles are only available for certain courses.
NetWARS Tournament

Experience NetWARS at CDI 2019
Sunday, December 15 & Monday, December 16

Choose from:

- Core NetWars  
- Cyber Defense NetWars
- DFIR NetWars
- ICS NetWars

Develop skills in:

- Cyber Defense
- Digital Forensics and Incident Response
- ICS/SCADA Security
- Penetration Testing

NetWars takes place in the evening, after class, and gives you an immediate opportunity to apply what you’ve learned in a fun and collaborative environment.

- Play NetWars solo or on a team of up to 5 players.
- Experience NetWars for free when taking a 4-, 5-, or 6-day course at SANS Cyber Defense Initiative® 2019.
- Add NetWars when you register for your course, as seating is limited.

What Our Students Think

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

“Core NetWars was challenging but not frustrating for newbies. My first time doing NetWars has been a blast.”
- Rachael Murray, Northwestern Mutual

“Learned a lot and had a lot of fun.”
- Gustavo Bobbio, Amazon

“I learned so much in six hours of NetWars.”
- Peter Smith, Best Western International

sans.org/netwars
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.

“SEC301 is an extremely valuable course, even for someone with 12 years of IT experience!”

-Brian Pfau, Banfield Pet Hospital

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 a MIS director for a small company before joining AT&T/Lucent as a Senior Security Architect working on engagements with the Department of Defense 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, GCIA, GCED, GISeF, CEH, Security+, Network+, A+, CTT+).
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 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 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 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 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

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 (WiFi 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, including 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

You Will Be Able To

- Apply what you learned directly to your job when you go back to work
- Design and build a network architecture using VLANs, NAC, and 802.1x based on advanced persistent threat indicators of compromise
- 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
- Install VMWare and create virtual machines to create a virtual lab to test and evaluate tools/security of systems
- Create an effective policy that can be enforced within an organization and design a checklist to validate security and create metrics to tie into training and awareness
- Identify visible weaknesses of a system using various tools and, once vulnerabilities are discovered, cover ways to configure the system to be more secure
- Build a network visibility map that can be used for hardening of a network – validating the attack surface and covering ways to reduce that surface by hardening and patching
- Sniff open protocols like telnet and ftp and determine the content, passwords, and vulnerabilities using WireShark

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, GCIA, 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 SEC501: Advanced Security Essentials – Enterprise Defender; SEC505: Securing Windows and Powershell Automaton; and SEC511: Continuous Monitoring and Security Operations.
# Course Day Descriptions

## 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

---

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/cdi/courses](http://www.sans.org/cdi/courses)
Is your organization looking for a quick and effective way to onboard new security analysts, engineers, and architects? Do your Security Operations Center (SOC) managers need additional technical perspective on how to improve analysis quality, reduce turnover, and run an efficient SOC?

SEC450 is an accelerated on-ramp for new cyber defense team members and SOC managers. This course introduces students to the tools common to a defender’s work environment, and packs in all the essential explanations of tools, processes, and data flow that every blue team member needs to know.

Students will learn the stages of security operations: how data are collected, where they are collected, and how threats are identified within those data. The class dives deep into tactics for triage and investigation of events that are identified as malicious, as well as how to avoid common mistakes and perform continual high-quality analysis. Students will learn the inner workings of the most popular protocols, and how to identify weaponized files as well as attacks within the hosts and data on their network.

The course employs practical, hands-on instruction using a simulated SOC environment with:

- Security Information and Event Management (SIEM)
- An incident tracking and management system
- A threat intelligence platform
- Packet capture and analysis
- Automation tools

While cyber defense can be a challenging and engaging career, many SOCs are negatively affected by turnover. To preemptively tackle this problem, this course also presents research-backed information on preventing burnout and how to keep engagement high through continuous growth, automation, and false positive reduction. Students will finish the course with a full-scope view of how collection and detection work, how SOC tools are used and fit together, and how to keep their SOC up and running over the long term.

“I was able to use the information presented in the morning, during a work call at lunch, on day 1! The course paid for itself on the first day.”

- Lawrence Nunn, ARCYBER

John Hubbard is a SOC consultant and speaker, the course author of SEC450 and SEC455. Additionally, John is an instructor for SANS blue team courses such as SEC511 and SEC555. Through his years of experience as a Lead Cyber Security Analyst and SOC Manager for GlaxoSmithKline, John developed real-world, first-hand knowledge of what it takes to defend an organization against advanced cyber-attacks. Today, John specializes in security operations, threat hunting, network security monitoring, SIEM design and optimization, and constructing defensible networks that allow organizations to protect their most sensitive data. John’s mission to improve blue teams worldwide led him to partner with SANS to help develop the next generation of defensive talent around the world. John holds a bachelor’s degree in electrical engineering from Purdue and a master’s degree in computer engineering, focusing on information security, from SUNY Binghamton. In his free time, John enjoys FPV drone racing, coffee roasting, and slowly turning his home into a data center.

@SecHubb
**Course Day Descriptions**

**DAY 1: Blue Team Tools and Operations**
This day starts with an introduction to the Blue Team, the mission of a SOC, and how to understand an organization’s threat model and risk appetite. It is focused on top-down learning to explain the mindset of an analyst, the workflow, and monitoring tools used in the battle against attackers. Throughout this course, students will learn how SOC information management tools fit together, including incident management systems, threat intelligence platforms, SIEMs, and SOAR tools. We end the day describing the various groups of attackers, how their methods differ, and their motivations.

**Topics:** Introduction to the Blue Team Mission; SOC Overview; Defensible Network Concepts; Events, Alerts, Anomalies, and Incidents; Incident Management Systems; Threat Intelligence Platforms; SIEM; Automation and Orchestration; Who Are Your Enemies?

**DAY 2: Understanding Your Network**
Day 2 begins the technical journey of understanding the environment. To defend a network, you must thoroughly understand its architecture and the impact that it will have on analysis. This day introduces the concepts of a modern organization’s network traffic flow by dissecting a basic home Internet connection and describing the features necessary for segmentation and monitoring. These modules ensure that students have a firm grasp on how network design affects their “view of the world” as an analyst. We then go in-depth on common network services. Day 2 provides thorough working explanations of the current and upcoming features of DNS, HTTPS(5), SMTP, and more, with a focus on the most important points for analysts to understand. These sections explain what normal data look like, as well as the common fields and areas that are used to spot anomalous behavior. The focus will be on quickly recognizing the common tricks used by attackers to turn these everyday services against us.

**Topics:** Corporate Network Architecture; Traffic Capture and Visibility; Understanding DNS; DNS Analysis and Attacks; Understanding HTTP and HTTPS; Analyzing HTTP for Suspicious Activity; How SMTP and Email Attacks Work; Additional Important Protocols

**DAY 3: UnderstandingEndpoints, Logs, and Files**
It is extremely difficult to succeed at cyber defense without knowing where and how your data are produced, so day 3 takes us down to the host, logging, and file level. Starting with an overview of common endpoint-based attack tactics, we orient students to the array of techniques that are used against their hosts. These first sections, followed by a section on defense in-depth, will give students an idea of how each step of the attack lifecycle aligns with its defensive tools, and what students can use to prevent and detect adversary attack advancement on their endpoints. The course then turns to the parsing and enrichment of logs, as well as how the SIEM normalization and categorization processes work. These topics give a complete view of what happens from the moment a log is generated to when it shows up in our security tools. The final part of day 3 provides students with the concepts needed to reason through the answer, diving into files at the byte level. Students will finish this day understanding how different common file formats work, how they are typically weaponized, and how to quickly decide whether a given sample is likely to be malicious.

**Topics:** Endpoint Attack Tactics; Endpoint Defense In-Depth; How Windows Logging Works; How Linux Logging Works; Interpreting Important Events; Kerberos and Active Directory Events; Log Collection, Parsing, and Normalization; Files Contents and Identification; Identifying and Handling Suspicious Files

**DAY 4: Triage and Analysis**
Now that the course has covered the ground required to understand the tools and data most frequently encountered by analysts, it’s time to focus on analysis itself. This day will focus on how the analysis process works and explain how to avoid the common mistakes new analysts can slip into. We can combat the tendency to overlook the obvious by examining how our memory perception affects analysis and how cognitive biases cause us to fail to see what is right in front of us. The goal is to teach students not only how to think clearly, but also how to explain and leave a trail of how they reached their conclusions that can support future analysis and act as an audit trail. In addition, we will cover many of the mental models and concepts used in information security from both the offensive and defensive perspectives. Students will then use these models to look at an alert queue and get a quick and intuitive understanding of which alerts may pose the biggest threat, and thus must be attended to first. Safe analysis techniques and operational security concerns are covered to ensure that we do not give up our tactical advantage during the investigation process. We’ll discuss specifics on alert triage methods and prioritization, as well as investigation techniques, so that students will leave this day better prepared to understand their alert queues and perform error-free investigation.

**Topics:** Alert Triage and Prioritization; Perception and Investigation; Memory and Investigation; Mental Models for Information Security; Structured Analysis Techniques; Analysis Tactics and OPSEC; Network, File, and Event Alerts; Intrusion Discovery; Incident Closing and Quality Review

**DAY 5: Continuous Improvement, Analytics, and Automation**
This day focuses squarely on improving the efficiency and enthusiasm of working in SOCs by tackling the most common problems head on. Through process optimization, careful analytic design and tuning, and workflow efficiency improvements, we can eliminate many of these common pain points. This frees us from the repetitive work we loathe and allows us to focus on what we do best – analysis! Having the time for challenging and novel work leads to a virtuous cycle of growth and engagement throughout the SOC – while improving everyone’s life in the process. This day will focus on tuning your tools using clever analysis techniques and process automation to remove the monotonous and non-value-added activities from your day. We also cover containment activities, including the tools you can use and how to decide when to use them. Students will also have the opportunity to develop incident or infection from the host or network angle. We’ll wrap up the day with recommendations on skill growth, long-term career development, and how to get more involved in the cyber defense community.

**Topics:** Improving Life in the SOC; Analytic Features and Enrichment; New Analytic Design, Testing, and Sharing; Tuning and False Positive Reduction, Automation and Orchestration; Improving Operational Efficiency and Workflow, Containing Identified Intrusions; Skill and Career Development

**DAY 6: Capstone: Defend the Flag**
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 be challenged to progress through multiple levels and missions designed to ensure mastery of the concepts and data covered during the course.

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/cdi/courses](http://www.sans.org/cdi/courses)
SEC487: **Open-Source Intelligence (OSINT) Gathering and Analysis**

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.

**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

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

-Dave Huffman, Rockwell Automation

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
Course Day Descriptions

**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, Divining 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 they 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 two 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

**Who Should Attend**

- Cyber incident responders
- Digital Forensics and Incident Response (DFIR) analysts
- Penetration testers
- Social engineers
- Law enforcement personnel
- Intelligence personnel
- Recruiters
- Private investigators
- Insurance investigators
- Human resources personnel
- Researchers

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

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

“Immediate value of putting concepts into standard practice.”

- Manny Cadiz, EMF Broadcasting

“If you want get deep-dive about enterprise security, then you must take SANS course SEC501.”

- Nikolai Vinogradov, JSC Severstal Management

Register at www.sans.org/cdi | 301-654-SANS (7267)
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 triaging 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 engine 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.
SEC503: Intrusion Detection In-Depth

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

SEC503 is one of the most important courses that you will take in your information security career. While past students describe it as the most difficult class they have ever taken, they also tell us it was the most rewarding. This course isn’t for people who are simply looking to understand alerts generated by an out-of-the-box Intrusion Detection System (IDS). It’s for people who want to deeply understand what is happening on their network today, and who suspect that there are very serious things happening right now that none of their tools are telling them about. If you want to be able to find zero-day activities on your network before disclosure, this is definitely the class for you.

What sets this course apart from any other training is that we take a bottom-up approach to teaching network intrusion detection and network forensics. Rather than starting with a tool and teaching you how to use that tool in different situations, this course teaches you how and why TCP/IP protocols work the way they do. After spending the first two days examining what we call “Packets as a Second Language,” we add in common application protocols and a general approach to researching and understanding new protocols. With this deep understanding of how network protocols work, we turn our attention to the most widely used tools in the industry to apply this deep knowledge. The result is that you will leave this class with a clear understanding of how to instrument your network and the ability to perform detailed incident analysis and reconstruction.

These benefits alone make this training completely worthwhile. What makes the course as important as we believe it is (and students tell us it is), is that we force you to develop your critical thinking skills and apply them to these deep fundamentals. This results in a much deeper understanding of practically every security technology used today.

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.

“SEC503 has changed my view on my network defense tools and the need to correlate data through multiple tools. The course is outstanding!”

-Ben Clark, EY LLP

David Hoelzer
SANS Faculty Fellow

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/RG). 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.

