Protect Your Business and Advance Your Career

35+ hands-on, immersion-style information security courses taught by real-world practitioners

- Cyber Defense
- Detection & Monitoring
- Penetration Testing
- Incident Response
- Cyber Threat Intelligence
- Ethical Hacking
- Management
- Secure Development
- ICS/SCADA Security
- SIEM

“If you desire the best training and education, along with professional peer networking, SANS is where you belong.”

- Bill O., U.S. Department of Justice

SAVE $400
Register and pay by Oct 18th – Use code EarlyBird17

REGISTER AT www.sans.org/cdi
Ed Skoudis here. We’ve got something cool for you to check out! It’s an incredible training event called the **SANS Cyber Defense Initiative (CDI) 2017** to be held in Washington, D.C. from December 12-19.

This is an exciting time to work in the cybersecurity industry, and CDI 2017 will help you build the vital skills you and your organization need to more effectively combat the growing wave of breaches and cyber attacks. With attackers growing more brazen and exploiting mission-critical computer systems, it’s more important than ever that you have the latest skills and techniques to stop them in their tracks. That’s what CDI is all about. I urge you to reserve some time on your calendar and register today.

### What Makes CDI 2017 the Best Training and Education Investment?

SANS immersion training is intensive and hands-on, and our courseware is unrivaled in the industry. Our instructors and course authors are leading industry experts and practitioners. With more than 35 courses to choose from at CDI 2017, all types of professionals can learn valuable skills applicable to their security roles that they will be able to implement immediately. Learn cutting-edge content across a range of skill areas that span the industry, including Cyber Defense, Digital Forensics & Incident Handling, Threat Hunting, Management, Penetration Testing, Cyber Threat Intelligence, Industrial Control Systems Security, and Secure Software Development. The courses will prepare you to meet today’s threats and tomorrow’s challenges.

### Which SANS Courses Will Be Offered at CDI 2017?

The CDI 2017 schedule offers a full lineup of classic SANS courses as well as new courses, including:

- **SEC503: Intrusion Detection In-Depth** *(Includes NEW hands-on Netwars IDS Challenge)*
- **SEC545: Cloud Security Architecture and Operations**
- **SEC555: SIEM with Tactical Analysis**
- **SEC564: Red Team Operations and Threat Emulation**
- **DEV534: Secure DevOps: A Practical Introduction**

Many of these 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. Add the corresponding GIAC certification and OnDemand bundle when registering for your course to receive the discounted rates (subject to availability).

### Bonus Experiences

Our brand-new Core NetWars Experience, free for all students attending a five- or six-day course, provides the opportunity to apply the hands-on skills you learn in class during interactive evening sessions. NetWars also gives you a chance to network and have some fun as you take on new challenges. You can participate in the various events on your own or on a team. At CDI 2017, you can play in either Core NetWars, Cyber Defense NetWars, or DFIR NetWars.

If you can’t travel to CDI 2017, you can still attend the most popular courses offered there from the comfort of your own office or home via SANS Simulcast. Students who register for a Simulcast course at CDI 2017 can attend remotely by logging into a virtual classroom and joining the live class. With Simulcast, the SANS team focuses on bringing you all the in-class action and learning, no matter where you are located.

I look forward to seeing you at CDI 2017 and proving why SANS is recognized around the world as the leader in information security training. Visit [www.sans.org/cdi](http://www.sans.org/cdi) to learn more, to review the course list and event details, and to find out how our training can help you reach your professional goals.

### Don’t forget – register and pay by October 18, 2017 to save $400!

Ed Skoudis
SANS Fellow and Curriculum Lead, Penetration Testing
<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></td>
</tr>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
<td></td>
</tr>
<tr>
<td>SEC440</td>
<td>Critical Security Controls: Planning, Implementing, and Auditing</td>
<td></td>
</tr>
<tr>
<td>SEC501</td>
<td>Advanced Security Essentials – Enterprise Defender</td>
<td></td>
</tr>
<tr>
<td>SEC503</td>
<td>Intrusion Detection In-Depth</td>
<td></td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td></td>
</tr>
<tr>
<td>SEC505</td>
<td>Securing Windows and PowerShell Automation</td>
<td></td>
</tr>
<tr>
<td>SEC511</td>
<td>Continuous Monitoring and Security Operations</td>
<td></td>
</tr>
<tr>
<td>SEC542</td>
<td>Web App Penetration Testing and Ethical Hacking</td>
<td></td>
</tr>
<tr>
<td>SEC545</td>
<td>Cloud Security Architecture and Operations</td>
<td></td>
</tr>
<tr>
<td>SEC546</td>
<td>IPv6 Penetration Testing and Ethical Hacking</td>
<td></td>
</tr>
<tr>
<td>SEC550</td>
<td>Active Defense, Offensive Countermeasures, and Cyber Deception</td>
<td></td>
</tr>
<tr>
<td>SEC555</td>
<td>SIEM with Tactical Analytics</td>
<td></td>
</tr>
<tr>
<td>SEC560</td>
<td>Network Penetration Testing and Ethical Hacking</td>
<td></td>
</tr>
<tr>
<td>SEC564</td>
<td>Red Team Operations and Threat Emulation</td>
<td></td>
</tr>
<tr>
<td>SEC566</td>
<td>Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td></td>
</tr>
<tr>
<td>SEC567</td>
<td>Social Engineering for Penetration Testers</td>
<td></td>
</tr>
<tr>
<td>SEC573</td>
<td>Automating Information Security with Python</td>
<td></td>
</tr>
<tr>
<td>SEC575</td>
<td>Mobile Device Security and Ethical Hacking</td>
<td></td>
</tr>
<tr>
<td>SEC580</td>
<td>Metasploit Kung Fu for Enterprise Pen Testing</td>
<td></td>
</tr>
<tr>
<td>SEC582</td>
<td>Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques</td>
<td></td>
</tr>
<tr>
<td>FOR500</td>
<td>Windows Forensic Analysis (formerly FOR408)</td>
<td></td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Digital Forensics, Incident Response, and Threat Hunting</td>
<td></td>
</tr>
<tr>
<td>FOR526</td>
<td>Memory Forensics In-Depth</td>
<td></td>
</tr>
<tr>
<td>FOR572</td>
<td>Advanced Network Forensics and Analysis</td>
<td></td>
</tr>
<tr>
<td>FOR578</td>
<td>Cyber Threat Intelligence</td>
<td></td>
</tr>
<tr>
<td>FOR585</td>
<td>Advanced Smartphone Forensics</td>
<td></td>
</tr>
<tr>
<td>FOR610</td>
<td>Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td>
<td></td>
</tr>
<tr>
<td>MGT414</td>
<td>SANS Training Program for CISSP® Certification</td>
<td></td>
</tr>
<tr>
<td>MGT415</td>
<td>A Practical Introduction to Cybersecurity Risk Management</td>
<td></td>
</tr>
<tr>
<td>MGT433</td>
<td>Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program</td>
<td></td>
</tr>
<tr>
<td>MGT512</td>
<td>SANS Security Leadership Essentials for Managers with Knowledge Compression™</td>
<td></td>
</tr>
<tr>
<td>MGT514</td>
<td>IT Security Strategic Planning, Policy, and Leadership</td>
<td></td>
</tr>
<tr>
<td>DEV522</td>
<td>Defending Web Applications Security Essentials</td>
<td></td>
</tr>
<tr>
<td>DEV534</td>
<td>Secure DevOps: A Practical Introduction</td>
<td></td>
</tr>
<tr>
<td>ICS410</td>
<td>ICS/SCADA Security Essentials</td>
<td></td>
</tr>
<tr>
<td>ICS515</td>
<td>ICS Active Defense and Incident Response</td>
<td></td>
</tr>
<tr>
<td>Core NetWars Experience</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DFIR NetWars Tournament</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Courses at a Glance**

