SECURITY EAST 2018
New Orleans, LA | January 8-13

Protect Your Business and Advance Your Career
20 hands-on, immersion-style information security courses taught by real-world practitioners

- Cyber Defense
- Detection & Monitoring
- Penetration Testing
- Incident Response
- Threat Hunting
- Ethical Hacking
- Digital Forensics
- Security Management
- ICS/SCADA Security
- SIEM

“Amazing training that every professional security practitioner should take.”
-Efren Izquierdo-Ramirez, General Dynamics

SAVE $400
Register and pay by Nov 15th – Use code EarlyBird18

REGISTER AT www.sans.org/security-east
Cybersecurity threats change daily and attacks are becoming more aggressive. You can stay ahead of the curve by attending **SANS Security East 2018 from January 8-13**. You'll learn actionable steps to prevent cyber attacks and keep your organization safe.

> “SANS training is worth every penny. In a cyber world that changes every day, this instruction brings the student to the front of the learning curve.”
> — G. Boresky, U.S. Department of Health and Human Services

### Why Is SANS Security East 2018 the Best Training and Education Investment?

SANS courseware is unrivaled in the industry and we constantly update our courses to teach the tools and techniques that are proven to keep networks safe. With 20+ courses to choose from at SANS Security East 2018, all taught by our world-class instructors, you and your team can learn valuable skills applicable to your security roles that you’ll be able use as soon as you get back to work.

> “Top-notch instructors who are truly experts in their field, and have the teaching skills to convey the topic.” — Steven Seifert, Eli Lilly and Company

> “SANS hands-on training and labs provide skills you can use the day you return to work! SANS instructors are some of the most technical people I’ve met and their ability to deep dive into anything was fantastic. I learned more this week than I did in any single semester of college!” — Ryan Russell, USAA

### Bonus Experiences

At **SANS Security East 2018**, you can test your security defense skills at the Core NetWars Experience and the all-new Cyber Defense NetWars Tournament scheduled for the evenings of January 11 and 12. The Core NetWars Experience is an interactive, Internet-based environment for computer attacks and analyzing defenses. The Cyber Defense NetWars Tournament is a defense-focused challenge that tests your ability to solve problems and secure your systems from compromise. Professionals from all skill levels will gain valuable knowledge and experience from participating, so put your security skills to the test! Registration is limited and free for students attending any 5- or 6-day course at **SANS Security East 2018**.

> “Having participated in the NetWars Tournament, I can honestly say that it was the most intellectually challenging and enjoyable test of technical skills in which I have had the privilege to participate.” — Kees Leune, Adelphi University

**SANS Security East 2018** will also feature a number of other opportunities to learn new skills, techniques, and trends, including SANS@Night talks, lunch-and-learn sessions, and networking with your peers. You’ll hear about the latest and most important issues from SANS practitioners who are leading the global conversation on cybersecurity.

### GIAC Certifications and OnDemand Options

Many SANS courses prepare you for a GIAC certification, one of the most prestigious security certifications in the field. You can also bundle four months of OnDemand online training with your live course at a discounted rate to extend your study. You can add the corresponding GIAC certification and OnDemand bundle when registering for your course to receive the discounted rates (subject to availability).

> “The GIAC certification has enabled me to take the next step in my Information Security career. It has allowed me to prove that my value was more than just that of a security-minded Sys Admin.” — J. Klein, Enterprise Information System, Cedars-Sinai Medical Center

SANS' award-winning faculty has proven that they understand the challenges you face daily, and they are eager to help you learn the vital skills needed to secure your environment. Nothing beats a SANS live training event to learn from cybersecurity experts who are uniquely equipped to give you the best training available in the industry today. Take a first-hand look at why SANS is the most trusted source for information security training, certification, and research.

> “Bar none, SANS is the best training you can get. I thought I knew security before training, but after this fantastic course, I realized just how little I knew, but in a good way.” — Lance Freeman, Blue Cross and Blue Shield of Louisiana

Visit [www.sans.org/security-east](http://www.sans.org/security-east) to review the full course list and training-event details. **Register and pay by November 15 to receive an early-bird discount!** We look forward to seeing you in New Orleans!
### Courses at a Glance

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC301</td>
<td>Intro to Information Security</td>
<td>12</td>
</tr>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
<td>8</td>
</tr>
<tr>
<td>SEC503</td>
<td>Intrusion Detection In-Depth</td>
<td>14</td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td>10</td>
</tr>
<tr>
<td>SEC511</td>
<td>Continuous Monitoring and Security Operations</td>
<td>16</td>
</tr>
<tr>
<td>SEC542</td>
<td>Web App Penetration Testing and Ethical Hacking</td>
<td>26</td>
</tr>
<tr>
<td>SEC555</td>
<td>SIEM with Tactical Analytics</td>
<td>18</td>
</tr>
<tr>
<td>SEC560</td>
<td>Network Penetration Testing and Ethical Hacking</td>
<td>24</td>
</tr>
<tr>
<td>SEC566</td>
<td>Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td>20</td>
</tr>
<tr>
<td>SEC573</td>
<td>Automating Information Security with Python</td>
<td>28</td>
</tr>
<tr>
<td>SEC579</td>
<td>Virtualization and Software-Defined Security</td>
<td>22</td>
</tr>
<tr>
<td>SEC660</td>
<td>Advanced Penetration Testing, Exploit Writing, and Ethical Hacking</td>
<td>30</td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Digital Forensics, Incident Response, and Threat Hunting</td>
<td>32</td>
</tr>
<tr>
<td>FOR578</td>
<td>Cyber Threat Intelligence</td>
<td>34</td>
</tr>
<tr>
<td>FOR610</td>
<td>Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td>
<td>36</td>
</tr>
<tr>
<td>MGT414</td>
<td>SANS Training Program for CISSP® Certification</td>
<td>40</td>
</tr>
<tr>
<td>MGT512</td>
<td>SANS Security Leadership Essentials for Managers with Knowledge Compression™</td>
<td>38</td>
</tr>
<tr>
<td>MGT514</td>
<td>IT Security Strategic Planning, Policy, and Leadership</td>
<td>42</td>
</tr>
<tr>
<td>DEV540</td>
<td>Secure DevOps and Cloud Application Security</td>
<td>44</td>
</tr>
<tr>
<td>ICS410</td>
<td>ICS/SCADA Security Essentials</td>
<td>46</td>
</tr>
<tr>
<td>Core NetWars Experience</td>
<td></td>
<td>50</td>
</tr>
<tr>
<td>Cyber Defense NetWars Tournament</td>
<td></td>
<td>50</td>
</tr>
</tbody>
</table>

**CONTENTS**

- SANS Training Roadmap ........................................ 2-3
- SANS OnDemand Bundles ........................................ 49
- SANS Instructors ............................................. 4
- NetWars Experience ........................................... 50
- About SANS ..................................................... 5
- Future SANS Training Events ................................ 51
- Securing Approval and Budget for Training ............. 6
- Hotel Information .............................................. 52
- GIAC Certifications ............................................ 7
- Registration Information ..................................... 52
- Bonus Sessions ................................................ 48
- Registration Fees ............................................. 53
SANS’s World-Class Instructors

For instructor bios, visit: [www.sans.org/event/security-east-2018/instructors](http://www.sans.org/event/security-east-2018/instructors)

*SANS instructors are real-world practitioners who specialize in the subjects they teach. All instructors undergo rigorous training and testing in order to teach SANS courses, which guarantees what you learn in class will be up to date and relevant to your job. The lineup of instructors for SANS Security East 2018 includes:*

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Twitter Handle</th>
<th>Teaching Course</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eric Conrad</td>
<td>Senior Instructor</td>
<td>@eric_conrad</td>
<td>SEC511</td>
</tr>
<tr>
<td>Bryce Galbraith</td>
<td>Principal Instructor</td>
<td>@brycegalbraith</td>
<td>SEC560</td>
</tr>
<tr>
<td>David Hoelzer</td>
<td>Faculty Fellow</td>
<td>@it_audit</td>
<td>SEC503</td>
</tr>
<tr>
<td>Robert M. Lee</td>
<td>Certified Instructor</td>
<td>@RobertMLee</td>
<td>FOR578</td>
</tr>
<tr>
<td>Seth Misenar</td>
<td>Senior Instructor</td>
<td>@sethmisenar</td>
<td>SEC555</td>
</tr>
<tr>
<td>Billy Rios</td>
<td>Certified Instructor</td>
<td>@XSSniper</td>
<td>ICS410</td>
</tr>
<tr>
<td>James Tarala</td>
<td>Senior Instructor</td>
<td>@isaudit</td>
<td>SEC566</td>
</tr>
<tr>
<td>Mark Baggett</td>
<td>Senior Instructor</td>
<td>@MarkBaggett</td>
<td>SEC573</td>
</tr>
<tr>
<td>G. Mark Hardy</td>
<td>Principal Instructor</td>
<td>@g.mark</td>
<td>MGT512</td>
</tr>
<tr>
<td>Eric Johnson</td>
<td>Certified Instructor</td>
<td>@emjohn20</td>
<td>DEV540</td>
</tr>
<tr>
<td>Tim Medin</td>
<td>Certified Instructor</td>
<td>@timmedin</td>
<td>SEC660</td>
</tr>
<tr>
<td>Michael Murr</td>
<td>Principal Instructor</td>
<td>@mikemurr</td>
<td>SEC504</td>
</tr>
<tr>
<td>Moses Hernandez</td>
<td>Certified Instructor</td>
<td>@mosesrenegade</td>
<td>SEC542</td>
</tr>
<tr>
<td>Rob Lee</td>
<td>Faculty Fellow</td>
<td>@roblee, @sansforensics</td>
<td>FOR508</td>
</tr>
<tr>
<td>David R. Miller</td>
<td>Certified Instructor</td>
<td>@DRM_CyberDude</td>
<td>MGT414</td>
</tr>
<tr>
<td>Keith Palmgren</td>
<td>Senior Instructor</td>
<td>@kpalmgren</td>
<td>SEC301</td>
</tr>
<tr>
<td>Bryan Simon</td>
<td>Certified Instructor</td>
<td>@BryanOnSecurity</td>
<td>SEC401</td>
</tr>
</tbody>
</table>


*SANS’s World-Class Instructors*

For instructor bios, visit: [www.sans.org/event/security-east-2018/instructors](http://www.sans.org/event/security-east-2018/instructors)

*SANS instructors are real-world practitioners who specialize in the subjects they teach. All instructors undergo rigorous training and testing in order to teach SANS courses, which guarantees what you learn in class will be up to date and relevant to your job. The lineup of instructors for SANS Security East 2018 includes:*

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Twitter Handle</th>
<th>Teaching Course</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eric Conrad</td>
<td>Senior Instructor</td>
<td>@eric_conrad</td>
<td>SEC511</td>
</tr>
<tr>
<td>Bryce Galbraith</td>
<td>Principal Instructor</td>
<td>@brycegalbraith</td>
<td>SEC560</td>
</tr>
<tr>
<td>David Hoelzer</td>
<td>Faculty Fellow</td>
<td>@it_audit</td>
<td>SEC503</td>
</tr>
<tr>
<td>Robert M. Lee</td>
<td>Certified Instructor</td>
<td>@RobertMLee</td>
<td>FOR578</td>
</tr>
<tr>
<td>Seth Misenar</td>
<td>Senior Instructor</td>
<td>@sethmisenar</td>
<td>SEC555</td>
</tr>
<tr>
<td>Billy Rios</td>
<td>Certified Instructor</td>
<td>@XSSniper</td>
<td>ICS410</td>
</tr>
<tr>
<td>James Tarala</td>
<td>Senior Instructor</td>
<td>@isaudit</td>
<td>SEC566</td>
</tr>
<tr>
<td>Mark Baggett</td>
<td>Senior Instructor</td>
<td>@MarkBaggett</td>
<td>SEC573</td>
</tr>
<tr>
<td>G. Mark Hardy</td>
<td>Principal Instructor</td>
<td>@g.mark</td>
<td>MGT512</td>
</tr>
<tr>
<td>Eric Johnson</td>
<td>Certified Instructor</td>
<td>@emjohn20</td>
<td>DEV540</td>
</tr>
<tr>
<td>Tim Medin</td>
<td>Certified Instructor</td>
<td>@timmedin</td>
<td>SEC660</td>
</tr>
<tr>
<td>Michael Murr</td>
<td>Principal Instructor</td>
<td>@mikemurr</td>
<td>SEC504</td>
</tr>
<tr>
<td>Moses Hernandez</td>
<td>Certified Instructor</td>
<td>@mosesrenegade</td>
<td>SEC542</td>
</tr>
<tr>
<td>Rob Lee</td>
<td>Faculty Fellow</td>
<td>@roblee, @sansforensics</td>
<td>FOR508</td>
</tr>
<tr>
<td>David R. Miller</td>
<td>Certified Instructor</td>
<td>@DRM_CyberDude</td>
<td>MGT414</td>
</tr>
<tr>
<td>Keith Palmgren</td>
<td>Senior Instructor</td>
<td>@kpalmgren</td>
<td>SEC301</td>
</tr>
<tr>
<td>Bryan Simon</td>
<td>Certified Instructor</td>
<td>@BryanOnSecurity</td>
<td>SEC401</td>
</tr>
</tbody>
</table>