@it_audit

Register at www.sans.org/cdi | 301-654-SANS (7267)
**Course Day Descriptions**

**DAY 1: Fundamentals of Traffic Analysis – Part 1**
Day 1 begins our bottom-up coverage of the TCP/IP protocol stack, providing a refresher or introduction, depending on your background, to TCP/IP. This is the first step in what we think of as a “Packets as a Second Language” course. Students begin to be introduced to the importance of collecting the actual packets involved in attacks and are already immersed in low-level packet analysis. We will cover the essential foundations such as the TCP/IP communication model, theory of bits, bytes, binary and hexadecimal, and the meaning and expected behavior of every field in the IP header. Students are introduced to the use of open-source Wireshark and tcpdump tools for traffic analysis.

**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 first section ended. Students will gain a deep understanding of the primary transport layer protocols used in the TCP/IP model. Two essential tools, Wireshark and tcpdump, are further explored, with advanced features to give you the skills to analyze your own traffic. The focus of these tools is to filter large scale data down to traffic of interest using Wireshark display filters and tcpdump Berkeley Packet Filters. These are used in the context of our exploration of the TCP/IP transport layers covering TCP, UDP, and ICMP. Once again, we discuss the meaning and expected function of every header field, covering a number of modern innovations that have very serious implications for modern network monitoring, and we 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; Real-World Analysis – Command Line Tools

**DAY 3: Application Protocols and Traffic Analysis**
Day 3 builds on the foundation of the first two sections of the course, moving into the world of application layer protocols. Students are introduced to the versatile packet crafting tool Scapy. This 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. Various practical scenarios and uses for Scapy are provided throughout this section.

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

**DAY 4: Network Monitoring: Signatures vs. Behaviors**
The fundamental knowledge gained from the first three sections provides the foundation for deep discussions of modern network intrusion detection systems during section 4. Everything that students have learned so far is now synthesized and applied to designing optimized detection rules for Snort/Firepower, and this is extended even further with behavioral detection using Zeek. The day begins with a discussion on network architecture, including the features of intrusion detection and prevention devices, along with a discussion about options and requirements for devices that can sniff and capture the traffic for inspection. This section provides an overview of deployment options and considerations, and allows students to explore specific deployment considerations that might apply to their respective organizations.

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

**DAY 5: Network Traffic Forensics**
Day 5 continues the trend of less formal instruction and more practical application in hands-on exercises. It consists of three major topics, beginning with practical network forensics and an exploration of data-driven monitoring vs. alert-driven monitoring, followed by a hands-on scenario that requires students to use all of the skills developed so far. The second topic continues the theme of data-driven analysis by introducing large-scale analysis and collection using NetFlow and IPFIX data.

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

**DAY 6: Advanced IDS Capstone Event**
The course culminates with a fun, hands-on, score-server-based IDS challenge. Students compete as solo players or on teams to answer many questions that require using tools and theory covered in the first five sections. The challenge presented is based on hours of live-fire, real-world data in the context of a time-sensitive incident investigation. The challenge is designed as a “ride-along” event, where students are answering questions based on the analysis that a team of professional analysts performed of these same data.

**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/cdi/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 lsdf 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 Nessus 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

Michael Murr
SANS Principal Instructor

Michael has been a forensic analyst with Code-X Technologies for over five years, conducted numerous investigations and computer forensic examinations, and performed specialized research and development. In addition to teaching SEC504, Michael has taught FOR508: Computer Forensics, Investigation, and Response, and SANS FOR610: Reverse-Engineering Malware. He has led SANS Online Training courses and is a member of the GIAC Advisory Board. Currently, Michael is working on an open-source framework for developing digital forensics applications. He holds the GCIH, GCFA, and GREM certifications and has a degree in computer science from California State University at Channel Islands. Michael also blogs about digital forensics on his forensic computing blog @mikemurr
Putting It All Together
Topics:
- Attribution.
- To obscure an attacker’s presence and disguise
- and explore future trends in malware designed
- the most commonly used malicious code specimens
- underlying system. In this course, we will analyze
- tools requires specialized defenses to protect the
- their nefarious deeds. Each of these categories of
- manipulate the underlying kernel itself to hide
- backdoors, apply Rootkits, and sometimes even
- covering their tracks. Computer attackers install
- of many hacker attacks: maintaining access and
- This course day covers the fourth and fifth phases
- Endpoint Security Bypass

 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 day-long course covers the details associated with reconnaissance and scanning, the first two phases of many computer attacks.

Topics: Reconnaissance; Scanning; Intrusion Detection System (IDS) Evasion; Enumerating Windows Active Directory Targets

 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 course day 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: Physical-layer Attacks; Gathering and Parsing Packets; Operating System and Application-level Attacks; Netcat: The Attacker’s Best Friend; Endpoint Security Bypass

 DAY 4: Computer and Network Hacker Exploits – Part 3
This course day 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

 DAY 5: Computer and Network Hacker Exploits – Part 4
This course day 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 and explore future trends in malware designed to obscure an attacker’s presence and disguise attribution.

Topics: Maintaining Access; Covering the Tracks; Putting It All Together

 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
- General security practitioners and security architects who want to design, build, and operate their systems to prevent, detect, and respond to attacks

“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
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 defensive 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
Course Day Descriptions

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?, Writing 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; Script Execution with Group Policy; Server Hardening Automation; PowerShell for Active Directory

DAY 3: Smart Tokens and Public Key Infrastructure (PKI)
Running a Public Key Infrastructure (PKI) is pretty much mandatory for Microsoft security and cloud computing today. The best form of multi-factor authentication (MFA) is a USB smart token integrated into Active Directory. We need digital certificates for SSL/TLS, wireless authentication, VPN gateways, code signing, and much more. This day 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/token certificate deployment, and, of course, lots of PowerShell examples.
Topics: Why is a PKI Necessary?, How to Install the Windows PKI; How to Manage Your PKI; Deploying Smart Cards; MFA Smart Tokens, Smart Cards and TPMS

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: Restricting Unnecessary 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 and PowerShell; TCP/UDP Port Permissions for Role-Based Access Control; Windows Defender Firewall; PowerShell for Firewall and IPsec Rules

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

“In SEC505, real-life solutions are offered by someone who understands the roadblocks in the way. This is information I could implement tomorrow and make my network more secure.”

~Mary Becken, Egan Company

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

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, GCFE, and GSEC certifications. Eric also blogs about information security at ericconrad.com.

@eric_conrad
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

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

“SEC511 provides a high-level view all the way down to packets. It’s a great, great course on detecting/preventing threats. This course is hands-down worth every dollar. I learned more actionable things in a week than in four semesters of school!”
-Matt McCullough, MN IT
SEC530: Defensible Security Architecture and Engineering

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

SEC530: Defensible Security Architecture and Engineering 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.

“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.

“I have reviewed many courses in the past and this is one of my favorites. The content was...as my field is not the main focus of the content I have often found that I have learned something new I can use in everyday life.”

-Shayne Douglass, AMEWAS Inc.

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, GWAPT, GSNA, GMON, CISSP®, ITIL, CISM, and IRCA 27001 Lead Auditor from Bureau Veritas UK.

@aboutsecurity
# Course Day Descriptions

<table>
<thead>
<tr>
<th>Day</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DAY 1: Defensible Security Architecture and Engineering</strong></td>
<td>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 <em>The Tao of Network Security Monitoring</em>, 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. <strong>Topics:</strong> Traditional Security Architecture Deficiencies; Defensible Security Architecture; Threat, Vulnerability, and Data Flow Analysis; Layer 1 Best Practices; Layer 2 Best Practices; Netflow</td>
</tr>
<tr>
<td><strong>DAY 2: Network Security Architecture and Engineering</strong></td>
<td>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. <strong>Topics:</strong> 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; Proxy</td>
</tr>
<tr>
<td><strong>DAY 3: Network-Centric Security</strong></td>
<td>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. <strong>Topics:</strong> NGFW, NIDS/NIPS; Network Security Monitoring; Sandboxing; Encryption; Secure Remote Access; Distributed Denial-of-Service (DDOS)</td>
</tr>
<tr>
<td><strong>DAY 4: Data-Centric Security</strong></td>
<td>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. <strong>Topics:</strong> 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</td>
</tr>
<tr>
<td><strong>DAY 5: Zero-Trust Architecture: Addressing the Adversaries Already in Our Networks</strong></td>
<td>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 can be used to change access levels dynamically. 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. <strong>Topics:</strong> 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</td>
</tr>
<tr>
<td><strong>DAY 6: Hands-On Secure-the-Flag Challenge</strong></td>
<td>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. <strong>Topics:</strong> Capstone – Design/Detect/Defend</td>
</tr>
</tbody>
</table>
SEC545: Cloud Security Architecture and Operations

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 SEC545 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

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

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.

@daveshackelford
Course Day Descriptions
Thu, Dec 12 – Mon, Dec 16
9:00am – 5:00pm
Hands-on labs

**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 SEC465 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.

**Topics:** Cloud Security: In-House versus Cloud; A Virtualization Security Primer; Cloud Network Security; Instance and Image Security; Identity and Access Management; Data Security for the Cloud; Application Security for the Cloud; Provider Security: Cloud Risk Assessment

**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 to 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
You Will Be Able To

- Deploy the SANS SOF-ELK VM in production environments
- Demonstrate ways most SIEMs commonly lag current open-source solutions (e.g., SOF-ELK)
- Get up to speed on SIEM use, architecture, and best practices
- Know what type of data sources to collect logs from
- Deploy a scalable logs solution with multiple ways to retrieve logs
- Operationalize ordinary logs into tactical data
- Develop methods to handle billions of logs from many disparate data sources
- Understand best practice methods for collecting logs
- Dig into log manipulation techniques challenging many SIEM solutions
- Build out graphs and tables that can be used to detect adversary activities and abnormalities
- Combine data into active dashboards that make analyst review more tactical
- Utilize adversary techniques against them by using frequency analysis in large data sets
- Develop baselines of network activity based on users and devices
- Develop baselines of Windows systems with the ability to detect changes from the baseline
- Apply multiple forms of analysis such as long tail analysis to find abnormalities
- Correlate and combine multiple data sources to achieve more complete understanding
- Provide context to standard alerts to help understand and prioritize them

Tim Garcia
SANS Certified Instructor

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

Timothy Garcia is a seasoned security professional who loves the challenge and continuously changing landscape of defense. Tim started his career as an engineer in IT and after working on a few security incidents related to Code Red and Nimda, he realized he had found his calling. Tim currently works as an Information Security Engineer for a Fortune 100 financial institution where he provides security consulting to project teams to ensure security of IT operations and compliance with policies and regulations. Tim also leads the team that is tasked with Firewall review, SIEM management and privileged access monitoring and policy compliance. Tim has worked as a Systems Engineer and DBA and has expertise in systems engineering, project management and information security principles and procedures/compliance. He previously worked for Intel and served in the U.S. Navy. Tim also works with the OnDemand team as a subject-matter expert, is a mentor for the Vet Success program and provides consulting and content review for the SANS Securing The Human Project. Tim holds the CISSP®, GSEC, GSLE, GISF, GMON, GAWN, GCCC, GCED, and NSM-IAM certifications. He has extensive knowledge of security procedures and legislation such as Sarbanes-Oxley, GLBA, CobiT, COSO, and ISO 1779. When Tim is not defending systems, he enjoys playing sports, snowboarding and most of all spending time with his wife and four children.

@SecurityMapper
Day 1: SIEM Architecture
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 get them 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; Applying 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: Identifying Authorized and Unauthorized Assets; Identifying 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 a 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: Centralizing NIDS and HIDS Alerts; Analyzing Endpoint Security Logs; Augmenting Intrusion Detection Alerts; Analyzing Vulnerability Information; Correlating Malware Sandbox Logs with Other Systems to Identify Victims Across the Enterprise; Monitoring 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.”

-Mikhale Vitebskiy, Lexington Partners
Brian Ventura is an Information Security Architect with 20 years of industry experience. With a diverse background in public and private sector consulting and project management, Brian brings a comprehensive view of security and technology. As an architect, he currently focuses on enterprise information security governance, risk and compliance. Brian advises public and private entities on security best practices generally and within large projects. Brian regularly speaks on the NIST CyberSecurity Framework, the CIS Controls, and other security topics. Brian volunteers with ISSA and OWASP, focusing on educational opportunities and maturing the Information Security field. He completed his bachelor of science in information technology – security from Western Governors University and holds various industry certifications including the CISSP®, GSEC, GCIH, GCCC, and GCFA. 
@brianwifaneye

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.

