Security West 2020
San Diego | May 6-13 | netwars

No matter what cybersecurity skills you need to learn or which certifications you’re hoping to obtain, SANS and GIAC have you covered. Choose from 35+ hands-on courses taught by the industry’s top practitioners, giving you the knowledge and skills you need to validate your expertise with a GIAC certification.

“With multiple real-world examples, labs that provide direct application of the course material, and top-notch instructors, there is nothing compared to SANS.”

— Matthew Arnsdorff, Target
### Courses at a Glance

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

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Page No.</th>
<th>Available via Simulcast</th>
<th>Bundle On-Demand with this course</th>
<th>Meets DoDD 8570 (815) Requirements</th>
<th>Instructor</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC301</td>
<td>Introduction to Cyber Security</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td>Keith Palmgren</td>
</tr>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td>Bryan Simon</td>
</tr>
<tr>
<td>SEC440</td>
<td>Critical Security Controls: Planning, Implementing, and Auditing</td>
<td>80</td>
<td></td>
<td></td>
<td></td>
<td>Randy Marchany</td>
</tr>
<tr>
<td>SEC450</td>
<td>Blue Team Fundamentals: Security Operations and Analysis</td>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td>Staff</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>David Mashburn</td>
</tr>
<tr>
<td>SEC501</td>
<td>Advanced Security Essentials – Enterprise Defender</td>
<td>18</td>
<td></td>
<td></td>
<td></td>
<td>Shane Hanchey</td>
</tr>
<tr>
<td>SEC503</td>
<td>Intrusion Detection In-Depth</td>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td>David Hoelzer</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>Jon Gorenflo</td>
</tr>
<tr>
<td>SEC505</td>
<td>Securing Windows and PowerShell Automation NEW!</td>
<td>24</td>
<td></td>
<td></td>
<td></td>
<td>Jason Fessen</td>
</tr>
<tr>
<td>SEC511</td>
<td>Continuous Monitoring and Security Operations</td>
<td>26</td>
<td></td>
<td></td>
<td></td>
<td>Maxim Deweerdt</td>
</tr>
<tr>
<td>SEC530</td>
<td>Defensible Security Architecture and Engineering</td>
<td>28</td>
<td></td>
<td></td>
<td></td>
<td>Ryan Nicholson</td>
</tr>
<tr>
<td>SEC545</td>
<td>Cloud Security Architecture and Operations</td>
<td>30</td>
<td></td>
<td></td>
<td></td>
<td>Kenneth G. Hartman</td>
</tr>
<tr>
<td>SEC566</td>
<td>Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td>32</td>
<td></td>
<td></td>
<td></td>
<td>James Tarala</td>
</tr>
<tr>
<td>SEC599</td>
<td>Defeating Advanced Adversaries – Purple Team Tactics &amp; Kill Chain Defenses</td>
<td>34</td>
<td></td>
<td></td>
<td></td>
<td>James Shewmaker</td>
</tr>
<tr>
<td>SEC640</td>
<td>Enterprise Threat and Vulnerability Assessment</td>
<td>38</td>
<td></td>
<td></td>
<td></td>
<td>Matthew Toussain</td>
</tr>
<tr>
<td>SEC542</td>
<td>Web App Penetration Testing and Ethical Hacking</td>
<td>40</td>
<td></td>
<td></td>
<td></td>
<td>Eric Conrad</td>
</tr>
<tr>
<td>SEC560</td>
<td>Network Penetration Testing and Ethical Hacking</td>
<td>42</td>
<td></td>
<td></td>
<td></td>
<td>Tim Medin</td>
</tr>
<tr>
<td>SEC596</td>
<td>Red Team Exercises and Adversary Emulation NEW!</td>
<td>44</td>
<td></td>
<td></td>
<td></td>
<td>Jorge Orchiles</td>
</tr>
<tr>
<td>SEC573</td>
<td>Automating Information Security with Python</td>
<td>64</td>
<td></td>
<td></td>
<td></td>
<td>Mark Baggett</td>
</tr>
<tr>
<td>SEC575</td>
<td>Mobile Device Security and Ethical Hacking</td>
<td>46</td>
<td></td>
<td></td>
<td></td>
<td>Christopher Crowley</td>
</tr>
<tr>
<td>SEC617</td>
<td>Wireless Penetration Testing and Ethical Hacking</td>
<td>48</td>
<td></td>
<td></td>
<td></td>
<td>Joshua Wright</td>
</tr>
<tr>
<td>FOR498</td>
<td>Battlefield Forensics &amp; Data Acquisition NEW!</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td>Kevin Ripa</td>
</tr>
<tr>
<td>FOR500</td>
<td>Windows Forensics Analysis</td>
<td>52</td>
<td></td>
<td></td>
<td></td>
<td>Rob Lee</td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Incident Response, Threat Hunting, and Digital Forensics</td>
<td>54</td>
<td></td>
<td></td>
<td></td>
<td>Eric Zimmerman</td>
</tr>
<tr>
<td>FOR518</td>
<td>Mac and iOS Forensic Analysis and Incident Response</td>
<td>56</td>
<td></td>
<td></td>
<td></td>
<td>Sarah Edwards</td>
</tr>
<tr>
<td>FOR572</td>
<td>Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response</td>
<td>58</td>
<td></td>
<td></td>
<td></td>
<td>Philip Hagen</td>
</tr>
<tr>
<td>FOR585</td>
<td>Smartphone Forensics Analysis In-Depth</td>
<td>60</td>
<td></td>
<td></td>
<td></td>
<td>Domenica Crogna</td>
</tr>
<tr>
<td>FOR610</td>
<td>Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td>
<td>62</td>
<td></td>
<td></td>
<td></td>
<td>Anuj Soni</td>
</tr>
<tr>
<td>MG1466</td>
<td>SANS Training Program for CISSP® Certification</td>
<td>64</td>
<td></td>
<td></td>
<td></td>
<td>David R. Miller</td>
</tr>
<tr>
<td>MG1512</td>
<td>Security Leadership Essentials for Managers</td>
<td>66</td>
<td></td>
<td></td>
<td></td>
<td>Jeff Frick</td>
</tr>
<tr>
<td>MG1514</td>
<td>Security Strategic Planning, Policy, and Leadership</td>
<td>68</td>
<td></td>
<td></td>
<td></td>
<td>G. Mark Hardy</td>
</tr>
<tr>
<td>SEC540</td>
<td>Cloud Security and DevOps Automation</td>
<td>70</td>
<td></td>
<td></td>
<td></td>
<td>Eric Johnson</td>
</tr>
<tr>
<td>IC5456</td>
<td>ICS/SCADA Security Essentials</td>
<td>72</td>
<td></td>
<td></td>
<td></td>
<td>Paul Piotrowski</td>
</tr>
<tr>
<td>IC5515</td>
<td>ICS Active Defense and Incident Response</td>
<td>74</td>
<td></td>
<td></td>
<td></td>
<td>Jason Christopher</td>
</tr>
<tr>
<td>IC612</td>
<td>ICS Cybersecurity In-Depth NEW!</td>
<td>76</td>
<td></td>
<td></td>
<td></td>
<td>Robert M. Lee</td>
</tr>
<tr>
<td>HOSTED</td>
<td>Successful Infosec Consulting NEW!</td>
<td>78</td>
<td></td>
<td></td>
<td></td>
<td>Tim Conway</td>
</tr>
<tr>
<td>NETWARS</td>
<td>Core NetWars Tournament</td>
<td>37</td>
<td></td>
<td></td>
<td></td>
<td>Ted Demopoulos</td>
</tr>
<tr>
<td>NETWARS</td>
<td>Cyber Defense NetWars Tournament</td>
<td>37</td>
<td></td>
<td></td>
<td></td>
<td>Staff</td>
</tr>
<tr>
<td>DEFI</td>
<td>DEFI NetWars Tournament</td>
<td>37</td>
<td></td>
<td></td>
<td></td>
<td>Eric Conrad</td>
</tr>
</tbody>
</table>

### Contents

- **SANS Institute** .................................. 2
- **The SANS Faculty** .................................. 3
- **Securing Approval & Budget for Training** ........ 4
- **Build a High-Performing Security Organization** .. 5
- **SANS Training Roadmap** .......................... 6-7
- **GIAC Certifications** ............................. 36
- **SANS OnDemand Bundle** .......................... 8
- **GIAC Certification Bundle** ........................ 8
- **Bonus Sessions** .................................. 81-82
- **Benefits of Attending a Live SANS Training Event** .... 9
- **Upcoming SANS Training Events** ................. 83
- **SANS Voucher Program** ........................... 84
- **SANS OnDemand Bundle** .......................... 8
- **NetWars** .......................................... 37
- **GIAC Certifications** ............................. 81-82
- **Exhibitor-Sponsored Events** ...................... 82
- **Hotel Information** .................................. 84
- **Registration Information** .......................... 84
- **Free Resources** .................................... 84
- **Back Cover** ........................................ 84
- **SANS Simulcast Registration** ...................... 84
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.

The SANS curriculum spans the full range of cybersecurity fields, including Cyber Defense, Penetration Testing & Ethical Hacking, Digital Forensics & Incident Response, Threat Hunting, Audit, Management, Critical Infrastructure and Control Systems Security, Secure Software Development, and more.

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 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 rewatch 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 sans.org

Test drive 45+ SANS courses
For those new to SANS or unsure of the subject area or skill level to select for your next training course, SANS offers free one-hour course previews via our OnDemand platform. Preview our courses at sans.org/demo
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 120 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:
sans.org/security-west/instructors
Securing Approval and Budget for Training

As a cybersecurity professional, you already know that SANS is the most trusted resource for the training you need. But getting buy-in from your manager or the C-Suite can be a challenge—especially if they don’t yet understand the benefits that SANS training can bring. By following some simple guidelines, you can show them what they need to know, and get them to support your training.

Packaging matters

Submit a formal request

- Most successful training requests are made via written document—a short memo or a few slides—justifying the need for training. Training request templates are available for popular SANS courses. They can be found in the “Justify Your Training” section of the course page. Most managers will respect and value the effort you put in to provide written justification.
- A formal request is a chance for you to provide all the necessary information in one place. If you include additional SANS resources, you can give your manager context and present your request as a complete package. Some helpful additions include the “Why SANS?” web page, the Training Roadmap, an instructor bio, and a course description.

Clearly state the benefits

Be specific

- How does the course relate to your job? Will it help you establish baseline skills? Transition to a more focused role? Decision-makers need to understand the plan.
- Highlight specific tasks you’ll be able to do as a result of the training. Each SANS course description includes a section titled “You Will Be Able To;” include this section in your request to make the benefits clear. Match the training to your job tasks and goals.

Set the context

Establish long-term expectations

- Cybersecurity is a specialized career path within IT. Its practices evolve as attacks change. Because of this, organizations should expect to spend 6%-10% of team salaries to keep skills current. Training for such a dynamic field is an annual, per-person expense—not a once-and-done item.
- Sign up for the related GIAC certification in order to validate that you learned the skills taught in the class. Your employer can be confident you learned what they paid for, since GIAC exams are psychometrically designed to confirm competency in job-related tasks.
- Consider offering trade-offs for the investment. Many professionals build annual training expenses into their employment agreements when they’re hired; some offer to stay for a year after they complete the training.
Build a High-Performing Security Organization

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

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

Prioritize your efforts within these areas using the Center for Internet Security Critical Controls as you mature your own organization.

Determine the number and types of professionals you need to perform the hands-on work, then launch an ongoing campaign to develop a team with the appropriate skills in mind. Cybersecurity is a specialized practice area within IT, and demands specialized training.

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

Four critical job roles typically emerge:

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

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

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

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

Within (or beyond) these four areas, a high-performing security organization will develop its professional staff even further, with some individuals covering more areas while others go deeper into just one specialty. Along the entire spectrum from active defense to cloud defense, and from Python for InfoSec professionals to malware reengineering, SANS offers more than 30 courses to train for specialized roles or learn about more advanced topics, meeting the needs of security professionals at every level.
SANS’ comprehensive course offerings enable professionals to deepen their technical skills in key practice areas. The courses also address other topics and audiences, such as security training for software developers, industrial control engineers, and non-technical personnel in management, legal, and audit.

### Training Roadmap

**Baseline Skills**

**New to Cyber Security**
- Concepts, Tools, & Skills
  - Cyber Security Fundamentals: SEC301 Introduction to Cyber Security | GSF

**You are experienced in technology, but need to learn hands-on, essential security skills and techniques**
- Care Techniques
  - Every Security Professional Should Know
    - Security Essentials: SEC415 Security Essentials Bootcamp Style | GEC
    - Hacker Techniques: SEC324 Hacker Tools, Techniques, Exploits, and Incident Handling | GOCN

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.

**Penetration Testing**
- Vulnerability Analysis, Ethical Hacking
  - Every Pen Tester Should Know
    - Networks: SEC606 Network Penetration Testing and Ethical Hacking | GPN
    - Web Apps: SEC421 Web App Penetration Testing and Ethical Hacking | GWAPT

The professional who can find weaknesses is often a different breed than one focused exclusively on building defenses. A basic tenant of red team/blue team deployments is that finding vulnerabilities requires a different way of thinking, and different tools, but it’s essential for defense specialists to improve their defenses.