*SANS’s World-Class Instructors*

For instructor bios, visit: [www.sans.org/event/security-east-2018/instructors](http://www.sans.org/event/security-east-2018/instructors)

*SANS instructors are real-world practitioners who specialize in the subjects they teach. All instructors undergo rigorous training and testing in order to teach SANS courses, which guarantees what you learn in class will be up to date and relevant to your job. The lineup of instructors for SANS Security East 2018 includes:*

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Twitter Handle</th>
<th>Teaching Course</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eric Conrad</td>
<td>Senior Instructor</td>
<td>@eric_conrad</td>
<td>SEC511</td>
</tr>
<tr>
<td>Bryce Galbraith</td>
<td>Principal Instructor</td>
<td>@brycegalbraith</td>
<td>SEC560</td>
</tr>
<tr>
<td>David Hoelzer</td>
<td>Faculty Fellow</td>
<td>@it_audit</td>
<td>SEC503</td>
</tr>
<tr>
<td>Robert M. Lee</td>
<td>Certified Instructor</td>
<td>@RobertMLee</td>
<td>FOR578</td>
</tr>
<tr>
<td>Seth Misenar</td>
<td>Senior Instructor</td>
<td>@sethmisenar</td>
<td>SEC555</td>
</tr>
<tr>
<td>Billy Rios</td>
<td>Certified Instructor</td>
<td>@XSSniper</td>
<td>ICS410</td>
</tr>
<tr>
<td>James Tarala</td>
<td>Senior Instructor</td>
<td>@isaudit</td>
<td>SEC566</td>
</tr>
<tr>
<td>Mark Baggett</td>
<td>Senior Instructor</td>
<td>@MarkBaggett</td>
<td>SEC573</td>
</tr>
<tr>
<td>G. Mark Hardy</td>
<td>Principal Instructor</td>
<td>@g.mark</td>
<td>MGT512</td>
</tr>
<tr>
<td>Eric Johnson</td>
<td>Certified Instructor</td>
<td>@emjohn20</td>
<td>DEV540</td>
</tr>
<tr>
<td>Tim Medin</td>
<td>Certified Instructor</td>
<td>@timmedin</td>
<td>SEC660</td>
</tr>
<tr>
<td>Michael Murr</td>
<td>Principal Instructor</td>
<td>@mikemurr</td>
<td>SEC504</td>
</tr>
<tr>
<td>Moses Hernandez</td>
<td>Certified Instructor</td>
<td>@mosesrenegade</td>
<td>SEC542</td>
</tr>
<tr>
<td>Rob Lee</td>
<td>Faculty Fellow</td>
<td>@roblee, @sansforensics</td>
<td>FOR508</td>
</tr>
<tr>
<td>David R. Miller</td>
<td>Certified Instructor</td>
<td>@DRM_CyberDude</td>
<td>MGT414</td>
</tr>
<tr>
<td>Keith Palmgren</td>
<td>Senior Instructor</td>
<td>@kpalmgren</td>
<td>SEC301</td>
</tr>
<tr>
<td>Bryan Simon</td>
<td>Certified Instructor</td>
<td>@BryanOnSecurity</td>
<td>SEC401</td>
</tr>
</tbody>
</table>
The SANS Institute’s mission is to deliver cutting-edge information security knowledge and skills to companies, military organizations, and governments in order to protect people and assets.

CUTTING-EDGE TRAINING

More than 55 unique courses are designed to align with dominant security team roles, duties, and disciplines. The courses prepare students to meet today’s threats and tomorrow’s challenges.

The SANS curriculum spans Cyber Defense, Digital Forensics & Incident Response, Threat Hunting, Audit, Management, Penetration Testing, Industrial Control Systems Security, Secure Software Development, and more. Each curriculum offers a progression of courses that can take professionals from a subject’s foundations right up to top-flight specialization.

We constantly update and rewrite these courses to teach the most cutting-edge tools and techniques that are proven to keep networks safe.

Our training is designed to be practical. Students are immersed in hands-on lab exercises designed for them to practice, hone, and perfect what they’ve learned.

LEARN FROM EXPERTS

SANS courses are taught by an unmatched faculty of active security practitioners. Each instructor brings a wealth of real-world experience to every classroom – both live and online. SANS instructors work for high-profile organizations as red team leaders, chief information security officers, technical directors, and research fellows.

Along with their respected technical credentials, SANS instructors are also expert teachers. Their passion for the topics they teach shines through, making the SANS classroom dynamic and effective.

WHY SANS IS THE BEST TRAINING AND EDUCATIONAL INVESTMENT

SANS immersion training is intensive and hands-on, and our courseware is unrivaled in the industry.

SANS instructors and course authors are leading industry experts and practitioners. Their real-world experience informs their teaching and training content. SANS training strengthens a student’s ability to achieve a GIAC certification.

THE SANS PROMISE

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

SANS FORMATS

The most popular option to take SANS training is to attend a 5- or 6-day technical course taught live in a classroom at one of our 200+ training events held around the world throughout the year. SANS training events provide an ideal learning environment and offer the chance to network with other security professionals, as well as SANS instructors and staff.

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

HOW TO REGISTER FOR SANS TRAINING

Students can learn more and register online by visiting www.sans.org/online.
Securing Approval and Budget for Training

Packaging matters

Write a formal request

• All organizations are different, but because training requires a significant investment of both time and money, most successful training requests are made via a written document (short memo and/or a few powerpoint slides) that justifies the need and benefit. Most managers will respect and value the effort.

• Provide all the necessary information in one place. In addition to your request, provide all the right context by including the summary pages on Why SANS?, the Training Roadmap, the instructor bio, and additional benefits available at our live events or online.

Be specific

• How does the course relate to the job you need to be doing? Place the particular course you wish to take into the context on the SANS Career Roadmap. Are you establishing baseline skills? Transitioning to a more focused role? Decision-makers need to understand the plan and context for the decision.

• Highlight specifics of what you will be able to do afterwards. Each SANS course description includes a section titled “You Will Be Able To.” Be sure to include these in your request so that you make the benefits clear. The clearer the match between the training and what you need to do at work, the better.

Establish longer-term expectations

• Information security is a specialized career path within IT, with practices that evolve as attacks change. Because of this, organizations should expect to spend 6%-10% of salaries to keep professionals current and improve their skills. Training for such a dynamic field is an annual, per-person expense—not a once-and-done item.

• Take a GIAC Certification exam to prove the training worked. Employers value the validation of learning that passing a GIAC exam offers. Exams are psychometrically designed to establish competency for related job tasks.

• Consider offering trade-offs for the investment. Many professionals build annual training expense into their employment agreements even before joining a company. Some offer to stay for a year after they complete the training.
GIAC
The Highest Standard in Cybersecurity Certification

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.

“I think the exam was both fair and practical. These are the kind of real world problems I expect to see in the field.”
- Carl Hallberg, Wells Fargo, GIAC Reverse Engineering Malware (GREM)

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

“It feels like SANS and GIAC are working with the candidates to help them to meet the required standards, which are achievable with hard work.”
- Thomas Gurney, GIAC Certified Intrusion Analyst (GCIA)

“lt’s an awesome effort: great questions, excellent material and presentation throughout the (training event) week. I’ve really enjoyed it and will recommend it to many. Thank you GIAC/SANS!”
- Nicolas B., Intrasyss, GIAC Certified Incident Handler (GCIH)
Six-Day Program
Mon, Jan 8 - Sat, Jan 13
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Bryan Simon

Security Essentials Bootcamp Style

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

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 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, SEC401 will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

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.

“Hands-on labs reinforce the class teachings – this is tremendously valuable to be able to grasp the concepts.” -LAURA INASKI, WALT DISNEY PARKS AND RESORTS TECHNOLOGY

Bryan Simon  SANS Certified Instructor

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 regularly 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 GSEC, GCWN, GCIA, GCED, GCUX, GISF, and GMON. Bryan’s scholastic achievements have resulted in the honor of sitting as a current member of the SANS Institute Advisory Board and in his acceptance into the prestigious SANS Cyber Guardian program. Bryan teaches SEC401: Security Essentials Bootcamp Style; SEC501: Advanced Security Essentials – Enterprise Defender; SEC505: Securing Windows and Powershell Automaton; and SEC511: Continuous Monitoring and Security Operations. @BryanOnSecurity
Course Day Descriptions

401.1 HANDS ON: Networking Concepts

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 of how networks and the related protocols like TCP/IP work is critical to being able to analyze network traffic and determine what is hostile. It is just as important to know how to protect against these attacks using devices such as routers and firewalls. These essentials, and more, will be covered during this course day in order to provide a firm foundation for the consecutive days of training.

Topics: Setting Up a Lab with Virtual Machines; Network Fundamentals; IP Concepts; IP Behavior; Virtual Machines

401.2 HANDS ON: Defense In-Depth

To secure an enterprise network, you must have an understanding of the general principles of network security. In this course, you will learn about six key areas of network security. The day starts with information assurance foundations. Students look at both current and historical computer security threats, and how they have impacted confidentiality, integrity, and availability. The first half of the day also covers creating sound security policies and password management, including tools for password strength on both Unix and Windows platforms. The second half of the day is spent on understanding the information warfare threat and the six steps of incident handling. The day draws to a close by looking at attack strategies and how the offense operates.

Topics: Information Assurance Foundations; Computer Security Policies; Contingency and Continuity Planning; Access Control; Password Management; Incident Response; Offensive and Defensive Information Warfare; Attack Strategies and Methods

401.3 HANDS ON: Internet Security Technologies

Military agencies, banks, and retailers offering electronic commerce services, as well as dozens of other types of organizations, are striving to understand the threats they are facing and what they can do to address those threats. On day 3, you will be provided with a roadmap to help you understand the paths available to organizations that are considering deploying or planning to deploy various security devices and tools such as intrusion detection systems and firewalls. When it comes to securing your enterprise, there is no single technology that is going to solve all your security issues; however, by implementing an in-depth defense strategy that includes multiple risk-reducing measures, you can go a long way toward securing your enterprise.

Topics: Firewalls and Perimeters; Honeypots; Host-based Protection; Network-based Intrusion Detection and Prevention; Vulnerability Scanning and Remediation; Web Security

401.4 HANDS ON: Secure Communications

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. Day 4 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. The day finishes by looking at using the Critical Security Controls for metrics-based dashboards and performing risk assessment across an organization.

Topics: Cryptography; Steganography; Critical Security Controls; Risk Assessment and Auditing

401.5 HANDS ON: Windows Security

Windows is the most widely-used and hacked 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: Security Infrastructure; Service Packs, Patches, and Backups; Permissions and User Rights; Security Policies and Templates; Securing Network Services; Auditing and Automation

401.6 HANDS ON: Unix/Linux Security

While organizations do not have as many Unix/Linux systems, for those that do have them, these systems are often among the most critical systems that need to be protected. Day 6 provides step-by-step guidance to improve the security of any Linux system by combining practical how-to instructions with background information for Linux beginners, as well as security advice and best practices for administrators with all levels of expertise.

Topics: Linux Landscape; Permissions and User Accounts; Linux OS Security; Maintenance, Monitoring, and Auditing Linux; Linux Security Tools

You Will Be Able To

- Design and build a network architecture using VLANs, NAC and 802.1x based on an APT indicator 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 operate a virtual lab to test and evaluate the tools/security of systems
- Create an effective policy that can be enforced within an organization and prepare a checklist to validate security, creating metrics to tie into training and awareness
- Identify visible weaknesses of a system utilizing various tools including dumpsec and OpenVAS, 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 it through hardening and patching
- Sniff open protocols like telnet and ftp and determine the content, passwords and vulnerabilities utilizing WireShark
- Apply what you learned directly to your job when you go back to work

“This course fills in the gaps that traditional instruction and industry experience leave behind while remaining easy to digest and follow.”

- Tyler Jarmon, Amazon

www.sans.edu

MEETS DoDD 8140

(8570) REQUIREMENTS

www.sans.org/8140

www.sans.edu

BUNDLE

ONDEMAND

WITH THIS COURSE

www.sans.org/ondemand

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/security-east-2018/courses
SEC504

Hacker Tools, Techniques, Exploits, and Incident Handling

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.

“The hands-on labs and the technical background about how attacks work in SEC504 are very insightful and show us how hackers operate.”
-Christopher Miller, Global Payments Inc.