For an up-to-date course list, please check the website at [www.sans.org/event/cyber-defense-initiative-2017/schedule](http://www.sans.org/event/cyber-defense-initiative-2017/schedule)

**Contents**

- SANS Training Roadmap .................................. 2-3
- SANS Instructors ........................................ 4-5
- About SANS ............................................... 6
- NetWars Experience ....................................... 28
- Vendor-Sponsored Events ................................. 40
- SANS OnDemand and Simulcast ............................ 41
- SANS Voucher Program .................................... 46
- Securing Approval and Budget for Training ........... 62
- Future SANS Training Events .............................. 77
- Bonus Sessions ......................................... 78-79
- Hotel Information ........................................ 80
- Registration Information ................................. 80
- Registration Fees ........................................ 81
- Core NetWars Experience .................................. 28
- Cyber Defense NetWars Tournament ....................... 28
- DFIR NetWars Tournament .................................. 28
**Baseline Skills Focus Job Roles**

**Focus Job Roles**

**Crucial Skills, Specialized Roles**

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

**Industrial Control Systems Security**

- ICS410 ICS/SCADA Security Essentials | GCCP (p. 72)
- ICS456 Essentials for NERC Critical Infrastructure Protection
- ICS515 ICS Active Defense and Incident Response | GRID (p. 73)

**Management**

- MGT154 IT Security Strategic Planning, Policy, and Leadership | GSRT (p. 68)
- MGT157 Managing Security Operations: Detection, Response, and Intelligence
- MGT125 IT Project Management, Effective Communication, and PMP® Exam Prep | GCPM

**Audit | Legal**

- AUS507 Auditing & Monitoring Networks, Perimeters, and Systems | GSNA
- SEC566 Implementing and Auditing the Critical Security Controls – In-Depth | GCCC (p. 26)
- LEG523 Law of Data Security and Investigations | GLEG

**Core Security Techniques: Defend & Maintain**

Every security professional should know the defense-in-depth techniques taught in SEC401, and SEC304 completes the "offense informs defense" preparation that teaches defense-specialists how attacks occur and how to respond. If you've got the core defense skills, start with SEC304.

**Security Monitoring & Detection**

- **SEC503** Intrusion Detection In-Depth
- **SEC511** Continuous Monitoring and Security Operations

**Penetration Testing & Vulnerability Analysis**

- **SEC560** Network Penetration Testing and Ethical Hacking
- **SEC562** Web App Penetration Testing and Ethical Hacking

**Incident Response and Enterprise Forensics**

- **FOR508** Advanced Digital Forensics, Incident Response, and Threat Hunting
- **FOR572** Advanced Network Forensics and Analysis

**Digital Forensics and Incident Response**

- **FOR500** Windows Forensic Analysis
- **FOR539** Mac Forensic Analysis
- **FOR526** Memory Forensics In-Depth
- **FOR528** Cyber Threat Intelligence (Certification Coming Soon)
- **FOR585** Advanced Smartphone Forensics
- **FOR510** Reverse-Engineering Malware: Malware Analysis Tools and Techniques | GREM (p. 60)

**Software Security**

- **DEV522** Defending Web Applications Security Essentials
- **DEV541** Secure Coding in Java/JEE: Developing Defensible Applications | GSSP-JAVA
- **DEV544** Secure Coding in .NET: Developing Defensible Applications | GSSP-.NET

**New to Cybersecurity?**

- **SEC301** Introduction to Information Security
- **GSEC Certification** Information Security Professional (p. 66)
- **MGT414** SANS Training Program for CISSP® Certification
- **GCFE Certification** Security Essentials (p. 8)
- **GSEC Certification** Security Essentials (p. 64)
- **GSLC Certification** Security Leadership (p. 64)
- **GCCC Certification** Critical Security Controls – In-Depth (p. 26)

**www.sans.org/roadmap**
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. This guarantees that what you learn in class will be up to date and relevant to your job. The lineup of instructors for SANS CDI 2017 includes:

**Ovie Carroll**
Principal Instructor
@ovie
Teaching FOR500 (formerly FOR408)

**Eric Conrad**
Senior Instructor
@eric_conrad
Teaching SEC511

**Christopher Crowley**
Principal Instructor
@CCrowMontance
Teaching SEC575

**Russell Eubanks**
Certified Instructor
@russelleubanks
Teaching SEC440

**Kevin Fiscus**
Certified Instructor
@kevinbfiscus
Teaching SEC560 & SEC580

**Bryce Galbraith**
Principal Instructor
@brycegalbraith
Teaching SEC550 & SEC564

**Philip Hagen**
Certified Instructor
@PhilHagen
Teaching FOR572

**G. Mark Hardy**
Principal Instructor
@g_mark
Teaching MGT512

**Paul A. Henry**
Senior Instructor
@phenrycissp
Teaching SEC501

**David Hoelzer**
Faculty Fellow
@it_audit
Teaching SEC503

**Micah Hoffman**
Certified Instructor
@WebBreacher
Teaching SEC542 & SEC567

**Eric Johnson**
Certified Instructor
@emjohn20
Teaching DEV534

**Frank Kim**
Certified Instructor
@fykim
Teaching MGT514

**Robert M. Lee**
Certified Instructor
@RobertMLee
Teaching ICS515

For instructor bios, visit: www.sans.org/event/cyber-defense-initiative-2017/instructors
Heather Mahalik  
Senior Instructor  
@HeatherMahalik  
Teaching FOR585