SEC566: Implementing and Auditing the Critical Security Controls – In-Depth

You Will Be Able To
- Apply a security framework based on actual threats that is measurable, scalable, and reliable in stopping known attacks and protecting organizations’ important information and systems
- Understand the importance of each control and how it is compromised if ignored, and explain the defensive goals that result in quick wins and increased visibility of networks and systems
- Identify and utilize tools that implement controls through automation
- Learn how to create a scoring tool for measuring the effectiveness of each control
- Employ specific metrics to establish a baseline and measure the effectiveness of security controls
- Understand how the Critical Controls map to standards such as NIST 800-53, ISO 27002, the Australian Top 35, and more
- Audit each of the Critical Security Controls, with specific, proven templates, checklists, and scripts provided to facilitate the audit process
Course Day Descriptions

Thu, Dec 12 – Mon, Dec 16
9:00am – 5:00pm
Hands-on labs

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

Who Should Attend
- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel and contractors
- Staff and clients of federal agencies
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC/AUD440, SEC401, SEC501, SANS Audit classes, and MGT512

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/cdi/courses
You Will Be Able To

- Understand how recent high-profile attacks were delivered and how they could have been stopped
- Implement security controls throughout the different phases of the Cyber Kill Chain and the MITRE ATT&CK framework to prevent, detect, and respond to attacks
- Highlighting key bypass strategies for script controls (Unmanaged PowerShell, AMSI bypasses, etc.)
- Detecting and preventing malware persistence
- Leveraging the Elastic stack as a central log analysis solution
- Detecting and preventing lateral movement through Sysmon, Windows event monitoring, and group policies
- Blocking and detecting command and control through network traffic analysis
- Leveraging threat intelligence to improve your security posture

Topics To Be Addressed

- Leveraging MITRE ATT&CK as a “common language” in the organization
- Building your own Cuckoo sandbox solution to analyze payloads
- Developing effective group policies to improve script execution (including PowerShell, Windows Script Host, VBA, HTA, etc.)
- Highlighting key bypass strategies for application whitelisting (focus on AppLocker)
- Highlighting key bypass strategies for script controls (Unmanaged PowerShell, AMSI bypasses, etc.)
- Detecting and preventing malware persistence
- Leveraging the Elastic stack as a central log analysis solution
- Detecting and preventing lateral movement through Sysmon, Windows event monitoring, and group policies
- Blocking and detecting command and control through network traffic analysis
- Leveraging threat intelligence to improve your security posture

You just got hired to help our virtual organization “SYNTechLabs” 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 tactics are 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 & Kill Chain Defenses will arm you with the knowledge and expertise you need to overcome today’s threats. Recognizing that a prevent-only strategy is not sufficient, we will introduce security controls aimed at stopping, detecting, and responding to your adversaries.

Course authors Stephen Sims and Erik Van Buggenhout (both certified as GIAC Security Experts) are hands-on practitioners who have built a deep understanding of how cyber attacks work through penetration testing and incident response. While teaching penetration testing courses, they were often asked the question: “How do I prevent or detect this type of attack?” Well, this is it! SEC599 gives students real-world examples of how to prevent attacks. The course features 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.

Our six-part journey will start off with an analysis of recent attacks through in-depth case studies. We will explain what types of attacks are occurring and introduce formal descriptions of adversary behavior such as the Cyber Kill Chain and the MITRE ATT&CK framework. In order to understand how attacks work, you will also compromise our virtual organization “SYNTechLabs” in section one exercises.

In sections two, three, four and five we will discuss how effective security controls can be implemented to prevent, detect, and respond to cyber attacks.

SEC599 will finish with a bang. During the Defend-the-Flag challenge in the final course section, 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?

“SEC599 handles a lot of important aspects (of the entire Kill Chain). It gives good insight into potential attacks and mitigation.”

-Kevin Giesekam, Dutch Police

Erik Van Buggenhout is the lead author of SEC599: Defeating Advanced Adversaries. In addition, Erik teaches SEC560: Network Penetration Testing and Ethical Hacking and SEC562: 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, GPEC, GWAPT, GCIH, 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
### DAY 1: Introduction and Reconnaissance

Our six-part journey starts with an analysis of recent attacks through in-depth case studies. We will explain what’s happening in real situations and introduce the Cyber Kill Chain and MITRE ATT&CK framework as a structured approach to describing adversary tactics and techniques. We will also explain what purple teaming is, typical tools associated with it, and how it can be best organized in your organization. In order to understand how attacks work, students will also compromise our virtual organization “SYNCTECHLABS” during section one exercises.

**Topics:** Course Outline and Lab Setup; Adversary Emulation and the Purple Team, Reconnaissance

---

### DAY 2: Payload Delivery and Execution

Section 2 will cover how the attacker attempts to deliver and execute payloads in the organization. We will first cover adversary techniques (e.g., creation of malicious executables and scripts), then focus on how both payload delivery (e.g., phishing mails) and execution (e.g., double-clicking of the attachment) can be hindered. We will also introduce YARA as a common payload description language and SIGMA as a vendor-agnostic use-case description language.

**Topics:** Common Delivery Mechanisms, Hindering Payload Delivery, Preventing Payload Execution

---

### DAY 3: Exploitation, Persistence, and Command and Control

Section 3 will first explain how exploitation can be prevented or detected. We will show how security should be an integral part of the software development lifecycle and how this can help prevent the creation of vulnerable software. We will also explain how patch management fits in the overall picture. Next, we will zoom in on exploit mitigation techniques, both at compile-time (e.g., ControlFlowGuard) and at run-time (ExploitGuard). We will provide an in-depth explanation of what the different exploit mitigation techniques (attempt to) cover and how effective they are. We’ll then turn to a discussion of typical persistence strategies and how they can be detected using Autoruns and OSQuery. Finally, we will illustrate how command and control channels are being set up and what controls are available to the defender for detection and prevention.

**Topics:** Protecting Applications from Exploitation, Avoiding Installation, Foiling Command and Control

---

### DAY 4: Lateral Movement

Section 4 will focus on how adversaries move laterally throughout an environment. A key focus will be on Active Directory (AD) structures and protocols (local credential stealing, NTLMv2, Kerberos, etc.). We will discuss common attack strategies, including Windows privilege escalation, UAC bypasses, (Over-) Pass-the-Hash, Kerberoasting, Silver Tickets, and others. We’ll also cover how BloodHound can be used to develop attack paths through the AD environment. Finally, we will discuss how lateral movement can be identified in the environment and how cyber deception can be used to catch intruders red-handed!

**Topics:** Protecting Administrative Access, Key Attack Strategies against AD, How Can We Detect Lateral Movement?

---

### DAY 5: Action on Objectives, Threat Hunting, and Incident Response

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

- How does the adversary obtain “domain dominance” status? This includes the use of Golden Tickets, Skeleton Keys, and directory replication attacks such as DCSync and DCShadow.
- How can data exfiltration be detected and stopped?
- How can threat intelligence aid defenders in the Cyber Kill Chain?
- How can defenders perform effective incident response?

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

**Topics:** Domain Dominance, Data Exfiltration, Leveraging Threat Intelligence, Threat Hunting and Incident Response

---

### DAY 6: APT Defender Capstone

The course culminates in a team-based Defend-the-Flag competition. Section six is a full chapter of hands-on work applying the principles taught throughout the course. Your team will progress through multiple levels and missions designed to ensure mastery of the modern cybersecurity controls promoted all week long. This challenging exercise will reinforce key principles in a fun, hands-on, team-based challenge. Note that OnDemand students will enjoy this exercise on an individual basis. As always, SANS subject-matter experts are available to support every OnDemand student’s experience.

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

---

### Who Should Attend

- Security architects and security engineers
- Red teamers and penetration testers
- Technical security managers
- Security Operations Center analysts, engineers, and managers
- 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 different topics covered in this course can bring eye-opening layers of defense to any organization.”

-Mike Marx, Carbon Black
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.

“Attackers are always evolving, and having a GIAC cert prepares you to evolve with them. It allows you to implement the appropriate methods and best practices in your company while understanding it’s a continuous fight.”

– Jason Sevilla, Cyber Intelligence Analyst

“Earning 3 GIAC certifications after I graduated from college has enabled me to enter the InfoSec field. Not only did they set me apart from my peers, GIAC certs also made my resume more appealing to recruiters.”

– Kim Ngoc, GuardSight, Inc.
Want to launch a career in cybersecurity?

Earn an Undergraduate Certificate in Applied Cybersecurity

Gain fundamental technical knowledge and skills, choose an elective course to begin developing a specialized skillset, and earn GIAC certifications that employers are looking for.

Rapid Career Preparation
Complete the program in 18 months or choose an accelerated option to finish in 7 months.

Flexibility
Pursue the certificate alongside undergraduate studies or while working full-time. Take courses online or at immersive weeklong events throughout the country.

“A I was having a hard time getting a job in information security due to my lack of hands-on experience. SANS gave me extraordinary training and the opportunity to rise to the top of the résumé pile.”

– AJ Langlois
Cyber Analyst II, BB&T

Learn more at sans.edu/acs
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

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

Mathew Toussain is the founder of Open Security and a penetration tester with Black Hills Information Security. As an avid information security researcher, Mathew 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. Mathew 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, Mathew 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.
Course Day Descriptions

**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 precursors 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 Policies;

**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 Dictionary-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, incubating, 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 Metrics 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 VOIP 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;

**Who Should Attend**
- Vulnerability assessors
- IT System administrators
- Security auditors
- Compliance professionals
- Penetration testers
- Vulnerability program managers
- Security analysts
- Security architects
- Senior security engineers
- Technical security managers

**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 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:**
- Domain Password Auditing; Creating and Navigating Vulnerability Prioritization Schemes in Acheron; Developing a Web of Network and Host Affiliations; Modeling Account Relationships on Active Directory Forests; Creating Effective Vulnerability Assessment Reports; Transforming Triage Listing into the Vulnerability Remediation Plan; 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 jealo...
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

Hassan El Hadary
SANS Certified Instructor

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.

Hassan is an expert in application security who has performed application security assessments, secure code reviews, and penetration tests for security critical applications. He started his career as a programmer, during which time he developed his passion for information security. Hassan received his master’s degree in computer science from the American University in Cairo with a thesis in the field of secure software engineering. Hassan is an active security researcher in bug bounty programs. He has been acknowledged and rewarded by several vendors such as Google, Apple, Facebook, Yahoo, Oracle, Twitter, PayPal, eBay, Etsy, AT&T, Gift Cards, Cisco Meraki, and Groupon.

Published vulnerabilities are available on the blog http://hassanhadary.blogspot.com.eg/ @hassan_hadary
**Course Day Descriptions**

**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 Clients and Servers; Discussion of the Various Web Architectures; Discovering How Session State Works; Discussion of the Different Types of Vulnerabilities; WHOIS and DNS Reconciliation; The HTTP Protocol; WebSocket; Secure Sockets Layer (SSL) Configurations and Weaknesses; 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 your 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:** Scanning with Nmap; Discovering the Infrastructure within the Application; Identifying the Machines and Operating Systems; Exploring Virtual Hosting and its Impact on Testing; Learning Methods to Identify Load Balancers; Software Configuration Discovery; Learning Tools to Spider a Website; Brute Forcing Unlinked Files and Directories; Discovering and Exploiting Shellshock; Web Authentication; Username Harvesting and Password Guessing; Fuzzing; Burp Intruder

**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:** Session Tracking; Authentication Bypass Flaws, MultiIdae, Command Injection; Directory Traversal; Local File Inclusion (LFI), Remote File Inclusion (RFI); SQL Injection; Blind SQL Injection; Error-Based SQL Injection; Exploiting SQL Injection; SQL Injection Tools; sqlmap

**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:** Cross-Site Request Forgery (CSRF); Python for Web App Penetration Testing; WPScan; w3af; Metasploit for Web Penetration Testers; Leveraging Attacks to Gain Access to the System; How to Pivot Our Attacks Through a Web Application; Exploiting Applications to Steal Cookies; Executing Commands Through Web Application Vulnerabilities; When Tools Fail

**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

Jeff McJunkin
SANS Certified Instructor

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, scoping 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

Jeff McJunkin is a senior staff member at Counter Hack Challenges with more than nine years of experience in systems and network administration and network security. His greatest strength is his breadth of experience – from network and web application penetration testing to digital/mobile forensics, and from technical training to systems architecture. Jeff is a computer security/information assurance graduate of Southern Oregon University and holds many professional certifications. He has also competed in many security competitions, including taking first place at a regional NetWars competition and a U.S. Cyber Challenge capture-the-flag competition, as well as joining the Red Team for the Pacific Rim Collegiate Cyber Defense Competition. His personal blog can be found at http://jeffmcjunkin.com.

@jeffmcjunkin
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 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 (CSRF), 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 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 WMIC 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.