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 tools provided in SEC504 are ready-to-use in the real world, and I can already see how I’ll be using and applying this course to my job.” - Jennifer Chavarria, Freeport LNG

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

“1 love Mike Murr’s analogies; they are spot-on and help break down complex information.”
- Elizabeth Murrell, Boston Medical Center

Michael Murr SANS Principal Instructor

Michael has been a forensic analyst with Code-X Technologies for over five years. He has conducted numerous investigations and computer forensic examinations, and has performed specialized research and development. Michael has taught SANS SEC504: Hacker Techniques, Exploits, and Incident Handling, SANS FOR508: Computer Forensics, Investigation, and Response, and SANS FOR610: Reverse-Engineering Malware. He has also led SANS Online Training courses and is a member of the GIAC Advisory Board. Currently, Michael is working on an open-source framework for developing digital forensics applications. He holds the GCIH, GCFA, and GREM certifications and has a degree in computer science from California State University at Channel Islands. Michael also blogs about digital forensics on his forensic computing blog (www.forensicblog.org). @mikemurr

Six-Day Program
Mon, Jan 8 - Sat, Jan 13
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs

Laptop Required
(A wired connection is required in class; if your laptop supports only wireless, please bring a USB ethernet adapter with you.)

This course has extended hours

Instructor: Michael Murr

www.giac.org/gcih
504.1 **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

---

504.2 **HANDS ON: Computer and Network Hacker Exploits — PART 1**

Seemingly innocuous data leaking from your network could provide the clue needed by an attacker to blow your systems wide open. This day-long course covers the details associated with reconnaissance and scanning, the first two phases of many computer attacks.

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

---

504.3 **HANDS ON: 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 covers the third step of many hacker attacks — gaining access. Attackers employ a variety of strategies to take over systems from the network level up to the application level. This section covers the attacks in depth, from the details of buffer overflow and format string attack techniques to the latest in session hijacking of supposedly secure protocols.

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

---

504.4 **HANDS ON: Computer and Network Hacker Exploits — PART 3**

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

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

---

504.5 **HANDS ON: Computer and Network Hacker Exploits — PART 4**

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

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

---

504.6 **HANDS ON: 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

--

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.edu/ondemand](http://www.sans.edu/ondemand)
To determine if the SANS SEC301 course is right for you, ask yourself five simple questions:

- Do you have basic computer knowledge, but are new to information security 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 (with some technical knowledge) 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 information security and need formal training/certification?

If you answer yes to any of these questions, the SEC301: Intro to Information Security training course is for you. Jump-start your security knowledge by receiving insight and instruction from real-world security experts on critical introductory topics that are fundamental to information security. This completely revised, five-day comprehensive course covers everything from core terminology to the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles.

This course is designed for students who have a basic knowledge of computers and technology but have no prior knowledge of cybersecurity. The hands-on, step-by-step teaching approach will enable you to grasp all of the information presented, even if some of the topics are new to you. You’ll learn the fundamentals of information security that will serve as the foundation of your InfoSec 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 course up the line, 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.

“This course presents a unique opportunity to learn the broad scope of information security with a knowledgeable instructor and superior training material.” –RA Hubert, FedEx

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 DoD and the National Security Agency. Later, as Security Consulting Practice Manager for both Sprint and Netigy, Keith built and ran the security consulting practice. He was responsible for all security consulting world-wide and for leading dozens of security professionals on many consulting engagements across all business spectrums. For the last several years, Keith has run his own company, NetIP, Inc. He divides his time between consulting, training, and freelance writing projects. In his career, Keith has trained over 10,000 IT professionals and authored more than 20 IT security training courses, including the SANS SEC301 course. Keith currently holds 10 computer security certifications (CISSP, GSEC, GCIH, GCED, GISF, CEH, Security+, Network+, A+, CTT+). @kpalmgren
Course Day Descriptions

301.1 HANDS ON: Security’s Foundation

Every good security practitioner and 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 the Confidentiality, Integrity, and Availability (CIA) Triad, 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.

301.2 HANDS ON: 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 ASCII (American Standard Code for Information Interchange). 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. Day two 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 you’ll finally grasp what is meant by 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 and never quite understood: TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS.

301.3 HANDS ON: An Introduction to Cryptography

One of the most complex issues faced by security practitioners, cryptography 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, but we’ll look at 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?

301.4 HANDS ON: Cybersecurity 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. From there, we move into a discussion of network security technologies and methods including compartmentalization, firewalls, intrusion detection and prevention systems, sniffers, content filters, and so on. 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 technologies.

301.5 HANDS ON: Cybersecurity Technologies – PART 2

The final day of our SEC301 journey continues the discussion of cybersecurity technologies. The day begins by looking at the system security to include hardening operating systems, patching, virtual machines, cloud computing, and backup. We move to application security to learn about browser security and web security, as well as email and instant messaging concerns. We discuss competitive intelligence gathering methods and how you can defend against them. We close the course with an explanation of awareness training and social engineering so that students understand what it is and why it’s so difficult to defend against.

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
> Gain an understanding of computer network basics
> Have a fundamental grasp of any number of critical technical networking acronyms: TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS
> Utilize built-in Windows tools to see your network settings
> Recognize and discuss various security technologies including anti-malware, firewalls, and intrusion detection systems
> Determine your “Phishing IQ” to more easily identify SPAM email messages
> Understand physical security issues and how they support cybersecurity
> Understand incident response, business continuity, and disaster recovery planning at an introductory level
> Access a number of websites to better understand password security, encryption, phishing, browser security, etc.

“This was my first IT course, and it was very informative class. I highly recommend this course if you’re starting to build your career in information security.”

-CRISTIAN MERCADO, CIM GROUP

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/security-east-2018/courses
Six-Day Program
Mon, Jan 8 - Sat, Jan 13
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: David Hoelzer

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

“Reports of prominent organizations being hacked and suffering irreparable reputational damage have become all too common. How can you prevent your company from becoming the next victim of a major cyber attack?”

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

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

SEC503: Intrusion Detection In-Depth delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence. You will learn about the underlying theory of TCP/IP and the most used application protocols, such as DNS and HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to master different open-source tools like tcpdump, Wireshark, Snort, Bro, tshark, and SiLK. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that you can transfer knowledge to execution. Basic exercises include assistive hints, while advanced options provide a more challenging experience for students who may already know the material or who have quickly mastered new material.

David Hoelzer  SANS Faculty Fellow

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

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

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

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

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

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

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

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

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

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

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

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

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/security-east-2018/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

“Overall this course has a ton of solid takeaways that can address your short-term and long-term goals as they apply to any information security role.”
- Mohammed Dennis, MTA

“Amazing course, I have a much deeper knowledge of network traffic and feel comfortable identifying malicious activity.”
- Paul Ladd, AMOCO FCU

www.sans.org/cyber-guardian

MEETS DoDD 8140 (8570) REQUIREMENTS

For this course
www.sans.org/8140
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 GIAC GPPEN, GCIAH, GCFA, GAWN, and GSEC certifications. Eric also blogs about information security at ericconrad.com. 

Eric Conrad  SANS Senior Instructor
**Course Day Descriptions**

511.1 HANDS ON: Current State Assessment, SOCs, and Security Architecture

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

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

511.2 HANDS ON: 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

511.3 HANDS ON: Network Security Monitoring

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

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

511.4 HANDS ON: Endpoint Security Architecture

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

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

511.5 HANDS ON: Automation and Continuous Security Monitoring

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

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

---

**You Will Be Able To**

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

---

“Just the background information about current threats is valuable information for anyone interested in security, but the detection info is getting it done!”

-JEFF MURRAY, CAMPELL SCIENTIFIC

---

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/security-east-2018/courses](http://www.sans.org/event/security-east-2018/courses)
Many organizations have logging capabilities but lack the people and processes to analyze them. In addition, logging systems collect vast amounts of data from a variety of data sources that require an understanding of the sources for proper analysis. This class is designed to provide individuals with training, methods, and processes for enhancing existing logging solutions. This class will also help you understand when, what, and why behind the logs. This is a lab-heavy course that utilizes SOF-ELK, a SANS-sponsored free Security Information and Event Management (SIEM) solution, to provide hands-on experience and the mindset for large-scale data analysis.

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

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

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

“One can conquer the SIEM world with this course.”
- Robert Lee Smith, RL Smith & Associates
555.1 HANDS ON: **SIEM Architecture and SOF-ELK**

Logging and analysis is a critical component in cyber network defense and allows for both reactive and proactive detection of adversarial activities. When properly utilized it becomes the backbone for agile detection and provides understanding to the overall environment. Logging and analysis products and techniques have been around for many years and are quickly gaining more and more functionality. This section will introduce free logging and analysis tools and focus on techniques to make sense of and augment traditional logs. It also covers how to handle the big data problem of handling billions of logs and how advances in free tools are starting to give commercial solutions a run for their money. Day one is designed to bring all students up to speed on SIEM concepts and to bring all students to a base level to carry them through the rest of the class. It is designed to also cover SIEM best practices. During day one we will be introducing Elasticsearch, Logstash, and Kibana within SOF-ELK and immediately go into labs to get students comfortable with ingesting, manipulating, and reporting on log data.

**Topics:** State of the SOC/SIEM; Log Monitoring; Logging Architecture; SIEM Platforms; Planning a SIEM; SIEM Architecture; Ingestion Techniques and Nodes; Data Queuing and Resiliency; Storage and Speed; Analytical Reporting

555.2 HANDS ON: **Service Profiling with SIEM**

A vast majority of network communication occurs over key network protocols, yet it is uncommon for organizations to use or collect these data. The sheer volume can be overwhelming. However, these common data sources provide an opportunity to identify modern day attacks. This section covers how to collect and handle this massive amount of data. Methods for collecting these logs through service logs such as from DNS servers will be covered as well as passive ways of pulling the same data from the network itself. Techniques will be demonstrated to augment and add valuable context to the data as they are collected. Finally, analytical principles will be covered for finding the needles in the stack of needles. We will cover how, even if we have the problem of searching through billions of logs, we can surface only meaningful items of interest. Active dashboards will be designed to quickly find the logs of interest and to provide analysts with additional context for what to do next.

**Topics:** Detection Methods and Relevance to Log Analysis; Analyzing Common Application Logs that Generate Tremendous Amounts of Data; Apply Threat Intelligence to Generic Network Logs; Active Dashboards and Visualizations

555.3 HANDS ON: **Advanced Endpoint Analytics**

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

**Topics:** Endpoint Logs

555.4 HANDS ON: **Baselining and User Behavior Monitoring**

Know thyself is often quoted to defenders as a key defense strategy, and yet this is one of the most difficult things to accomplish. Take something such as having a list of all assets in an organization and knowing if any non-company assets are on the network. The task sounds simple but ends up being incredibly difficult to maintain in today’s ever-evolving networks. This section focuses on applying techniques to automatically maintain a list of assets and their configurations as well as methods to distinguish if they are authorized or unauthorized. Key locations to provide high-fidelity data will be covered and techniques to correlate and combine multiple sources of data together will be demonstrated to build a master inventory list. Other forms of knowing thyself will be introduced such as gaining hands-on experience in applying network and system baselining techniques. We will monitor network flows and identify abnormal activity such as C2 beaconing as well as look for unusual user activity. Finally, we will apply large data analysis techniques to sift through massive amounts of endpoint data. This will be used to find things such as unwanted persistence mechanisms, dual-homed devices, and more.

**Topics:** Identify Authorized and Unauthorized Assets; Identify Authorized and Unauthorized Software; Baseline Data

555.5 HANDS ON: **Tactical SIEM Detection and Post-Mortem Analysis**

Multiple security devices exist but often are designed to be independent. Analysts are commonly divided into specialty areas and focus on their respective area such as a network intrusion detection system. However, alerts from a single security device lack context and are akin to the common analogy of “looking up from the bottom of a well.” This section focuses on combining multiple security logs for central analysis. More importantly, we will cover methods for combining multiple sources to provide improved context to analysts. We will also show how providing context with asset data can help prioritize analyst time, saving money and addressing risks that matter. After covering ways to optimize traditional security alerts, we will jump into new methods to utilize logging technology to implement virtual tripwires. While it would be ideal to prevent attackers from gaining access to your network, it is a given that at some point you will be compromised. However, compromise is just the beginning and not the end goal. Adversaries will crawl your systems and network to achieve their own ends. Knowing this, we will implement logging-based tripwires—and if a single one is stepped on, we can quickly detect it and respond to the adversary.