**Incident Response & Threat Hunting**
- Host & Network Forensics
  - Every Forensics and IR Professional Should Know
    - Endpoint Forensics: FOR510 Windows Forensic Analysis | GCF
    - Network Forensics: FOR521 Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response | GCF

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

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

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

**Focus Job Roles**

**Crucial Skills, Specialized Roles**

**Cyber Defense Operations**

**Specialized Defensive Area**

| Blue Team | SEC549 Blue Team Fundamentals: Security Operations and Analysis |
| GSINT | SEC640 Open-Source Intelligence (OSINT) Gathering and Analysis |
| Cloud Security | SEC246 Cloud Security Architecture and Operations |
| Linux/ Unix Defense | SEC206 SECuring Linux/Unix | GCLI |
| SIEM | SEC535 SIEM with Tactical Analytics | GDA |

**Penetration Testing**

**Focused Techniques & Areas**

<table>
<thead>
<tr>
<th>In-Depth Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Assessment: SEC440 Enterprise Threat and Vulnerability Assessment</td>
</tr>
<tr>
<td>Networks: SEC640 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking</td>
</tr>
<tr>
<td>Web Apps: SEC662 Advanced Web App Testing, Ethical Hacking, and Exploitation Techniques</td>
</tr>
<tr>
<td>Mobile: SEC255 Mobile Device Security and Ethical Hacking</td>
</tr>
<tr>
<td>Wireless: SEC261 Wireless Penetration Testing and Ethical Hacking</td>
</tr>
<tr>
<td>Python Coding: SEC271 Automating Information Security with Python</td>
</tr>
</tbody>
</table>

**Digital Forensics, Malware Analysis, & Threat Intel**

**Specialized Investigative Skills**

<table>
<thead>
<tr>
<th>Malware Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Intelligence: FOR560 Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td>
</tr>
<tr>
<td>Cyber Threat Intelligence: FOR581 Cyber Threat Intelligence</td>
</tr>
<tr>
<td>Digital Forensics &amp; Media Exploitation</td>
</tr>
<tr>
<td>Triage &amp; Data Collection: FOR460 Battlefield Forensics &amp; Data Acquisition</td>
</tr>
<tr>
<td>Incident Response: FOR551 Advanced Network Forensics: Threat Detection</td>
</tr>
<tr>
<td>Memory Forensics: FOR552 Memory Forensics: Threat Detection</td>
</tr>
<tr>
<td>Malware Forensics: FOR591 Mal and ICS Forensic Analysis and Incident Response</td>
</tr>
</tbody>
</table>

**Advanced Management**

**Advanced Leadership, Audit, Legal**

<table>
<thead>
<tr>
<th>Planning, Policy, Leadership</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOR502 Advanced Leadership, Audit, Legal</td>
</tr>
<tr>
<td>Management Skills</td>
</tr>
<tr>
<td>FOR583 Advanced Planning, Security, and Management Skills</td>
</tr>
<tr>
<td>Managing Vulnerabilities: FOR586 Managing Security Vulnerabilities: Enterprise and Cloud</td>
</tr>
<tr>
<td>Project Management: FOR585 IT Project Management, Effective Communication, and PMBOK Exam Prep</td>
</tr>
<tr>
<td>Audit &amp; Legal</td>
</tr>
<tr>
<td>AUD601 Auditing and Monitoring Networks, Perimeters, and Systems</td>
</tr>
<tr>
<td>Law &amp; Investigations</td>
</tr>
<tr>
<td>LEG521 Law of Data Security and Investigations</td>
</tr>
</tbody>
</table>

**Development Paths**

**Industrial Controls**

**Every ICS Security Professional Should Know**

<table>
<thead>
<tr>
<th>Essentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>KCS40 ICS Security Essentials</td>
</tr>
<tr>
<td>KCS50 ICS Security &amp; Incident Response</td>
</tr>
<tr>
<td>KCS30 ICS Advanced Security</td>
</tr>
<tr>
<td>NERC Protection</td>
</tr>
<tr>
<td>NERC Security Essentials</td>
</tr>
</tbody>
</table>

**DevSecOps**

**Every Developer Should Know**

<table>
<thead>
<tr>
<th>Secure Web-Apps</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOR953 Defending Web Applications Security Essentials</td>
</tr>
<tr>
<td>Secure DevOps: SEC440 Cloud Security and DevOps Automation</td>
</tr>
</tbody>
</table>

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

To learn more about SANS courses, go to sans.org/courses

65+ hands-on courses
Extend and Validate Your Training

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

Extend Your Training Experience with an OnDemand Bundle

• Four months of supplemental online review
• 24/7 online access to your course lectures, materials, quizzes, and labs
• Subject-matter-expert support to help you increase your retention of course material

OnDemand Bundle price – $799

Get Certified with GIAC Certifications

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

GIAC bundle price – $799

“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

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

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

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

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

SANS live training events provide you with:

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

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

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

Visit sans.org/live-training to view the 2020 live training calendar and register for your courses.
SEC301: Introduction to Cyber Security

You Will Be Able To

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

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

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

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

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

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

“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 an 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, GCID, GCED, GISF, CEH, Security+, Network+, A+, CTT+).

Keith Palmgren is an IT security professional with over 30 years of experience specializing in the field. He began his career with the U.S. Air Force working with cryptographic keys and codes management. He also worked in what was at the time the newly-formed Air Force computer security department. Following the Air Force, Keith worked as an MIS director for a small company before joining AT&T/Lucent as a Senior Security Architect working on engagements with the 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, GCID, GCED, GISF, CEH, Security+, Network+, A+, CTT+).

Keith Palmgren
SANS Senior Instructor

Keith Palmgren is an IT security professional with over 30 years of experience specializing in the field. He began his career with the U.S. Air Force working with cryptographic keys and codes management. He also worked in what was at the time the newly-formed Air Force computer security department. Following the Air Force, Keith worked as an MIS director for a small company before joining AT&T/Lucent as a Senior Security Architect working on engagements with the 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, GCID, GCED, GISF, 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 explain networking starting in non-technical terms and gradually progress to more technical detail as students are ready to take the next step. By the end of our discussions, you’ll have a fundamental grasp of any number of critical technical networking acronyms that you’ve often heard but never quite understood, including TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS.

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

DAY 4: Cyber Security Technologies – Part 1
Our fourth day in the classroom begins our exploration of cybersecurity technologies. We begin with wireless network security (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
You Will Be Able To

- 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, GCLA, 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.

@BryanOnSecurity
**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 following days of training.


**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 as they likely should, many of the more 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 sans.org/security-west/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 a real, fully-integrated toolset that includes:

- 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.

**Author Statement**

“As someone who has held every position from entry-level analyst to SOC manager at a 100,000-employee company, I thoroughly understand the struggle of starting your first position in cyber defense. While there is a seemingly infinite amount of information to learn, there are certain central concepts that, when explained systematically, can greatly shorten the time required to become a productive member of the team. This course was written to pass this knowledge on to you, giving you both the high- and low-level concepts required to propel your career in cyber defense. It’s packed with the concepts that I expected new employees to understand, as well as the thought process we tried to cultivate throughout analysts’ careers to ensure the success of the individual and the organization. I have also worked hard to distill the lessons I’ve learned through the years on staying excited and engaged in cyber defense work. While some believe SOC positions can feel like a grind, they do not need to be that way! This course goes beyond technical knowledge to also teach the concepts that, if implemented in your SOC, will keep you and your colleagues challenged, happy, and constantly growing in your day-to-day work, leading to a successful, life-long career on the blue team!”

— John Hubbard
Course Day Descriptions

**DAY 1: Blue Team Tools and Operations**
This day starts with an introduction to the blue team, the mission of a Security Operations Center (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 day 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, HTTP(S), 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: Understanding Endpoints, 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 a survey 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 day 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 and how they are often weaponized, and how to quickly decide whether or not 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; File 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 analyst 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 how to halt a developing 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.

**Who Should Attend**
- Security analysts
- Incident investigators
- Security engineers and architects
- Technical security managers
- SOC managers looking to gain additional technical perspective on how to improve analysis quality, reduce turnover, and run an efficient SOC
- Anyone looking to start their career on the blue team

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/security-west/courses
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
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 setting levels and ensuring that all students understand the background behind what we do in the OSINT field. We also establish the foundation for the rest of the week by learning how to document findings and set up an OSINT platform, and we discuss effective research habits for OSINT analysts. This day is a key component for the success of an OSINT analyst because without these concepts and processes in place, researchers can get themselves into serious trouble during assessments by inadvertently alerting their targets or improperly collecting data, making it less useful when delivered to the customer.
Topics: Understanding OSINT; Goals of OSINT Collection; Diving into Collecting; Taking Excellent Notes; Determining Your Threat Profile; Setting Up an OSINT Platform; Effective Research Habits; Creating Sock Puppets

DAY 2: Gathering, Searching, and Analyzing OSINT
OSINT data collection begins on day two after we get a glimpse of some of the fallacies that could influence our conclusions and recommendations. From this point in the class forward, we examine distinct categories of data and think about what 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 this course sets up the student with a whole range of OSINT tools that are essential for investigation!”
— Selvi Krishnan, Blue Voyant
Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad reputational damage. SEC501: Advanced Security Essentials – Enterprise Defender builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

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

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

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

**You Will Be Able To**

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

**Who Should Attend**

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

**“Immediate value of putting concepts into standard practice.”**

— Manny Cadiz, EMF Broadcasting

**“If you want to take a deep-dive into enterprise security, then you must take SEC501.”**

— Nikolai Vinogradov, JSC Severstal Management

Shane Harsch is an information security professional with over 25 years of experience ranging from military to manufacturing and security consulting and professional services. He has managed and architected SOCs for the military and managed service providers. Shane is a commissioned officer in the U.S. Army with a master’s degree in business. He holds the intrusion analyst (GCIA), incident handling (GCIH), enterprise defense (GCED), and CISSP® certifications. Shane is currently a Senior Solution Success Manager with RSA. His soft skills are founded in theater, music, and foreign languages, all cultivated while living in Germany. Additionally, Shane spent 12 years in the U.S. Army, receiving a commission and attaining the rank of Chief Warrant Officer, experience that has served him well as a leader, mentor, and team member. Shane enjoys skiing, fiction of all kinds, and is an active designer and writer in the tabletop gaming industry.
**Course Day Descriptions**

**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 and analyze 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 dissemble a live Ransomware specimen from static analysis through code analysis. You will get hands-on experience with tricking the malware through behavioral analysis techniques, as well as decrypting files encrypted by Ransomware by extracting the keys through reverse engineering. All steps are well defined and tested to ensure that the process to achieve these goals is actionable and digestible.

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

**DAY 6: Enterprise Defender Capstone**
The concluding section of the course will serve as a real-world challenge for students by requiring them to work in teams, use the skills they have learned throughout the course, think outside the box, and solve a range of problems from simple to complex. A web server scoring system and Capture-the-Flag 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.

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/security-west/courses
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
- Comprehend the need to employ network forensics to investigate traffic to identify and investigate a possible intrusion
- Use open-source traffic analysis tools to identify signs of an 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.

“The course has equipped me with super powers. I can see everything! I don’t know how I was able to do my job without this knowledge. This course is a must for any cyber defense analyst.”

— Joe Morrissey, Nationwide

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

"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

"SEC504 is the essential cert course needed to trust if a candidate is valuable enough to do incident response."
— Troy Merritt, Blueshield of CA

Jon is the founder of and Principle Consultant for Fundamental Security, a small consulting firm focused on penetration testing, incident response, and strategic security. He has worked in information technology since 2004, and has focused on information security since 2006. Most recently, he was the application security testing manager for a Fortune 500 financial institution, and a security architect and penetration tester for a Fortune 500 retailer. In all, he has performed security engineering, security architecture, incident response, and penetration testing in the government, retail, and financial sectors. Passionate about security and leadership, Jon loves trying to ignite those passions in other people. Jon is proud to have served in the Army Reserve for 11 years, where he became a Warrant Officer and served one tour in Afghanistan. He currently maintains the GCIH, GPEN, GAWN, GMOB, CISSP®, and Security+. 
@flakpaket
Course Day Descriptions

**DAY 1: Incident Handling Step-by-Step and Computer Crime Investigation**

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

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

**DAY 2: Computer and Network Hacker Exploits – Part 1**

Seemingly innocent 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 disguising 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 how to use PowerShell to automate Windows security management across an Active Directory enterprise.

**DON’T JUST LEARN POWERSHELL SYNTAX, LEARN HOW TO LEVERAGE POWERSHELL AS A PLATFORM FOR SECURITY**

You’ve run a vulnerability scanner and applied patches – now what? 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. We need to prevent pass-the-hash attacks and Kerberos Golden Ticket attacks as much as possible, not just detect them.

Perhaps you’ve taken a hacking course at SANS and you now want to learn more Windows and Active Directory attack mitigations: SEC505 is that course.

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 free in GitHub (just go to http://SEC505.com).

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 security, it can save money too.

SEC505 IS DESIGNED FOR THE BLUE TEAM TO BLOCK THE ATTACKS OF THE RED TEAM.

The focus of this course is on how to automate the NSA Top 10 Mitigations, the CIS Critical Security Controls related to Windows, and the MITRE ATT&CK mitigations for Windows, especially the ones that are the 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 attendees, we will examine 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!

**You Will Be Able To**

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

Jason Fossen
SANS Faculty Fellow
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: Why is PowerShell So Important and Dangerous?, Writing Your Own Scripts, Functions, and Modules, PowerShell Remoting, Getting Up and Running Quickly with PowerShell

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, Remote PowerShell Script Execution with Group Policy, Server Hardening Automation, PowerShell for Active Directory

DAY 3: Smart Tokens and Public Key Infrastructure
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: How to Install a Windows PKI, How to Manage Your PKI, Deploying MFA Smart Tokens, Smart Cards, and TPMS

DAY 4: Protecting Admin Credentials and PowerShell Just Enough Admin
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, including Microsoft’s Windows Admin Center browser-based administrative web application.

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

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

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

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

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

Maxim Deweerdt likes to stick to the basics and think out of the box – which has helped secure whatever environment he has been working in throughout his career. He is a well-respected cybersecurity advisor, whose focus is on incident response and threat hunting. He has a deep technical understanding of the challenges defenders face and has the experience to translate these challenges into a no-nonsense security program. When Maxim is not busy leading an incident response and threat hunting team in the Middle East and North Africa region, he teaches the SEC511: Continuous Monitoring and Security Operations, which also happens to be his favorite course. Maxim will immerse you into the true mindset of the defender using the excellent course material combined with numerous anecdotes and tips drawn from his work with governments and the financial, oil-and-gas and defense industries.

@AlfaSec
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 Principles/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 detection 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 detection 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 detection 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 know when our systems, networks, and applications are at an increased likelihood for compromise. A strong way to achieve this is through Continuous Security Monitoring (CSM) or Continuous Diagnostics and Mitigation (CDM). Rather than waiting for the results of a quarterly scan or an annual penetration test to determine what needs to be addressed, continuous monitoring proactively and repeatedly assesses and reassesses the current security posture for potential weaknesses that need to be addressed.

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

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

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

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

“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 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 to aid in building a robust security infrastructure.

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

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

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

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

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

— Merv Hammer, Workday Inc.

“**SEC530 provided an excellent understanding of application attacks and how to protect against them.”**

— Shayne Douglass, AMEWAS Inc.