**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 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 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 packlets: 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, Netcat for the Pen Tester, Monitoring Services during a Scan

---

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

In this course section, 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

---

**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

---

**Course Day Descriptions**

**Thu, Dec 12 – Tue, Dec 17**

**9:00am – 7:15pm (Day 1)**

**9:00am – 5:00pm (Days 2-6)**

**Extended hours; hands-on labs**

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

**45**
SEC573: Automating Information Security with Python

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 forensic 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 forensic 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 a payload from tools such as Metasploit.

All security professionals, including penetration testers, forensic analysts, network defenders, security administrators, and incident responders, have one experience in common: CHANGE. Tools, technologies, and threats change constantly, but Python is a simple, user-friendly language that can help you keep pace with change, allowing you to write custom tools and automate tasks to effectively manage and respond to your unique threats.

Whether you are new to coding or have been coding for years, 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 with 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.

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 forensic artifacts that would be invaluable for your investigation, if only you had a tool to access it. Often for new features and forensic 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. The answer is simple if you have the skills: Write tools to automate various aspects of 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 or modify existing capabilities to make them perform as you need them to.

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. Learn Python in-depth with us to become fully weaponized.

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 challenge. We set the stage for students to learn at their own pace in the pyWars lab environment, which is 100 percent hands-on. 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. This section continues the hands-on, lab-centric approach established at the beginning of the course. It covers data structures and more detailed programming concepts. Next, we focus on invaluable tips and tricks to make you a better Python programmer and to show you 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. Forensic examiners and offensive security professionals won’t be left out because reading and writing files and parsing data are also essential skills they 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**
In our forensics-themed section, we will assume the role of a forensic 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 the skills covered in this section 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 PIL; SQL Queries; HTTP Communications with Python Built in Libraries; Web Communications with the Requests Module

**DAY 5: Offensive Python**
During our offensive-themed section, 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; Using the Select Module for 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 to 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!

**Who Should Attend**
- Security professionals who benefit from automating routine tasks so they can focus on what’s most important
- Forensic analysts who can no longer wait on someone else to develop a commercial tool to analyze artifacts
- Network defenders who sift through mountains of logs and packets to find evil-doers in their networks
- Penetration testers who are ready to advance from script kiddie to professional offensive computer operations operator
- Security professionals who want to evolve from security tool consumer to security solution provider

**You Will Receive**
- A USB containing a virtual machine filled with sample code and working examples
- A copy of *The Python Pocket Reference* published by O’Reilly Press
- MP3 audio files of the complete course lecture

---

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

- Caleb Jaren, Microsoft

---

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/cdi/courses](http://www.sans.org/cdi/courses)
SEC660: **Advanced Penetration Testing, Exploit Writing, and Ethical Hacking**

- **6 Day Program**
- **46 CPEs**
- **Laptop Required**

**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

**Who Should Attend**

- Network and systems penetration testers
- Incident handlers
- Application developers
- IDS engineers

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.

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 and is a course author and senior instructor for the SANS Institute. He is the author of SANS’s 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: Network Attacks for Penetration Testers**
Day one serves as an advanced network attack module, building on knowledge gained from SEC560. The focus will be on obtaining access to the network; manipulating the network to gain an attack position for eavesdropping and attacks, and for exploiting network devices, leveraging weaknesses in network infrastructure; and taking advantage of client frailty.

**Topics:** Bypassing Network Access/Admission Control (NAC), 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; IPv6 for Penetration Testers; Exploiting OSPF Authentication to Inject Malicious Routing Updates; Using Evilgrade to Attack Software Updates; Overcoming SSL Transport Encryption Security with Sslstrip, Remote Cisco Router Configuration File Retrieval.

**DAY 2: Crypto, Network Booting Attacks, and Escaping Restricted Environments**
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; PowerShell Essentials; Enterprise PowerShell; Post-Exploitation with PowerShell and Metasploit; Escaping Software Restrictions; Two-hour Evening Capture-the-Flag Exercise Against a Modern Network with Hardened Servers, Desktops and vApp Targets.

**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 .docx 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; Identifying and Analyzing Stack-Based Overflows on the Linux OS; Performing Return-to-libc (ret2libc) Attacks on the Stack; Return-Oriented Programming; 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 and Capture-the-Flag engine will be provided to score students as they capture flags. More difficult challenges will be worth more points. The web server will provide a range of problems from simple to complex. A web server scoring system and Capture-the-Flag engine 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
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

Master 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, geo-location, 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.

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
Forensics: Firefox, Internet Explorer, and Chrome

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

Examining of Browser Artifacts; Tools Used

Understanding Browser Timestamps, Internet Explorer; Edge; Firefox; Chrome; Browser Forensics: History, Cache, Searches, Downloads, Topics: browsing remnants.

restore, tracking cookies, zoom levels, predictive site prefetching, and private every significant artifact stored by the browser and how to analyze some Edge, Firefox, and Google Chrome. The analyst will learn how to examine web browser evidence created during the use of Internet Explorer, 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 Browser Timestamps, Internet Explorer; Edge; Firefox; Chrome; Examining of Browser Artifacts; Tools Used

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

“Excellent and engaging course that provides in-depth knowledge taught by true professionals.”
-Callum Wilson, Grant Thornton

“This course has really helped me gain critical and useful knowledge that I can use directly at my work.”
-Daniel Frasure, KPMG

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 has become 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 Browser Timestamps, Internet Explorer; Edge; Firefox; Chrome; Examining 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 10 Forensic Challenge

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

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 beaconhead and spear phishing attack mechanisms
- Target advanced adversary anti-forensics techniques like hidden and time-stomped 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 Incident Response, Threat Hunting, and Digital Forensics will help you to:
- Detect how and when a breach occurred
- Identify compromised and affected systems
- Perform damage assessments and determine what was stolen 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.

The key is to constantly look for attacks that get past security systems, and to catch intrusions in progress, rather than after attackers have completed their objectives and done significant damage to the organization. For the incident responder, this process is known as “threat hunting.” Threat hunting uses known adversary behaviors to proactively examine the network and endpoints in order to identify new data breaches.

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 hacktivists. Constantly updated, FOR508: Advanced 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.

ADVANCED THREATS ARE IN YOUR NETWORK – IT’S TIME TO GO HUNTING!

Chad Tilbury
SANS Senior Instructor

Chad has nearly 20 years of experience working with government agencies, defense contractors, and Fortune 500 companies. He has served as a special agent with the U.S. Air Force Office of Special Investigations, where he conducted computer forensics examinations of a variety of crimes and ushered counter-espionage techniques into the digital age. Chad has led international forensic teams and was selected to provide computer forensic support to the United Nations Weapons Inspection Team. In addition, Chad has worked as a computer security engineer and forensic lead for a major defense contractor and served as the vice president of worldwide Internet enforcement for the Motion Picture Association of America. In that role, he managed Internet anti-piracy operations for the seven major Hollywood studios in over 60 countries. Today, Chad brings his wealth of experience to his role as a consultant, where he specializes in incident response, corporate espionage, and computer forensics. In addition to being a graduate of the U.S. Air Force Academy, Chad holds B.S. and M.S. degrees in computer science, as well as the GCFA, GCIH, GREM, and ENCE certifications.

@chadtilbury

Register at www.sans.org/cdi | 301-654-SANS (7267)
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: Threat Hunting in the Enterprise, Incident Response and Hunting across Endpoints, Malware Defense Evasion and Identification, Malware Persistence Identification, Investigating WMI-Based Attacks

**DAY 2: Intrusion Analysis**
Cyber defenders have a wide variety of tools and artifacts available to identify, hunt, and track adversary activity in a network. Each attacker 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. As an example, at some point attackers will need to run code to accomplish their objectives. We can identify this activity via application execution artifacts. Attackers will also need one or more accounts to run code. Consequently, account auditing is a powerful means of identifying malicious actions. Attackers also need a means to move throughout the network, so we look for artifacts left by the relatively small number of ways there are to accomplish this part of their mission. 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:** Stealing and Utilization of Legitimate Credentials, Advanced Evidence of Execution Detection, Lateral Movement Adversary Tactics, Techniques, and Procedures (TTPs), Log Analysis for Incident Responders and Hunters

**DAY 3: Memory Forensics in Incident Response and Threat Hunting**
Now a critical component of many incident response and threat hunting teams that regularly detect advanced adversaries 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, PowerShell, and advanced malware used by APT attackers. In fact, some attacks may be nearly impossible to unravel without memory analysis. Memory analysis was traditionally the domain of Windows internals experts, but the recent development of new tools and techniques makes it accessible today to all investigators, 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 cover many of the most powerful memory analysis capabilities available and give you a solid foundation of advanced memory forensic skills to super-charge investigations, regardless of the toolset employed.

**Topics:** Remote and Enterprise Incident Response, Triage and Endpoint Detection and Response, Memory Acquisition, Memory Forensics Analysis Process for Response and Hunting, Memory Forensics Examinations, Memory Analysis Tools

**DAY 4: Timeline Analysis**
Learn advanced incident response and hunting techniques uncovered via timeline analysis directly from the authors who pioneered timeline analysis tradecraft. Temporal data are located everywhere on a computer system. Filesystem modified/access/creation/change times, log files, network data, registry data, and Internet history files all contain time data that can be correlated into critical analysis to successfully solve cases. Pioneered by Rob Lee in 2001, timeline analysis has become a critical incident response, hunting, and forensics technique. New timeline analysis frameworks provide the means to conduct simultaneous examinations of a multitude of time-based artifacts. The analysis that once took days now takes minutes. 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 and Analysis; Super Timeline Creation and Analysis

**DAY 5: Incident Response & 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:** Cyber Threat Intelligence, Malware and Anti-Forensics Detection; Anti-Forensic Detection Methodologies; Identifying Compromised Hosts without Active Malware

**DAY 6: The APT Threat Group 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 to 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
- Security Operations Center analysts
- 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

“FOR508 was outstanding. The breadth and depth of the content was impressive.”
-Al Sears, Skechers, USA

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/cdi/courses](http://www.sans.org/cdi/courses)
FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response | NEW!

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

You will leave this week with a well-stocked toolbox and the knowledge to use it on your entire bag of skills: forensic techniques and methodologies, full-stake networking and reporting. Still others engage with an adversary in real time, seeking to contain and eradicate the attacker from the victim’s environment. In these situations and more, the artifacts left behind from attackers’ communications can provide an invaluable view into their intent, capabilities, successes, and failures.

In FOR572, we focus on the knowledge necessary to examine and characterize communications that have 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.

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-based dissection, 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 under way.

FOR572 is truly an advanced course – we hit the ground running on day one. Bring your entire bag of skills: forensic techniques and methodologies, full-stake networking knowledge (from the wire all the way up to user-facing services), Linux shell utilities, and everything in between. They will all benefit you throughout the course as you hone your skills to fight crime.

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

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 has 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

www.giac.org/gnfa
Analyst GNFA
### Course Day Descriptions

#### DAY 1: Off the Disk and Onto the Wire

Although many fundamental network forensic concepts align with those of any other digital forensic investigation, the network presents many nuances that require special attention. Today you will learn how to apply what you already know about digital forensics and incident response to network-based evidence. You will also become acclimated to the basic tools of the trade.

**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 countless network protocols that may be in use in a production network environment. We will cover those that are most likely to benefit the forensic analyst 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 misuse of the 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 visibility 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
- Firewall, Intrusion Detection System, and Network Security Monitoring Logs
- Logging Protocol and Aggregation

#### 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 forensic analyst 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 forensic analyst's toolkit. We’ll explore the various roles that commercial tools generally fulfill, 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 – otherwise the attacker can quickly pivot, nullifying our progress.

**Topics:**
- Encoding, Encryption, and SSL/TLS
- Meddler-in-the-Middle
- Network Protocol Reverse Engineering
- Investigation OPSEC and Threat Intel

Josh Lemon
SANS Certified Instructor

Josh Lemon is a director at Salesforce.com in its international Computer Security Incident Response Team (CSIRT), managing their APAC team. He also heads up their Advanced Incident Response service that provides tactical support for complicated incidents. Prior to Salesforce, Josh was the CSIRT Manager for the Commonwealth Bank of Australia, leading one of the largest dedicated incident response teams in that country’s commercial sector. He previously worked as a managing consultant for BAE Systems Applied Intelligence, where he was responsible for all technical cybersecurity services for the Asia Pacific region, including overseeing large and complex incident response and offensive security engagements. Josh has provided incident response, digital forensics and penetration testing services to government, law enforcement, and the commercial sector. He was one of the co-creators for SecTalks in Sydney Australia, a monthly information security community event dedicated to presenting and teaching technical information security skills. Josh has a varied background in the cybersecurity industry includes project management, lead incident responder, forensics analysis, reverse engineer, penetration testing, secure network design, and software development. He currently holds the GREM, GCFA, GNFA, GCIH, Oatten, and GPCy certifications, and lectures on investigating cyber attacks at universities in Sydney and to international audiences for the SANS Institute.