**Topics:** Centralize NIDS and HIDS Alerts; Analyze Endpoint Security Logs; Augment Intrusion Detection Alerts; Analyze Vulnerability Information; Correlate Malware Sandbox Logs with Other Systems to Identify Victims Across Enterprise; Monitor Firewall Activity; SIEM Tripwires; Post Mortem Analysis

555.6 HANDS ON: **Capstone: Design, Detect, Defend**

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

**Topics:** Defend-the-Flag Challenge – Hands-on Experience
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 on how to implement 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 threats 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.
You Will Be Able To

➤ Apply a security framework based on actual threats that is measurable, scalable, and reliable in stopping known attacks and protecting organizations’ important information and systems
➤ Understand the importance of each Control, how it is compromised if ignored, and explain the defensive goals that result in quick wins and increased visibility of networks and systems
➤ Identify and utilize tools that implement Controls through automation
➤ Learn how to create a scoring tool for measuring the effectiveness of each Control
➤ Employ specific metrics to establish a baseline and measure the effectiveness of the Controls
➤ Audit each of the Critical Controls with specific, proven templates, checklists, and scripts provided to facilitate the audit process

Course Day Descriptions

566.1 HANDS ON: 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

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

566.2 HANDS ON: 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

566.3 HANDS ON: 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

566.4 HANDS ON: 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

566.5 HANDS ON: 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)

“The 20 Controls presented in the course are requirements found in most regulated industries. I found the format and layout of each Control well explained and easy to follow.”

-JOSH ELLIS, IBERDROLA USA

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/security-east-2018/courses
One of today’s most rapidly evolving and widely deployed technologies is server virtualization. **SEC579: Virtualization and Software-Defined Security** is intended to help security, IT operations, and audit and compliance professionals build, defend, and properly assess both virtual and converged infrastructures, as well as understand software-defined networking and infrastructure security risks.

Many organizations are already realizing cost savings from implementing virtualized servers, and systems administrators love the ease of deployment and management of virtualized systems. More and more organizations are deploying desktop, application, and network virtualization as well. There are even security benefits of virtualization: easier business continuity and disaster recovery, single points of control over multiple systems, role-based access, and additional auditing and logging capabilities for large infrastructure.

With these benefits comes a dark side, however. Virtualization technology is the focus of many new potential threats and exploits, and it presents new vulnerabilities that must be managed. There are also a vast number of configuration options that security and system administrators need to understand, with an added layer of complexity that has to be managed by operations teams. Virtualization technologies also connect to network infrastructure and storage networks, and require careful planning with regard to access controls, user permissions, and traditional security controls.

In addition, many organizations are evolving virtualized infrastructure into private clouds using converged infrastructure that employs software-defined tools and programmable stack layers to control large, complex data centers. Security architecture, policies, and processes will need to be adapted to work within a converged infrastructure, and there are many changes that security and operations teams will need to accommodate to ensure that assets are protected.

This course will cover core operational functions such as secure network design and segmentation, building secure systems, and secure virtualization implementation and controls. Cutting-edge topics like software-defined networking and container technology will also be covered in detail with an emphasis on security techniques and controls. Security-focused virtualization, integration, and monitoring will be covered at length. Attacks and threats to virtual environments will be discussed, and students will learn how to perform vulnerability assessments and penetration tests in their virtual environments. We’ll also look at how to implement network intrusion detection and access controls, implement log and event management, and perform forensics and incident handling in virtual and converged data centers. Finally, students will learn how to perform technical audits and assessments of their in-house and public cloud environments, creating reports and documenting technical controls. This instruction will heavily emphasize automation and scripting techniques.

**Who Should Attend**

- Security personnel who are tasked with securing virtualization and private cloud infrastructure
- Network and systems administrators who need to understand how to architect, secure, and maintain virtualization and cloud technologies
- Technical auditors and consultants who need to gain a deeper understanding of VMware virtualization from a security and compliance perspective

“This course gave me a much better understanding of how to securely manage our virtualized infrastructure. I can use what I’ve learned the first day I get back to work.”

-Kris Normand, USAA

**Dave Shackleford  SANS Senior Instructor**

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

@daveshackleford
579.1 HANDS ON: Core Concepts of Virtualization Security

The first day of class will cover the foundations of virtualization infrastructure and different types of technology. We will define and clarify the differences between server, desktop, application, and storage virtualization, and dissect the various virtualization elements that make up the architecture one by one, with a focus on the security configurations that will help you create or revise your virtualization design to be as secure as possible.

**Topics:** Virtualization Components and Architecture Designs; Different Types of Virtualization, Ranging from Desktops to Servers and Applications; Hypervisor Lockdown Controls for VMware, Microsoft Hyper-V, and Citrix Xen; Virtual Machine Security Configuration Options, with a Focus on VMware VMX Files; Storage Security and Design Considerations; Locking Down Management Servers and Clients for vCenter, XenServer, and Microsoft SCVMM; Security Design Considerations for VDI

579.2 HANDS ON: Virtualization and Software-Defined Security Architecture and Design

Day 2 starts with several topics that round out our discussions on virtualization and infrastructure components, delving into container technology and converged infrastructure platforms and tools (along with security considerations for both). We’ll then begin our discussion of virtualization and software-defined architecture and networking. We’ll cover design concepts and models, network capabilities and models in virtual environments, with time devoted to virtual switches and other platforms, and look at how network security adapts to fit into a virtual infrastructure.

**Topics:** Container Technology Security Considerations; Converged Infrastructure Security Considerations; Defining Software-Defined Components and Architectural Models; Designing Security for Software-Defined Environments; Virtual Network Design Cases with Pros and Cons of Each; Virtual Switches and Port Groups, with Security Options Available; Commercial and Open-Source Virtual Switches Available, with Configuration Options; Segmentation Techniques, Including VLANs and PVLANs; Software-Defined Networking and Architecture; Network Isolation and Access Control; Adapting Firewalls, IPS, Proxies, and More to Virtual Environments; Products and Capabilities Available Today

579.3 HANDS ON: Virtualization Threats, Vulnerabilities, and Attacks

This session will delve into the offensive side of security specific to virtualization and cloud technologies. We will first examine a number of specific attack scenarios, then go through the entire penetration testing and vulnerability assessment lifecycle, with an emphasis on virtualization tools and technologies. We’ll progress through scanners and how to use them to assess virtual systems, then turn to virtualization exploits and attack toolkits that can be easily added into existing penetration test regimens. We will also cover some specific techniques that may help in cloud environments, providing examples of scenarios where certain tools and exploit are less effective or more risky to use than others.

**Topics:** Threats and Attack Research Related to Virtualization Infrastructure; Attack Models That Pertain to Virtualization and Cloud Environments; Threat Modeling for Virtualization and Software-Defined Technology; Specific Virtualization Platform Attacks and Exploits; Pen Testing Cycles with a Focus on Virtualization Attack Types; Password Attacks Against Virtualization and Software-Defined Platforms; How to Modify Vulnerability Management Processes and Scanning Configuration to Get the Best Results in Virtualized Environments; How to Use Attack Frameworks Like VASTO to Exploit Virtualization Systems

579.4 HANDS ON: Defending Virtualization and Software-Defined Technologies

We will start off with an analysis of anti-malware techniques, looking at traditional antivirus, whitelisting, and other tools and techniques to combat malware, with a specific eye toward virtualization and converged environments. Then we will turn to intrusion detection, monitoring traffic and learning about logs and log management in virtual environments. The second half of this session will focus on incident response and forensics in a virtualized or converged infrastructure and how students can adapt forensics processes and tools to work in virtual environments.

**Topics:** Data Protection in Virtual and Converged Environment; Identity and Access Management in Virtual and Software-Defined Environments; How to Implement Intrusion Detection Tools and Processes in a Virtual Environment; What Kinds of Logs and Logging Are Most Critical for Identifying Attacks and Live Incidents in Virtual Environments; How Anti-Malware Tools Function in Virtual Environments; How the Six-Step Incident Response Process Can Be Modified and Adapted to Work with Virtual Infrastructure; What Kinds of Incidents to Look for Within Virtual Environments, and What the Warning Signs Are; Processes and Procedures to Build and Grow Incident Response Capabilities for Virtual Environments; How Forensics Processes and Tools Should Be Used and Adapted for Virtual Systems; What Tools Are Best to Get the Most Accurate Results from Virtual Machine System Analysis?; How to Most Effectively Capture Virtual Machines for Forensic Evidence Analysis; What Can Be Done to Analyze Hypervisor Platforms, and What Does the Future Hold for VM Forensics?

579.5 HANDS ON: Virtualization Operations, Auditing, and Monitoring

Today’s session will start off with a lively discussion on virtualization assessment and auditing. We will cover the top virtualization configuration and hardening guides from DISA, CIS, Microsoft, and VMware, and talk about the most critical information to take away from these guides and implement. Students will learn to implement audit and assessment techniques by scripting with the VI CLI, as well as some general shell scripting! We will look at automation and orchestration tools and techniques that can help to streamline and manage configuration and auditing (examples include Chef, Puppet, and more), as well as monitoring techniques that provide a feedback loop.

**Topics:** Key Configuration Controls from the Leading DISA, CIS, VMware, and Microsoft Hardening Guides; Sound Configuration Management and Patching in Virtual Infrastructure; Scripting Techniques in VI CLI and PowerShell for Automating Audit and Assessment Processes; Sample Scripts That Help Implement Key Audit Functions; Automation and Orchestration with Puppet, Chef, ManageEngine, etc.; Full Hardening-Guide-Scripted Audit

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/security-east-2018/courses](http://www.sans.org/event/security-east-2018/courses)
Network Penetration Testing and Ethical Hacking

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 more than 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 masterfully.

**Learn the best ways to test your own systems before the bad guys attack.**

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test – and on the last day of the course you’ll do just that. After building your skills in comprehensive and challenging labs over five days, the course culminates with a final full-day, 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 knowledge you’ve mastered in this course.

**You will bring comprehensive penetration testing and ethical hacking know-how back to your organization.**

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

**Bryce Galbraith  SANS Principal Instructor**

As a contributing author to the internationally bestselling book *Hacking Exposed: Network Security Secrets & Solutions*, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. Bryce has held security positions at global ISPs and Fortune 500 companies, he was a member of Foundstone’s renowned penetration testing team, and he served as a senior instructor and co-author of Foundstone’s Ultimate Hacking: Hands-On course series. Bryce is currently the owner of Layered Security, where he provides specialized vulnerability assessment and penetration testing services for clients. He teaches several of the SANS Institute’s most popular courses and develops curricula around current topics. He has taught the art of ethical hacking and countermeasures to thousands of IT professionals from a “who’s who” of top companies, financial institutions, and government agencies around the globe. Bryce is an active member of several security-related organizations, holds several security certifications, and speaks at conferences around the world.  @brycegalbraith
In this section of the course, you will develop the skills needed to conduct a best-of-breed, high-value penetration test. We will go in-depth on how to build 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 will 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 the anti-virus tools the organization relies on.

**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

**560.2 HANDS ON: In-Depth Scanning**

We next focus on the vital task of mapping the target environment’s attack surface by creating a comprehensive inventory of machines, accounts, and potential vulnerabilities. We will 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 will also conduct a deep dive into some of the most useful tools available to pen testers today for formulating packet capture: Scapy and Netcat. We finish the day 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 will examine the best ways to conduct your scans safely and efficiently.

**Topics:** Tips for Awesome Scanning; Tcpdump for the Pen Tester; Nmap In-Depth; 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

**560.3 HANDS ON: 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/Stages; Strategies and Tactics for Anti-Virus Evasion; In-Depth Meterpreter Analysis, Hands-On; Implementing Port Forwarding Relays for Merciless Pivots; How to Leverage Shell Access of a Target Environment

**560.4 HANDS ON: Post-Exploitation and Merciless Pivoting**

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

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

**560.5 HANDS ON: In-Depth Password Attacks and Web App Pen Testing**

In this section of the course, 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 see how Rainbow Tables really work to make password cracking much more efficient, 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 Rainbow Tables to Maximum Effectiveness; Pass-the-Hash Attacks with Metasploit and More; Finding and Exploiting Cross-Site Scripting; Cross-Site Request Forgery; SQL Injection; Leveraging SQL Injection to Perform Command Injection; Maximizing Effectiveness of Command Injection Testing

**560.6 HANDS ON: Penetration Test and Capture-the-Flag Workshop**

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 so far in a full-day, 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 with a team 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; Scanning; Exploitation; Post-Exploitation; Merciless Pivoting; Analyzing Results
Web App Penetration Testing and Ethical Hacking

Six-Day Program
Mon, Jan 8 - Sat, Jan 13
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Moses Hernandez

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

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

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

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

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

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

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

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

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

Moses Hernandez  **SANS Certified Instructor**

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

542.1 HANDS ON: Introduction and Information Gathering

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

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

542.2 HANDS ON: Configuration, Identity, and Authentication Testing

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

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

542.3 HANDS ON: Injection

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

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

542.4 HANDS ON: JavaScript 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: Cross-Site Scripting (XSS); Cross-Site Request Forgery (CSRF); Session Flaws; Session Fixation; AJAX; Logic Attacks; Data Binding Attacks; Automated Web Application Scanners; w3af; XML and JSON

542.5 HANDS ON: CSRF, Logic Flaws, and Advanced Tools

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

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

542.6 HANDS ON: Capture the Flag

On day six, students form teams and compete in a web application penetration testing tournament. This NetWars-powered Capture-the-Flag exercise 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.