Ryan Nicholson
SANS Instructor

Ryan’s passion with information technology started in 2001 when he found himself constantly trying to make his high school’s computers and even calculators do things that they weren’t exactly intended to do. They lacked games, so he changed that by learning how to create some. Yes, some may call this hacking. Ryan called it “fun,” which led to attending college with intentions of becoming a software engineer. Ryan started working as a system administrator for the U.S. Department of Defense and quickly took on a more security-focused role as a field office network security officer. It didn’t stop there. After addressing the security and compliance needs of the small field office, Ryan took his knowledge on the road and became what most organizations dread – a cybersecurity lead auditor. He then moved on from government service to address the larger issue at hand – security awareness – by creating and teaching cybersecurity-focused courses for the DoD’s system administrators and analysts. Throughout these years, Ryan has picked up a number of industry certifications and is constantly trying to expand his technical and cybersecurity expertise. His certifications include GIAC’s GSLC and GSEC, Offensive Security’s OSCP, ISC2’s CISSP®, EC Council’s CEH and CFHI, the AWS Certified Solutions Architect Associate.

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

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

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

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

| **DAY 3: Network-Centric Security** |
| 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 mechanisms that an organization already owns with a modern mindset. By thinking outside the box, even old controls like a spam appliance can be used to catch modern attacks such as phishing via cousin domains and other spoofing techniques. And again, by engineering defenses for modern attacks, both prevention and detection capabilities gain significantly.

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

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

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

| **DAY 5: Zero-Trust Architecture: Addressing the Adversaries Already in Our Networks** |
| Today, a common security mantra is “trust but verify.” But this is a broken concept. Computers are capable of calculating trust on the fly, so rather than thinking in terms of “trust but verify” organizations should be implementing “verify then trust.” By doing so, access can be constrained to appropriate levels at the same time that access can become more fluid. This section focuses on implementing a zero-trust architecture where trust is no longer implied but must be proven. By doing so, a model of variable trust 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.

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

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

**Topics:** Capstone – Design/Detect/Defend
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

Kenneth G. Hartman
SANS Certified Instructor

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.

“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

Kenneth G. Hartman is a security engineering leader in Silicon Valley. Ken’s motto is “I help my company earn and maintain the trust of our customers in our products and services.” Toward this end, Ken drives a comprehensive program portfolio of technical security initiatives focused on securing customers’ data in the AWS Cloud. Ken has worked for a variety of cloud service providers in architecture, engineering, compliance, and security product management roles. From 2002-2011, Ken helped launch and lead a company called Visonex into a profitable, nation-wide dialysis-specific electronic medical record using a software-as-a-service (SaaS) business model. Ken holds a BS in electrical engineering from Michigan Technological University and a masters degree in information security engineering from SANS Technology Institute. Ken has earned the CISSP®, as well as multiple GIAC security certifications, including the GIAC Security Expert. Ken is also a Licensed PI in Michigan as required by law to consult on criminal cases involving digital forensics. @KennethGHartman

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

Topics: Introduction to the Cloud and Cloud Security Basics; Cloud Security Alliance Guidance; Cloud Policy and Planning; SaaS Security; Cloud Access Security Brokers; Intro to PaaS and IaaS Security Controls

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

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 and network security. We delve into these in significant depth, as they can form the backbone of a sound cloud security strategy. We then look at architecture and design for data security, touching on encryption technologies, key management, and what the different options are today. We wrap up our third day with another crucial topic: availability. Redundant and available design is as important as ever, but we need to use cloud provider tools and geography to our advantage. At the same time, we need to make sure we evaluate the cloud provider’s disaster recovery and continuity, and so this is covered as well.

Topics: Cloud Security Architecture Overview; Cloud Architecture and Security Principles; Infrastructure and Core Component Security; Access Controls and Compartmentalization; Confidentiality and Data Protection; Availability

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

Topics: Threats to Cloud Computing; Vulnerability Management in the Cloud; Cloud Pen Testing; Intrusion Detection in the Cloud; Cloud IR and Event Management; Cloud Forensics

DAY 5: Cloud Security Automation and Orchestration
On our final day, we’ll focus explicitly on how to automate security in the cloud, both with and without scripting techniques. We will use tools like the AWS CLI and AWS Lambda to illustrate the premises of automation, then turn our attention toward SecDevOps principles. We begin by explaining what that really means, and how security teams can best integrate into DevOps and cloud development and deployment practices. We’ll cover automation and orchestration tools like Ansible and Chef, as well as how we can develop better and more efficient workflows with AWS CloudFormation and other tools. Continuing some of the topics from day four, we will look at event-driven detection and event management, as well as response and defense strategies that work. While we won’t automate everything, some actions and scenarios really lend themselves to monitoring tools like CloudWatch, tagging assets for identification in security processes, and initiating automated response and remediation to varying degrees. We wrap up the class with a few more tools and tactics, followed by a sampling of real-world use cases.

Topics: Scripting and Automation in the Cloud; SecDevOps Principles; Creating Secure Cloud Workflows; Building Automated Event Management; Building Automated Defensive Strategies; Tools and Tactics; Real-World Use Cases; Class Wrap-Up
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.

James Tarala is a principal consultant with Enclave Security and is based in Venice, Florida. He is a regular speaker for the SANS Institute as well as a courseware author and editor for many SANS auditing and security courses. As a consultant, he has spent the past few years developing large enterprise IT security and infrastructure architectures, specifically working with many Microsoft-based directory services, e-mail, terminal services, and wireless technologies. He has also spent a large amount of time consulting with organizations to assist them with their security management, operational practices, and regulatory compliance issues, and he often performs independent security audits and assists internal audit groups in developing their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University and his graduate work at the University of Maryland. He holds numerous professional certifications.

@isaudit
Course Day Descriptions

**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 [sans.org/security-west/courses](http://sans.org/security-west/courses)
SEC599: **Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses**

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

Cyber threats are on the rise: ransomware tactics are affecting small, mid-size, 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 “SYNCTECHLABS” in section one exercises.

In sections two through 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 on the final course day, you will be pitted against advanced adversaries in an attempt to keep your network secure. Can you protect the environment against the different waves of attacks? The adversaries aren’t slowing down, so what are you waiting for?

**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

**Topics To Be Addressed**
- Leverage 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 script controls (unmanaged Powershell, AMSI bypasses, etc.)
- Stopping 0-day exploits using ExploitGuard and application whitelisting
- Highlighting key bypass strategies in application whitelisting (focus on AppLocker)
- 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

James Shewmaker
SANS Certified Instructor

James Shewmaker is the founder and principal consultant at Bluenotch Corporation in Long Beach, California, which provides customized security services focusing on investigations, penetration testing and analysis. James authored and maintains the post-exploitation content in the SANS Security 660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking course. Before becoming a SANS Certified Instructor in 2009, his creative technical work led him on many adventures, including “The Great Translator Invasion of 2003.” James led the development and operations for NetWars as a U.S. Cyber Challenge game in June 2009. He is currently developing an independent cyber challenge, Bunker011, and is involved in the U.S. Cyber Challenge as an instructor at Cyber Camps. James regularly teaches a Tactical Offense and Defense day at these events.

@jimshew

---

**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

**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 script controls (unmanaged Powershell, AMSI bypasses, etc.)
- Stopping 0-day exploits using ExploitGuard and application whitelisting
- Highlighting key bypass strategies in application whitelisting (focus on AppLocker)
- 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

James Shewmaker
SANS Certified Instructor

James Shewmaker is the founder and principal consultant at Bluenotch Corporation in Long Beach, California, which provides customized security services focusing on investigations, penetration testing and analysis. James authored and maintains the post-exploitation content in the SANS Security 660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking course. Before becoming a SANS Certified Instructor in 2009, his creative technical work led him on many adventures, including “The Great Translator Invasion of 2003.” James led the development and operations for NetWars as a U.S. Cyber Challenge game in June 2009. He is currently developing an independent cyber challenge, Bunker011, and is involved in the U.S. Cyber Challenge as an instructor at Cyber Camps. James regularly teaches a Tactical Offense and Defense day at these events.

@jimshew

---

**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

**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 script controls (unmanaged Powershell, AMSI bypasses, etc.)
- Stopping 0-day exploits using ExploitGuard and application whitelisting
- Highlighting key bypass strategies in application whitelisting (focus on AppLocker)
- 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

James Shewmaker
SANS Certified Instructor

James Shewmaker is the founder and principal consultant at Bluenotch Corporation in Long Beach, California, which provides customized security services focusing on investigations, penetration testing and analysis. James authored and maintains the post-exploitation content in the SANS Security 660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking course. Before becoming a SANS Certified Instructor in 2009, his creative technical work led him on many adventures, including “The Great Translator Invasion of 2003.” James led the development and operations for NetWars as a U.S. Cyber Challenge game in June 2009. He is currently developing an independent cyber challenge, Bunker011, and is involved in the U.S. Cyber Challenge as an instructor at Cyber Camps. James regularly teaches a Tactical Offense and Defense day at these events.

@jimshew

---

**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

**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 script controls (unmanaged Powershell, AMSI bypasses, etc.)
- Stopping 0-day exploits using ExploitGuard and application whitelisting
- Highlighting key bypass strategies in application whitelisting (focus on AppLocker)
- 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

James Shewmaker
SANS Certified Instructor

James Shewmaker is the founder and principal consultant at Bluenotch Corporation in Long Beach, California, which provides customized security services focusing on investigations, penetration testing and analysis. James authored and maintains the post-exploitation content in the SANS Security 660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking course. Before becoming a SANS Certified Instructor in 2009, his creative technical work led him on many adventures, including “The Great Translator Invasion of 2003.” James led the development and operations for NetWars as a U.S. Cyber Challenge game in June 2009. He is currently developing an independent cyber challenge, Bunker011, and is involved in the U.S. Cyber Challenge as an instructor at Cyber Camps. James regularly teaches a Tactical Offense and Defense day at these events.

@jimshew
Course Day Descriptions

**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 OSHunt. Finally, we will illustrate how control 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, DAC 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 five 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 day 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 résumé more appealing to recruiters.”

— Kim Ngoc, GuardSight, Inc.
Choose from:
• Core NetWars
• Cyber Defense NetWars
• DFIR NetWars

Develop skills in:
• Cyber Defense
• Digital Forensics & Incident Response
• Malware Analysis
• Packet Analysis
• 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 solo or on a team of up to 5 players.
• Experience NetWars for free when taking a 5- or 6-day course.
• 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

“SANS NetWars should be a course requirement. Nothing instills the knowledge and skills from the classroom like it!”
— Frank DePaola, EnPro Industries

“Great experience. Fantastic learning.”
— Shenshen Zhao, Verizon

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

sans.org/netwars
SEC460: Enterprise Threat and Vulnerability Assessment

You Will Be Able To

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

Matthew Toussain
SANS Certified Instructor

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

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

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

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

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

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

— Eric Osmus, ConocoPhillips Company

Matthew Toussain is the founder of Open Security and a penetration tester with Black Hills Information Security. As an avid information security researcher, Matthew regularly hunts for vulnerabilities in computer systems and releases tools to demonstrate the effectiveness of attacks and countermeasures. He has been a guest speaker at many conference venues, including DEFCON, the largest security conference in the world. Matthew is an author of SEC460: Enterprise Threat and Vulnerability Assessment. After graduating from the U.S. Air Force Academy, where he architected and instructed the summer cyber course that now trains over 400 cadets per year, Matthew served as the Senior Cyber Tactics Development Lead for the U.S. Air Force. He led 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

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. This focus will direct us to the quantitative facets underlying cybersecurity vulnerabilities and drive our discussion of impact, risk, and triage. Each topic discussed will focus on identifying, observing, inciting, or assessing the entry points that threats leverage during network attacks. Later in the day, we will apply our understanding of the vulnerability concept to evolve our PowerShell skills and take action on an enterprise scale.

Topics: Enhanced Vulnerability Scanning: Risk Assessment Matrices and Rating Systems; Quantitative Analysis Techniques Applied to Vulnerability Scoring; Performing Tailored Risk Calculation to Drive Triage; General Purpose vs. Application Specific Vulnerability Scanning; Tuning the Scanner to the Task, the Enterprise, and Tremendous Scale; Scan Policies and Compliance Auditing; Performing Vulnerability Discovery with Open-Source and Commercial Appliances; Nmap Scripting Engine and OpenVAS; Testing for Insecure Cryptographic Implementations Including SSL; Assessing 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

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

Topics: 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 jealous nation-state actors. Teams will work together to help squash issues that would lead to a compromise of The Foundry’s precious assets.

Topics: Tactical Employment of the Vulnerability Assessment Framework; Threat Modeling; Discovery; Vulnerability Scanning; Validation, Data Management and Triage

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

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/security-west/courses
SEC542: Web App Penetration Testing and Ethical Hacking

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

Eric Conrad
SANS Faculty Fellow

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.

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, GCIA, GCFA, GAWN, and GSEC certifications. Eric also blogs about information security at ericconrad.com.

@eric_conrad
**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 Servers and Clients; Discussion of the Various Web Architectures; Discovering How Session State Works; Discussion of the Different Types of Vulnerabilities; WHOIS and DNS Reconnaissance; 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 our target application, and building a profile of each server, including the operating system, specific software and configuration. The discussion is underscored through several practical, hands-on labs in which we conduct reconnaissance against in-class targets.

**Topics:** 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; MultiIdaes; 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.

---

**“Knowing everything from the Internet is not enough. This class has a sequential structure to understand the basics of pen testing.”**
— Vinita Mhapsekar, Kaiser Permanente
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.

### Tim Medin

**SANS Principal 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 tools 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 on the final day 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

---

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

@timmedin
DAY 1: Comprehensive Pen Test Planning, Scoping, and Recon
In this course section, you’ll develop the skills needed to conduct a best-of-breed, high-value penetration test. We’ll go in-depth on how to build a penetration testing infrastructure that includes all the hardware, software, network infrastructure, and tools you will need to conduct great penetration tests, with specific low-cost recommendations for your arsenal. We’ll then cover formulating a pen test scope and rules of engagement that will set you up for success, including a role-play exercise. We’ll also dig deep into the reconnaissance portion of a penetration test, covering the latest tools and techniques, including hands-on document metadata analysis to pull sensitive information about a target environment, as well as a lab using Recon-ng to plunder a target’s DNS infrastructure for information such as which anti-virus tools the target organization uses.

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

DAY 2: In-Depth Scanning
This course section focuses on the vital task of mapping the target environment’s attack surface by creating a comprehensive inventory of machines, accounts, and potential vulnerabilities. We look at some of the most useful scanning tools freely available today and run them in numerous hands-on labs to help hammer home the most effective way to use each tool. We also conduct a deep dive into some of the most useful tools available to pen testers today for formulating packets: Scapy and Netcat. We finish the module covering vital techniques for false-positive reduction, so you can focus your findings on meaningful results and avoid the sting of a false positive. And we examine the best ways to conduct your scans safely and efficiently.