David R. Miller  
Certified Instructor  
@DRM_CyberDude  
Teaching MGT414

Seth Misenar  
Senior Instructor  
@sethmisenar  
Teaching SEC555

Michael Murr  
Principal Instructor  
@mikemurr  
Teaching SEC504

Keith Palmgren  
Senior Instructor  
@kpalmgren  
Teaching SEC301

Billy Rios  
Certified Instructor  
@XSSniper  
Teaching ICS410

Justin Searle  
Senior Instructor  
@meeas  
Teaching SEC642

Dave Shackleford  
Senior Instructor  
@daveshackleford  
Teaching SEC545

Bryan Simon  
Certified Instructor  
@BryanOnSecurity  
Teaching SEC401

Stephen Sims  
Senior Instructor  
@Steph3nSims  
Teaching SEC660

Lance Spitzner  
Certified Instructor  
@lspitzner  
Teaching MGT433

James Tarala  
Senior Instructor  
@isaudit  
Teaching SEC566 & MGT415

Chad Tilbury  
Senior Instructor  
@chadtilbury  
Teaching FOR508

Alissa Torres  
Certified Instructor  
@sibertor  
Teaching FOR526

Johannes Ullrich, PhD  
Senior Instructor  
@johullrich  
Teaching DEV522 & SEC546

Jake Williams  
Certified Instructor  
@MalwareJake  
Teaching FOR578

Lenny Zeltser  
Senior Instructor  
@lennyzeltser  
Teaching FOR610

Register at www.sans.org/cdi  |  301-654-SANS (7267)
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, CISOs, 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.
The foundation of a successful career in information security – whether technical or managerial – should be comprehensive and rooted in real-world expertise. Learn more about the SANS courses and certifications recommended for baseline skills below and on the pages that follow in this catalog.

**Summary:** Every hands-on technical professional should possess the baseline set of knowledge and skills taught in SEC401 and SEC504. These courses cover the essentials of defense-in-depth, the mental model for how attacks work, and the proven methods for handling incidents when they occur.

**Who This Path Is For:** Hands-on technical professionals such as network administrators and engineers, security analysts, and consultants who need well-rounded and effective baseline security skills.

**Why This Training Is Important:** This training gives you essential knowledge and understanding about how a variety of attacks occur and how to respond to them.

“The focus on methodologies was superb because the techniques taught are applicable to every environment regardless of the tools utilized.”

–Conrad Bovell, DSS

“Excellent resources for defense! Attackers’ perspectives are realistic and real-world scenarios are relevant.”

–Nathan P., U.S. Air Force
Six-Day Program
Thu, Dec 14 - Tue, Dec 19
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Bryan Simon

This course has evening
Bootcamp Sessions

Who Should Attend

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

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 Inasaki, 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 on a regular basis at international conferences and with the press on matters of cybersecurity. He has instructed individuals from the FBI, NATO, and the UN in matters of cybersecurity, on two continents. Bryan has specialized expertise in defensive and offensive capabilities. He has received recognition for his work in IT security and was most recently profiled by McAfee (part of Intel Security) as an IT Hero. Bryan holds 13 GIAC Certifications including GSEC, GCWN, GCIAH, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, GCUX, GISF, and GMON. Bryan’s scholastic achievements have resulted in the honor of sitting as a current member of the SANS Institute Advisory Board and in his acceptance into the prestigious SANS Cyber Guardian program. 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 has given me a great start on truly understanding the fundamentals of security and applying it every day.”

-John Houser, First Citizens Bank

www.sans.edu

MEETS DODD #1402 (8570) REQUIREMENTS

www.sans.org/8140

“BUNDLE ONSMART”

WITH THIS COURSE
www.sans.org/ondemand

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/cyber-defense-initiative-2017/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 Chavarría, 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

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

-Michael Hoffman, Shell Oil Products US

### Michael Murr  SANS Principal Instructor

Michael has been a forensic analyst with Code-X Technologies for over five years. 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.  

@mikemurr

---

### Details

#### Six-Day Program

- **Thu, Dec 14 - Tue, Dec 19**
- **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.)

Instructor: Michael Murr

**This course has extended hours**

---

**Also Available Via Simulcast**

See page 80 for details.
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

You Will Be Able To

- Apply incident handling processes in-depth, including preparation, identification, containment, eradication, and recovery, to protect enterprise environments
- Analyze the structure of common attack techniques in order to evaluate an attacker’s spread through a system and network, anticipating and thwarting further attacker activity
- Utilize tools and evidence to determine the kind of malware used in an attack, including rootkits, backdoors, and trojan horses, choosing appropriate defenses and response tactics for each
- Use built-in command-line tools such as Windows tasklist, vmic, and reg as well as Linux netstat, ps, and lsoll to detect an attacker’s presence on a machine
- Analyze router and system ARP tables along with switch CAM tables to track an attacker’s activity through a network and identify a suspect
- Use memory dumps and the Volatility tool to determine an attacker’s activities on a machine, the malware installed, and other machines the attacker used as pivot points across the network
- Gain access to a target machine using Metasploit, and then detect the artifacts and impacts of exploitation through process, file, memory, and log analysis
- Analyze a system to see how attackers use the Netcat tool to move files, create backdoors, and build relays through a target environment
- Run the Nmap port scanner and Nessus vulnerability scanner to find openings on target systems, and apply tools such as tcpdump and netstat to detect and analyze the impacts of the scanning activity
- Apply the tcpdump sniffer to analyze network traffic generated by a covert backdoor to determine an attacker’s tactics
- Employ the netstat and lsoll tools to diagnose specific types of traffic-flooding denial-of-service techniques and choose appropriate response actions based on each attacker’s flood technique
- Analyze shell history files to find compromised machines, attacker-controlled accounts, sniffers, and backdoors
SEC301

Intro to Information Security

Five-Day Program
Thu, Dec 14 - Mon, Dec 18
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Keith Palmgren

Who Should Attend

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

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 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, GCCH, GCED, GISF, CEH, Security+, Network+, A+, CTT+). @kpalmgren
Every good security practitioner and every good security program begins with the same mantra: learn the fundamentals. SEC301 starts by instilling familiarity with core security terms and principles. By the time you leave the classroom after the first day, you will fully understand the Principle of Least Privilege and 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.

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 you 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.

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?

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.

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.

“\nThis training was excellent. Keith Palmgren is a great instructor with a strong balance of teaching and real-world experience. The course material was taught in such a manner as to work well for IT and non-IT learners.”