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/security-east-2018/courses
Automating Information Security with Python

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

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

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

Finally, what do you do when “off-the-shelf” tools and exploits fall short? As a penetration tester you need to evolve as quickly as the threats you are paid to emulate, so the answer is simple, if you have the skills: You write your own tool.

Writing a tool is easier said than done, right? Not really. Python is a simple, user-friendly language that is designed to make automating tasks that security professionals perform quick and easy. Whether you are new to coding or have been coding for years, SEC573: Automating Information Security with Python will have you creating programs to make your job easier and make you more efficient. This self-paced class starts from the very beginning assuming you have no prior experience or knowledge of programming. We cover all of the essentials of the language up front. If you already know the essentials, you will find that the pyWars lab environment allows advanced developers to quickly accelerate to more advanced material in the class. The self-paced style of the class will meet you where you are to let you get the most out of the class. Beyond the essentials we discuss file analysis, packet analysis, forensics artifact carving, networking, database access, website access, process execution, exception handling, object-oriented coding, and more.

This course 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 in automating the daily routine of today’s information security professional, and in achieving more value in less time. Again and again, organizations serious about security don’t evolve with them, we’ll become ineffective and irrelevant, unable to provide the vital defenses our organizations increasingly require.

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

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 Python for Penetration testers course (SEC573). 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.

“Excellent class for beginners and advanced alike. It has something for everyone.”
-Mike Perez, Disney

“SEC573 gave me exposure to tools and techniques I wouldn’t have normally considered, but now are part of my arsenal.”
-Allen C., Department of Defense
You Will Be Able To

- Develop forensics tool to carve artifacts from forensics evidence for which no other tool exists or use third-party modules for well-known artifacts that hide evidence relevant to your investigations.
- Create offensive tools to automate the analysis of log file and network packets using hash team techniques to track down attackers in your network.
- Implement custom whitelisting, blacklisting, signature detection, long tail and short tail analysis, and other data analysis techniques to find attacks overlooked by conventional methods.
- Write penetration testing tools including several backdoors with features like process execution, upload and download payloads, port scanning and more.
- Build essential tools that evade antivirus software and allow you to establish that required foothold inside your target.
- Understand Python coding fundamentals required to automate common information security tasks. Language essentials like variables, loops, if-then-else, logic, file operations, command line arguments, and debugging are all covered assuming no prerequisite knowledge.
- Tap into the wealth of existing Python modules to complete tasks using Regular Expressions, Database interactions with SQL, IP Networking, and Exception handling.
- Interact with websites using Requests, Packet Analysis, Packet reassembly techniques, and much more.

You Will Receive

- A virtual machine with sample code and working examples
- A copy of the book Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers, which shows how to forge your own weapons using the Python programming language
- MP3 audio files of the complete course lecture

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/security-east-2018/courses](http://www.sans.org/event/security-east-2018/courses)
This course is designed as a logical progression point for those who have completed SEC560: Network Penetration Testing and Ethical Hacking, or for those with existing penetration testing experience. Students with the prerequisite knowledge to take this course will walk through dozens of real-world attacks used by the most seasoned penetration testers. The methodology of a given attack is discussed, followed by exercises in a real-world lab environment to solidify advanced concepts and allow for the immediate application of techniques in the workplace. Each day includes a two-hour evening bootcamp to allow for additional mastery of the techniques discussed and even more hands-on exercises. A sample of topics covered includes weaponizing Python for penetration testers, attacks against network access control (NAC) and VLAN manipulation, network device exploitation, breaking out of Linux and Windows restricted environments, IPv6, Linux privilege escalation and exploit-writing, testing cryptographic implementations, fuzzing, defeating modern OS controls such as ASLR and DEP, return-oriented programming (ROP), Windows exploit-writing, and much more!

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

SEC660 starts off by introducing the advanced penetration concept, and provides an overview to help prepare students for what lies ahead. The focus of day one is on network attacks, an area often left untouched by testers. Topics include accessing, manipulating, and exploiting the network. Attacks are performed against NAC, VLANs, OSPF, 802.1X, CDP, IPv6, VOIP, SSL, ARP, SNMP, and others.

Day two starts off with a technical module on performing penetration testing against various cryptographic implementations. The rest of the day is spent on network booting attacks, escaping Linux restricted environments such as chroot, and escaping Windows restricted desktop environments. Day three jumps into an introduction of Python for penetration testing, Scapy for packet crafting, product security testing, network and application fuzzing, and code coverage techniques. Days four and five are spent exploiting programs on the Linux and Windows operating systems. You will learn to identify privileged programs, redirect the execution of code, reverse-engineer programs to locate vulnerable code, obtain code execution for administrative shell access, and defeat modern operating system controls such as ASLR, canaries, and DEP using ROP and other techniques. Local and remote exploits, as well as client-side exploitation techniques, are covered. The final course day is dedicated to numerous penetration testing challenges requiring you to solve complex problems and capture flags.

“I am very impressed at how well the instructor conveyed the material in SEC660. This is a hard topic, but I have a lot I can take home with me and practice. This material puts me at that next level.”

-Adam Logue, Spectrum Health

Tim Medin  SANS Certified Instructor

Tim Medin is a senior technical analyst at Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through the course of his career, Tim has performed penetration tests on a wide range of organizations and technologies. Prior to Counter Hack, Tim was a senior security consultant for FishNet Security, where most of his focus was on penetration testing. He gained information security experience in a variety of industries including previous positions in control systems, higher education, financial services, and manufacturing. Tim regularly contributes to the SANS Penetration Testing Blog (pen-testing.sans.org/blog) and the Command Line Kung Fu Blog (blog.commandlinekungfu.com). He is also project lead for the Laudanum Project, a collection of injectable scripts designed to be used in penetration testing.  @timmedin
Course Day Descriptions

660.1 HANDS ON: Network Attacks for Penetration Testers

Day one serves as an advanced network attack module, building on knowledge gained from SEC560. The focus will be on obtaining access to the network, manipulating the network to gain an attack position for eavesdropping and attacks, and for exploiting network devices; leveraging weaknesses in network infrastructure; and taking advantage of client frailty.

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

660.2 HANDS ON: Crypto and Post Exploitation

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

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

660.3 HANDS ON: Python, Scapy, and Fuzzing

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

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

660.4 HANDS ON: Exploiting Linux for Penetration Testers

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

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

660.5 HANDS ON: Exploiting Windows for Penetration Testers

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

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

660.6 HANDS ON: Capture-the-Flag Challenge

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

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/security-east-2018/courses
FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting

FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting will help you to:

- Detect how and when a breach occurred
- Identify compromised and affected systems
- Determine what attackers took or changed
- Contain and remediate incidents
- Develop key sources of threat intelligence
- Hunt down additional breaches using knowledge of the adversary

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

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

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 hactivism. Constantly updated, FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting addresses today’s incidents by providing hands-on incident response and threat hunting tactics and techniques that elite responders and hunters are successfully using to detect, counter, and respond to real-world breach cases.

“Great content that will directly help improve existing and define new forensics processes in my organization.”

- Pete Ryan, Serco

Rob Lee  SANS Faculty Fellow

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.” @robllee & @sansforensics

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

508.1 HANDS ON: Advanced Incident Response and Threat Hunting
Incident responders and threat hunters should be armed with the latest tools, memory analysis techniques, and enterprise methodologies to identify, track, and contain advanced adversaries and to remediate incidents. Incident response and threat hunting analysts must be able to scale their analysis across thousands of systems in their enterprise. This section examines the six-step incident response methodology as it applies to an enterprise’s response to a targeted attack.

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

508.2 HANDS ON: Memory Forensics in Incident Response & Threat Hunting
Now a critical component of many incident response and threat hunting teams that detect advanced threats in their organization, memory forensics has come a long way in just a few years. Memory forensics can be extraordinarily effective at finding evidence of worms, rootkits, and advanced malware used by an APT group of attackers. This extremely popular section will introduce some of the most capable tools available and give you a solid foundation to add core and advanced memory forensic skills to your incident response and forensics capabilities.

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

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

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

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

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

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

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

508.6 HANDS ON: The APT Incident Response Challenge
This incredibly rich and realistic enterprise intrusion exercise is based on a real-world advanced persistent threat (APT) group. It brings together techniques learned earlier in the week and tests your newly acquired skills in a case that simulates an attack by an advanced adversary. The challenge brings it all together using a real intrusion into a complete Windows enterprise environment. You will be asked to uncover how the systems were compromised in the initial intrusion, find other systems the adversary moved 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

You Will Be Able To

▶ Learn and master the tools, techniques, and procedures necessary to effectively hunt, detect, and contain a variety of adversaries and to remediate incidents
▶ Detect and hunt unknown live, dormant, and custom malware in memory across multiple Windows systems in an enterprise environment
▶ Hunt through and perform incident response across hundreds of unique systems simultaneously using F-Response Enterprise and the SIFT Workstation
▶ Identify and track malware beaconing outbound to its command and control (C2) channel via memory forensics, registry analysis, and network connection residue
▶ Determine how the breach occurred by identifying the beachhead and spear phishing attack mechanisms
▶ Target advanced adversary anti-forensics techniques like hidden and time-stomped malware, along with utility-ware used to move in the network and maintain an attacker’s presence
▶ Use memory analysis, incident response, and threat hunting tools in the SIFT Workstation to detect hidden processes, malware, attacker command lines, rootkits, network connections, and more
▶ Track user and attacker activity second-by-second on the system you are analyzing through in-depth timeline and super-timeline analysis
▶ Recover data cleared using anti-forensics techniques via Volume Shadow Copy and Restore Point analysis
▶ Identify lateral movement and pivots within your enterprise, showing how attackers transition from system to system without detection
▶ Understand how the attacker can acquire legitimate credentials — including domain administrator rights — even in a locked-down environment
▶ Track data movement as the attackers collect critical data and shift them to exfiltration collection points
▶ Recover and analyze archives and .rar files used by APT-like attackers to exfiltrate sensitive data from the enterprise network
▶ Use collected data to perform effective remediation across the entire enterprise
▶ Use collected data to perform effective remediation across the entire enterprise
Cyber Threat Intelligence

Make no mistake: current network defense, threat hunting, and incident response practices contain a strong element of intelligence and counterintelligence that cyber analysts must understand and leverage in order to defend their networks, proprietary data, and organizations.

FOR578: Cyber Threat Intelligence will help network defenders, threat hunting teams, and incident responders to:

- Understand and develop skills in tactical, operational, and strategic-level threat intelligence
- Generate threat intelligence to detect, respond to, and defeat advanced persistent threats (APTs)
- Validate information received from other organizations to minimize resource expenditures on bad intelligence
- Leverage open-source intelligence to complement a security team of any size
- Create Indicators of Compromise (IOCs) in formats such as YARA, OpenIOC, and STIX

The collection, classification, and exploitation of knowledge about adversaries – collectively known as cyber threat intelligence – gives network defenders information superiority that is used to reduce the adversary’s likelihood of success with each subsequent intrusion attempt. Responders need accurate, timely, and detailed information to monitor new and evolving attacks, as well as methods to exploit this information to put in place an improved defensive posture.

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

During a targeted attack, an organization needs a top-notch and cutting-edge threat hunting or incident response team armed with the threat intelligence necessary to understand how adversaries operate and to counter the threat. FOR578: Cyber Threat Intelligence will train you and your team in the tactical, operational, and strategic-level cyber threat intelligence skills and tradecraft required to make security teams better, threat hunting more accurate, incident response more effective, and organizations more aware of the evolving threat landscape.

Robert M. Lee  SANS Certified Instructor

Robert is the CEO and founder of his own company, Dragos, Inc., a firm that provides cybersecurity solutions for industrial control system networks. Robert got his start in information security making small control systems for humanitarian missions. He joined the U.S. Air Force and became a cyberspace warfare operations officer in the U.S. intelligence community. In that role, he created and led a mission examining nation-states targeting ICS, the first mission of its kind in the U.S. intelligence community. When the Ukraine power grid went down due to a cyber attack in 2015, Robert helped form a specialized team to analyze the event, then passed the information on to the impacted parties as well as the U.S. government and private sector. He and his team also analyzed the malware from the 2016 cyber-attack on Ukraine’s Kiev substation and dubbed it CRASHOVERRIDE as the first ever malware tailored to specifically disrupt electric 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
Course Day Descriptions

578.1 HANDS ON: Cyber Threat Intelligence

Cyber threat intelligence is a rapidly growing field. However, intelligence was a profession long before the word “cyber” entered the lexicon. Understanding the key points regarding intelligence terminology, tradecraft, and impact is vital to understanding and using cyber threat intelligence. This section introduces students to the most important concepts of intelligence, analysis tradecraft, and levels of threat intelligence, and the value they can add to organizations. As with all sections, the day includes immersive hands-on labs to ensure that students have the ability to turn theory into practice.