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

DAY 3: Exploitation
In this section, we look at the many kinds of exploits that penetration testers use to compromise target machines, including client-side exploits, service-side exploits, and local privilege escalation. We’ll see how these exploits are packaged in frameworks like Metasploit and its mighty Meterpreter. You’ll learn in-depth how to leverage Metasploit and the Meterpreter to compromise target environments. We’ll also analyze the topic of anti-virus evasion to bypass the target organization’s security measures, as well as methods for pivoting through target environments, all with a focus on determining the true business risk of the target organization.

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

DAY 4: Password Attacks 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 msconsole route command.

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

DAY 5: In-Depth Password Attacks and Web App Pen Testing
In this course section, we’ll go even deeper in exploiting one of the weakest aspects of most computing environments: passwords. You’ll custom-compile John the Ripper to optimize its performance in cracking passwords. You’ll look at the amazingly full-featured Cain tool, running it to crack sniffed Windows authentication messages. We’ll use the incredible Hashcat tool for increased speed in cracking passwords, all hands-on. And we’ll cover powerful “pass-the-hash” attacks, leveraging Metasploit, the Meterpreter, and more. We then turn our attention to web application pen testing, covering the most powerful and common web app attack techniques, with hands-on labs for every topic we address. We’ll cover finding and exploiting cross-site scripting (XSS), cross-site request forgery (XSRF), command injection, and SQL injection flaws in applications such as online banking, blog sites, and more.

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

DAY 6: Penetration Test and Capture-the-Flag Challenge
This lively session represents the culmination of the network penetration testing and ethical hacking course. You’ll apply all of the skills mastered in the course in a comprehensive, hands-on workshop during which you’ll conduct an actual penetration test of a sample target environment. We’ll provide the scope and rules of engagement, and you’ll work to achieve your goal of finding out whether the target organization’s Personally Identifiable Information (PII) is at risk. As a final step in preparing you for conducting penetration tests, you’ll make recommendations about remediating the risks you identify.

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

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

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/security-west/courses

43
SEC573: Automating Information Security with Python

6 Day Program | 36 CPEs | Laptop Required

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

Mark Baggett
SANS Senior Instructor
**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 experts 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

“Excellent class for learning how to construct automated and advanced discovery analytics for information systems.”
— Mary Gutierrez, Booz Allen Hamilton

“**SEC573 is excellent. I went from having almost no Python coding ability to being able to write functional and useful programs.**”
— Caleb Jaren, Microsoft
Imagine an attack surface that is spread across your organization and in the hands of every user. It moves from place to place regularly, stores highly sensitive and critical data, and sports numerous different wireless technologies all ripe for attack. Such a surface already exists today; mobile devices. These devices are the biggest attack surface in most organizations, yet these same organizations often don’t have the skills needed to assess them.

SEC575 NOW COVERS ANDROID PIE and iOS 12

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

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

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

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

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

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

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

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

Chris Crowley has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area focusing on effective computer network defense. His work experience includes penetration testing, security operations, incident response, and forensic analysis. He holds the GSEC, GCIA, GCIH (gold), GCFI, GPE, GMP, GASF, GREM, GXP, and CISSP® certifications. His teaching experience includes FOR585, SEC401, SEC503, SEC504, SEC560, SEC575, and SEC580; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor of the year award which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities. Chris spends his spare time mountain biking, rock climbing, and savoring epicurean treats.

@_s16
Day 1: Device Architecture and Common Mobile Threats

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

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

Day 2: Mobile Platform Access and Application Analysis

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

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

Who Should Attend

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

“SEC575 provides an incredible amount of information, and the hands-on labs are awesome. It is a must-have for mobile penetration testers.” — Richard Takacs, Integrity360

Day 3: Mobile Application Reverse Engineering

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

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

Day 4: Penetration Testing Mobile Devices – Part 1

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

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

Day 5: Penetration Testing Mobile Devices – Part 2

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

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

Day 6: Hands-on Capture-the-Flag Event

In the final module of SEC575 we will pull together all the concepts and technology covered during the week in a comprehensive Capture-the-Flag event. In this hands-on exercise, you will have the option to participate in multiple roles, including designing a secure infrastructure for the deployment of mobile phones, monitoring network activity to identify attacks against mobile devices, extracting sensitive data from a compromised iPad, and attacking a variety of mobile phones and related network infrastructure components. During this mobile security event you will put into practice the skills you have learned in order to evaluate systems and defend against attackers, simulating the realistic environment you will be prepared to protect when you get back to the office.
This course is designed for professionals seeking a comprehensive technical ability to understand, analyze, and defend the various wireless technologies that have become ubiquitous in our environments and, increasingly, key entrance points for attackers.

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

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

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

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

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

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

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

Joshua Wright is a senior technical analyst with Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through his experiences as a penetration tester, Josh has worked with hundreds of organizations on attacking and defending mobile devices and wireless systems, ethically disclosing significant product and protocol security weaknesses to well-known organizations. As an open-source software advocate, Josh has conducted cutting-edge research resulting in several software tools that are commonly used to evaluate the security of widely deployed technology targeting WiFi, Bluetooth, and ZigBee wireless systems, smart grid deployments, and the Android and Apple iOS mobile device platforms. As the technical lead of the innovative CyberCity, Josh also oversees and manages the development of critical training and educational missions for cyber warriors in the U.S. military, government agencies, and critical infrastructure providers. @josw1ght
DAY 1: WiFi Data Collection and Analysis
The first section of the course quickly looks at wireless threats and attack surfaces and analyzes where you will likely see non-WiFi systems deployed in modern networks. We start off with a look at fundamental analysis techniques for evaluating WiFi networks, including the identification and analysis of rogue devices, and finish with a dive into remote penetration testing techniques using compromised Windows 10 and macOS devices to pivot.
Topics: Characterize the Wireless Threat; Sniffing WiFi; Rogue Access Point (AP) Analysis

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

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

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

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

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

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/security-west/courses

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

“SEC617 is great for someone looking for a top-to-bottom rundown in wireless attacks.” — Garret Picchioni, Salesforce
THE CLOCK IS TICKING. YOU NEED TO PRIORITIZE THE MOST VALUABLE EVIDENCE FOR PROCESSING. LET US SHOW YOU HOW.

The FOR498: Battlefield Forensics & Data Acquisition course will help you to:

- Acquire data effectively from:
  - PCs, Microsoft Surface, and Tablet PCs
  - Apple Devices, Mac, and Macbooks
  - RAM and Memory
  - Smartphones and portable mobile devices
  - Cloud storage and services
  - Network storage repositories

- Produce actionable intelligence in 90 minutes or less

The first step in any investigation is the gathering of evidence. Digital forensic investigations are no different. The evidence used in this type of investigation is data, and these data can live in many varied formats and locations. You must be able to first identify the data that you might need, determine where those data reside, and, finally, formulate a plan and procedures for collecting those data. With digital forensic acquisitions, you will typically have only one chance to collect data properly. If you manage the acquisition incorrectly, you run the risk of not only damaging the investigation, but more importantly, destroying the very data that could have been used as evidence.

With the wide range of storage media in the marketplace today, any kind of standardized methodology for all media is simply untenable. Many mistakes are being made in digital evidence collection, and this can cause the guilty to go free and, more importantly, the innocent to be incarcerated. The disposition of millions and millions of dollars can rest within the bits and bytes that you are tasked with properly collecting and interpreting. An examiner can no longer rely on “dead box” imaging of a single hard drive. In today’s cyber sphere, many people utilize a desktop, laptop, tablet, and cellular phone within the course of a normal day. Compounding this issue is the expanding use of cloud storage and providers, and the proper collection of data from all these domains can become quite overwhelming.

This in-depth digital acquisition and data handling course will provide first responders and investigators alike with the advanced skills necessary to properly identify, collect, respond to, and preserve data from a wide range of storage devices and repositories, ensuring that the integrity of the evidence is beyond reproach. Constantly updated, FOR498 addresses today’s need for widespread knowledge and understanding of the challenges and techniques that investigators require when addressing real-world cases.

Numerous hands-on labs throughout the course will give first responders, investigators, and digital forensics teams the practical experience needed when performing digital acquisition from hard drives, memory sticks, cellular phones, network storage areas, and everything in between. During a digital forensics response and investigation, an organization needs the most skilled responders possible, lest the investigation end before it has begun.
Course Day Descriptions

**DAY 1: Evidence File Quick Wins and Dealing with Smartphones**

Investigators will often be responding to high-stress environments where many different entities are critically scrutinizing the collection scene. Personnel need to be properly trained and equipped to work in less than optimal surroundings, and be confident that they have managed the scene, identified all necessary data, collected the data in a properly defensible manner, and maintained its integrity. One of the most common scenarios that can cause headaches is receiving an evidence file (usually an E01), and being expected to provide answers immediately. The common approach is to mount the image and then start running carving and other tools against it. These automated tasks can take many hours (and sometimes days) just by themselves! Portable devices bring their own set of challenges. We will acquire memory and image the device, but we may also be faced with non-functioning media. Learn about the inner workings of hard drives, and how to revive them to a point where you can then create your forensic image. We will also be looking at the “best of breed” data recovery tools, from those that are free to those that cost many thousands of dollars.

**DAY 2: Evidence Acquisition and Collection**

Investigators and first responders should be armed with the latest tools, digital container access techniques, and, enterprise methodologies to identify, access, and preserve evidence across a vast range of devices and repositories. Personnel must also be able to scale their identification and collection across thousands of systems in your environment. This course will make you more efficient and effective at finding the right tool, and get at those data as fast as possible. An effective battlefield forensicator needs to be extracting data, and quicker to do it directly from the storage itself. But what happens with devices such as iPads, iPhones, and other devices that are not physically designed to be imaged? The usefulness of file and stream carving cannot be overstated. The Deeper Dive

**DAY 3: Quick Win Forensics**

Given that 99% of the necessary evidence typically exists in 1-2% of the data acquired, it is easy to see how a great deal of time can be wasted following the normal procedures in today’s digital forensics world. Instead, let’s focus on this 1-2% and perform a very rapid triage collection that can be used to start our investigation sooner. Far too often, computers are seized in an “on” state, and immediately powered down because “that is how we’ve always done it.” With today’s computers this means you are throwing away (essentially destroying) many gigabytes of data. The RAM in a computer holds an incredibly important treasure trove of data, from keystrokes to network connections, running services, and, quite importantly, passwords and decryption keys. With the vastly increasing spread of file-less malware, in many cases the only place that evidence will exist is in memory. Another often-overlooked factor is full disk encryption. In cases like this, “live” acquisition will be your only hope.

**DAY 4: Non-Traditional and Cloud Acquisition**

When we think about acquisition, it usually involves opening the side of the computer, removing the hard drive, connecting to a write blocker or imaging equipment, and completing the task. While this is not an inaccurate assessment, it does not address a great deal of the access and acquisition questions surrounding so much data today. If full disk imaging is necessary, then it is certainly easier and quicker to do it directly from the storage itself. But what happens with devices such as iPads, iPhones, and other such equipment, where it is glue and not screws that hold them together? Volume Shadow Copies also contain a wealth of historic data that are of great use to investigators. Knowing how to access and collect data from these shadow copies is critical in cases involving the Windows operating system. Battlefield forensics is considered the bleeding edge of digital forensics. It requires in-depth knowledge of where the most valuable data reside on the computer and how to get to that data as fast as possible. An effective battlefield forensicator needs to be extracting actionable intelligence in 90 minutes or less, but the clock does not start when the forensic imaging is done. Rather, it starts from the moment you lay your hands on the device. Learn how to identify and access data in non-traditional storage areas. In today's world so much data live off site, and there are very few methods in place to access and properly acquire those data. In this section, we will identify these locations, including SharePoint, Exchange, webmail, network locations, cloud storage, and social media, not to mention Dropbox, Google Drive, and the Internet of Things. This also includes RAID storage and how to best collect these devices regardless of configuration.

**DAY 5: Apple Acquisition, Internet of Things, and Online Attribution**

There are very few tools and techniques available when it comes to acquisition of Apple products, as compared to Windows. The tools that exist can be quite expensive, and free tools are simply few and far between. In this section, we will explore the fundamentals of acquiring data from the devices, not only iPhones and iPads, but also MacBooks and Macs. We will discuss how to acquire memory and image the device, but we may also be faced with non-functioning media. Learn about the inner workings of hard drives, and what you can (and cannot) do to do what you can (and cannot) do to revive them to a point where you can then create your forensic image. We will also be looking at the “best of breed” data recovery tools, from those that are free to those that cost many thousands of dollars.

**DAY 6: Beyond the Forensic Tools: The Deeper Dive**

The usefulness of file and stream carving cannot be overstated. Some data simply do not live in the defined file space that can be readily accessed by a viewer. From partially overwritten to deleted data, we will explore techniques you can employ when traditional tools fail. Data carving is a skill that is increasingly important. Once the reference to a file is destroyed, how can the data still be recovered? File carving tools will assist in this, but examiners must understand the limitations of their tools. Without the proper pieces of the original file, a carver is useless. At some point, you will be faced with non-functioning media. Learn about the inner workings of hard drives, and what you can (and cannot) do to do what you can (and cannot) do to revive them to a point where you can then create your forensic image. We will also be looking at the “best of breed” data recovery tools, from those that are free to those that cost many thousands of dollars.

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/security-west/courses

51
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

### REQUIREMENTS
- 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, geolocation, file download, anti-forensics, and detailed system usage
  - Focus your capabilities on analysis instead of on how to use a particular tool
  - Extract critical answers and build an in-house forensic capability via a variety of free, open-source, and commercial tools provided within the SANS Windows SIFT Workstation

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

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

Proper analysis requires real data for students to examine. The completely updated FOR500 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7, Windows 8/8.1, Windows 10, Office and Office365, Cloud Storage, SharePoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques 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.

### Register at

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

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

“The hands-on [labs] are excellent – best I have had in 15 years of forensics classes – and the books are the best as well.”

— Shawn Bostick, AR AG

“It’s great to hear real-world examples that apply to the concepts that are being taught. It helps answer the ‘why’ behind the process.”