-Jorge Henneke, CA DEPT. OF CONSERVATION

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/cyber-defense-initiative-2017/courses

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

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

“This was the most informative class that I have attended at this time. It went into more detail than previous classes. The labs were also very informative. This class is a must if you are new to network security.”

-Kyle Butis, Pitzer College

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

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

501.1 HANDS ON: Defensive Network Infrastructure
Making your network secure from attack starts with designing, building, and implementing a robust network infrastructure. There are many aspects to implementing a defense-in-depth network that are often overlooked when companies focus only on functionality. Achieving the proper balance between business drivers and core information security requires that an organization build a secure network that is mission-resilient to a variety of potential attacks. On the first day students will learn how to design and implement a functionality-rich, secure network and how to maintain and update it as the threat landscape evolves.

Topics: Introducing Network Infrastructure as Targets for Attack; Implementing the Cisco Gold Standard to Improve Security; Advanced Layer 2 and 3 Controls

501.2 HANDS ON: Packet Analysis
Packet analysis and intrusion detection are at the core of timely detection. Detecting attacks is becoming more difficult as attacks become more stealthy and more difficult to find. Only by understanding the core principles of traffic analysis can one become a skilled analyst and distinguish normal traffic from attack traffic. Security professionals must be able to detect new, advanced zero-day attacks before they compromise a network. Prevention, detection, and reaction must all be closely knit so that once an attack is detected, defensive measures can be adapted, proactive forensics implemented, and the organization can continue to operate.

Topics: Architecture Design & Preparing Filters; Detection Techniques and Measures; Advanced IP Packet Analysis; Intrusion Detection Tools

501.3 HANDS ON: Pentest
An organization must understand the changing threat landscape and compare that against its own vulnerabilities. On day three students will be shown the variety of tests that can be run and how to perform penetration testing in an effective manner. Students will learn about external and internal penetration testing and the methods of black, gray, and white box testing. Penetration testing is critical to identify an organization’s exposure points, but students will also learn how to prioritize and fix these vulnerabilities to increase the overall security of an organization.

Topics: Variety of Penetration Testing Methods; Vulnerability Analysis; Key Tools and Techniques; Basic Pen Testing; Advanced Pen Testing

501.4 HANDS ON: First Responder
Any organization connected to the Internet or with employees is going to have attacks launched against it. Security professionals need to understand how to perform incident response, analyze what is occurring, and restore their organization back to a normal state as soon as possible. Day four will equip students with a proven six-step process to follow in response to an attack – prepare, identify, contain, eradicate, recover, and learn from previous incidents. Students will learn how to perform forensic investigations and find indications of an attack. This information will be fed into the incident response process to ensure that the attack is prevented from occurring again in the future.

Topics: Incident Handling Process and Analysis; Forensics and Incident Response

501.5 HANDS ON: Malware
As security professionals continue to build more proactive security measures, attackers’ methods will continue to evolve. A common way for attackers to target, control, and break into as many systems as possible is through the use of malware. Therefore it is critical that students understand what type of malware is currently available to attackers as well as the future trends and methods of exploiting systems. With this knowledge students can then learn how to analyze, defend, and detect malware on systems and minimize the impact to the organization.

Topics: Malware; Microsoft Malware; External Tools and Analysis

501.6 HANDS ON: Data Loss Prevention
Cybersecurity is all about managing, controlling, and mitigating risk to critical assets, which in almost every organization are composed of data or information. Perimeters are still important, but we are moving away from a fortress model and moving towards a focus on data. This is based on the fact that information no longer solely resides on servers where properly configured access control lists can limit access and protect our information; it can now be copied to laptops and plugged into networks. Data must be protected no matter where it resides.

Topics: Risk Management; Data Classification; Digital Rights Management; Data Loss Prevention (DLP)

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

“The focus on real-world simulations allows immediate implementation upon return to work.”
-MALCOLM DALTON, GILA RIVER INDIAN COMMUNITY

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/cyber-defense-initiative-2017/courses
**Reports of prominent organizations being hacked and suffering irreparable reputational damage have become all too common. How can you prevent your company from becoming the next victim of a major cyber attack?**

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

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

**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 holds a B.S. in IT, Summa Cum Laude, having spent time either attending or consulting for Stony Brook University, Binghamton University, and American Intercontinental University.  

@it_audit
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.
SECG05
Securing Windows and PowerShell Automation

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

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

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

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

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

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

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

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

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

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

Jason Fossen SANS Faculty Fellow

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

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

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

#### 505.2 HANDS ON: Continuous Secure Configuration Enforcement
Running a vulnerability scanner is easy, but remediating vulnerabilities in a large enterprise is hard. Most vulnerabilities are fixed by applying patches, but this course does not talk about patch management, you’re doing that already. What about the other vulnerabilities, the ones not fixed by applying patches? These vulnerabilities are, by definition, remediated by configuration changes. That’s the hard part. We need a secure architecture designed for SecOps/DevOps.

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

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

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

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

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

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

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

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

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

---

**You Will Be Able To**
- Execute PowerShell commands on remote systems and begin to write your own PowerShell scripts
- Harden PowerShell itself against abuse, and enable transcription logging
- Use Group Policy to execute PowerShell scripts on an almost unlimited number of hosts, while using Group Policy Object permissions, organizational units, and Windows Management Instrumentation (WMI) to target just the systems that need the scripts run
- Use PowerShell Desired State Configuration (DSC) and Server Manager scripting for the sake of SecOps/DevOps automation of server hardening
- Assuming a breach will occur, use Group Policy and PowerShell to grant administrative privileges in a way that reduces the harm if an attack succeeds
- Configure PowerShell remoting to use Just Enough Admin (JEA) policies to create a Windows version of Linux sudo and setuid root
- Configure mitigations against attacks such as pass-the-hash, Kerberos golden tickets, Remote Desktop Protocol (RDP) man-in-the-middle, Security Access Token abuse, and other attacks discussed in some SANS hacking courses
- Use PowerShell and Group Policy to manage the Microsoft Enhanced Mitigation Experience Toolkit (EMET), AppLocker whitelisting rules, INF security templates, Windows Firewall rules, IPSec rules, and many other security-related settings
- Install and manage a full Windows Public Key Infrastructure (PKI), including smart cards, certificate auto-enrollment, Online Certificate Status Protocol (OCSP) web responders, and detection of spoofed root Certification Authorities (CAs)
- Harden SSL/TLS, RDP, DNS, and SMB against attacks. This includes deploying DNSSEC, DNS sinkholes for malware, SMB encryption, and TLS cipher suite optimization
- Use PowerShell with the WMI service, such as remote command execution, searching event logs, and doing a remote inventory of user applications

“Learning to combine PowerShell with WMI, as well as security-required protocols, is invaluable knowledge to have.”