Topics: Case-Study: Carbanak, “The Great Bank Robbery”; Understanding Intelligence; Understanding Cyber Threat Intelligence; Tactical Threat Intelligence Introduction; Operational Threat Intelligence Introduction; Strategic Threat Intelligence Introduction

578.2 HANDS ON: Tactical Threat Intelligence: Kill Chain for Intrusion Analysis

Tactical cyber threat intelligence requires that analysts extract and categorize indicators and adversary tradecraft from intrusions. These actions enable all other levels of threat intelligence by basing intelligence on observations and facts that are relevant to the organization. One of the most commonly used models for assessing adversary intrusions is the “kill chain.” This model is a framework to understand the steps an adversary must accomplish to be successful. This section will help tactical threat intelligence develop the skills required to be successful by using the kill chain as a guide. Students will then pivot into open-source intelligence-gathering tradecraft to enrich their understanding of the analyzed intrusion. The section walks students through multi-phase intrusions from initial notification of adversary activity to the completion of analysis of the event. The section also highlights the importance of this process to structuring and defining adversary campaigns.

Topics: Kill Chain Courses of Action; Tactical Threat Intelligence Requirements; Kill Chain Deep Dive; Handling Multiple Kill Chains; Pivoting to Open-Source Intelligence

578.3 HANDS ON: Tactical/Operational Threat Intelligence: Campaigns and Open-Source Intelligence

Developing an understanding of adversary campaigns and tradecraft requires piecing together individual intrusions and data points. Organizations of any size will need to complement what they know from internal analysis with open-source intelligence (OSINT) to enrich and validate the information. This allows security personnel to understand dedicated adversaries more fully and consistently defend their environments. In this section, students learn what campaigns are, why they are important, and how to define them. From this baseline intelligence, gaps and collection opportunities are identified for fulfillment via open-source resources and methods. Common types and implementations of open-source data repositories, as well as their use, are explored in-depth through classroom discussion and exercises. These resources can produce an enormous volume of intelligence about intrusions, which may contain obscure patterns that further elucidate campaigns or actors. Tools and techniques to expose these patterns within the data through higher-order analysis will be demonstrated in narrative and exercise form. The application of the resulting intelligence will be articulated for correlation, courses of action, campaign assembly, and more.

Topics: Case Study: Axiom; OSINT Pivoting, Link Analysis, and Domains; OSINT From Malware; Case Study: GlassRAT; Intelligence Aggregation and Data Visualization; Defining Campaigns; Communicating About Campaigns

578.4 HANDS ON: Operational Threat Intelligence: Sharing Intelligence

Many organizations seek to share intelligence but often falter in understanding the value of shared intelligence, its limitations, and the right formats to choose for each audience. This section will focus on identifying both open-source and professional tools that are available for students as well as sharing standards for each level of cyber threat intelligence both internally and externally. Students will learn about YARA and generate YARA rules to help incident responders, security operations personnel, and malware analysts. They will gain hands-on experience with STIX and understand the CybOX and TAXII frameworks for sharing information between organizations. Finally, the section will focus on sharing intelligence at the strategic level in the form of reports, briefings, and analytical assessments in order to help organizations make required changes to counter persistent threats and safeguard business operations.

Topics: Storing Threat Intelligence; Sharing: Tactical; Case Study: Sony Attack; Sharing: Operational; Sharing: Strategic

578.5 HANDS ON: Strategic Threat Intelligence: Higher-Order Analysis

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

Topics: Logical Fallacies and Cognitive Biases; Analysis of Competing Hypotheses; Case Study: Stuxnet; Human Elements of Attribution; Nation-State Attribution; Case Study: Sofacy; A Look Backward; Case Study: Cyber Attack on the Ukrainian Power Grid; Active Defense

Author Statements

The author team of Mike Cloppert, Chris Sperry, and Robert M. Lee originally developed FOR578 with the understanding that the community was in need of a single concise collection of tradecraft. Cloppert and Sperry initiated the development of the course with the understanding that their schedules would not permit them to be able to constantly teach it. However, it was through their thought leadership that the class has become what it is today. Their influence on the course development remains, and SANS thanks them for their leadership.

“When considering the value of threat intelligence, most individuals and organizations ask themselves three questions: What is threat intelligence? When am I ready for it? How do I use it? This class answers these questions and more at a critical point in the development of the field of threat intelligence in the wider community. The course will empower analysts of any technical background to think more critically and be prepared to face persistent and focused threats.”

- Robert M. Lee

“When threat intelligence is a powerful tool in the hands of a trained analyst. It can provide insight to all levels of a security program, from security analysts responding to tactical threats against the network to executives reporting strategic-level threats to the Board of Directors. This course will give students an understanding of the role of threat intelligence in security operations and how it can be leveraged as a game-changing resource to combat an increasingly sophisticated adversary.”

-Rebekah Brown

“Before threat intelligence was a buzzword, it was something we all used to just do as part of incident response. But I'll admit that most of us used to do it badly. Or more accurately, ad hoc at best. We simply lacked structured models for intrusion analysis, campaign tracking, and consistent reporting of threats. Today, we need analysts trained in intelligence analysis techniques ready to perform proper campaign modeling, attribution, and threat analysis. The Cyber Threat Intelligence course teaches students all of that, as well as how to avoid cognitive biases in reporting and the use of alternative competing hypotheses in intelligence analysis. These are critical skills that most in industry today absolutely lack.”

-Jake Williams

★ II Bundle ON Demand WITH THIS COURSE

www.sans.org/ondemand
Reverse-Engineering Malware: Malware Analysis Tools and Techniques

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

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

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

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

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

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

"Extremely heavy concepts in a way most people can understand is nearly miraculous."

- Jimmy Simpson, SECTI

Jake Williams  SANS Certified Instructor

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

@MalwareJake
Course Day Descriptions

610.1 HANDS ON: 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 (RE)Mux 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

610.2 HANDS ON: Reversing Malicious Code

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

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

610.3 HANDS ON: 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

610.4 HANDS ON: 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

610.5 HANDS ON: Examining Self-Defending Malware

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

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

610.6 HANDS ON: 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

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/security-east-2018/courses 37
MGT512

SANS Security Leadership Essentials for Managers with Knowledge Compression™

This course has extended hours

Who Should Attend

▷ All newly appointed information security officers
▷ Technically skilled administrators who have recently been given leadership responsibilities
▷ Seasoned managers who want to understand what their technical people are telling them

“MGT512 is one of the most valuable courses I’ve taken with SANS. It really did help bridge the gap from security practitioner to security orchestrator. Truly a gift!”
- John Madick, Epic Systems, Inc.

This completely updated course is designed to empower advancing managers who want to 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. Lecture sections are intense; the most common student comment is that it’s like drinking from a fire hose. The diligent manager will learn vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to U.S. government managers and supporting contractors.

Essential security topics covered in this management track include network fundamentals and applications, power, cooling and safety, architectural approaches to defense in depth, cyber attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, web application security, and offensive and defensive information warfare, culminating with our management practicum. The material uses Knowledge Compression™ special charts, and other proprietary SANS techniques to help convey the key points of critical slides and keep the information flow rate at a pace senior executives demand every teaching hour of the course. The course has been evaluated and approved by CompTIA’s CAQC program for Security+ 2008 to ensure that managers and their direct reports have a common baseline for security terminology and concepts. You will be able to put what you learn into practice the day you get back into the office.

Knowledge Compression™

Maximize your learning potential!

Knowledge Compression™ is an optional add-on feature to a SANS class that aims to maximize the absorption and long-term retention of large amounts of data over a relatively short period of time. Through the use of specialized training materials, in-class reviews, examinations and test-taking instruction, Knowledge Compression™ ensures students have a solid understanding of the information presented to them. By attending classes that feature this advanced training product, you will experience some of the most intense and rewarding training programs SANS has to offer, in ways that you never thought possible!

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 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 and 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.
512.1 Managing the Enterprise, Planning, Network, and Physical Plant

The course starts with a whirlwind tour of the information an effective IT security manager must know to function in today’s environment. We will cover safety, physical security, and how networks and the related protocols like TCP/IP work, and equip you to review network designs for performance, security, vulnerability scanning, and return on investment. You will learn more about secure IT operations in a single day than you ever thought possible.

Topics: Budget Awareness and Project Management; The Network Infrastructure; Computer and Network Addressing; IP Terminology and Concepts; Vulnerability Management; Managing Physical Safety, Security, and the Procurement Process

512.2 IP Concepts, Attacks against the Enterprise, and Defense-in-Depth

You will learn about information assurance foundations, which are presented in the context of both current and historical computer security threats, and how they have impacted confidentiality, integrity, and availability. You will also learn the methods of the attack and the importance of managing attack surface.

Topics: Attacks Against the Enterprise; Defense in Depth; Managing Security Policy; Access Control and Password Management

512.3 Secure Communications

This course section examines various cryptographic tools and technologies and how they can be used to secure a company’s assets. A related area called steganography, or information hiding, is also covered. Learn how malware and viruses often employ cryptographic techniques in an attempt to evade detection. We will learn about managing privacy issues in communications and investigate web application security.

Topics: Cryptography; Wireless Network Security; Steganography; Managing Privacy; Web Communications and Security; Operations Security, Defensive and Offensive Methods

512.4 The Value of Information

On this day we consider the most valuable resource an organization has: its information. You will learn about intellectual property, incident handling, and how to identify and better protect the information that is the real value of your organization. We will then formally consider how to apply everything we have learned, as well as practice briefing management on our risk architecture.

Topics: Managing Intellectual Property; Incident Handling Foundations; Information Warfare; Disaster Recovery/Contingency Planning; Managing Ethics; IT Risk Management

512.5 Management Practicum

On the fifth and final day, we pull it all together and apply the technical knowledge to the art of management. The management practicum covers a number of specific applications and topics concerning information security. We’ll explore proven techniques for successful and effective management, empowering you to immediately apply what you have learned your first day back at the office.

Topics: The Mission; Globalization; IT Business and Program Growth; Security and Organizational Structure; Total Cost of Ownership; Negotiations; Fraud; Legal Liability; Technical People

Security leaders and managers earn the highest salaries (well into six figures) in information security and are near the top of IT. Needless to say, to work at that compensation level, excellence is demanded. These days, security managers are expected to have domain expertise as well as the classic project management, risk assessment, and policy review and development skills.
SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that is specifically designed to prepare students to successfully pass the CISSP® exam.

MGT414 focuses solely on the eight domains of knowledge as determined by (ISC)² that form a critical part of the CISSP® exam. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

After completing the course students will have:

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

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

“This is the most complete training to get CISSP® certified. No doubt.” - PIERRE DEFROY, JEAN COUTU

“David was awesome! He showed great depth of knowledge, and was able to convey that in easy-to-understand ways.” - KEVIN SPINNATO, UPI

“This training was a comprehensive overview of all topics covered in the CISSP® exam. All in attendance were there for a common goal, including the instructor. It was easy to follow, and the real-world examples given were priceless.”

-RON PINNOCK, NAVY EXCHANGE SERVICE COMMAND

David R. Miller  SANS Certified Instructor

David 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 through policy writing; network architecture design including security zones; development of incident response teams and programs; design and implementation of public key infrastructures; security awareness training programs; specific security solution designs like secure remote access and strong authentication architectures; disaster recovery planning and business continuity planning; and pre-audit compliance gap analysis and remediation. 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

Six-Day Program
Mon, Jan 8 - Sat, Jan 13
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPEs
Laptop NOT Needed
Instructor: David R. Miller

This course has evening bootcamp sessions

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

Register at www.sans.org/security-east     |     301-654-SANS (7267)
414.1 Introduction; Security and Risk Management
On the first day of training for the CISSP® exam, MGT414 introduces the specific requirements needed to obtain certification. The exam update will be discussed in detail. We will cover the general security principles needed to understand the eight domains of knowledge, with specific examples for each domain. The first of the eight domains, Security and Risk Management, is discussed using real-world scenarios to illustrate the critical points.

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

414.2 Asset Security and Security Engineering – Part 1
Understanding asset security is critical to building a solid information security program. The Asset Security domain, the initial focus of today’s course section, describes data classification programs, including those used by both governments and the military as well as the private sector. We will also discuss ownership ranging from business/mission owners to data and system owners. We will examine data retention and destruction in detail, including secure methods for purging data from electronic media. We then turn to the first part of the Security Engineering domain, including new topics for the 2017 exam such as the Internet of Things, Trusted Platform Modules, Cloud Security, and much more.