@joshlemon

---

**Who Should Attend**

- Incident response team members and forensicators
- Hunt team members
- Law enforcement officers, federal agents, and detectives
- Network security managers
- Network defenders
- IT professionals
- Network engineers
- Anyone interested in computer network intrusions and investigations
- Security Operations Center personnel and information security practitioners

---

“Excellent tools and strategies to bring back to the workplace.”

- Branco Jacob, NCDOC

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

Jake Williams is a principal consultant at Rendition Infosec. He has more than a decade of experience in secure network design, penetration testing, incident response, forensics, and malware reverse engineering. Before founding Rendition Infosec, Jake worked with various cleared government agencies in information security roles. He is well-versed in cloud forensics and previously developed a cloud forensics course for a U.S. government client. Jake regularly responds to cyber intrusions by state-sponsored actors in the financial, defense, aerospace, and healthcare sectors using cutting-edge forensics and incident response techniques. He often develops custom tools to deal with specific incidents and malware-reversing challenges. Additionally, Jake performs exploit development and has privately disclosed a multitude of zero day exploits to vendors and clients. He found vulnerabilities in one of the state counterparts to healthcare.gov and recently exploited antivirus software to perform privilege escalation. Jake developed Dropsmack, a pentesting tool (okay, malware) that performs command and control and data exfiltration over cloud file-sharing services. Jake also developed an anti-forensics tool for memory forensics, Attention Deficit Disorder (ADD). This tool demonstrates weaknesses in memory forensics techniques.

@MalwareJake

“...This course does a great job of teaching a sound methodology and an evidence-based approach to IT and in breaking down biases and reconstructing analytical pathways.”

-Sveva Vittoria Scenarreli, PwC UK
<table>
<thead>
<tr>
<th>DAY 1: Cyber Threat Intelligence and Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>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, as well as 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.</td>
</tr>
<tr>
<td><strong>Topics:</strong> 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)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DAY 2: The Fundamental Skill Set: Intrusion Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intrusion analysis is at the heart of threat intelligence. It is a fundamental skill set 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.</td>
</tr>
<tr>
<td><strong>Topics:</strong> Primary Collection Source: Intrusion Analysis; Kill Chain Courses of Action, Kill Chain Deep Dive; Handling Multiple Kill Chains; Collection Source: Malware</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DAY 3: Collection Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
<tr>
<td><strong>Topics:</strong> 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</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DAY 4: Analysis and Dissemination of Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
<tr>
<td><strong>Topics:</strong> Analysis: Exploring Hypotheses; Analysis: Building Campaigns; Dissemination: Tactical; Case Study: Sony Attack; Dissemination: Operational</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DAY 5: Higher-Order Analysis and Attribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 course 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.</td>
</tr>
<tr>
<td><strong>Topics:</strong> Logical Fallacies and Cognitive Biases; Dissemination Strategies; Case Study: Stuxnet; Fine-Tuning Analysis; Case Study: Sofacy; Attribution</td>
</tr>
</tbody>
</table>

“This training summarizes CTI very well and connects all the dots. The training gives you clear answers to the following questions: what is CTI, how important is it, what is it built upon, and how can it be applied in practice?”

- Nikita Martynov, NNI A/S

“I could take this course five times more and get something new each time! So much valuable info to take back to my organization.”

- Charity Willhoite, Armor Defense, Inc.
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

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 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 31 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!

Terrance Maguire is the chief scientist and managing member of Digital Forensics Academy LLC, conducting digital forensic investigations, research and development in computer forensics and providing training to the government and commercial sectors. He has over 27 years of experience in physical and digital forensic investigations, has developed and led training programs in varied areas of law enforcement and digital evidence, and has experience implementing counterintelligence intrusion detection programs. His prior experience includes serving as a senior-level forensic computer analyst for the U.S. State Department, where he was responsible for conducting analysis on digital evidence. As a cyber operations specialist for the Department of Defense, he implemented network surveillance, network packet analysis, wireless surveys, and intrusion detection. In addition, at the Defense Computer Investigations Training Program (DCITP), Terrance developed and presented a broad range of instruction to federal law enforcement in the area of cybercrime.
Course Day Descriptions

**DAY 1: Smartphone Overview, Misfit Devices, SQLite Introduction, and Android Forensics Overview**

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, misfit devices, SQLite database examination, and query development. They’ll also gain an overview of Android devices and manually crack locked Androids. Students will become familiar with the forensic tools required to complete comprehensive examinations of smartphone data structures. We realize that not everyone examines BlackBerry and knock-off devices, which is why we offer “choose your own adventure” labs, meaning that students can select the labs most relevant to them. BlackBerry 10 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 10 device file systems. Knock-off devices are another outlier than can be parsed and decoded once you become familiar with the file system structures.

**Topics:** The SIFT Workstation; Forensic Acquisition Concepts of Smartphones; Smartphone Components; Introduction to SQLite; Android Forensic Overview; Handling Locked Android Devices

**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. Unfortunately, gaining access to these devices isn’t as easy as it used to be. Android devices contain substantial amounts of data that can be decoded and interpreted into useful information. However, without honing the appropriate skills to bypass locked Androids and correctly interpret the data stored on them, you will be unprepared for the rapidly evolving world of smartphone 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. Additionally, Android and Google cloud data store tons of valuable information. You will find Google artifacts from iOS users as well.

**Topics:** Android Acquisition Considerations; Android File System Structures; Android Evidentiary Locations; Traces of User Activity on Android Devices; Android Backup Files; Google Cloud Data and Extractions

**DAY 3: iOS Device Forensics**

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:** iOS Forensic Overview and Acquisition; iOS File System Structures; iOS Evidentiary Locations; Handling Locked iOS Devices; Traces of User Activity on iOS Devices

**DAY 4: iOS Backups, Malware and Spyware Forensics, and Detecting Evidence Destruction**

iOS backups are extremely common and are found in the cloud and on hard drives. Users create backups, and we often find that our best data can be derived from creating an iOS backup for forensic investigation. This section will cover methodologies to extract backups and cloud data and analyze the artifacts for each. Malware affects a plethora of smartphone devices. We 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 day alone! The day ends with the students challenging themselves using tools and methods learned throughout the week to recover user data from a wiped smartphone.

**Topics:** iOS Backup File Forensics; Locked iOS Backup Files; iCloud Data Extraction and Analysis; Malware and Spyware Forensics; Detecting Evidence Destruction

**DAY 5: Third-Party Application Analysis**

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, recovery of 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; Mobile Browsers; Secure Chat Applications

**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.

**Topics:** Identification and Scoping; Forensic Examination; Forensic Reconstruction

**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

“This course addresses the ever-increasing challenges that continually emerge in smartphone forensics.”

-Hilary Tiony, Directorate of E-govt Kenya

---

“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
You Will Be Able To

- Build an isolated, controlled laboratory environment for analyzing code and behavior of malicious programs
- Employ network and system-monitoring tools to examine how malware interacts with the file system, registry, network, and other processes in a Windows environment
- Uncover and analyze malicious JavaScript and VBScript components of web pages, which are often used by exploit kits for drive-by attacks
- Control relevant aspects of the malicious program’s behavior through network traffic interception and code patching to perform effective malware analysis
- Use a disassembler and a debugger to examine the inner workings of malicious Windows executables
- Bypass a variety of packers and other defensive mechanisms designed by malware authors to misdirect, confuse, and otherwise slow down the analyst
- Recognize and understand common assembly-level patterns in malicious code, such as DLL injection and anti-analysis measures
- Assess the threat associated with malicious documents, such as PDF and Microsoft Office files
- Derive Indicators of Compromise (IOCs) from malicious executables to strengthen incident response and threat intelligence efforts

Anuj Soni
SANS Certified Instructor

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-defensive measures, including code injection, sandbox evasion, flow misdirection, and other measures.

The course culminates with a series of Capture-the-Flag challenges designed to reinforce the techniques learned in class and provide additional opportunities to learn practical, hands-on malware analysis skills in a fun setting.

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

- Individuals who have dealt with incidents involving malware and want to learn how to understand key aspects of malicious programs
- Technologists who have informally experimented with aspects of malware analysis and are looking to formalize and expand their expertise in this area
- Forensic investigators and IT practitioners looking to expand their skill sets and learn how to play a pivotal role in the incident response process

Anuj Soni initially pursued a career fighting cybercrime for the thrill of the hunt. These days, Anuj feeds his passion for technical analysis through his role as a Senior Threat Researcher at Cylance, where he performs malware research and reverse engineering. Anuj also brings his problem-solving abilities to his position as a SANS Certified Instructor, which gives him the opportunity to impart his deep technical knowledge and practical skills to students. When teaching Reverse-Engineering Malware (FOR610) and Advanced Digital Forensics and Incident Response (FOR508), Anuj emphasizes establishing goals for analysis, creating and following a process, and prioritizing tasks. Since entering the information security field in 2005, Anuj has performed numerous intrusion investigations to help government and commercial clients mitigate attacks against the enterprise. His malware hunting and technical analysis skills have resulted in the successful identification, containment, and remediation of multiple threat actor groups.

@asoni
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 (REMnux) 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 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 executables. 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:** How Malware Detects Debuggers and Protects Embedded Data; Unpacking Malicious Software that Employs Process Hollowing; Bypassing the Attempts by Malware to Detect and Evade the Analysis Toolkit; Handling Code Misdirection Techniques, Including SEH and TLS Callbacks; Unpackaging Malicious Executable by Anticipating the Packer’s Actions

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 given, is a great introduction for the possibilities and approaches one can take when fighting malware.”

– Max de Bruijn, Fox-IT
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:

“[This 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

David R. Miller has been a technical instructor since the early 1980s and has specialized in consulting, auditing, and lecturing on information systems security, legal and regulatory compliance, and network engineering. David has helped many enterprises develop their overall compliance and security programs. He serves as a security lead and forensic investigator on numerous enterprise-wide IT design and implementation projects for Fortune 500 companies, providing compliance, security, technology, and architectural recommendations and guidance. Projects David has worked on include Microsoft Windows Active Directory directory services, Security Information and Event Management systems, intrusion detection and protection systems, endpoint protection systems, patch management systems, configuration monitoring systems, and enterprise data encryption for data at rest, in transit, in use, and within email systems. David is an author, lecturer and technical editor of books, curriculum, certification exams, and computer-based training videos.

@DRM_CyberDude
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

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

-Kelley O’Neil, Wells Fargo

Who Should Attend

Security professionals and 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
My-Ngoc Nguyen (pronounced Mee-Nop Wynn) is the CEO/Principal Consultant for Secured IT Solutions. She brings 15 years of experience in information systems and technology, with the past 12 years focused on cybersecurity and information assurance for both the government and commercial sectors. My-Ngoc is highly experienced in IT security and risk methodologies, and in legal and compliance programs. She led a cybersecurity program under a federal agency for a highly regulated, first-of-a-kind project of national importance. With that experience, she has been assisting client organizations in both public and private sectors to implement secure and compliant business processes and IT solutions using defense-in-depth and risk-based approaches. Along with a master’s degree in management information systems, she carries top security certifications that include the GPEN, GCIH, GSEC, and CISSP®, and is a former QSA. She is a member of the FBI’s InfraGard, the Information Systems Security Association (ISSA), the Information Systems Audit and Control Association (ISACA), and the International Information Systems Security Certification Consortium (ISC). My-Ngoc founded the non-profit organization CyberSafeNV to raise security awareness among Nevada residents and is currently the organization’s chairperson.

MGT512: Security Leadership Essentials for Managers

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 course empowers you to become an effective security manager and get up to speed quickly on information security issues and terminology. You won’t just learn about security, you will learn how to manage security.

To accomplish this goal, MGT512 covers a wide range of security topics across the entire security stack. Data, network, host, application, and user controls are covered in conjunction with key management topics that address the overall security lifecycle. This also includes governance and technical controls focused on protecting, detecting, and responding to security issues.

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.

“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

My-Ngoc Nguyen (pronounced Mee-Nop Wynn) is the CEO/Principal Consultant for Secured IT Solutions. She brings 15 years of experience in information systems and technology, with the past 12 years focused on cybersecurity and information assurance for both the government and commercial sectors. My-Ngoc is highly experienced in IT security and risk methodologies, and in legal and compliance programs. She led a cybersecurity program under a federal agency for a highly regulated, first-of-a-kind project of national importance. With that experience, she has been assisting client organizations in both public and private sectors to implement secure and compliant business processes and IT solutions using defense-in-depth and risk-based approaches. Along with a master’s degree in management information systems, she carries top security certifications that include the GPEN, GCIH, GSEC, and CISSP®, and is a former QSA. She is a member of the FBI’s InfraGard, the Information Systems Security Association (ISSA), the Information Systems Audit and Control Association (ISACA), and the International Information Systems Security Certification Consortium (ISC). My-Ngoc founded the non-profit organization CyberSafeNV to raise security awareness among Nevada residents and is currently the organization’s chairperson.