-Dan Christy, Indiana University School of Public Health

[For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/cyber-defense-initiative-2017/courses]
We continue to underestimate the tenacity of our adversaries! Organizations are investing significant time and financial and human resources to combat cyber threats and prevent cyber attacks, but despite this tremendous effort, organizations are still getting compromised. The traditional perimeter-focused, prevention-dominant approach to security architecture has failed to prevent intrusions. No network is impenetrable, which is a reality that business executives and security professionals alike have to accept. Prevention is crucial, and we can't lose sight of it as the primary goal. However, a new proactive approach to security is needed to enhance the capabilities of organizations to detect threats that will inevitably slip through their defenses.

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

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

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

Your SEC511 journey will conclude with one last hill to climb! The final day (Day 6) features a Capture-the-Flag competition that challenges you to apply the skills and techniques learned in the course to detect and defend the modern security architecture that has been designed. Course authors Eric Conrad and Seth Misenar have designed the Capture-the-Flag competition to be fun, engaging, comprehensive, and challenging. You will not be disappointed!
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 SP800-137
> Determine requisite monitoring capabilities for a SOC environment
> Determine capabilities required to support continuous monitoring of key Critical Security Controls

“This particular class provided common-sense approaches and techniques that I literally started using on Monday when I returned to work. The instructor’s intimate knowledge of the tools and practices really helped this course shine. An incredible experience, and I feel more confident and better armed to defend our environment.”

-Shane Wolfe, Space Telescope Science Institute

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/cyber-defense-initiative-2017/courses
As more organizations move data and infrastructure to the cloud, security is becoming a major priority. Operations and development teams are finding new uses for cloud services, and executives are eager to save money and gain new capabilities and operational efficiency by using these services. But will information security prove to be an Achilles’ heel? Many cloud providers do not provide detailed control information about their internal environments, and quite a few common security controls used internally may not translate directly to the public cloud.

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

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

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

**545.1 HANDS ON: Cloud Security Foundations**

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

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

**545.2 HANDS ON: Core Security Controls for Cloud Computing**

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

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

**545.3 HANDS ON: Cloud Security Architecture and Design**

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

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

**545.4 HANDS ON: Cloud Security – Offense and Defense**

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

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

**545.5 HANDS ON: Cloud Security Automation and Orchestration**

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

**Topics:** Scripting and Automation in the Cloud; SecDevOps Principles; Creating Secure Cloud Workflows; Building Automated Event Management; Building Automated Defensive Strategies; Tools and Tactics; Real-World Use Cases; Class Wrap-Up
Many organizations have logging capabilities but lack the people and processes to analyze them. In addition, logging systems collect vast amounts of data from a variety of data sources that require an understanding of the sources for proper analysis. This class is designed to provide individuals training, methods, and processes for enhancing existing logging solutions. This class will also help you understand the when, what, and why behind the logs. This is a lab-heavy course that utilizes SOF-ELK, a SANS-sponsored free Security Incident and Events 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.

“Although I might not be 100% proficient with ELK by day 6, EVERYTHING covered in class I can take back to my environment and apply.” - EVERETT SHERLOCK, KAPSTONE

Seth Misenar  SANS Senior Instructor

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

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

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/cyber-defense-initiative-2017/courses](http://www.sans.org/event/cyber-defense-initiative-2017/courses)
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.

James Tarala  SANS Senior Instructor

James Tarala is a principal consultant with Enclave Security and is based in Venice, Florida. He is a regular speaker for the SANS Institute as well as a courseware author and editor for many SANS auditing and security courses. As a consultant, he has spent the past few years developing large enterprise IT security and infrastructure architectures, specifically working with many Microsoft-based directory services, e-mail, terminal services, and wireless technologies. He has also spent a large amount of time consulting with organizations to assist them with their security management, operational practices, and regulatory compliance issues, and he often performs independent security audits and assists internal audit groups in developing their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University and his graduate work at the University of Maryland. He holds numerous professional certifications. @isaudit
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.
- Understand how the Critical Controls map to standards such as NIST 800-53, ISO 27002, the Australian Top 35, and more.
- Audit each of the Critical 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/cyber-defense-initiative-2017/courses

www.sans.edu

www.sans.org/ondemand
Hands-On Information Security Challenges

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

– Kyle McDaniel, Lenovo

DEVELOP SKILLS IN:

- Cyber Defense
- Industrial Control Systems
- Penetration Testing
- Digital Forensics & Incident Response

www.sans.org/netwars
Focus Job Roles and Specialized Skills
Penetration Testing & Vulnerability Analysis

Summary: High-performing security organizations need specially trained professionals who can continuously challenge the defenses and monitoring systems set up by the cyber defense operating teams and discover vulnerabilities to be addressed that might otherwise be exploited by attackers. Professionals focusing on this career path must be able to test both network and wireless vulnerabilities and understand these environments before advancing to additional areas.

SEC560 and SEC542 teach you the skills that are core to this type of role. An additional nine SANS penetration testing courses, in advanced and specialized topics, allow you to mold your career into a particular practice area or task. Review the following pages for detailed information about all of these courses and the certifications that validate your acquired skills.

Who This Path Is For: Information Security Engineers, Analysts, and Risk Consultants need to master this coursework in particular to hone their penetration testing, ethical hacker, and vulnerability analysis skills.

Why This Training Is Important: These courses teach proper planning, scoping, and recon, while diving deep into scanning, target exploitation, password attacks, web app configuration, identity, authentication, custom scripting, and interception proxies. Together with dozens of detailed, hands-on labs, this training allows you to go back to work with the practical, real-world examples and practice needed to do your job efficiently and masterfully.

“I was pleasantly humbled, challenged, encouraged and trained. I feel 100% more qualified to defend my company’s network after taking this training.”

-Ivan Dominguez, NWCU.com
Six-Day Program
Thu, Dec 14 - Tue, Dec 19
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Kevin Fiscus

This course has extended hours

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

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.

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

Kevin Fiscus is the founder of and lead consultant for Cyber Defense Advisors, where he performs security and risk assessments, vulnerability and penetration testing, security program design, policy development and security awareness with a focus on serving the needs of small and mid-sized organizations. Kevin has over 20 years of IT experience and has focused exclusively on information security for the past 12 years. Kevin currently holds the CISA, GPEN, GREM, GCED, GCIA-Gold, GCFA-Gold, GCIAH, GAWN, GPPA, GCGN, GCSC-Gold, GSEC, SCFA, RCE, and SnortCP certifications and is proud to have earned the top information security certification in the industry, the GIAC Security Expert. He has also achieved the distinctive title of SANS Cyber Guardian for both red team and blue team. Kevin has taught many of SANS’s most popular classes including SEC401, SEC464, SEC503, SEC504, SEC542, SEC560, SEC561, SEC575, FOR508, and MGT414. @kevinbfiscus

Register at www.sans.org/cdi     |     301-654-SANS (7267)
560.1 HANDS ON: Comprehensive Pen Test Planning, Scoping, and Recon

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 packets: Scapy and Nettcat. 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; Nettcat 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

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/cyber-defense-initiative-2017/courses
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.