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

414.3 Security Engineering – Part 2; Communication and Network Security
This section continues the discussion of the Security Engineering domain, including a deep dive into cryptography. The focus is on real-world implementation of core cryptographic concepts, including the three types of cryptography: symmetric, asymmetric, and hashing. Salts are discussed, as well as rainbow tables. We will round out Domain 3 with a look at physical security before turning to Domain 4, Communication and Network Security. The discussion will cover a range of protocols and technologies, from the Open Systems Interconnection (OSI) model to storage area networks.

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

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

Topics: Domain 5: Identity and Access Management

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

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

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

Topics: Domain 8: Software Development Security
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 undertake three critical tasks:

• 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.

How the Course Works
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.

Ted Demopoulos  SANS Principal Instructor
Ted Demopoulos’ first significant exposure to computers was in 1977 when he had unlimited access to his high school’s PDP-11 and hacked at it incessantly. He consequently almost flunked out but learned he liked playing with computers a lot. His business pursuits began in college and have been continuous ever since. His background includes over 25 years of experience in information security and business, including 20+ years as an independent consultant. Ted helped start a successful information security company, was the CTO at a “textbook failure” of a software startup, and has advised several other businesses. Ted is a frequent speaker at conferences and other events, quoted often by the press. He also has written two books on social media, has an ongoing software concern in Austin, Texas in the virtualization space, and is the recipient of a Department of Defense Award of Excellence. In his spare time, he is also a food and wine geek, and enjoys flyfishing and playing with his children.  @TedDemop
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

“This course has a lot of value and information for anyone tasked with developing security strategy and communicating value propositions.”

-MOBOLAJI MOYOSORE, TESORO CORPORATION

“MGT514 targets the exact information needs of my organization.”

-TIM HOFFMAN, UCSF

“This course is highly recommended for all cybersecurity leaders as it provides great structure and frameworks about managing cyber teams, and building strategic plans that map to needs of business.”

-KHASH KIANI, ED CS HPE CYBER SECURITY

Course Day Descriptions

514.1 Strategic Planning Foundations
Creating strategic plans for security requires a fundamental understanding of the business and a deep understanding of the threat landscape.

Topics: Vision & Mission Statements; Stakeholder Management; PEST Analysis; Porter’s Five Forces; Threat Actors; Asset Analysis; Threat Analysis

514.2 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

514.3 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

514.4 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

514.5 Strategic Planning Workshop
Using the case study method, students will work through real-world scenarios by applying the skills and knowledge learned throughout the course. Case studies are taken directly from Harvard Business School, the pioneer of the case-study method, and focus specifically on information security management and leadership competencies. The Strategic Planning Workshop serves as a capstone exercise for the course, allowing students to synthesize and apply concepts, management tools, and methodologies learned in class.

Topics: Creating a Security Plan for the CEO; Understanding Business Priorities; Enabling Business Innovation; Working with BYOD; Effective Communication; Stakeholder Management

“This training was valuable because it helped me examine myself from an outside point of view.”

-DJ, ZOETIS
Secure DevOps and Cloud Application Security  NEW!

This course covers how developers and security professionals can build and deliver secure software using DevOps and cloud services, specifically Amazon Web Services (AWS). It explains how principles, practices, and tools in DevOps and AWS can be leveraged to improve the reliability, integrity, and security of applications.

The first two days of the course cover how Secure DevOps can be implemented using lessons from successful DevOps security programs. Students build a secure DevOps CI/CD toolchain and understand how code is automatically built, tested, and deployed using popular open-source tools such as git, Puppet, Jenkins, and Docker. In a series of labs you learn to inject security into your CI/CD toolchain using various security tools, patterns, and techniques.

The final three days of the course cover how developers and security professionals can utilize AWS services to build secure software in the cloud. Students leverage the CI/CD toolchain to push application code directly to the cloud instead of to local servers on their class virtual machines. Students analyze and fix applications hosted in the cloud using AWS services and features such as API Gateway, IAM, signed cookies, Security Token Service, autoscaling, KMS, encryption, WAF, and Lambda for Serverless computing.

The course makes extensive use of open-source materials and tooling for automated configuration management (“Infrastructure as Code”), Continuous Integration, Continuous Delivery, Continuous Deployment, containerization, micro-segmentation, automated compliance (“Compliance as Code”), and Continuous Monitoring.

This course also makes extensive use of AWS and associated developer tools such as CloudFormation, CodeCommit, CodeBuild, CodePipeline, and other cloud application services so students can experience how these services can be utilized in their applications.

“SANS training is solid, useful, and well-rounded. It benefits anyone who attends, regardless of time in the industry.”

-D. Turner, Texas Workforce Commission

Who Should Attend

- Anyone working in the DevOps environment or transitioning to a DevOps environment
- Anyone who wants to understand where to add security checks, testing, and other controls to DevOps and Continuous Delivery
- Anyone interested in learning how to migrate DevOps workflows to the cloud, specifically Amazon Web Services (AWS)
- Anyone interested in learning how to leverage cloud application security services provided by AWS
- Developers
- Software architects
- Operations engineers
- System administrators
- Security analysts
- Security engineers
- Auditors
- Risk managers
- Security consultants

Eric Johnson  SANS Certified Instructor

Eric Johnson is a senior security consultant at Cypress Data Defense and the Application Security Curriculum Product Manager at SANS. He is the lead author and instructor for DEV544: Secure Coding in .NET, as well as an instructor for DEV541: Secure Coding in Java/JEE. Eric serves on the advisory board for the SANS Securing The Human Developer awareness training program and is a contributing author for the developer security awareness modules. His experience includes web and mobile application penetration testing, secure code review, risk assessment, static source code analysis, security research, and developing security tools. Eric completed a bachelor of science in computer engineering and a master of science in information assurance at Iowa State University, and currently holds the CISSP, GWAPT, GSSP-.NET, and GSSP-Java certifications. He is based in West Des Moines, Iowa and outside the office enjoys spending time with his wife and daughter, attending Iowa State athletic events, and golfing on the weekends. @emjohn20
This section will help you to expand the usage of cloud application security services to provide encryption, monitoring, and automation. This includes how security controls can be folded into or wired into the CD pipeline, and how to automate security checks and tests in CD.

**Topics: Introduction to DevOps; Case Studies on DevOps unicorns; DevOps Principles; Working in DevOps; From Continuous Integration to Continuous Delivery; Building a CD pipeline; Kata deployment; Secure Continuous Delivery: Challenges and issues; Introducing Security into CD; Static Analysis in CD; Pen Testing and Manual Assessments: How Do They Fit in DevOps?; Vulnerability Management in CD; Securing Your Software Supply Chain; Automated Security Testing and Scanning in CI/CD**

### PART 2

#### 540.2 HANDS ON: Moving to Production

Building on the ideas and frameworks developed in Section 1, you 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 also learn how to secure the pipeline, including RASP and other run-time defense technologies. This includes containerization and security issues when using containers like Docker. Next you learn how to protect the secrets utilized by the automated tools used for CI/CD. Finally, you learn how to build compliance into Continuous Delivery, using the security controls and guardrails that have been built in the DevOps toolchain.

**Topics:** Securing your CD Pipeline; Runtime Checks and Monitoring: Monkeys and Smart Checks; Run-Time Defense: RASP, IAST and Other Run-Time Security Solutions; Security in Monitoring; Red Teaming, Bug Bounties and Blameless Postmortems; Secure Infrastructure as Code; Security with Puppet Lab; Managing Secrets; Container Security: Introduction to Containers, Docker, and Docker Security Risks and Tools; Compliance as Code: Going Forward: Introducing Security into DevOps – and DevOps into Security

#### 540.3 HANDS ON: Moving to the Cloud

Utilizing DevOps principles you learn how to move your CI/CD toolchain into the cloud. This section provides an overview of Amazon Web Services (AWS) and introduces the foundational tools and practices needed to securely deploy your applications in the cloud.

**Topics:** Introduction to the Cloud; Introduction to Amazon Web Services (AWS); Cloud Infrastructure as Code; Cloud CI/CD; Cloud Container Orchestration

#### 540.4 HANDS ON: Cloud Application Security — PART 1

This section will teach you to leverage cloud application security services to ensure that applications have appropriate authentication and access control functionality while maintaining availability even while patching critical security defects.

**Topics:** Authentication and Access Control; API Gateway; Availability; Patch Management

#### 540.5 HANDS ON: Cloud Application Security — PART 2

This section will help you to expand the usage of cloud application security services to provide encryption, monitoring, and automation.

**Topics:** Encryption; Security Monitoring; Security Automation; Serverless Security

---

“Valuable information that is presented in an easy-to-understand method. The hands-on activities are also important to drive the points.”

-Brian Calkin, Symantec

---

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/security-east-2018/courses](http://www.sans.org/event/security-east-2018/courses)
ICS410: ICS/SCADA Security Essentials

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

The course will provide you with:

- An understanding of industrial control system 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

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 industrial control system penetration testing, vulnerability analysis, malware analysis, forensics, secure coding, and red team training, most of these courses do not focus on the people who operate, manage, design, implement, monitor, and integrate critical infrastructure production control systems.

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

When these different groups of professionals complete this course, they will have developed an appreciation, understanding, and common language that will enable them to work together to secure their industrial control system 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.

Billy Rios  SANS Certified Instructor

Billy is an accomplished author and speaker, and is recognized as one of the world’s most respected experts on emerging threats related to industrial control systems (ICS), critical infrastructure, and medical devices. He discovered thousands of security vulnerabilities in hardware and software supporting ICS and critical infrastructure. He has been publically credited by the Department of Homeland Security (DHS) over 50 times for his support to the DHS ICS Cyber Emergency Response Team (ICS-CERT). Billy was a Lead at Google, where he led the front-line response for externally reported security issues and incidents. Prior to Google, Billy was the Security Program Manager at Internet Explorer (Microsoft). During his time at Microsoft, Billy led the company’s response to several high-profile incidents, including the response to Operation Aurora. Billy has also worked as a penetration tester, an intrusion detection analyst, and served as an active duty Marine Corps officer. He currently holds an MBA and a Master of Science in Information Systems. He was a contributing author for several publications including Hacking, the Next Generation (O’Reilly), Inside Cyber Warfare (O’Reilly), and The Virtual Battle Field (IOS Press).  @XSSniper
Course Day Descriptions

410.1 HANDS ON: ICS Overview

Students will develop and reinforce a common language and understanding of Industrial Control System (ICS) cybersecurity as well as the important considerations that come with cyber-to-physical operations within these environments. Each student will receive programmable logic controller (PLC) hardware to keep. The PLC contains physical inputs and outputs that will be programmed in class and mapped to an operator interface, or HMI, also created in class. This improved hardware-enabled approach provides the necessary cyber-to-physical knowledge that allows students to better understand 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; Field Components; Programming Controllers; Supervisory Components; Types of ICS Systems; IT & ICS Differences; Physical Security; ICS Network Architecture

410.2 HANDS ON: ICS Attack Surface

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, defenders will develop a better understanding of where these specific attack vectors exist, as well as the tools to use to discover vulnerabilities and exploit them. Each student will use a vulnerable target virtual machine to further understand attacks targeting the types of web servers used on many ICS devices for management purposes. Simulators will be configured to allow students to conduct attacks against unauthenticated ICS protocols. A variety of data samples are used to examine additional attack vectors on remote devices.

Topics: ICS Attack Surface; Attacks on HMIs and UIs; Attacks on Control Servers; Attacks on Network Communications; Attacks on Remote Devices

410.3 HANDS ON: Defending ICS Servers and Workstations

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. We’ll 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.

Topics: Windows in ICS; Linux/Unix in ICS; Updates and Patching; Processes and Services; Configuration Hardening; Endpoint Defenses; Automation and Auditing; Log Management; Databases and Historians

410.4 HANDS ON: Defending ICS Networks and Devices

With an understanding of the ICS environment, the attack vectors that exist, and the defender-specific capabilities available on servers, workstations, and applications, students will now learn network-specific defense approaches. We’ll first examine common IT protocols and network components used within ICS environments, then discuss ICS-specific protocols and devices. Technologies used to defend ICS networks will be reviewed along with implementation approaches. Students will interact with ICS traffic and develop skills to analyze it, then work through a number of tools to further explore a series of staged adversary actions conducted in a lab environment.

Topics: Network Fundamentals; Ethernet; TCP/IP Protocol Suite; ICS Protocols over TCP/IP; Enforcement Zone Devices; Honeypots; Wireless in Control Systems; Network Capture Forensics; Field and Plant Floor Equipment; Cryptography Fundamentals

410.5 HANDS ON: ICS Security Governance

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

Topics: Information Assurance Foundations; Security Policies; Contingency and Continuity Planning; Risk Assessment and Auditing; Attack Tree Analysis; Password Management; Incident Handling; Incident Response

You Will Be Able To

- 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
- Better understand various industrial control systems and their purpose, application, function, and dependencies on network IP and industrial communications
- Work with operating systems (system administration concepts for Unix/Linux and/or Windows operating systems)
- Work with network infrastructure design (network architecture concepts, including topology, protocols, and components)
- Better understand the systems’ lifecycles
- Better understand information assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)
- Use your skills in computer network defense (detecting host and network-based intrusions via intrusion detection technologies)
- Implement incident response and handling methodologies

“Targeted ICS knowledge; vast subject matter broken down in simple speak!”