— Bradley Chapple, Virustream

Course Day Descriptions

Fri, May 8 – Wed, May 13
9:00am – 5:00pm
Hands-on labs

53
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 remediate incidents
- Detect and hunt unknown live, dormant, and custom malware in memory across multiple Windows systems in an enterprise environment
- Hunt through and perform incident response across hundreds of unique systems simultaneously using F-Response Enterprise and the SIFT Workstation
- Identify and track malware beaconing outbound to its command and control (C2) channel via memory forensics, registry analysis, and network connection residue
- Determine how the breach occurred by identifying the beachhead and spear phishing attack mechanisms
- Target advanced adversary anti-forensics techniques like hidden and time-stomped malware, along with utilityware 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

Eric Zimmerman
SANS Certified Instructor

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. 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, Threat Hunting, and Digital Forensics 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!

When Eric Zimmerman was a Special Agent with the FBI, one of his responsibilities was managing on-scene triage. He identified several gaps in an existing process and started creating solutions to address them. What began as building and expanding a few live response tools took Eric down a path that eventually led to him writing more than 50 programs that are now used by nearly 8,800 law enforcement officers in over 80 countries. Much of Eric’s work involved designing and building software related to investigations of sexual abuse of children. In a single year, Eric’s programs led to the rescue of hundreds of these children. As a result, in May 2012, Eric was given a National Center for Missing and Exploited Children’s Award, which honors outstanding law enforcement professionals who have performed above and beyond the call of duty. Eric was also presented with the U.S. Attorney’s Award for Excellence in Law Enforcement in 2013. Today, Eric serves as a Senior Director at Kroll in the company’s cybersecurity and investigations practice. He is a two-time winner of the SANS DFIR NetWars Tournament (2014, 2015). Eric is also the award-winning author of the X-Ways Forensics Practitioner’s Guide, and has created many world-class, open-source forensic tools.

@EricZimmerman

Register at sans.org/security-west | 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 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

**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

“Favorite SANS class so far. Really excellent material. Really excellent delivery.”

— Joshua Sitta, Center State Bank

**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, track, and contain advanced adversaries and remediate incidents. This advanced session will demonstrate techniques used by first responders to identify, track, and contain advanced adversaries and remediate incidents. This advanced session will demonstrate techniques used by first responders to identify, track, and contain advanced adversaries and remediate incidents. This advanced session will demonstrate techniques used by first responders to identify, track, and contain advanced adversaries and remediate incidents.

**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

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/security-west/courses
Digital forensic investigators have traditionally dealt with Windows machines, but what if they find themselves in front of a new Apple Mac or iDevice? The increasing popularity of Apple devices can be seen everywhere, from coffee shops to corporate boardrooms, yet most investigators are familiar with Windows-only machines.

The constantly updated FOR518: Mac and iOS Forensic Analysis and Incident Response course provides the techniques and skills necessary to take on any Mac or iOS case without hesitation. The intense hands-on forensic analysis and incident response skills taught in the course will enable analysts to broaden their capabilities and gain the confidence and knowledge to comfortably analyze any Mac or iOS device. In addition to traditional investigations, the course presents intrusion and incident response scenarios to help analysts learn ways to identify and hunt down attackers that have compromised Apple devices.

This course will teach you:

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

FOR518: Mac and iOS Forensic Analysis and Incident Response aims to train a well-rounded investigator by diving deep into forensic and intrusion analysis of Mac and iOS. The course focuses on topics such as the HFS+ and APFS file systems, Mac-specific data files, tracking of user activity, system configuration, analysis and correlation of Mac logs, Mac applications, and Mac-exclusive technologies. A computer forensic analyst who completes this course will have the skills needed to take on a Mac or iOS forensics case.

**FORENSICATE DIFFERENTLY!**

**You Will Be Able To**

- Parse the HFS+ file system by hand, using only a cheat sheet and a hex editor
- Determine the importance of each file system domain
- Conduct temporal analysis of a system by correlating data files and log analysis
- Profile individuals’ usage of the system, including how often they used it, what applications they frequented, and their personal system preferences
- Determine remote or local data backups, disk images, or other attached devices
- Find encrypted containers and FileVault volumes, understand keychain data, and crack Mac passwords
- Analyze and understand Mac metadata and their importance in the Spotlight database, Time Machine, and Extended Attributes
- Develop a thorough knowledge of the Safari Web Browser and Apple Mail applications
- Identify communication with other users and systems through iChat, Messages, FaceTime, Remote Login, Screen Sharing, and AirDrop
- Conduct an intrusion analysis of a Mac for signs of compromise or malware infection
- Acquire and analyze memory from Mac systems
- Acquire iOS and analyze devices in-depth

**You Will Be Able To**

- Parse the HFS+ file system by hand, using only a cheat sheet and a hex editor
- Determine the importance of each file system domain
- Conduct temporal analysis of a system by correlating data files and log analysis
- Profile individuals’ usage of the system, including how often they used it, what applications they frequented, and their personal system preferences
- Determine remote or local data backups, disk images, or other attached devices
- Find encrypted containers and FileVault volumes, understand keychain data, and crack Mac passwords
- Analyze and understand Mac metadata and their importance in the Spotlight database, Time Machine, and Extended Attributes
- Develop a thorough knowledge of the Safari Web Browser and Apple Mail applications
- Identify communication with other users and systems through iChat, Messages, FaceTime, Remote Login, Screen Sharing, and AirDrop
- Conduct an intrusion analysis of a Mac for signs of compromise or malware infection
- Acquire and analyze memory from Mac systems
- Acquire iOS and analyze devices in-depth

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

— Ian Spence, MOD

---

**Sarah Edwards**

**SANS Principal Instructor**

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

@iamevltwin

---

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

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

**Topics:** Apple Essentials; Mac Essentials and Acquisition; Disks & Partitions; iOS Essentials; iOS Acquisition; iOS Backups

---

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

**Topics:** HFS+ File System; Extended Attributes; File System Events Store Database; Spotlight; Portable Artifacts; Mac and iOS Triage; Most Recently Used (MRU)

---

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

**Topics:** User Data and System Configuration; Log Parsing and Analysis; Timeline Analysis and Data Correlation

---

**DAY 4: Application Data Analysis**
In addition to all the configuration and preference information found in the User Domain, the user can interact with a variety of native Apple applications, including the Internet, email, communication, photos, locational data, etc. These data can provide analysts with the who, what, where, why, and how for any investigation. This section will explore the various databases and other files where data are being stored. The student will be able to parse this information by hand without the help of a commercial tool parser.

**Topics:** Application Permissions; Native Application Fundamentals; Safari Browser; Apple Mail; Communication; Calendar and Reminders; Contacts; Notes; Apple Pay; Wallet; Passes; Photos; Maps; Location Data; Apple Watch; Third-Party Apps

---

**DAY 5: Advanced Analysis Topics**
Mac systems implement some technologies that are available only to those with Mac and iOS devices. These include data backup with Time Machine, Document Versions, and iCloud, and disk encryption with FileVault. Other advanced topics include data hidden in encrypted containers, live response, Mac intrusion and malware analysis, and Mac memory analysis.

**Topics:** Live Response; Time Machine; OS X Malware and Intrusion Analysis; iCloud; Versions; Memory Acquisitions and Analysis; Password Cracking and Encrypted Containers

---

**DAY 6: Mac Forensics & Incident Response Challenge**
Students will put their new Mac forensics skills to the test by running through a real-life scenario with team members.

**Topics:** In-Depth HFS+ File System Examination; File System Timeline Analysis; Advanced Computer Forensics Methodology; Mac Memory Analysis; File System Data Analysis; Metadata Analysis; Recovering Key Mac Files; Volume and Disk Image Analysis; Analysis of Mac Technologies including Time Machine, Spotlight, and FileVault; Advanced Log Analysis and Correlation; iDevice Analysis and iOS Artifacts

---

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

---

“With so much focus on Windows forensics, the Mac class is really necessary.”
— Paul Sieberth, Tulane University

---

“Best Mac class anywhere.”
— Eric Koebelen, Incident Response US
FOR572: **Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response**

**You Will Be Able To**

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

**Philip Hagen**  
SANS Senior Instructor

This course will help you take your system-based forensic knowledge onto the wire, enabling you to incorporate network evidence into your investigations, provide better findings, and get the job done faster.

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

FOR572 is designed to cover the most critical skills needed for the increased focus on network communications and artifacts in today’s investigative work, including numerous use cases. Many investigative teams are incorporating proactive threat hunting that uses existing evidence along with newly acquired threat intelligence to uncover evidence of previously unidentified incidents. Other teams focus on post-incident investigations 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. Put another way: Bad guys are talking – we’ll teach you to listen.

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will cover the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap-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
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 forensicator in typical casework, as well as several that help demonstrate analysis methods useful when facing new, undocumented, or proprietary protocols. By learning the "typical" behaviors of these protocols, we can more readily identify anomalies that may suggest 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; ELK Stack and the SOF-ELK Platform

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

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

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

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

DAY 5: Encryption, Protocol Reversing, OPSEC, and Intel
Advancements in common technology has 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 employ. 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

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

Topics: Network Forensic Case

“First course I’ve taken that gives insight into the forensic mindset required for investigating incidents.”
— Tyler Whittington, PWC

“First course I’ve taken that gives insight into the forensic mindset required for investigating incidents.”
— Tyler Whittington, PWC
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
- Incorporate manual decoding techniques to recover deleted data stored on smartphones and mobile devices
- Recover hidden or obfuscated communication from applications on smartphones
- Decrypt or decode application data that are not parsed by your forensic tools
- 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
- 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

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

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

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

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

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

Every time the smartphone thinks or makes a suggestion, the data are saved. It’s easy to get mixed up in what the forensic tools are reporting. Smartphone forensics is more than just pressing the find evidence button and getting answers. Your team cannot afford to rely solely on the tools in your lab. You have to understand how to use them correctly to guide your investigation, instead of just letting the tool report what it believes happened on the device.

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!

Domenica Crognale
SANS Certified Instructor

Domenica is one of the course co-authors of SANS FOR585: Smartphone Forensic Analysis In-Depth. She has been working in digital forensics for more than 10 years and specializing in mobile devices since 2009. In previous jobs she has provided training to military and government agencies, worked on high-profile cases, tested and validated various mobile forensics utilities and provided security assessments for many mobile applications. In her day job, she spends time dissecting third-party mobile applications where there is no shortage of interesting data left behind. She maintains multiple certifications including the GASF, EnCE, CCE, and CISSP®.

Register at sans.org/security-west | 301-654-SANS (7267)
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 many 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 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

“Mobile phones have become increasingly prevalent in digital investigations, and this course equips examiners with the latest techniques to perform a holistic examination.”

— Bilal Malik, Stroz Friedberg

**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

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/security-west/courses
FOR610: Reverse-Engineering Malware:
Malware Analysis Tools and Techniques

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

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

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

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

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

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

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.

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 executable files. The section begins by discussing how to examine suspicious websites that might host client-side exploits. Next, you will learn how to de-obfuscate malicious scripts with the help of script debuggers and interpreters, examine Microsoft Office macros, and assess the threats associated with PDF and RTF files using several techniques.

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

---

**DAY 4: In-Depth Malware Analysis**

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

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

---

**DAY 5: Examining Self-Defending Malware**

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

**Topics:** 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; Unpacking 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

---

“This is a truly a step-by-step mentorship course. The content is immediately applicable to DFIR job roles.”

— Chad Reams, Parsons Inc.

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/security-west/courses
MGT414: SANS Training Program for CISSP® Certification

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 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
SANS Certified Instructor

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 enterprise designs, 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
### Course Day Descriptions

<table>
<thead>
<tr>
<th>DAY 1: Introduction; Security and Risk Management</th>
<th>DAY 2: Asset Security and Security Engineering – Part 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>On the first day of training for the CISSP® exam, MGT414 introduces the specific requirements needed to obtain certification. The latest 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. <strong>Topics:</strong> Overview of CISSP® Certification, Introductory Material, Overview of the Eight Domains, Domain 1: Security and Risk Management</td>
<td>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 2020 exam such as the Internet of Things, Trusted Platform Modules, Cloud Security, and much more. <strong>Topics:</strong> Domain 2: Asset Security; Domain 3: Security Engineering (Part 1)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>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. <strong>Topics:</strong> Domain 3: Security Engineering (Part 2), Domain 4: Communication and Network Security</td>
<td>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. <strong>Topics:</strong> Domain 5: Identity and Access Management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>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. <strong>Topics:</strong> Domain 6: Security Assessment; Domain 7: Security Operations</td>
<td>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. <strong>Topics:</strong> Domain 8: Software Development Security</td>
</tr>
</tbody>
</table>

**Who Should Attend**

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

---

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

— Kelley O’Neil, Wells Fargo
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.

You Will Be Able To

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

Jeff Frisk currently serves as the director of the GIAC Certifications program and is a member of the SANS Technology Institute Curriculum Committee. Jeff holds a PMP® credential and a GIAC GSEC certification. He also is the course author for MGT525. He has worked on many projects for SANS and GIAC, including courseware, certification, and exam development. Jeff has an engineering degree from the Rochester Institute of Technology and more than 15 years of IT project management experience with computer systems, high-tech consumer products, and business development initiatives. Jeff has held various positions including managing operations, product development, and electronic systems/computer engineering. He has many years of international and high-tech business experience working with both big and small companies to develop computer hardware/software products and services.

“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

Jeff Frisk
SANS Certified Instructor
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 and 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

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/security-west/courses

---

**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

---

67
As security professionals we have seen the landscape change. Cybersecurity is now more vital and relevant to the growth of your organization than ever before. As a result, information security teams have more visibility, more budget, and more opportunity. However, with this increased responsibility comes more scrutiny.

This course teaches security professionals how to do three things:

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

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

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

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

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

---

**You Will Be Able To**

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

---

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

— Mike Parkin, Chapters Health System

---

**G. Mark Hardy**
SANS Principal Instructor

---

G. Mark Hardy is founder and president of National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for over 35 years, and is an internationally recognized expert and keynote speaker who has presented at over 250 events world-wide. He provides consulting services as a virtual CISO, expert witness testimony, and domain expertise in blockchain and cryptocurrency. G. Mark serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. He is a retired U.S. Navy captain who was entrusted with nine command assignments, including responsibility for leadership training for 70,000 sailors. A graduate of Northwestern University, he holds a B.S. in computer science, a B.A. in mathematics, a master’s degree in business administration, and a master’s degree in strategic studies, and holds the GSLC, CISSP®, CISM and CISA certifications.