Micah Hoffman  **SANS Certified Instructor**

Micah Hoffman has been working in the information technology field since 1998 supporting federal government, commercial, and internal customers in their searches to discover and quantify information security weaknesses within their organizations. He leverages years of hands-on, real-world penetration testing and incident response experience to provide excellent solutions to his customers. Micah holds the GMON, GAWN, GWAPT, and GPEN certifications as well as the CISSP®. Micah is an active member in the NoVAnHackers community, writes Recon-ng modules and enjoys tackling issues with the Python scripting language. When not working, teaching, or learning, Micah can be found hiking or backpacking on the Appalachian Trail or the many park trails in Maryland.  @WebBreacher
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 Sessions Work; 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 Zombify Browsers; Browser Exploitation Framework (BeEF); Walking Through an Entire Attack Scenario; Leveraging Attacks to Gain Access to the System; How to Pivot Our Attacks Through a Web Application; Understanding Methods of Interacting with a Server Through SQL Injection; Exploiting Applications to Steal Cookies; Executing Commands Through Web Application Vulnerabilities

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.

You Will Be Able To

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

For course updates, prerequisites, special notes, or laptop requirements, visit: www.sans.org/event/cyber-defense-initiative-2017/courses
Five-Day Program
Thu, Dec 14 - Mon, Dec 18
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Bryce Galbraith

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

The current threat landscape is shifting. Traditional defenses are failing us. We need to develop new strategies to defend ourselves. Even more importantly, we need to better understand who is attacking us and why. You may be able to immediately implement some of the measures we discuss in this course, while others may take a while. Either way, consider what we discuss as a collection of tools that will be at your disposal when you need them to annoy attackers, determine who is attacking you, and, finally, attack the attackers.

SEC550: Active Defense, Offensive Countermeasures, and Cyber Deception is based on the Active Defense Harbinger Distribution live Linux environment funded by the Defense Advanced Research Projects Agency (DARPA). This virtual machine is built from the ground up for defenders to quickly implement Active Defenses in their environments. The course is very heavy with hands-on activities – we won’t just talk about Active Defenses, we will work through labs that will enable you to quickly and easily implement what you learn in your own working environment.

You Will Learn:
› How to force an attacker to take more moves to attack your network – moves that in turn may increase your ability to detect that attacker
› How to gain better attribution as to who is attacking you and why
› How to gain access to a bad guy’s system
› Most importantly, you will find out how to do the above legally

What You Will Receive
› A fully functioning Active Defense Harbinger Distribution ready to deploy
› Class books and a DVD with the necessary tools and the OCM virtual machine, which is a fully functional Linux system with the OCM tools installed and ready to go for the class and for the students’ work environments

“SEC550 is the next step in the evolution of cyber defense – learning how to make hackers’ jobs harder, tracking their movement, and getting attribution.”
- MICK LEACH, NATIONWIDE

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 curriculum 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

“SEC550 is great training--it is very helpful to better understand the analytical part of offensive security and how to improve protection.”
- STEFANIA INNELLI, PALO ALTO NETWORKS
For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/cyber-defense-initiative-2017/courses

Course Day Descriptions

550.1 HANDS ON: Setup and Baseline
Day 1 topics:
- Setup
- Mourning Our Destiny, Leaving Youth and Childhood Behind
- Bad Guy Defenses
- Basics and Fundamentals (Or, Don’t Get Owned Doing This)
- Playing With Advanced Backdoors
- Software Restriction Policies
- Legal Issues
- Venom and Poison

You Will Be Able To
- Track bad guys with callback Word documents
- Use Honeybadger to track web attackers
- Block attackers from successfully attacking servers with honeyports
- Block web attackers from automatically discovering pages and input fields
- Understand the legal limits and restrictions of Active Defense
- Obfuscate DNS entries
- Create non-attributable Active Defense Servers
- Combine geolocation with existing Java applications
- Create online social media profiles for cyber deception
- Easily create and deploy honeypots

Course Author Statement
“I wrote this course to finally make defense fun, to finally sow some confusion among the attackers, and to change the way we all look at defense. One of the most frequent questions I get is why offensive countermeasures are so important. Many people tell me that we cannot ignore patching, firewalls, policies, and other security management techniques. I could not agree more. The techniques presented in this course are intended for organizations that have gone through the process of doing things correctly and want to go further. Get your house in order, and then play. Of course, there will be challenges for anyone trying to implement offensive countermeasures in their organization. However, they can all be faced and overcome.”

- John Strand

550.2 HANDS ON: Annoyance
Day 2 topics:
- How to Connect to Evil Servers (Without Getting Shot)
- Remux.py
- Recon on Bad Servers and Bad People
- Honeypots
- Honeyports
- Kippo
- Deny Hosts
- Artillery
- More Evil Web Servers
- Cryptolocked

550.3 HANDS ON: Attribution
Day 3 topics:
- Dealing with TOR
- Decloak
- Word Web Bugs (Or Honeydocs)
- More Evil Web Servers
- Cryptolocked

550.4 HANDS ON: More Attribution and Attack
Day 4 topics:
- Nova
- Infinitely Recursive Windows Directories
- Web Application Street Fighting with BeEF!
- Wireless and Brotherly Love
- Evil Java Applications with SET
- AV Bypass (for the Good Guys!)
- Arming Word Documents
- Python Injection
- Ghostwriting
- HoneyBadger
- Let’s Try to Trojan Some Java Applications

550.5 HANDS ON: Capture the Flag
The Capture-the-Flag challenge draws on what you have learned over the previous four days of the course.

“SEC550 is the best course I’ve taken. Everything else pretty much says the same thing or reinforces the same concepts, but this is the first course that talks about going outside the box to fight the attackers. Excellent!”