@MenopN
**Course Day Descriptions**

**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

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

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

**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

*“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/cdi/courses](http://www.sans.org/cdi/courses)
AUD507: Auditing & Monitoring Networks, Perimeters, and Systems

You Will Be Able To

- Understand the different types of controls (e.g., technical vs. non-technical) essential to perform a successful audit
- Conduct a proper risk assessment of a network to identify vulnerabilities and prioritize what will be audited
- Establish a well-secured baseline for computers and networks, constituting a standard against which one can conduct audits
- Perform a network and perimeter audit using a seven-step process
- Audit firewalls to validate that rules/settings are working as designed, blocking traffic as required
- Utilize vulnerability assessment tools effectively to provide management with the continuous remediation information necessary to make informed decisions about risk and resources
- Audit web application configuration, authentication, and session management to identify vulnerabilities attackers can exploit
- Utilize scripting to build a system to baseline and automatically audit Active Directory and all systems in a Windows domain

“You Will Be Able To

AUD507 provides insight on different aspects related to system configurations and associated risks.”

-Yosra Al-Basha, Yemen LNG Co.

Clay Risenhoover
SANS Certified Instructor

One of the most significant obstacles facing many auditors today is how exactly to go about auditing the security of an enterprise. What systems really matter? How should the firewall and routers be configured? What settings should be checked on the various systems under scrutiny? Is there a set of processes that can be put into place to allow an auditor to focus on the business processes rather than the security settings? How do we turn this into a continuous monitoring process? All of these questions and more will be answered by the material covered in this course.

This course is specifically organized to provide a risk-driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practices, the students will have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation are taken from real-world examples.

One of the struggles that IT auditors face today is helping management understand the relationship between the technical controls and the risks to the business that these controls address. In this course these threats and vulnerabilities are explained based on validated information from real-world situations. The instructor will take the time to explain how this can be used to raise the awareness of management and others within the organization to build an understanding of why these controls specifically and auditing in general are important. From these threats and vulnerabilities, we will explain how to build the ongoing compliance monitoring systems and automatically validate defenses through instrumentation and automation of audit checklists.

You’ll be able to use what you learn immediately. Five of the six days in the course will help you produce your own checklist, or provide you with a general checklist that can be customized for your audit practice. Each of these days includes hands-on exercises with a variety of tools discussed during the lecture sections so that you will leave knowing how to verify each and every control described in the class. Each of the six hands-on days gives you the chance to perform a thorough technical audit of the technology being considered by applying the checklists provided in class to sample audit problems in a virtualized environment.

A great audit is more than marks on a checklist; it is the understanding of what the underlying controls are, what the best practices are, and why. Sign up for this course and gain the mix of theoretical, hands-on, and practical knowledge to conduct a great audit.

Clay is the president of Risenhoover Consulting, Inc., an IT management consulting firm based in Durant, Oklahoma. Founded in 2003, RCI provides IT audit and IT management consulting services to clients in multiple sectors. Clay’s past experience includes positions in software development, technical training, LAN and WAN operations, and IT management in both the private and public sector. He has a master’s degree in computer science and holds a number of technical and security certifications, including the GPEN, GSNA, CISA, CISM, GWEB, and CISSP®.

@AuditClay
Course Day Descriptions

**DAY 1: Effective Audit Management, Risk Assessment, and Virtualization Auditing**

After laying the foundation for the role and function of an auditor in the information security field, this day’s material will give you two extremely useful risk assessment methods that are particularly effective for measuring the security of enterprise systems, identifying control gaps and risks, and gaining the knowledge to be able to recommend additional compensating controls to address the risk. Nearly a third of the day is spent covering important audit considerations and questions dealing with virtualization and cloud computing.

**Topics:** Auditor’s Role in Relation to Policy Creation, Policy Conformance, and Incident Handling; Basic Auditing and Assessing Strategies; Risk Assessment; The Six-Step Audit Process; Virtualization and Cloud Computing

**DAY 2: Effective Network and Perimeter Auditing/Monitoring**

On this day we will build from the ground up dealing with security controls, proper deployment, and effective auditing/continuous monitoring of configuration from Layer 2 all the way up the stack. Students will learn how to identify insecurely configured VLANs, determine perimeter firewall requirements, examine enterprise routers, and much more.

**Topics:** Secure Layer 2 Configurations; Router and Switch Configuration Security; Firewall Auditing, Validation, and Monitoring; Wireless; Network Population Monitoring; Vulnerability Scanning

**DAY 3: Web Application Auditing**

Web applications have consistently been rated for the past several years as one of the top five vulnerabilities that enterprises face. Unlike the other top vulnerabilities, however, enterprises continue to accept this risk, since most modern corporations need an effective web presence to do business today. One of the most important lessons that we are learning as an industry is that installing an application firewall is not enough!

**Topics:** Identifying Controls Against Information Gathering Attacks; Processing Controls to Prevent Hidden Information Disclosures; Control Validation of the User Sign-on Process; Examining Controls Against User Name Harvesting; Validating Protections Against Password Harvesting; Best Practices for OS and Web Server Configuration; How to Verify Session Tracking and Management Controls; Identification of Controls to Handle Unexpected User Input; Server-side Techniques for Protecting Your Customers and Their Sensitive Data

**DAY 4: Advanced Windows Auditing and Monitoring**

Microsoft’s business-class system makes up a large part of the typical IT infrastructure. Quite often, these systems are also the most difficult to effectively secure and control because of the enormous number of controls and settings within the operating system. This course day will provide you with the techniques and tools to build an effective long-term audit program for your Microsoft Windows environment. More importantly, during the course a continuous monitoring and reporting system is built out, allowing you to easily and effectively scale the testing discussed within your enterprise when you return home.

**Topics:** Progressive Construction of a Comprehensive Audit Program; Automating the Audit Process; Windows Security Tips and Tricks; Maintaining a Secure Enterprise

**DAY 5: Advanced Unix Auditing and Monitoring**

Students will gain a deeper understanding of the inner workings and fundamentals of the Unix operating system as applied to the major Unix environments in use in business today. Students will have the opportunity to explore, assess and audit Unix systems hands-on. Lectures describe the different audit controls that are available on standard Unix systems, as well as access controls and security models.

**Topics:** Auditing to Create a Secure Configuration; Auditing to Maintain a Secure Configuration; Auditing to Determine What Went Wrong

**DAY 6: Audit the Flag Capstone Exercise**

This final day of the course presents a capstone experience with additional learning opportunities. Leveraging the well-known NetWars engine, students have the opportunity to connect to a simulated enterprise network environment. Building on the tools and techniques learned throughout the week, each student is challenged to answer a series of questions about the enterprise network, working through various technologies explored during the course.

**Topics:** Network Devices; Servers; Applications; Workstations

---

**Who Should Attend**

- Auditors seeking to identify key controls in IT systems
- Audit professionals looking for technical details on auditing
- Managers responsible for overseeing the work of an audit or security team
- Security professionals newly tasked with audit responsibilities
- System and network administrators looking to better understand what an auditor is trying to achieve, how auditors think, and how to better prepare for an audit
- System and network administrators seeking to create strong change control management and detection systems for the enterprise
- Anyone looking to implement effective continuous monitoring processes within the enterprise

---

“The entire course has been fantastic—it far exceeded my expectations. I think SANS training is far superior to other training programs.”

-Paul Petrasko, Bemis Company
SEC540: Cloud Security and DevOps Automation

You Will Be Able To

- Build a Secure DevOps workflow in your organization
- Create automated security tasks in Continuous Integration/Continuous Delivery (CI/CD) systems
- Configure and run scanners from the Secure DevOps Toolchain
- Perform cloud infrastructure security audits for common misconfiguration vulnerabilities
- Perform secure secrets management using on-premise and cloud-hosted secrets management tools
- Audit microservice architectures for security vulnerabilities in containers, serverless, and API gateway appliances
- Leverage cloud automation to automate patching and software deployments without downtime
- Build serverless functions to monitor, detect and actively defend cloud services and configurations

SEC540 provides development, operations, and security professionals with a methodology to build and deliver secure infrastructure and software using DevOps and cloud services. Students will explore how the principles, practices, and tools of DevOps can improve the reliability, integrity, and security of on-premise and cloud-hosted applications.

Starting with on-premise deployments, the first two days of the course examine the Secure DevOps methodology and its implementation using lessons from successful DevOps security programs. Students will gain hands-on experience using popular open-source tools such as Puppet, Jenkins, GitLab, Vault, Grafana, and Docker to automate Configuration Management (“infrastructure as Code”), Continuous Integration (CI), Continuous Delivery (CD), containerization, micro-segmentation, automated compliance (“Compliance as Code”), and Continuous Monitoring. The lab environment starts with a CI/CD pipeline that automatically builds, tests, and deploys infrastructure and applications. Leveraging the Secure DevOps toolchain, students perform a series of labs injecting security into the CI/CD pipeline using a variety of security tools, patterns, and techniques.

After laying the DevSecOps foundation, the final three days move DevOps workloads to the cloud, build secure cloud infrastructure, and deliver secure software. SEC540 provides in-depth analysis of the Amazon Web Services (AWS) toolchain, while lightly covering comparable services in Microsoft Azure. Using the CI/CD toolchain, students build a cloud infrastructure that can host containerized applications and microservices. Hands-on exercises analyze and fix cloud infrastructure and application vulnerabilities using security services and tools such as API Gateway, Identity and Access Management (IAM), CloudFront Signing, Security Token Service (STS), Key Management Service (KMS), managed WAF services, serverless functions, CloudFormation, AWS Security Benchmark, and much more.

Authors’ Statement

“DevOps and the cloud are radically changing the way that organizations design, build, deploy, and operate online systems. Leaders like Amazon, Etsy, and Netflix are able to deploy hundreds or even thousands of changes every day, continuously learning, improving, and growing—and leaving their competitors far behind. Now DevOps and the cloud are making their way from Internet ‘Unicorns’ and cloud providers into enterprises.

“Traditional approaches to security can’t come close to keeping up with this rate of accelerated change. Engineering and operations teams that have broken down the ‘walls of confusion’ in their organizations are increasingly leveraging new kinds of automation, including Infrastructure as Code, Continuous Delivery and Continuous Deployment, microservices, containers, and cloud service platforms. The question is: can security take advantage of the tools and automation to better secure its systems?

“Security must be reinvented in a DevOps and cloud world.”

-Ben Allen, Jim Bird, Eric Johnson, and Frank Kim

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. He also 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
Who Should Attend

- Anyone working in 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 to migrate DevOps workflows to the cloud, specifically Amazon Web Services (AWS)
- Anyone interested in leveraging cloud application security services provided by AWS
- Developers
- Software architects
- Operations engineers
- System administrators
- Security analysts
- Security engineers
- Auditors
- Risk managers
- Security consultants

---

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 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; Working in DevOps; Security Challenges in DevOps; Building a CD Pipeline; DevOps Deployment Data; Secure Continuous Delivery; Security in Pre-Commit; Security in Commit; Security in Acceptance

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. Because the automated CD pipeline is so critically important to DevOps, you’ll also learn to secure the pipeline, including RASP and other run-time defense technologies. As the infrastructure and application code moves to production, we’ll spend the second half of the day exploring container security issues associated with tools such as Docker and Kubernetes, as well as how to protect secrets using Vault and how to build continuous security monitoring using Graphana, Graphite, and StatsD. Finally, we’ll discuss how to build compliance into Continuous Delivery, using the security controls and guardrails that have been built in the DevOps toolchain.

Topics: Secure Configuration Management Using Infrastructure as Code; Securing Configuration Management and Continuous Integration/ Continuous Delivery Pipelines; Container Security, Hardening, and Orchestration; Continuous Monitoring and Feedback Loops; Secure Secrets Management; Automating Compliance as Code

DAY 3: Moving to the Cloud

Observing DevOps principles, you’ll learn to deploy infrastructure, applications, and the CI/CD toolchain into the cloud. This section provides an overview of Amazon Web Services (AWS) and introduces the foundational tools and practices you’ll need to securely deploy your applications in the cloud.

Topics: Introduction to the Cloud; Cloud Architecture Overview; Secure Cloud Deployment; Security Scanning in CI/CD

DAY 4: Cloud Application Security

In this section, you’ll learn to leverage cloud application security services to ensure that applications have appropriate encryption, authentication, authorization, and access control, while also maintaining functional and high-availability systems.