@g_mark

---

**G. Mark Hardy: Security Strategic Planning, Policy, and Leadership**

**Day Program**

5 Day Program | 30 CPEs | Laptop Not Needed

---

Register at sans.org/security-west | 301-654-SANS (7267)
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

---

**Who Should Attend**
- CISOs
- Information security officers
- Security directors
- Security managers
- Aspiring security leaders
- Other security personnel who have team lead or management responsibilities

---

“*This training is valuable because it shines a light on the many business aspects of security, while also providing excellent guidance for applying learnings in real life.*”

— Alyssa DeVita, Marriott

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/security-west/courses

69
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.

Course 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 and continuous integration pipelines. At the SANS Institute, Eric authors application security courses on DevOps, cloud security, secure coding, and defending mobile apps. He serves on the advisory board for the SANS Securing The Human Developer awareness training program, delivers security training around the world, and has presented his security research at conferences including BlackHat, OWASP, BSides, JavaOne, UberConf, and ISSA. Eric completed a bachelor of science degree in computer engineering and a master of science degree in information assurance at Iowa State University, and currently holds the CISSP®, GWAPT, GSSP-Java, vulnerability assessments, and many more.

Register at sans.org/security-west | 301-654-SANS (7267)
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 “Unicorns” – the Internet tech leaders that 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 (CD) – the automation engine in DevOps – and how to build up a CD 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

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

“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

5 Day Program  |  30 CPES  |  Laptop Required

You Will Be Able To

- Better understand various industrial control systems and their purpose, application, function, and dependencies on network IP and industrial communications
- Work with control network infrastructure design (network architecture concepts, including topology, protocols, and components) and their relation to IEC 62443 and the Purdue Model.
- Run Windows command line tools to analyze the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat, etc.) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Work with operating systems (system administration concepts for Unix/Linux and/or Windows operating systems)
- Better understand the systems’ security lifecycle
- Better understand information assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)
- Use your skills in computer network defense to detect host and network-based intrusions via intrusion detection technologies
- Implement incident response and handling methodologies
- Map different ICS technologies, attacks, and defenses to various cybersecurity standards including the NIST Cyber Security Framework, ISA/IEC 62443, ISO/IEC 27001, NIST SP 800-53, the Center for Internet Security Critical Security Controls, and COBIT 5

Paul Piotrowski
SANS Instructor

SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. ICS410: ICS/SCADA Security Essentials provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems (ICS) is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

The course will provide you with:

- An understanding of ICS components, purposes, deployments, significant drivers, and constraints
- Hands-on lab learning experiences to control system attack surfaces, methods, and tools
- Control system approaches to system and network defense architectures and techniques
- Incident-response skills in a control system environment
- Governance models and resources for industrial cybersecurity professionals

When examining the greatest risks and needs in critical infrastructure sectors, the course authors looked carefully at the core security principles necessary for the range of tasks involved in supporting control systems on a daily basis. While other courses are available for higher-level security practitioners who need to develop specific skills such as ICS penetration testing, vulnerability analysis, malware analysis, forensics, secure coding, and red team training, most of these courses do not focus on the people who operate, manage, design, implement, monitor, and integrate critical infrastructure production control systems.

With the dynamic nature of ICS, many engineers do not fully understand the features and risks of many devices. For their part, IT support personnel who provide the communications paths and network defenses do not always grasp the systems’ operational drivers and constraints. This course is designed to help traditional IT personnel fully understand the design principles underlying control systems and how to support those systems in a manner that ensures availability and integrity. In parallel, the course addresses the need for control system engineers and operators to better understand the important role they play in cybersecurity. This starts by ensuring that a control system is designed and engineered with cybersecurity built into it, and that cybersecurity has the same level of focus as system reliability throughout the system lifecycle.

When these different groups of professionals complete this course, they will have developed an appreciation, understanding, and common language that will enable them to work together to secure their ICS environments. The course will help develop cyber-secure-aware engineering practices and real-time control system IT/OT support carried out by professionals who understand the physical effects of actions in the cyber world.

Paul Piotrowski is currently an automation engineer in Shell’s Global PCD Integrity Organization (Process Control Domain). Paul consults on global capital projects and supports Shell operated and non-operated assets across all business units. Paul has spent over 16 years with Shell in various security roles including network operations, risk governance and compliance, audit, incident management, forensics, pen testing and project management. He has travelled extensively for Shell, allowing him the opportunity to work across diverse cultures and landscapes that have shaped his view of the world. Paul possesses the valuable hybrid skill set of Operations Technology (OT) and Information Technology (IT). As a result of his work at over 50 Shell facilities across the globe, he has come to understand how to embed practical solutions between operations and corporate IT that reduce an organization's cybersecurity risk while minimizing operational impact. Paul was involved in the initial development of the GICSP course curriculum. He holds a BSc degree in computer science with a minor in management. He holds several certifications including the GICSP and CISSP®. In addition, he has participated in several executive development programs.
**Course Day Descriptions**

**DAY 1: ICS Overview**
On this first day, students will develop and reinforce a common language and understanding of industrial control system (ICS) cybersecurity as well as the important considerations that come with cyber-to-physical operations within these environments. Each student will receive programmable logic controller (PLC) hardware to keep. The PLC contains physical inputs and outputs that will be programmed in class and mapped to an operator interface, or HMI, also created in class. This improved hardware-enabled approach provides the necessary cyber-to-physical knowledge that allows students to better understand important ICS operational drivers and constraints that require specific safety protection, communications needs, system management approaches, and cybersecurity implementations. Essential terms, architectures, methodologies, and devices are all covered to build a common language for students from a variety of different roles.

**Topics:** Global Industrial Cybersecurity Professional (GICSP) Overview; Overview of ICS; Purdue Levels 0 and 1; Purdue Levels 2 and 3; ICS and SCADA; IT & ICS Differences; Physical Security and Cybersecurity; Secure ICS Network Architectures

**DAY 2: Field Devices and Controllers**
If you know the adversary’s approaches to attacking an ICS environment, you will be better prepared to defend that environment. Numerous attack vectors exist within an ICS environment. Some are similar to traditional IT systems, while others are more specific to ICS. During day 2, students will develop a better understanding of where these specific attack vectors exist and how to block them, starting at the lowest levels of the control network. Students will look at different technologies and communications used in Purdue Levels 0 and 1, the levels that are the most different from an IT network. Students will capture fieldbus traffic from the PLCs they programmed on day 1 and look at what other fieldbus protocols are used in the industry. Later in the day, students will analyze network captures containing other control protocols that traverse Ethernet-only networks and TCP/IP networks, set up a simulated controller, and interact with it through a control protocol.

**Topics:** ICS Attack Surface; Purdue Levels 0 and 1; Ethernet and TCP/IP

**DAY 3: Supervisory Systems**
Day 3 will take students through the middle layers of control networks. Students will learn about different methods to segment and control the flow of traffic through the control network. Students will explore cryptographic concepts and how they can be applied to communications protocols and on devices that store sensitive data. Students will learn about the risks of using wireless communications in control networks, which wireless technologies are commonly used, and available defenses for each. After a hands-on network forensics exercise where students follow an attacker from phishing campaign to HMI breach, students will look at HMI, historian, and user interface technologies used in the middle to upper levels of the control network, namely Purdue Levels 2 and 3, while performing attacks on HMI web technologies and interfaces susceptible to password brute force attacks.

**Topics:** Enforcement Zone Devices; Understanding Basic Cryptography; Wireless Technologies; Wireless Attacks and Defenses; Exercise: Network Forensics of an Attack; Purdue Level 2 and 3 Attacks

**DAY 4: Workstations and Servers**
Students will learn essential ICS-related server and workstation operating system capabilities, implementation approaches, and system management practices. Students will receive and work with both Windows- and Linux-based virtual machines in order to understand how to monitor and harden these hosts from attack. Students will examine concepts that benefit ICS systems such as system hardening, log management, monitoring, alerting, and audit approaches, then look at some of the more common applications and databases used in ICS environments across multiple industries. Finally, students will explore attacks and defenses on remote access for control systems.

**Topics:** Patching ICS Systems; Defending Microsoft Windows; Defending Unix and Linux; Endpoint Security Software; Event Logging and Analysis; Remote Access Attacks

**DAY 5: ICS Security Governance**
On the final course day students will learn about the various models, methodologies, and industry-specific regulations that are used to govern what must be done to protect critical ICS systems. Key business processes that consider risk assessments, disaster recovery, business impact analysis, and contingency planning will be examined from the perspective of ICS environments. Students will work together on an incident response exercise that places them squarely in an ICS environment that is under attack. This exercise ties together key aspects of what has been learned throughout the course and presents students with a scenario to review with their peers. Specific incident-response roles and responsibilities are considered, and actions available to defenders throughout the incident response cycle are explored. Students will leave with a variety of resources for multiple industries and will be well prepared to pursue the GICSP, an important ICS-focused professional certification.

**Topics:** Building an ICS Cybersecurity Program; Creating ICS Cybersecurity Policy; Disaster Recovery; Measuring Cybersecurity Risk; Incident Response; Exercise: Incident Response Tabletop Exercise; Final Thoughts and Next Steps

---

**Who Should Attend**
The course is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:

- IT (includes operational technology support)
- IT security (includes operational technology security)
- Engineering
- Corporate, industry, and professional standards

---

“**This is by far the best training course I have taken in my 30+ years as an engineer. My cybersecurity knowledge has increased significantly.”**
— Chris Butrick, HSE (UK)

---

“**Good comprehensive content with dynamic instructor really made this course good. This is the best training course I've taken in 25+ years.”**
— Curt Imanse, Accenture
ICS456: Essentials for NERC Critical Infrastructure Protection

You Will Be Able To

- Understand the cybersecurity objectives of the NERC Critical Infrastructure Protection (CIP) standards
- Understand the NERC regulatory framework, its source of authority, and the process for developing CIP standards, as well as their relationship to the other Bulk Electric System (BES) reliability standards
- Speak fluent NERC CIP and understand how seemingly similar terms can have significantly different meanings and impacts on your compliance program
- Break down the complexity to more easily identify and categorize BES cyber assets and systems
- Develop better security management controls by understanding what makes for effective cybersecurity policies and procedures
- Understand physical and logical controls and monitoring requirements
- Make sense of the CIP-007 system management requirements and their relationship to CIP-010 configuration management requirements, and understand the multiple timelines for assessment and remediation of vulnerabilities
- Determine what makes for a sustainable personnel training and risk assessment program
- Develop strategies to protect and recover BES cyber system information
- Know the keys to developing and maintaining evidence that demonstrates compliance and be prepared to be an active member of the audit support team
- Sharpen your CIP Ninja

You Will Learn:

- BES cyber system identification and strategies for lowering impact ratings
- Nuances of NERC-defined terms and the applicability of CIP standards and how subtle changes in definitions can have a big impact on your program
- The significance of properly determining cyber system impact ratings and strategies for minimizing compliance exposure
- Strategic implementation approaches for supporting technologies
- Effective implementations for cyber and physical access controls
- How to break down the complexity of NERC CIP in order to communicate with your leadership
- What to expect in your next CIP audit, how to prepare supporting evidence, and how to avoid common pitfalls
- How to understand the most recent Standards Development Team’s efforts and how that may impact your current CIP program

Jason Christopher
SANS Certified Instructor

This course empowers students with knowledge of the “what” and the “how” of the version 5/6 standards. The course addresses the role of the Federal Energy Regulatory Commission (FERC), North American Reliability Corporation (NERC), and the Regional Entities, provides multiple approaches for identifying and categorizing Bulk Electric System (BES) cyber systems, and helps asset owners determine the requirements applicable to specific implementations. Additionally, the course covers implementation strategies for the version 5/6 requirements with a balanced practitioner approach to both cybersecurity benefits, as well as regulatory compliance.

The course features 25 hands-on labs range from securing workstations to digital forensics and lock picking.

The SANS ICS456: Essentials for NERC Critical Infrastructure Protection course was developed by SANS ICS team members with extensive electricity industry experience, including former Registered Entity Primary Contacts, a former NERC officer, and a Co-Chair of the NERC Critical Infrastructure Protection (CIP) Interpretation Drafting Team. Together the authors bring real-world, practitioner experience gained from developing and maintaining NERC CIP and NERC 693 compliance programs and actively participating in the standards development process.

Jason Christopher is the Chief Technology Officer for Axio. His responsibilities include providing technical leadership on security and resilience issues relevant to Axio, its partners, and clients, and on the development of all Axio technology platforms for security metrics and benchmarking. Prior to Axio, Jason led the research for cybersecurity metrics and information assurance at the Electric Power Research Institute. Previously, he was the technical lead for cybersecurity capability and risk management at the U.S. Department of Energy, where he managed the Cybersecurity for Energy Delivery Systems Operations program, which included the Cybersecurity Capability Maturity Model and other collaborative efforts. Jason also served as the program lead for both Critical Infrastructure Protection Standards and Smart Grid Security at the Federal Energy Regulatory Commission. He has worked on a variety of infrastructure projects, particularly in the field of industrial control system design and implementation. He has also researched and designed technology systems across multiple industries, including energy, water, transportation, and communications. He has been a representative on the Federal Smart Grid Task Force, the Critical Infrastructure Protection Committee (CIPC), and other technical committees.
DAY 1: Asset Identification and Governance

A transition is under way from NERC CIP programs that are well defined and understood to a new CIP paradigm that expands its scope into additional environments and adds significantly more complexity. On day 1, students will develop an understanding of the electricity sector regulatory structure and history as well as an appreciation for how the CIP Standards fit into the overall framework of the reliability standards. Key NERC terms and definitions related to NERC CIP are reviewed using realistic concepts and examples that prepare students to better understand their meaning. We will explore multiple approaches to BES Cyber Asset identification and learn the critical role of strong management and governance controls. We’ll also examine a series of architectures, strategies, and difficult compliance questions in a way that highlights the reliability and cybersecurity strengths of particular approaches. Unique labs will include a scenario-based competition that helps bring the concepts to life and highlights the important role we play in defending the grid.

Topics: Regulatory History and Overview; NERC Functional Model; NERC Reliability Standards; CIP History; Terms and Definitions; CIP-002: BES Cyber System Categorization; CIP-003: Security Management Controls

DAY 2: Access Control and Monitoring

Strong physical and cyber access controls are at the heart of any good cybersecurity program. On day 2 we move beyond the what of CIP compliance to understanding the why and the how. Firewalls, proxies, gateways, IDS, and more – you’ll learn where and when they help as well as practical implementations to consider and designs to avoid. Physical protection includes more than fences, and you’ll learn about the strengths and weaknesses of common physical controls and monitoring schemes. Labs will reinforce the learnings throughout the day and introduce architecture review and analysis, firewall rules, IDS rules, compliance evidence demonstration, and physical security control reviews.