-JONATHAN MANAFI, MCLHENNY COMPANY
**SEC573**

Automating Information Security with Python

Six-Day Program  
Thu, Dec 14 - Tue, Dec 19  
9:00am - 5:00pm  
36 CPEs  
Laptop Required  
Instructor: Mark Baggett

Who Should Attend

- Security professionals who want to learn how to develop Python applications
- Penetration testers who want to move from being a consumer of security tools to being the creator of security tools
- Technologists who need custom tools to test their infrastructure and who want to create those tools themselves

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 emphasize their need for skilled tool builders. There is a huge demand for people who can understand a problem and then rapidly develop prototype code to attack or defend against it. Join us and learn Python in-depth and fully weaponized.

**Mark Baggett**  
SANS Senior Instructor  

Mark Baggett is the owner of Indepth Defense, an independent consulting firm that offers incident response and penetration testing services. Mark has more than 28 years of commercial and government experience ranging from Software Developer to Chief Information Security Officer. He is the author of the 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.  

@MarkBaggett
Course Day Descriptions

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

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

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

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

573.3 HANDS ON: Defensive Python
Day three includes in-depth coverage of how defenders can use Python automation as we cover Python modules and techniques that everyone can use. Forensicators and offensive security professionals will also learn essential skills they will apply to their craft. We will play the role of network defenders who needs to find the attackers on their network. We will discuss how to analyze network logs and packets to discover where the attackers are coming from and what they are doing. We will build scripts to empower continuous monitoring and disrupt the attackers before they exfiltrate your data.

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

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

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

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

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

573.6 HANDS ON: Capture the Flag
In this final section you will be placed on a team with other students. Working as a team, you will apply the skills you have mastered in a series of programming challenges. Participants will exercise the skills and code they have developed over the previous five days as they exploit vulnerable systems, break encryption cyphers, analyze packets, parse logs, and automate code execution on remote systems. Test your skills! Prove your might!
Who Should Attend
- Penetration testers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing, deploying or securing mobile phones and tablets
- Network and system administrators supporting mobile phones and tablets

"The explanations of the concepts behind the tools are great! SEC575 provides both the process and application of tools – not just a ton of tools and information."
- Sean Burden, Western Union

Imagine an attack surface spread throughout your organization and in the hands of every user. It moves from place to place regularly, stores highly sensitive and critical data, and sports numerous different wireless technologies all ripe for attack. You don’t need to imagine any further because this already exists today: mobile devices. These devices are the biggest attack surface in most organizations, yet these same organizations often don’t have the skills needed to assess them.

Mobile devices are no longer a convenience technology: they are an essential tool carried or worn by users worldwide, often displacing conventional computers for everyday enterprise data needs. You can see this trend in corporations, hospitals, banks, schools, and retail stores throughout the world. Users rely on mobile devices more today than ever before – we know it, and the bad guys do too.

This course is designed to give you the skills you need to understand the security strengths and weaknesses in Apple iOS, Android, and wearable devices including Apple Watch and Android Wear. With these skills, you will evaluate the security weaknesses of built-in and third-party applications. You’ll learn how to bypass platform encryption, and how to manipulate Android apps to circumvent obfuscation techniques. You’ll leverage automated and manual mobile application analysis tools to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels. You’ll safely work with mobile malware samples to understand the data exposure and access threats affecting Android and iOS devices, and you’ll exploit lost or stolen devices to harvest sensitive mobile application data.

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

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

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

Christopher Crowley  SANS Principal Instructor

Christopher has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, D.C. area. His work experience includes penetration testing, computer network defense, incident response, and forensic analysis. He is the course author for SANS MG1535: Incident Response Team Management and holds the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GREM, GMOB, and CISSP certifications. His teaching experience includes SEC401, SEC503, SEC504, SEC560, SEC575, SEC580, FOR585, and MG1535; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor of the Year Award, which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities. @CCrowMontance
575.1 HANDS ON: **Device Architecture and Common Mobile Threats**

The first section of the course quickly looks at the significant threats affecting mobile device deployments, highlighted with a hands-on exercise evaluating network traffic from a vulnerable mobile banking application. As a critical component of a secure deployment, we will examine the architectural and implementation differences and similarities in Android (including Android Marshmallow), Apple iOS 10, and the Apple Watch and Google Wear platforms. We will also look at the specific implementation details of popular platform features such as iBeacon, AirDrop, App Verification, and more. Hands-on exercises will be used to interact with mobile devices running in a virtualized environment, including low-level access to installed application services and application data.

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

575.2 HANDS ON: **Mobile Platform Access and Application Analysis**

With an understanding of the threats, architectural components and desired security methods, we dig deeper into iOS and Android mobile platforms focusing on sandboxing and data isolation models, and on the evaluation of mobile applications. This section is designed to help build skills in analyzing mobile device data and applications through rooting and jailbreaking Android and iOS devices and using that access to evaluate file system artifacts.

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

575.3 HANDS ON: **Mobile Application Reverse Engineering**

One of the critical decisions you will need to make in supporting a mobile device deployment is to approve or disapprove of unique application requests from end-users in a corporate device deployment. With some analysis skills, we can evaluate applications to determine the type of access and information disclosure threats they represent. In this section we will use automated and manual application assessment tools to evaluate iOS and Android apps. We’ll build upon the static application analysis skills covered in day 2 to manipulate application components, including Android intents and iOS URL extensions. We’ll also learn and practice techniques for manipulating iOS and Android applications: method swizzling on iOS, and disassembly, modification, and reassembly of iOS apps. The day ends with a look at a standard system for evaluating and grading the security of mobile applications in a consistent way through the application report card project.

**Topics:** Application Report Cards; Automated Application Analysis Systems; Manipulating App Behavior

575.4 HANDS ON: **Penetration Testing Mobile Devices – PART 1**

An essential component of developing a secure mobile phone deployment is to perform an ethical hacking assessment. Through ethical hacking or penetration testing, we examine the mobile devices and infrastructure from the perspective of an attacker, identifying and exploiting flaws that deliver unauthorized access to data or supporting networks. Through the identification of these flaws we can evaluate the mobile phone deployment risk to the organization with practical, useful risk metrics.

**Topics:** Fingerprinting Mobile Devices; Wireless Network Probe Mapping; Weak Wireless Attacks; Enterprise Wireless Security Attacks; Network Manipulation Attacks; Sidejacking Attacks

575.5 HANDS ON: **Penetration Testing Mobile Devices – PART 2**

Continuing our look at ethical hacking and penetration testing, we turn our focus to exploiting weaknesses on iOS and Android devices. We will also examine platform-specific application weaknesses and look at the growing use of web framework attacks in mobile application exploitation.