-TARONE W., U.S. AIR FORCE

www.sans.edu

Bundle OnDemand

With this course

www.sans.org/ondemand

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/security-east-2018/courses
KEYNOTE:  
**Actionable Detects: Blue Team Cyber Defense Tactics**  
Seth Misenar  
Organizations relying on third parties to detect breaches can go almost a full year before finding out they have been compromised. Detect the breach yourself, and on average you will find it within about a month of the initial occurrence. Mistaking detection and defense against modern adversaries as “too costly” to perform can result in a very expensive miscalculation – especially when you consider the substantially increased price of response and recovery with breach duration. Seth Misenar’s ever-evolving Actionable Detects provides you with the tactics, techniques, and procedures to once again take pride in your Blue Team cyber capabilities. Not applying these lessons learned could prove costly in the face of adapting threat actors. Dig in and learn to hold your head high when talking about your defensive cyber operations capabilities.

**Using an Open-Source Threat Model for Prioritized Defense**  
James Tarala  
Threat actors are not magic and there is not an unlimited, unique list of threats for every organization. Enterprises face similar threats from similar threat sources and threat actors, so why does every organization need to perform completely unique risk assessments and prioritized control decisions? This presentation will show how specific, community-driven threat models can be used to prioritize an organization’s defenses – without all the confusion. James Tarala will present a new, open, community-driven threat model that can be used by any industry to evaluate the risk it faces. Then he will show how to practically use this model to prioritize enterprise defense and map to compliance requirements for organizations today. Whether you are in the Department of Defense or work for a small mom-and-pop retailer, you will be able to use this model to specifically determine a prioritized defense for your organization.

**InfoSec State of the Union**  
Jake Williams  
Come attend this session and catch up with the latest InfoSec news and how it impacts your organization. In this session, we’ll talk about Russian election hacking, FBI investigative techniques, implications of the latest Shadow Brokers dumps, software product liability, DoJ protecting government exploits and more. Come hang with us for this session, and you’ll walk away bigger, badder, and smarter.

**Blockchain: The New Digital Swiss Army Knife?**  
G. Mark Hardy  
Now that the price of a single Bitcoin surpasses the price of an ounce of gold, is blockchain becoming a runaway train with businesses scrambling to hop on? If so, how can you take advantage of this opportunity, and will the mistakes be minor or catastrophic? Blockchain as a technology has been proposed as a solution to everything from frictionless currency transfer to tracking cargo on ships. With over $1 billion in venture funds invested and several hundred patents filed, every security professional must know the impact on organizations in terms of risk, volatility, and competitiveness. This talk will explore alternative uses for blockchain technology other than cryptocurrency, and provide a framework for utilizing and securing a technology considered as disruptive as the Internet was in the 1990s.

**Infosec Rock Star: Geek Will Only Get You So Far**  
Ted Demopoulos  
Some of us are so effective, and well known, that the term “Rock Star” is entirely accurate. What kind of skills do Rock Stars have and wannabe Rock Stars need to develop? Although we personally may never be swamped by groupies, we can learn the skills to be more effective, well respected, and well paid. Obviously it’s not just about technology; in fact most of us are very good at the technology part. The fact is that increasing our skills more on the social and business side will make most of us more effective at what we do than learning how to read hex better while standing on our heads, becoming “One with Metasploit,” or understanding the latest hot technologies.

**Analyzing CRASHOVERRIDE: The Grid-Targeted Malware**  
Robert M. Lee  
There have only ever been four pieces of ICS-tailored malware, and only one of those specifically targeted and disrupted a power grid: CRASHOVERRIDE. In this presentation, one of the security researchers who analyzed CRASHOVERRIDE will present the full timeline, including the 2015 and 2016 cyber attack on Ukraine’s power grid, analysis of the malware and what it is and is not capable of with relation to grid-impact scenarios, and detection and mitigation recommendations for defending against this and similar tradecraft. Participants can expect to leave the presentation with a deep appreciation of what security professionals must be doing as well as why the investments made into the security of infrastructure such as the power grid have so far put us in a great defensible situation.
Enhance Your Training Experience

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

$689 through December 31st
Bundle price increases to $729 on January 1st

"The course content and OnDemand delivery method have both exceeded my expectations."
- Robert Jones, Team Jones, Inc.

Get Certified With GIAC Certifications

- Distinguish yourself as an information security leader
- 30+ GIAC cybersecurity certifications available
- Two practice exams included
- Four months of access to complete the attempt

$689 through September 30th
Bundle price increases to $729 on October 1st

"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.
EXPERIENCE

DEVELOP SKILLS IN:

- CYBER DEFENSE
- INDUSTRIAL CONTROL SYSTEMS
- PENETRATION TESTING
- DIGITAL FORENSICS & INCIDENT RESPONSE

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

– Kyle McDaniel, Lenovo

www.sans.org/netwars
Future Training Events

Phoenix – Mesa ........................ Mesa, AZ ........................ Oct 9-14
Tysons Corner Fall ..................... McLean, VA .................... Oct 14-21
San Diego ............................. San Diego, CA .......... Oct 30 - Nov 4
Seattle .................................. Seattle, WA ............. Oct 30 - Nov 4
Miami .................................... Miami, FL ................ Nov 6-11
San Francisco Winter ................. San Francisco, CA .... Nov 27 - Dec 2
Austin Winter ............................ Austin, TX .......... Dec 4-9

Cyber Defense Initiative  
Washington, DC  
Dec 12-19

Security East  
New Orleans, LA  
Jan 8-13, 2018

Northern VA Winter – Reston ........ Reston, VA ............... Jan 15-20
Las Vegas ............................. Las Vegas, NV .......... Jan 28 - Feb 2
Miami .................................... Miami, FL .......... Jan 29 - Feb 3
Scottsdale ............................. Scottsdale, AZ .... Feb 5-10
Southern California .................. Anaheim, CA .......... Feb 12-17
Dallas ..................................... Dallas, TX .... Feb 19-24
New York City Winter ............... New York, NY .... Feb 26 - Mar 3
San Francisco Spring ................. San Francisco, CA ...... Mar 12-17
Pen Test Austin .......................... Austin, TX ...... Mar 19-24

Future Summit Events

Secure DevOps ............................ Denver, CO ............ Oct 10-17
Pen Test Hackfest ..................... Bethesda, MD ........ Nov 13-20
SIEM & Tactical Analytics ....... Scottsdale, AZ .... Nov 28 - Dec 5
Cyber Threat Intelligence ........ Bethesda, MD .... Jan 29 - Feb 5, 2018
Cloud Security .......................... San Diego, CA .... Feb 19-26

Future Community SANS Events

Local, single-course events are also offered throughout the year via SANS Community. Visit www.sans.org/community for up-to-date Community course information.
Registration Information

Register online at www.sans.org/security-east
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.

Special Hotel Rates Available
A special discounted rate of $204.00 single/double occupancy will be honored, based on space availability.

Limited government per diem rooms are available with proper ID, and government overflow venues will be announced once these rooms sell out. These rates include high-speed Internet in your room and are only available through December 16, 2017. To make a group or government reservation, please call 504-561-0500 and mention you are requesting the SANS Security East 2018 group or government rate.

Top 3 reasons to stay at the Hilton New Orleans Riverside
1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Hilton New Orleans Riverside, 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 Hilton New Orleans Riverside that you won’t want to miss!

Pay Early and Save*
Use code EarlyBird18 when registering early

<table>
<thead>
<tr>
<th>DATE</th>
<th>DISCOUNT</th>
<th>DATE</th>
<th>DISCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>11-15-17</td>
<td>$400.00</td>
<td>12-6-17</td>
<td>$200.00</td>
</tr>
</tbody>
</table>

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

SANS Voucher Program
Expand your training budget!
Extend your fiscal year. The SANS Voucher Program provides flexibility and may earn you bonus funds for training.

www.sans.org/vouchers

Cancellation & Access Policy
If an attendee must cancel, a substitute may attend instead. Substitution requests can be made at any time prior to the event start date. Processing fees will apply. All substitution requests must be submitted by email to registration@sans.org. If an attendee must cancel and no substitute is available, a refund can be issued for any received payments by December 20, 2017. A credit memo can be requested up to the event start date. All cancellation requests must be submitted in writing by mail or fax and received by the stated deadlines. Payments will be refunded by the method that they were submitted. Processing fees will apply.
## SANS Security East 2018 Registration Fees

Register online at [www.sans.org/security-east](http://www.sans.org/security-east)

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.

### Job-Based Long Courses

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Name</th>
<th>Paid before 11-15-17</th>
<th>Paid before 12-6-17</th>
<th>Paid after 12-6-17</th>
<th>Add GIAC Cert</th>
<th>Add OnDemand</th>
<th>Add NetWars Continuous</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC301</td>
<td>Intro to Information Security</td>
<td>$4,980</td>
<td>$5,180</td>
<td>$5,380</td>
<td>$729</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$729</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC503</td>
<td>Intrusion Detection In-Depth</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$729</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$729</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC511</td>
<td>Continuous Monitoring and Security Operations</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$729</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC542</td>
<td>Web App Penetration Testing and Ethical Hacking</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$729</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC555</td>
<td>SIEM with Tactical Analytics NEW!</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$729</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC560</td>
<td>Network Penetration Testing and Ethical Hacking</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$729</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC566</td>
<td>Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td>$4,980</td>
<td>$5,180</td>
<td>$5,380</td>
<td>$729</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC573</td>
<td>Automating Information Security with Python</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$729</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC579</td>
<td>Virtualization and Software-Defined Security</td>
<td>$4,980</td>
<td>$5,180</td>
<td>$5,380</td>
<td>$729</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC660</td>
<td>Advanced Penetration Testing, Exploit Writing, and Ethical Hacking</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$729</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Digital Forensics, Incident Response, and Threat Hunting</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$729</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>FOR578</td>
<td>Cyber Threat Intelligence</td>
<td>$4,980</td>
<td>$5,180</td>
<td>$5,380</td>
<td>$729</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>FOR610</td>
<td>Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$729</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>MGT414</td>
<td>SANS Training Program for CISSP® Certification</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$729</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>MGT512</td>
<td>SANS Security Leadership Essentials for Managers with Knowledge Compression™</td>
<td>$5,420</td>
<td>$5,620</td>
<td>$5,820</td>
<td>$729</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>MGT514</td>
<td>IT Security Strategic Planning, Policy and Leadership</td>
<td>$4,980</td>
<td>$5,180</td>
<td>$5,380</td>
<td>$729</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>DEV540</td>
<td>Secure DevOps and Cloud Application Security NEW!</td>
<td>$4,980</td>
<td>$5,180</td>
<td>$5,380</td>
<td>$729</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>ICS410</td>
<td>ICS/SCADA Security Essentials</td>
<td>$5,310</td>
<td>$5,510</td>
<td>$5,710</td>
<td>$729</td>
<td>$729</td>
<td>$1,260</td>
</tr>
</tbody>
</table>

### Special Courses

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Name</th>
<th>Course fee if taking a 4-6 day course</th>
<th>Course fee</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPECIAL</td>
<td>Core NetWars Experience – Tournament Entrance Fee</td>
<td>FREE</td>
<td>$1,595</td>
</tr>
<tr>
<td>SPECIAL</td>
<td>Cyber Defense NetWars Tournament – Tournament Entrance Fee</td>
<td>FREE</td>
<td>$1,595</td>
</tr>
</tbody>
</table>

---

### EARLY BIRD DISCOUNTS

Pay for any long course using the code **EarlyBird18**

at checkout by November 15th to get **$400 OFF***
or by December 6th to get **$200 OFF***

*Some restrictions apply. Early bird discounts do not apply to Hosted courses.*
Create a **SANS Account** today to enjoy these FREE resources:

**WEBCASTS**

- **Ask The Expert 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** – The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT Security issues.
- **Tool Talks** – Tool Talks are designed to give you a solid understanding of a problem, and how a vendor’s commercial tool can be used to solve or mitigate that problem.

**NEWSLETTERS**

- **NewsBites** – Twice weekly, high-level executive summary of the most important news relevant to cybersecurity professionals.
- **OUCH!** – The world’s leading free monthly 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.

**OTHER FREE RESOURCES**

- 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)

**www.sans.org/account**

SAVE $400 on SANS Cyber Defense Initiative 2017 courses!
Register and pay by October 18th (SAVE $400) or November 8th (SAVE $200) – www.sans.org/cdi