Topics: CIP-005: Electronic Security Perimeter(s); Interactive Remote Access; External Routable Communication and Electronic Access Points; CIP-006: Physical Security of BES Cyber Systems; Physical Security Plan; Visitor Control Programs; PACS Maintenance and Testing; CIP-014: Physical Security

DAY 3: System Management

CIP-007 has consistently been one of the most violated standards going back to CIP version 1. With the CIP Standards moving to a systematic approach with varying requirement applicability based on a system impact rating, the industry now has new ways to design and architect system management approaches. Throughout day 3, students will dive into CIP-007. We’ll examine various Systems Security Management requirements with a focus on implementation examples and the associated compliance challenges. We’ll also cover the CIP-010 requirements for configuration change management and vulnerability assessments that ensure systems are in a known state and under effective change control. We’ll move through a series of labs that reinforce the topics covered from the perspective of the CIP practitioner responsible for implementation and testing.

Topics: CIP-007: System Management; Physical and Logical Ports; Patch Management; Malicious Code Prevention; Account Management; CIP-010: Configuration Change Management and Vulnerability Assessments; Change Management Program; Baseline Configuration Methodology; Change Management Alerting/Prevention

DAY 4: Information Protection and Response

Education is key to every organization’s success with NERC CIP, and ICS456 graduates will be knowledgeable advocates for CIP when they return to their place of work. Regardless of their role, students can be a valued resource to their organization’s CIP-004 training program and the CIP-011 information protection program. Students will be ready with resources for building and running strong awareness programs that reinforce the need for information protection and cybersecurity training. On day 4, we’ll examine CIP-008 and CIP-009, covering identification, classification communication of incidents, and the various roles and responsibilities needed in an incident response or a disaster recovery event. Labs will introduce tools to ensure file integrity and the sanitization of files to be distributed, how to best utilize and communicate with the E-ISAC, and how to preserve incident data for future analysis.

Topics: CIP-004: Personnel & Training; Security Awareness Program; CIP Training Program; PRA Evaluation Process; CIP-011: Information Protection; Information Protection Program; Data Sanitization; CIP-008: Incident Reporting and Response Planning; Incident Response Plan/Testing; Reporting Requirements; CIP-009: Recovery Plans for BES Cyber Systems; Recovery Plans; System Backup

DAY 5: CIP Process

On the final course day students will learn the key components for running an effective CIP compliance program. We will review the NERC processes for standards development, violation penalty determination, Requests for Interpretation, and recent changes stemming from the Reliability Assurance Initiative. Additionally, we’ll identify recurring and audit-related processes that keep a CIP compliance program on track: culture of compliance, annual assessments, gap analysis, TFEs, and self-reporting. We’ll also look at the challenge of preparing for NERC audits and provide tips to be prepared to demonstrate the awesome work your team is doing. Finally, we’ll look at some real-life CIP violations and discuss what happened and the lessons we can take away. At the end of day 5, students will have a strong call to action to participate in the ongoing development of CIP within their organization and in the industry overall as well as a sense that CIP is do-able! Labs on day 5 will cover DOE C2M2, audit tools, and an audit-focused take on a blue team – red team exercise.

Topics: Scenario One: CIP Processes for Maintaining Compliance; Preparing for an Audit; Audit Follow-Up; CIP Industry Activities; Standards Process; CIP of the Future

Who Should Attend

- IT and OT (ICS) cybersecurity
- Field support personnel
- Security operations personnel
- Incident response personnel
- Compliance staff
- Team leaders
- Persons involved in governance
- Vendors/Integrators
- Auditors

“This is a great course that examines NERC CIP standards and compliance from a variety of perspectives. I recommend it to anyone working with CIP.”

— Tom Duffey, Accenture Security
ICS515: ICS Active Defense and Incident Response

You Will Be Able To

- Perform 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. The course will introduce and reinforce methodologies such as ICS network security monitoring and approaches to reducing the control system threat landscape
- Analyze ICS threats 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 whether operations must shut down or it is safe to respond to the threat and continue operations
- Use multiple security disciplines in tandem to leverage an active defense and safeguard an ICS, all reinforced with hands-on labs and technical concepts

Robert M. Lee
SANS Senior Instructor

ICS515: ICS Active Defense and Incident Response will help you deconstruct industrial control system (ICS) cyber attacks, leverage an active defense to identify and counter threats to your ICS, and use incident response procedures to maintain the safety and reliability of operations.

The 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, which is needed to counter advanced adversaries targeting ICS, as has been seen with malware such as STUXNET, HAVEX, CRASHOVERRIDE, and TRISIS. 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 threat analysis and incident response to ensure the safety and reliability of operations. The strategic and technical skills presented in this course serve as a basis for ICS organizations looking to show that defense is doable.

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, which you can keep after the class ends
- Gain hands-on experience with samples of Havex, BlackEnergy2, and Stuxnet by engaging in labs and de-constructing these threats and others
- Leverage technical tools such as Shodan, Security Onion, TCPDump, Wireshark, Snort, Bro, SGUIL, ELSA, Volatility, Redline, FTK Imager, PDF analyzers, malware sandboxes, and more
- Create indicators of compromise (IOCs) in OpenIOC and YARA and gain an understanding of 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

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 Kew 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
**DAY 1: Threat Intelligence**

Industrial control system (ICS) security professionals must be able to leverage internal and external threat intelligence to critically analyze threats, extract indicators of compromise (IOCs), document tactics, techniques, and procedures (TTPs), and guide security teams to find threats in the environment. On this first course day students will learn how threat intelligence is generated, how to critically analyze reports, and the basic tenets of active defense functions. Students will become better analysts and critical thinkers by learning skills useful in day-to-day operations, regardless of their jobs and roles. This day focuses five hands-on labs that include building a Programmable Logic Controller (PLC), identifying information available about assets online through Shodan, completing an analysis of competing hypotheses, visualizing the attack space, and ingesting threat intelligence reports to guide their practices over the rest of the labs in the course.

**Topics:** Case Study: STUXNET; Introduction to ICS Active Defense and Incident Response; Intelligence Life-Cycle and Threat Intelligence; ICS Cyber Kill Chain; Identifying and Reducing the Threat Landscape; Sharing and Consuming ICS Threat Intelligence

---

**DAY 2: Asset Identification and Network Security Monitoring**

Understanding the networked environment is the only way to fully defend it: you cannot defend what you do not know. This course section will teach students to use tools such as Wireshark, TCPDump, CyberLens, ELSA, Bro, and Snort to map their ICS network, collect data, detect threats, and analyze threats to drive incident response procedures. During this section, students will be introduced to the lab network and an advanced persistent threat (APT) that is present on it. Drawing on threat intelligence from the previous course section, students will have to discover, identify, and analyze the threat using their new active defense skills to guide incident responders to the affected Human Machine Interface (HMI).

**Topics:** Case Study: HAVEX; ICS Asset and Network Visibility; ICS Network Security Monitoring – Collection; ICS Network Security Monitoring – Detection; ICS Network Security Monitoring – Analysis

---

**DAY 3: Incident Response**

The ability to prepare for and perform ICS incident response is vital to the safety and reliability of control systems. ICS incident response is a core concept of ICS active defense and requires that analysts safely acquire digital evidence while scoping the environment for threats and their impact on operations. ICS incident response is a young field with many challenges, but during this section students will learn effective tactics and tools to collect and preserve forensic-quality data. Students will then use these data to perform timely forensic analysis and create IOCs. In the previous section’s labs, APT malware was identified in the network. In this section, the labs will focus on identifying which system is impacted and gathering a sample of the threat that can be analyzed.

**Topics:** Case Study: German Steelworks Attack; Incident Response and Digital Forensics Overview; Evidence Acquisition; Sources of Forensic Data in ICS Networks; Memory Forensics and Identifying Capabilities; Integrated Timely Analysis

---

**DAY 4: Threat and Environment Manipulation**

Understanding the threat is key to discovering its capabilities and its potential to affect the ICS. The information extracted from threats through processes such as malware analysis is also critical to being able to make the necessary changes to the environment to reduce the effectiveness of the threat. The information obtained is vital to an ICS active defense, which requires internal data collection to create and share threat intelligence. In this section, students will learn how to analyze initial attack vectors such as spearphishing emails, perform timely malware analysis techniques, analyze memory images, and create Indicators of Compromise in YARA. The previous section’s labs identified the infected HMI and gathered a sample of the APT malware. In this section’s labs, students will analyze the malware, extract information, and develop YARA rules to complete the active defense model introduced in the class and maintain the baseline.

**Topics:** Case Study: BlackEnergy2; ICS Threat and Environment Manipulation Goals and Considerations; Analyzing Acquired Evidence; Case Study: Ukraine Power Grid Attack, 2015; Malware Analysis Methodologies; Case Study: CRASHOVERRIDE; Documenting Knowledge; Case Study: TRISIS

---

**DAY 5: Active Defense and Incident Response Challenge**

This section focuses on reinforcing the strategy, methodologies, skillsets, and tools introduced in the first four sections of the course. This entirely hands-on section will present students with two different scenarios. The first involves data collected from an intrusion into SANS Cyber City. The second involves data collected from a Distributed Control System (DCS) infected with malware. This section will truly challenge students to utilize their ICS active defense and incident response skills and test themselves.

**Topics:**
- Scenario One:
  - Identify the Assets and Map the ICS Networks; Perform ICS Network Security Monitoring to Identify the Abnormalities; Execute ICS Incident Response Procedures Into the SANS Cyber City Data Files; Analyze the Malicious Capability and Determine if the Threat is an Insider Threat or a Targeted External Threat
- Scenario Two:
  - Identify the Software and Information Present on the DCS; Leverage ICS Active Defense Concepts to Identify the Real-World Malware; Determine the Impact on Operations and Remediation Needs

For course updates, prerequisites, special notes, or laptop requirements, visit [sans.org/security-west/courses](https://sans.org/security-west/courses)
ICS612: ICS Cybersecurity In-Depth

You Will Be Able To

- Gain hands-on experience with typical assets found within an industrial environment, including a Programmable Logic Controller (PLC), Operator Interfaces (OI) for local control, Human Machine Interface (HMI) servers, Historian server, switches, routers, and firewall(s).
- Gain an understanding of 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 (IDM2).
- Gain hands-on experience 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.
- Gain an understanding of 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.

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 Cybersecurity 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.

“Truly understanding the devices we are charged with defending is imperative to effectively implementing security measures.”

— Crystal B., U.S. Army

Tim Conway
SANS Certified Instructor

Tim serves as the Technical Director of ICS and SCADA programs at SANS, and is responsible for developing, reviewing, and implementing technical components of the SANS ICS and SCADA product offerings. He also performs contract and consulting work in the areas of ICS cybersecurity with a focus on energy environments. A recognized leader in CIP operations, Tim formerly served as the Director of CIP Compliance and Operations Technology at the Northern Indiana Public Service Company (NIPSCO), and was responsible for Operations Technology, NERC CIP Compliance, and the NERC training environments for the operations departments within NIPSCO Electric. Tim authored and instructs ICS456: Essentials for NERC Critical Infrastructure Protection. Outside of SANS, Tim continues to perform contract and consulting work in the areas of ICS cybersecurity with a focus on the energy sector. Before joining SANS, in his 15-year career with NIPSCO, Tim held management and leadership positions as well as EMS computer systems engineer responsibilities over the control system servers and the supporting network infrastructure. During his career, Tim has served as the chair of the RFC CIPC, the NERC CIP Interpretation Drafting Team, the NERC CIPC GridEx Working Group, and the NBISE Smart Grid Cyber Security panel.

Register at sans.org/security-west | 301-654-SANS (7267)
# Course Day Descriptions

**Day 1: Local Process**

Learning Objectives:
- Review of Lab Setup
- Introduction to the PLC Platform Application Tools
- Introduction to Programming a PLC
- Service Discovery on PLC
- Introduction to the HMI Platform Application Tools
- Understand HMI to PLC Communication

**Topics:**

---

**Day 2: System of Systems**

Learning Objectives:
- Introduction to Peer-to-Peer Communications
- Introduction to SCADA Systems
- OPC Communications

**Topics:**
- Components of Level 3: Peer-to-Peer Communications Between PLCs: SCADA/OPC Communications: Use and Dependencies of Traditional IT Services (DNS, AD, DHCP, NTP, etc.): Vendor Security Models and Industrial DMZs: Attack Vectors and Defense Techniques From Level 3

---

**Day 3: Network Infrastructure – Architecture Design & Implementation**

Learning Objectives:
- Network Architecture and Technology in ICS
- ICS Firewalls
- ICS Perimeter
- Historians
- Remote Access and Jump Host/2FA

**Topics:**

---

**Day 4: System Management Implementation**

Learning Objectives:
- ICS System Monitoring and Logging
- ICS Asset Management
- ICS Asset Validation

**Topics:**
- Logging and Traffic Collection in an ICS Environment: Monitoring and Alerting in ICS Networks: Monitoring and Alerting in a Serial Network: System Integrity Verification

---

**Day 5: Attack Vectors, ICS Targets, and Kill Chain Mapping**

Learning Objectives:
- Hands-on environment troubleshooting
- Attack/Defend – ICS NetWars Style Challenge

**Topics:**
- Pivoting and Positioning in an ICS Target Environment: Operational traffic reverse engineering: Protocol-Level Manipulation: Firmware Manipulation: Industrial Wireless Discovery and Attack: Time Synchronization Manipulation: Data Table and Scaling Modifications

---

**Who Should Attend**

- ICS410 course alumni – students who have successfully completed ICS410: ICS/SCADA Security Essentials will have the base knowledge as a prerequisite for this course.
- 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

---

*“The training starts with theory and quickly progresses into full hands-on interaction with all components. This experience is not easy to find. It is an amazing course.”*

— Bassem Hemida, Deloitte
Penetration Testing 2-Day Courses

**NEW! 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 to, 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.

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.

<table>
<thead>
<tr>
<th>2 Day Course</th>
<th>12 CPEs</th>
<th>Laptop Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wed, May 6 – Thu, May 7</td>
<td>9:00am – 5:00pm</td>
<td>Instructor: Jorge Orchilles</td>
</tr>
</tbody>
</table>

“The content from SEC564 is great and I will be able to implement it in my organization right away!”
— Kirk Hayes, Rapid 7

Cyber Defense 2-Day Course

**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.

<table>
<thead>
<tr>
<th>2 Day Course</th>
<th>12 CPEs</th>
<th>Laptop Not Needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wed, May 6 – Thu, May 7</td>
<td>9:00am – 5:00pm</td>
<td>Instructor: Randy Marchany</td>
</tr>
</tbody>
</table>

“Gives specific direction for understanding risks and building a program to address them.”
— Eric Pierce, Mindbody

Hosted Course

**NEW! HOSTED: Successful InfoSec Consulting**

Becoming a consultant seems like a dream: high pay, freedom, fascinating work and more. These can all be true yet there is more to the reality: as a consultant you are running a business and you need clients!