Topics: Data Protection; Secure Content Delivery; Microservice Security; Serverless Security; Security Automation with Lambda

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: Blue/Green Deployment Options; Security Automation; Security Monitoring; Compliance

---

“Mind-blowing! If you are a traditional security architect, tip-toeing around DevOps, get into SEC540. It takes you into the depths of DevSecOps and sets you up for the future!”

-Jatin Sachdeva, Cisco
ICS410: ICS/SCADA Security Essentials

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.

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 industrial control systems, 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 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 a mutual 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.

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 (detecting 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 the NIST Cyber Security Framework, ISA/IEC 62443, ISO/IEC 27001, NIST SP 800-53, Center for Internet Security Critical Security Controls, and COBIT 5

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

"This course provided a great understanding of the basics of ICS and was a good mix of lecture and hands-on activities.”

—Anthony Delio, PwC

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 (ASAP-SG). He currently leads the testing group at the National Electric Sector Cybersecurity Organization Resources (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, Nolicon, 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 GICSP certified Incident Handler (GCIH), Intrusion Analyst (GCLA), and Web Application Penetration Tester (GWAPT).

@meeas
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 quickly scope the environment and 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 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, SGUI, 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.

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

Robert M. Lee
SANS Certified Instructor

Robert is the CEO and founder of his own company, Dragos, Inc., which provides cybersecurity solutions for industrial control system (ICS) networks. Robert got his start in information security making small control systems 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 the 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

73
ICS-AWARE MALWARE AND ATTACKS ON CRITICAL INFRASTRUCTURE ARE INCREASING IN FREQUENCY AND SOPHISTICATION. YOU NEED TO IDENTIFY THREATS AND VULNERABILITIES AND METHODS TO SECURE YOUR INDUSTRIAL CONTROL SYSTEM ENVIRONMENT. LET US SHOW YOU HOW!

The ICS612: ICS Cyber Security In-Depth course will help you:

▐ Learn active and passive methods to safely gather information about an ICS environment
▐ Identify vulnerabilities in ICS environments
▐ Determine how attackers can maliciously interrupt and control processes and how to build defenses
▐ Implement proactive measures to prevent, detect, slow down, or stop attacks
▐ Understand ICS operations and what “normal” looks like
▐ Build choke points into an architecture and determine how they can be used to detect and respond to security incidents
▐ Manage complex ICS environments and develop the capability to detect and respond to ICS security events

The course concepts and learning objectives are primarily driven by the focus on hands-on labs. The in-classroom lab setup was developed to simulate a real-world environment where a controller is monitoring/controlling devices deployed in the field along with a field-mounted touchscreen Human Machine Interface (HMI) available for local personnel to make needed process changes. Utilizing operator workstations in a remotely located control center, system operators use a SCADA system to monitor and control the field equipment. Representative of a real ICS environment, the classroom setup includes a connection to the enterprise, allowing for data transfer (i.e., Historian), remote access, and other typical corporate functions.

The labs move students through a variety of exercises that demonstrate how an attacker can attack a poorly architected ICS (which, sadly, is not uncommon) and how defenders can secure and manage the environment.

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:

▐ ICS410 alumni
▐ Process control engineers
▐ Systems or safety system engineers
▐ Active defenders in ICS
▐ Anyone with significant control system experience interested in understanding processes and methods to secure the ICS environment

You Will Be Able To

▐ Deal with typical assets found within an industrial environment, including Programmable Logic Controller (PLC), Operator Interfaces (OI) for local control, Human Machine Interface (HMI) servers, Historian server, switches, routers, and firewall(s)
▐ Understand PLC execution through hands-on exercises
▐ Identify security methods that can be applied to real-time control and Input/Output systems
▐ Understand the pros and cons of various PLC and HMI architectures with recommendations for improving security postures of these real-time control systems
▐ Identify where critical assets exist within an industrial environment
▐ Understand the role and design of an Industrial Demilitarized Zone (IDMZ)
▐ Deal with firewalls placed within the industrial zone to achieve cell-to-cell isolation and perimeter restrictions
▐ Dissect multiple industrial protocols to understand normal and abnormal traffic used in the operational control of assets
▐ Better understand the role of IT network services within ICS and identify security methods that can be applied
▐ Use the RELICS virtual machine for asset and traffic identification
▐ Troubleshoot configuration errors within an operational environment
▐ Understand adversary approaches in targeting and manipulating industrial control systems

Tim Conway
SANS Certified Instructor

Jason Dely
SANS Instructor

Jeffrey Shearer
SANS Instructor

Instructor bios can be found at www.sans.org/cdi/instructors
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). The 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 enables you to see how to put the controls in place in your existing network through effective and 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. SEC566 will provide you with the skills to start implementing and auditing each of the Critical Security Controls on your first day back on the job.

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, but using those 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 themselves, saving their organizations both time and money, and facilitating faster collection and use of new log sources.

SEC455 serves as an important primer to those who are unfamiliar with the architecture of an Elastic-based SIEM. Students who have taken or plan to take additional cyber defense courses may find SEC455 to be a helpful supplement to the advanced concepts in courses such as SEC555. In addition, the material discussed in this course will enable students to not only build a new SIEM, but improve and supplement their already existing implementations, producing a more efficient solution that provides the answers they need more quickly and at a lower cost. The overall goal is to show students how to design and modify a SIEM, improve upon their current solution, and reach their original defensive goal – catching adversary activity in their environment.
Penetration Testing | 2-Day Courses

SEC580: **Metasploit Kung Fu for Enterprise Pen Testing**

Many enterprises today face regulatory or compliance requirements that mandate regular penetration testing and vulnerability assessments. Commercial tools and services for performing such tests can be expensive. While really solid free tools such as Metasploit are available, many testers do not understand the comprehensive feature sets of such tools and how to apply them in a professional-grade testing methodology. Metasploit was designed to help testers with confirming vulnerabilities using an open-source and easy-to-use framework. This course will help students get the most out of this free tool.

This class will show students how to apply the incredible capabilities of the Metasploit Framework in a comprehensive penetration testing and vulnerability assessment regimen, according to a thorough methodology for performing effective tests. Students who complete the course will have a firm understanding of how Metasploit can fit into their penetration testing and day-to-day assessment activities. The course will provide an in-depth understanding of the Metasploit Framework far beyond simply showing attendees how to exploit a remote system. The class will cover exploitation, post-exploitation reconnaissance, token manipulation, spear-phishing attacks, and the rich feature set of the Meterpreter, a customized shell environment specially created for exploiting and analyzing security flaws.

The course will also cover many of the pitfalls that a tester may encounter when using the Metasploit Framework and how to avoid or work around them, making tests more efficient and safe.

**SEC564: Red Team Exercises & Adversary Emulation**

Red Teaming is the process of using tactics, techniques, and procedures (TTPs) to emulate real-world adversaries in order to train and measure the effectiveness of the people, processes, and technology used to defend organizations. SEC564 will provide you with the skills to manage and operate a Red Team, conduct Red Team exercises and adversary emulations, and understand the role of the team and its importance in security testing.

Built on the fundamentals of penetration testing, Red Team exercises use a comprehensive approach to gain a holistic view of an organization’s security posture in order to improve its ability to detect, respond, and recover from an attack. When properly conducted, Red Team exercises significantly improve an organization’s security posture and controls, hone its defensive capabilities, and measure the effectiveness of its security operations.

Red Team exercises require a different approach from a typical security test and rely heavily on well-defined TTPs, which are critical to successfully emulate a realistic adversary. The Red Team exercises and adversary emulation results exceed a typical list of penetration test vulnerabilities, provide a deeper understanding of how an organization would perform against a real adversary, and identify where security strengths and weaknesses exist across people, processes, and technology.

Whether you support a defensive or offensive role in security, understanding how Red Team exercises can be used to improve security is extremely valuable. This intensive two-day course will explore Red Team concepts in-depth, provide the required fundamentals of adversary emulation, and help you improve your organization’s security posture.

“The content from SEC564 is great and I will be able to implement it in my organization right away!”

-Kirk Hayes, Rapid 7

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

“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

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. The 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.

DevSecOps | 2-Day Course

SEC534: Secure DevOps: A Practical Introduction

This course explains the fundamentals of DevOps and how DevOps teams can build and deliver secure software. You will learn DevOps principles, practices, and tools and how they can be leveraged to improve the reliability, integrity, and security of systems.

Using lessons from successful DevOps security programs, we will explain how Secure DevOps can be implemented. Students will gain hands-on experience using popular open-source tools such as Puppet, Jenkins, GitLab, Vault, Grafana, and Docker to automate Configuration Management (“Infrastructure as Code”), Continuous Integration (CI), Continuous Delivery (CD), containerization, micro-segmentation, automated compliance (“Compliance as Code”), and Continuous Monitoring. The lab environment starts with a CI/CD pipeline that automatically builds, tests, and deploys infrastructure and applications. Leveraging the Secure DevOps toolchain, students perform a series of labs injecting security into the CI/CD pipeline using a variety of security tools, patterns, and techniques.

“A fast-paced and illustrative two days on the current state of security for DevOps. It was well worth the time invested to take the class.”
-Michael Machado, Ring Central
Welcome Reception & Early Check-In

Kick off your SANS Cyber Defense Initiative 2019 experience at the Welcome Reception. Be part of this premier event and join the industry’s most powerful gathering of cybersecurity professionals. Share stories, make connections and learn how to make the most of your week in Washington, DC. Come join your colleagues for a fun, relaxing evening.

General Session – Welcome to SANS

Bryan Simon
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: Windows Exploratory Surgery with Process Hacker

Jason Fossen
In this talk, Jason Fossen, SANS Institute Fellow and SEC505 author, will rummage around inside the guts of Windows while on the lookout for malware, using a free tool named Process Hacker (similar to Process Explorer, but open-source). Understanding processes, threads, drivers, handles, and other OS internals is important for analyzing malware, understanding exploits, doing forensics, troubleshooting, and hardening the OS. Feel free to bring your laptop and install Process Hacker from https://github.com/processhacker/ in order to play along. This talk helps to prepare attendees for several of the courses at the conference by presenting key OS concepts like security access tokens, modules, sessions, DPCs, and more.

DevSecOps: Key Controls For Modern Security Success

Eric Johnson
Modern development teams deliver features at a rapid pace using new technologies such as containers, microservices, and serverless functions. Operations and infrastructure teams support these rapid delivery cycles using Infrastructure as Code, Test Driven Infrastructure (TDI), and cloud automation. However, security teams are using traditional security approaches that don’t keep up with the rate of accelerated change. Security must be reinvented in a DevOps world by taking advantage of the opportunities provided by continuous integration and delivery pipelines. This talk will introduce attendees to five key phases of DevOps: pre-commit, commit, acceptance, production, and operations. In each phase, we identify the key security controls and discuss several open-source tools for implementing the controls. Attendees will walk away with a practical and modern approach to building a successful DevSecOps program.

Open-Source Intelligence 101

John TerBush
This presentation will examine the current state of open-source intelligence (OSINT) and how you might be able to use collection from open sources to improve your work. Learn tips, techniques and tools that can make OSINT investigations more thorough and efficient.

Hunting Highs and Lows: Misadventures in Threat Hunting

David Mashburn
Threat hunting is often described as being an essential part of modern security operations. However, smaller or less mature security teams may face significant hurdles when trying to spin up this capability. This talk will explore some of the challenges related to building threat hunting capabilities, explore a few common pitfalls, and describe ways to try to maximize the value of your threat hunting activities in a small to mid-sized organization. We will also discuss how to leverage the tools already available to your team without adding new costs for deployment, and learn how they can be managed via existing channels.

Cloud Security Automation: From Infrastructure to App

Frank Kim
Learn how to leverage security automation in your cloud infrastructure, DevOps pipeline, and applications. Using the open-source Cloud Custodian tool you’ll see how AWS CloudTrail, CloudWatch, and Lambda are used to implement automated infrastructure monitoring and remediation. Then you’ll see how DevOps security automation and Infrastructure as Code is used to build a Blue/Green deployment infrastructure to quickly patch critical security vulnerabilities. Finally, using the open-source AWS WAF Security Automations project you’ll see how it can be automatically deployed via your Jenkins CI/CD pipeline, how the WAF leverages Lambda for automation, and how it automatically blocks critical application vulnerabilities.

GIAC Overview Presentation

Kim Lucht
GIAC Certifications is the leading provider and developer of Information Security Certifications. GIAC tests and validates the ability of practitioners in cyber defense, pen testing, forensics, software security, management, and ICS. GIAC certification holders are recognized as experts in the IT industry and are sought after for their ability of practitioners in cyber defense, pen testing, forensics, software security, management, and ICS. GIAC certification holders are recognized as experts in the IT industry and are sought after for their ability of practitioners in cyber defense, pen testing, and software security. GIAC certification is required to establish a career in the IT industry and is recognized as the standard by employers.