What does a successful consultant need to know? How do you find clients? How do you get started? This course answers these questions and more.

It is based on Ted Demopoulos’ nearly three decades of experience as an independent InfoSec consultant, extensive interviews with dozens of other successful consultants, and surveys of those interested in InfoSec consulting.

<table>
<thead>
<tr>
<th>2 Day Course</th>
<th>12 CPEs</th>
<th>Laptop Not Needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wed, May 6 – Thu, May 7</td>
<td>9:00am – 5:00pm</td>
<td>Instructor: Ted Demopoulos</td>
</tr>
</tbody>
</table>
Welcome Reception
Kick off your SANS Security West 2020 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 San Diego. 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.

Coffee & Donuts with the College Students
Join us for coffee, donuts, and conversation with SANS Technology Institute staff and students. Learn about SANS’ regionally accredited master’s degree and graduate certificate programs for InfoSec professionals and its undergraduate certificate program for people who want to launch a career in cybersecurity. Find out if the class you’re taking this week or GIAC certifications you’ve earned may be applied towards a graduate or undergraduate program. Visit www.sans.edu for complete information on curriculum, admissions, and funding options.

Malware Analysis: A Deep-Dive Experience
Anuj Soni
Join Anuj Soni for an in-depth examination of a real, in-the-wild malware sample. There will be no slides, pretty pictures or fluffy theory here – this is 100% demo, and it will expose attendees to the approaches, tools and struggles of reverse-engineering malware end-to-end. We will begin with static file analysis, proceed to behavioral analysis, and then perform static and dynamic code analysis. We will identify decoding routines, deobfuscate executable content, discuss a script to automate our work, and review a rule to detect similar files in the future. Come along for this accelerated but thorough discussion of key reverse-engineering activities.

Cloud Security: Attacking the Metadata Service
Eric Johnson
Cloud metadata services are popular targets for attackers trying to gain direct access to an organization’s cloud resources. The Capital One breach notification published in 2019 put a spotlight on metadata services and weaknesses. Using publicly available information from the breach, this presentation will demonstrate how the attacker compromised Amazon Web Services instance metadata credentials, gained access to privileged resources, and exfiltrated data from the account. The conversation will then shift to a post mortem discussion about cloud security controls that could have prevented or limited the blast radius of the attack.

The Future of the Cybersecurity Workforce
G. Mark Hardy
Our field has been growing like crazy, with an estimated 3.5 million unfilled cybersecurity jobs expected within the next few years. More certs, more quals, more money, right? But where are these people going to come from? It’s up to us to help find and train them. You are the vanguard of this cyber cadre of experts, but we’ll need to do more than just advertise for talent. In this presentation, we’ll look at possible future roles for our security experts, how Artificial Intelligence might figure into that (what will be automated and what we will still have to do ourselves), and how even if you are seeking your first SANS cert this week you can still be part of the senior cadre of security thought leadership going forward.

PowerShell 2020: State of the Art/Hack/Infection
Jason Fossen
Why has PowerShell become so popular for ransomware, hacking tools, cloud computing, and security automation? Several courses at SANS now include some amount of PowerShell, including courses on penetration testing, forensics, auditing, and log analysis. But isn’t PowerShell just another command shell? NO! Attend this talk by SANS Faculty Fellow Jason Fossen to see what PowerShell really is, how it’s being used (and abused) today, and future trends, like PowerShell on Linux. If you’re unfamiliar with PowerShell or you’re taking a SANS course with PowerShell labs, like SEC401, then this presentation is especially for you. You are welcome to bring your laptop to the talk too – you can get the latest version of PowerShell for macOS, Linux or Windows from https://github.com/powershell/ (it’s open-source).

“Wide variety of excellent courses. The SANS@Night talks and NetWars make this an excellent training opportunity.”
— Lee Neely, LLNL
### Bonus Sessions

**The Hacker’s Apprentice**  
Mark Baggett  
Mark Baggett has built an escape room in his house! In this presentation, Mark will describe how he used Python, smart-home Internet of Things devices, and a few puzzles to build it. And he’ll show how you too can install some pretty cool automation in your home, even without a lot of smart home devices.

**Kerberos And Attacks 101**  
Tim Medin  
Want to understand how Kerberos works? Would you like to understand modern Kerberos attacks? If so, then join Tim Medin as he walks you through how to attack Kerberos with ticket attacks and Kerberoasting. We will cover the basics of Kerberos authentication and then show you how the trust model can be exploited for persistence, pivoting, and privilege escalation.

**Protecting Your Way of Life: ICS Security Standards for Critical Infrastructure Protection**  
Jason Christopher  
Critical infrastructure describes the industries that maintain our modern society: water, power, transportation, pharmaceuticals, food processing, and more. You’ll often hear that these systems have their own unique security considerations and that, despite the drastic impact a cybersecurity attack may have, they are often less secure than “traditional IT” sectors like finance. While it is true that the industrial control systems (ICS) we rely on are vulnerable and are facing new and evolving threats, engineers are actively maturing and growing the field of ICS security. This session will explore the security standards, guidelines, and industry certifications available for engineers and IT professionals alike to tear down silos and solve the most difficult cyber risk challenge of our lifetime.

---

### Exhibitor-Sponsored Events

**Networking Lunch & Evening Reception**  
Tuesday, May 12 | 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!

**Lunch & Learns**  
Monday, May 11 | 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.

---

“**SANS training is well-organized, and the extra speaking topics presented in the evening were good. I appreciate these extra lectures, as they are beneficial.**”  
— Andrew Crouse, Epiq
## Future Events

### SANS Training Events

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security East</td>
<td>New Orleans, LA</td>
<td>Feb 1-8</td>
</tr>
<tr>
<td>Northern VA – Fairfax</td>
<td>Fairfax, VA</td>
<td>Feb 10-15</td>
</tr>
<tr>
<td>New York City</td>
<td>New York, NY</td>
<td>Feb 10-15</td>
</tr>
<tr>
<td>Scottsdale</td>
<td>Scottsdale, AZ</td>
<td>Feb 17-22</td>
</tr>
<tr>
<td>San Diego</td>
<td>San Diego, CA</td>
<td>Feb 17-22</td>
</tr>
<tr>
<td>Jacksonville</td>
<td>Jacksonville, FL</td>
<td>Feb 24-29</td>
</tr>
<tr>
<td>Northern VA – Reston Spring</td>
<td>Reston, VA</td>
<td>Mar 2-7</td>
</tr>
<tr>
<td>St. Louis</td>
<td>St. Louis, MO</td>
<td>Mar 8-13</td>
</tr>
<tr>
<td>Dallas</td>
<td>Dallas, TX</td>
<td>Mar 9-14</td>
</tr>
<tr>
<td>Norfolk</td>
<td>Norfolk, VA</td>
<td>Mar 16-21</td>
</tr>
<tr>
<td>San Francisco Spring</td>
<td>San Francisco, CA</td>
<td>Mar 16-27</td>
</tr>
<tr>
<td>Seattle Spring</td>
<td>Seattle, WA</td>
<td>Mar 23-28</td>
</tr>
<tr>
<td>Philadelphia</td>
<td>Philadelphia, PA</td>
<td>Mar 30 – Apr 4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS 2020</td>
<td>Orlando, FL</td>
<td>Apr 3-10</td>
</tr>
<tr>
<td>Bethesda</td>
<td>Bethesda, MD</td>
<td>Apr 14-19</td>
</tr>
<tr>
<td>Minneapolis</td>
<td>Minneapolis, MN</td>
<td>Apr 14-19</td>
</tr>
<tr>
<td>Boston Spring</td>
<td>Boston, MA</td>
<td>Apr 20-25</td>
</tr>
<tr>
<td>Pen Test Austin</td>
<td>Austin, TX</td>
<td>Apr 27 – May 2</td>
</tr>
<tr>
<td>Baltimore Spring</td>
<td>Baltimore, MD</td>
<td>Apr 27 – May 2</td>
</tr>
</tbody>
</table>

### SANS Summit Events

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open-Source Intelligence</td>
<td>Washington, DC</td>
<td>Feb 18-24</td>
</tr>
<tr>
<td>ICS Security</td>
<td>Orlando, FL</td>
<td>Mar 2-9</td>
</tr>
<tr>
<td>Blue Team</td>
<td>Louisville, KY</td>
<td>Mar 2-9</td>
</tr>
<tr>
<td>Cloud Security</td>
<td>Frisco, TX</td>
<td>May 27 – Jun 3</td>
</tr>
</tbody>
</table>

### Community SANS Events

Local, single-course events are also offered throughout the year via SANS Community. Visit [sans.org/community](http://sans.org/community) for up-to-date Community course information.

---

**Take SANS Training Anytime, Anywhere with SANS OnDemand**

More than 45 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](http://www.sans.org/ondemand) to learn more about your OnDemand training options.
Manchester Grand Hyatt San Diego
One Market Place  |  San Diego, CA 92101
619-232-1234
www.sans.org/security-west/location

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

Discover the vibrant culture and natural beauty of Southern California right outside your door at the Manchester Grand Hyatt San Diego. Ideally situated on San Diego Bay between the San Diego Convention Center and the city’s popular Seaport Village, this hotel offers a spectacular waterfront resort-like setting, complete with shopping, dining, and entertainment venues. The city comes to life at night, and the Manchester Grand Hyatt San Diego is within walking distance to restaurants, bars and nightclubs located in the ever popular Gaslamp District.

Special Hotel Rates Available
A special discounted rate of $235 S/D plus applicable taxes will be honored based on space availability.

Government per diem rooms are available with proper ID. All rates include high-speed Internet in your room and are only available through April 14, 2020.

SANS SIMULCAST
Live stream content directly from the classroom and interact with peers and in-class moderators. Simulcast includes four months of access to your course recordings and labs, and unlimited subject-matter-expert support. Visit sans.org/security-west/attend-remotely for more details.

Register Information
Register online at sans.org/security-west
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.

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: sans.org/vouchers

Pay Early and Save*
Use code EarlyBird20 when registering early

<table>
<thead>
<tr>
<th>DATE</th>
<th>DISCOUNT</th>
<th>DATE</th>
<th>DISCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 18</td>
<td>$300</td>
<td>Apr 8</td>
<td>$150</td>
</tr>
</tbody>
</table>

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

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 April 22, 2020. 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.
<table>
<thead>
<tr>
<th>Courses – 5-6 Days</th>
<th>Paid before 3-18-20</th>
<th>Paid before 4-8-20</th>
<th>Paid after 4-8-20</th>
<th>Add GIAC Cert*</th>
<th>Add OnDemand*</th>
<th>Add NetWars Continuous</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC301 Introduction to Cyber Security</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC401 Security Essentials Bootcamp Style</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC450 Blue Team Fundamentals: Security Operations and Analysis</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC460 Enterprise Threat and Vulnerability Assessment</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC487 Open-Source Intelligence (OSINT) Gathering and Analysis</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC501 Advanced Security Essentials – Enterprise Defender</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC503 Intrusion Detection In-Depth</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC505 Securing Windows and PowerShell Automation</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC511 Continuous Monitoring and Security Operations</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC530 Defensible Security Architecture and Engineering</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC540 Cloud Security and DevOps Automation</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC542 Web App Penetration Testing and Ethical Hacking</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC545 Cloud Security Architecture and Operations</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC560 Network Penetration Testing and Ethical Hacking</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC566 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>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC573 Automating Information Security with Python</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC575 Mobile Device Security and Ethical Hacking</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC599 Defeating Advanced Adversaries – Purple Team Tactics &amp; Kill Chain Defenses</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC617 Wireless Penetration Testing and Ethical Hacking</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>FOR500 Windows Forensic Analysis</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>FOR508 Advanced Incident Response, Threat Hunting, and Digital Forensics</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>FOR518 Mac and iOS Forensic Analysis and Incident Response</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>FOR527 Advanced Network Forensics: Threat Hunting, Analysis &amp; Incident Response</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>FOR558 Smartphone Forensic Analysis In-Depth</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>MGT414 SANS Training Program for CISSP® Certification</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>MGT512 Security Leadership Essentials for Managers</td>
<td>$6,300</td>
<td>$6,450</td>
<td>$6,600</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>MGT514 Security Strategic Planning, Policy, and Leadership</td>
<td>$6,300</td>
<td>$6,450</td>
<td>$6,600</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>ICS410 ICS/SCADA Security Essentials</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>ICS460 Essentials for NERC Critical Infrastructure Protection</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>ICS515 ICS Active Defense and Incident Response</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>ICS612 ICS Cybersecurity In-Depth</td>
<td>$5,790</td>
<td>$5,940</td>
<td>$6,090</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
</tbody>
</table>

**Skilled-Based Short Courses**

<table>
<thead>
<tr>
<th>Add</th>
<th>Course fee if taking a 4-6 day course</th>
<th>Add NetWars Continuous</th>
</tr>
</thead>
</table>
| EARLY BIRD DISCOUNTS | **Pay for any long course using the code EarlyBird20 at checkout by March 18th to get $300 OFF or by April 8th to get $150 OFF**  
*Some restrictions apply. Early bird discounts do not apply to Hosted courses. |

**Additional Discounts**

- **Early Bird**
  - **Code:** EarlyBird20
  - **Discount:** $315

**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.
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 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.

**@RISK: The Consensus Security Alert**
A reliable weekly summary of (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) how recent attacks worked, and (4) other valuable data.

**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.

**WhatWorks Webcasts**
SANS WhatWorks webcasts feature powerful customer experiences in resolving specific IT security issues.

**Tool Talks**
Tool Talks demonstrate how commercial tools can be used to solve or mitigate IT security problems.

**Course Demos**
Test drive more than 40 SANS courses and decide which is right for you. Our demos are delivered via the SANS OnDemand platform, and give you a close look at a course’s contents, pace, and features. sans.org/demo

**Other Free Resources (SANS.org account is not necessary)**
- 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 March 18th Use code EarlyBird20 sans.org/security-west

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

NALT-BRO-SECWEST20