Putting MITRE ATT&CK™ into Action with What You Have, Where You Are

Katie Nickels
MITRE ATT&CK™ has become widely adopted in the community as a way to frame adversary behaviors and improve defenses. But how can you use it for your team with what you have, where you are? Katie Nickels will break down the ATT&CK knowledge base so you understand how you can put it into action. She will explain the philosophy and approach behind ATT&CK, then dive into how you can use it, whether you’re a one-person shop or an advanced Security Operations Center. Katie will cover how you can use ATT&CK for detection, threat intelligence, assessments, and red teaming, with a focus on actionable takeaways to help your team move toward a threat-informed defense.

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.
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.

Evolving Threats
Paul Henry
For nearly two decades defenders have fallen into the “Crowd Mentality Trap” and have simply settled on doing the same thing everyone else was doing. At the same time, attackers have clearly evolved both in terms of malware delivery vectors and attack methodology. Today our defenses focus primarily on the gateway and on attempting to outwit attackers’ delivery methods. This leaves us woefully exposed and according to a recent Data Breach Report has resulted in 3,765 incidents, 806 million records exposed, and $157 billion in data breach costs in only the past six years. The Evolving Threats presentation is updated monthly and provides insight into mitigations of our most current threats.

Coffee & 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 the SANS graduate programs. SANS’s 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.

Building and Operating an OT/ICS SOC
Robert M. Lee
Security operations is an important aspect of countering targeted cyber threats. As organizations look at their industrial networks, such as operations technology (OT) and industrial control systems (ICS), the discussion naturally comes up as to whether to incorporate them into 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, and examine how to build and operate the OT SOC (whether it’s a dedicated entity or integrated).

Automated Adversary Emulation Using CALDERA
Erik Van Buggenhout
MITRE ATT&CK is quickly gaining traction and is becoming an important standard to assess the overall cybersecurity posture of an organization. Tools like ATT&CK Navigator and CALDERA facilitate corporate adoption and allow for a holistic overview of attack techniques and how the organization is preventing and detecting them. Furthermore, many vendors, technologies and open-source initiatives are aligning with ATT&CK. CALDERA is an automated adversary emulation system that performs post-compromise adversarial behaviour within Windows Enterprise networks. It generates plans during operations using a planning system and a pre-configured adversary model based on the Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) project. These features allow CALDERA to dynamically operate over a set of systems using variable behaviour, which better represents how human adversaries perform operations than systems that follow prescribed sequences of actions. During this talk, Erik will demonstrate some CALDERA strong points and weaknesses and how it can be further improved (e.g., how we can build additional steps to increase our ATT&CK coverage or adapt steps to handle new Windows 10 security features such as ExploitGuard and AMSI).

Failing to Succeed in Cyber Security & Risk Management
My-Ngoc Nguyen
The word “failure” (the other bad F word) has such a negative connotation, especially in the cybersecurity realm. This is because we are taught at an early age that an F is really bad. But is it? This talk will discuss how we need to fail forward in order to better succeed and improve our ability to manage risk. Managing risk is a complicated aspect of effective cybersecurity. In order to get better at it, we need to embrace calculated failures and mature our risk model.

Vendor-Sponsored Events

Vendor Showcase
Fri, Dec 13 | 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
Thu, Dec 12 & Sat, Dec 14 | 12:30p – 1:15pm
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.

The competition for top talent is intense. When you need to fill cybersecurity positions, the SANS Cyber Immersion Academies can help. Our qualified and diverse graduates include U.S. veterans and proven professionals. They are ready to join your team and work on day one!

Hire Our Cybersecurity Professionals

You have great people. Invest in their skills and everyone wins. SANS Cyber Immersion Academies quickly and cost-effectively meet the specific needs of organizations and employers seeking to develop and retain top cybersecurity talent. Our immersive, accelerated training programs help you develop the best available talent on the market.

Develop Your Own Cybersecurity Talent

The SANS Institute is renowned and respected for its world-class cyber training. CACI is pleased to team with SANS on this critical workforce development initiative, which will help fill a pressing need for cybersecurity experts in industry and government.

― Mike Mourelatos
Vice President & CTO
CACI, National Services & Intelligence Solutions

Our Academy Graduates are Seeking Opportunities!

For more information, contact IMMERSIONACADEMY@SANS.ORG or visit WWW.SANS.ORG/ACADEMY4EMPLOYERS

Diversity Cyber Academy
Simulcast Courses | SANS Cyber Defense Initiative® 2019

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

Register now at www.sans.org/cdi/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
Security Awareness Is Critical in Protecting Your Organization

What’s in your training content?

Expert Led
SANS awareness training content is built by the world’s leading cybersecurity practitioners. Cognitive experts, design theory animators, and leading security awareness experts deliver training content that protects your organization and changes human behaviors.

Relevant
Our content is constantly updated to match current threats. Training is available in multiple formats, with a variety of supplemental materials, to reach every audience in any language.

Easy
Modules are created to match important threats, designed in core and specialized training module-sets to cover all aspects of training.

World-class training offered from top experts, all available in a variety of formats, and prepared for a global audience. Let SANS Security Awareness training help you manage human risk.

Learn more at: sans.org/security-awareness

“Whether for our developers, administrators, or executives, the SANS Security Awareness training curriculum hits the nail on the head! I can’t begin to count how many conversations have been sparked, relevant questions have been asked, light bulbs of understanding have lit up, and less secure behaviors have changed as a result of this content.”

Jim Raub, CISO and Vice President, EagleDream Technologies
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.
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 November 13, 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.

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

Special Hotel Rates Available
A special discounted rate of $209 S/D will be honored based on space availability.
Government per diem rooms are also available with proper ID. All rates include high-speed Internet in your guest room and are only available through November 19, 2019.

Top three reasons to stay at the Washington Hilton
1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Washington Hilton, 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 Hilton that you won’t want to miss!

Register online at www.sans.org/cdi
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 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 & enter code by: Oct 16 $300 Nov 6 $150
*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 SANS Cyber Defense Initiative® 2019 Simulcast course. See page 81 or visit www.sans.org/cdi/attend-remotely for more details.

WASHINGTON HILTON
1919 Connecticut Ave. NW | Washington, DC 20009
202-483-3000
www.sans.org/cdi/location
From the Washington Hilton, you’ll enjoy easy access to the city’s most popular attractions while staying in one of DC’s most vibrant neighborhoods. Walk outside the doors to explore restaurants, museums, and national attractions or unwind in relaxing accommodations.

Register at www.sans.org/cdi | 301-654-SANS (7267)
# Registration Fees

If you don’t wish to register online, please call **301-654-SANS (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 Name</th>
<th>Prior to Early Bird</th>
<th>Early Bird</th>
<th>OnDemand</th>
<th>NetWars Continuous</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC301</td>
<td>Introduction to Cyber Security</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
</tr>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>SEC450</td>
<td>Blue Team Fundamentals: Security Operations and Analysis <strong>NEW!</strong></td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>SEC660</td>
<td>Enterprise Threat and Vulnerability Assessment</td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>SEC487</td>
<td>Open-Source Intelligence (OSINT) Gathering and Analysis</td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>SEC501</td>
<td>Advanced Security Essentials – Enterprise Defender</td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>SEC503</td>
<td>Intrusion Detection In-Depth</td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>SEC505</td>
<td>Securing Windows and PowerShell Automation</td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>SEC511</td>
<td>Continuous Monitoring and Security Operations</td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>SEC530</td>
<td>Defensible Security Architecture and Engineering</td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>SEC540</td>
<td>Cloud Security and DevOps Automation</td>
<td>$6,300</td>
<td>$6,450</td>
<td>$6,600</td>
<td>$799</td>
</tr>
<tr>
<td>SEC542</td>
<td>Web App Penetration Testing and Ethical Hacking</td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>SEC545</td>
<td>Cloud Security Architecture and Operations</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
</tr>
<tr>
<td>SEC555</td>
<td>SIEM with Tactial Analytics</td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>SEC560</td>
<td>Network Penetration Testing and Ethical Hacking</td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>SEC566</td>
<td>Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
</tr>
<tr>
<td>SEC573</td>
<td>Automating Information Security with Python</td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>SEC599</td>
<td>Defeating Advanced Adversaries – Purple Team Tactics &amp; Kill Chain Defenses</td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>SEC660</td>
<td>Advanced Penetration Testing, Exploit Writing, and Ethical Hacking</td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>FOR500</td>
<td>Windows Forensic Analysis</td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Incident Response, Threat Hunting, and Digital Forensics <strong>NEW!</strong></td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>FOR572</td>
<td>Advanced Network Forensics: Threat Hunting, Analysis &amp; Incident Response <strong>NEW!</strong></td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>FOR578</td>
<td>Cyber Threat Intelligence</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
</tr>
<tr>
<td>FOR585</td>
<td>Smartphone Forensic Analysis In-Depth</td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>FOR610</td>
<td>Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>MGT414</td>
<td>SANS Training Program for CISSP® Certification</td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>MGT512</td>
<td>Security Leadership Essentials for Managers</td>
<td>$6,300</td>
<td>$6,450</td>
<td>$6,600</td>
<td>$799</td>
</tr>
<tr>
<td>MGT514</td>
<td>Security Strategic Planning, Policy, and Leadership</td>
<td>$6,300</td>
<td>$6,450</td>
<td>$6,600</td>
<td>$799</td>
</tr>
<tr>
<td>AUD507</td>
<td>Auditing &amp; Monitoring Networks, Perimeters, and Systems</td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>ICS410</td>
<td>ICS/SCADA Security Essentials</td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>ICS515</td>
<td>ICS Active Defense and Incident Response</td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
<tr>
<td>ICS612</td>
<td>ICS Cyber Security In-Depth <strong>BETA!</strong></td>
<td>$6,720</td>
<td>$6,870</td>
<td>$7,020</td>
<td>$799</td>
</tr>
</tbody>
</table>

*Some restrictions apply. Early bird discounts do not apply to Hosted courses.

## Skill-Based Short Courses

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Name</th>
<th>Course Fee</th>
<th>Add OnDemand</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC440</td>
<td>Critical Security Controls: Planning, Implementing, and Auditing</td>
<td>$2,100</td>
<td>$315</td>
</tr>
<tr>
<td>SEC455</td>
<td>SIEM Design &amp; Implementation</td>
<td>$2,100</td>
<td>$315</td>
</tr>
<tr>
<td>SEC534</td>
<td>Secure DevOps: A Practical Introduction</td>
<td>$2,100</td>
<td>$315</td>
</tr>
<tr>
<td>SEC566</td>
<td>Red Team Exercises &amp; Adversary Emulation</td>
<td>$2,100</td>
<td>$315</td>
</tr>
<tr>
<td>SEC580</td>
<td>Metasploit Kung Fu for Enterprise Pen Testing</td>
<td>$2,100</td>
<td>$315</td>
</tr>
<tr>
<td>MGT415</td>
<td>A Practical Introduction to Cyber Security Risk Management</td>
<td>$2,100</td>
<td>$315</td>
</tr>
<tr>
<td>MGT433</td>
<td>SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program</td>
<td>$2,100</td>
<td>$315</td>
</tr>
<tr>
<td>SPECIAL</td>
<td>Core NetWars Experience – Tournament Entrance Fee</td>
<td>FREE</td>
<td>$1,795</td>
</tr>
<tr>
<td>SPECIAL</td>
<td>Cyber Defense NetWars Tournament – Tournament Entrance Fee</td>
<td>FREE</td>
<td>$1,795</td>
</tr>
<tr>
<td>SPECIAL</td>
<td>DFIR NetWars Tournament – Tournament Entrance Fee</td>
<td>FREE</td>
<td>$1,795</td>
</tr>
<tr>
<td>SPECIAL</td>
<td>ICS NetWars – Tournament Entrance Fee</td>
<td>FREE</td>
<td>$1,795</td>
</tr>
</tbody>
</table>

**EARLY BIRD DISCOUNTS**

Pay for any long course using the code **EarlyBird19** at checkout by **October 16th to get $300 OFF** or by **November 6th to get $150 OFF**

*Some restrictions apply. Early bird discounts do not apply to Hosted courses.*
As the leading provider of information defense, security, and intelligence training to military, government, and industry groups, the SANS Institute is proud to be a Corporate Member of the AFCEA community.

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
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

SAVE $300
Register and pay by Oct 16th
Use code EarlyBird19

To be removed from future mailings, please contact unsubscribe@sans.org or (301) 654-SANS (7267). Please include name and complete address.
NALT-BRO-CDI2019