**Topics:** SSL/TLS Attacks; Client-Side Injection (CSI) Attacks; Web Framework Attacks; Back-end Application Support Attacks

575.6 HANDS ON: **Capture the Flag**

On the last day of class we’ll pull in all the concepts and technology we’ve covered in the week for a comprehensive Capture-the-Flag (CTF) challenge. During the CTF event, you’ll have the option to participate in multiple roles, designing a secure infrastructure for the deployment of mobile phones, monitoring network activity to identify attacks against mobile devices, extracting sensitive data from a compromised iPad, and attacking a variety of mobile phones and related network infrastructure components. In the CTF, you’ll use the skills you’ve built to practically evaluate systems and defend against attackers, simulating the realistic environment you’ll be prepared to protect when you get back to the office.

---

**You Will Be Able To**

- Use jailbreak tools for Apple iOS and Android systems
- Conduct an analysis of iOS and Android filesystem data to plunder compromised devices and extract sensitive mobile device use information
- Analyze Apple iOS and Android applications with reverse-engineering tools
- Change the functionality of Android and iOS apps to defeat anti-jailbreaking or circumvent in-app purchase requirements
- Conduct an automated security assessment of mobile applications
- Use wireless network analysis tools to identify and exploit wireless networks used by mobile devices
- Intercept and manipulate mobile device network activity
- Leverage mobile-device-specific exploit frameworks to gain unauthorized access to target devices
- Manipulate the behavior of mobile applications to bypass security restrictions

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

-RICHARD TAKACS, INTEGRITY360

---

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/cyber-defense-initiative-2017/courses](www.sans.org/event/cyber-defense-initiative-2017/courses)
Stop by the Vendor Expo and get information on the leading tools in the market.

December 15, 2017 12-1:30 PM | 5:30-7:30 PM

For additional information please contact: vendor@sans.org
Can’t make it to SANS Live Training?
SANS Training is also available in several convenient online modalities to suit your learning style. SANS courses and instructors are available to you anytime, anywhere.

**World-Class Instructors | Same Content as Live Courses | Anytime Access | No Travel Costs or Time Away | Review and Rewind Content | Subject-Matter Expert Support for Questions | Same GIAC Exam Pass Rates as SANS Live Training**

**Don’t forget to add an OnDemand Bundle to your SANS Live training course!**

- 4 Months of additional access to content and labs
- Subject-Matter Expert Support
- Great GIAC Prep
- Helps you retain knowledge gained

To add your OnDemand Bundle, call 301-654-SANS (7267) today.

**SANS OnDemand** courses provide the flexibility to train online wherever and whenever it’s most convenient for you. With four months of access to the online course materials, including lectures, quizzes, and labs, you can master the course content on your schedule, at your own pace.

**SANS Simulcast** courses allow you to attend live SANS courses, via a virtual portal, from the comfort of your home or office. You’ll see and hear the material as it is presented in the live environment, all without the need to travel.

**SANS vLive** courses are six weeks long, with content presented in the evenings twice a week—perfect for extra study time between sessions. With smaller class sizes, you’ll also have more access to instructors throughout your training.

**SANS SelfStudy** offers the flexibility to complete your training at the convenience of your own schedule. This option includes: four months of course access, books, MP3s of lectures, and study materials.

Visit [www.sans.org/online](http://www.sans.org/online) to find your course, check for special offers, and get registered today!
## SEC642

### Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques

**Six-Day Program**  
Thu, Dec 14 - Tue, Dec 19  
9:00am - 5:00pm  
36 CPEs  
Laptop Required  
Instructor: Justin Searle

<table>
<thead>
<tr>
<th>Who Should Attend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web penetration testers</td>
</tr>
<tr>
<td>Red team members</td>
</tr>
<tr>
<td>Vulnerability assessment personnel</td>
</tr>
<tr>
<td>Network penetration testers</td>
</tr>
<tr>
<td>Security consultants</td>
</tr>
<tr>
<td>Developers</td>
</tr>
<tr>
<td>QA testers</td>
</tr>
<tr>
<td>System administrators</td>
</tr>
<tr>
<td>IT managers</td>
</tr>
<tr>
<td>System architects</td>
</tr>
</tbody>
</table>

**Can Your Web Apps Withstand the Onslaught of Modern Advanced Attack Techniques?**

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

“I highly recommend taking this class to learn advanced web app pen testing techniques!”  
- WALT CARRUTH, RealPage

**Are You Ready to Put Your Web Apps to the Test with Cutting-Edge Skills?**

This pen testing course is designed to teach you the advanced skills and techniques required to test modern web applications and next-generation technologies. The course uses a combination of lecture, real-world experiences, and hands-on exercises to teach you the techniques to test the security of tried-and-true internal enterprise web technologies, as well as cutting-edge Internet-facing applications. The final course day culminates in a Capture-the-Flag competition, where you will apply the knowledge you acquired during the previous five days in a fun environment based on real-world technologies.

**Hands-on Learning of Advanced Web App Exploitation Skills**

We begin by exploring advanced techniques and attacks to which all modern-day complex applications may be vulnerable. We’ll learn about new web frameworks and web backends, then explore encryption as it relates to web applications, digging deep into practical cryptography used by the web, including techniques to identify the type of encryption in use within the application and methods for exploiting or abusing it. We’ll look at alternative front ends to web applications and web services such as mobile applications, and examine new protocols such as HTTP/2 and WebSockets. The final portion of the class will focus on how to identify and bypass web application firewalls, filtering, and other protection techniques.

**Justin Searle** SANS Senior Instructor

Justin Searle is a managing partner of UtiliSec, specializing in Smart Grid security architecture design and penetration testing. Justin led the Smart Grid Security Architecture group in the creation of NIST Interagency Report 7628 and played key roles in the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG). He currently leads the testing group at the National Electric Sector Cybersecurity Organization Resources (NESCOR). Justin has taught courses in hacking techniques, forensics, networking, and intrusion detection for multiple universities, corporations, and security conferences. In addition to electric power industry conferences, Justin frequently presents at top international security conferences such as Black Hat, DEFCON, OWASP, Nullcon, and AusCERT. Justin co-leads prominent open-source projects including the Samurai Web Testing Framework (SamuraiWTF), the Samurai Security Testing Framework for Utilities (SamuraiSTFU), Middler, Yokoso!, and Laudanum. Justin has an MBA in international technology and is a CISSP and SANS GIAC Certified Incident Handler (GCIH), Intrusion Analyst (GCIA), and Web Application Penetration Tester (GWAPT). #meeas

Register at [www.sans.org/cdi](http://www.sans.org/cdi) | 301-654-SANS (7267)
642.1 HANDS ON: Advanced Attacks

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

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

642.2 HANDS ON: Web Frameworks

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

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

642.3 HANDS ON: Web Cryptography

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

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

642.4 HANDS ON: Alternative Web Interfaces

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

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

642.5 HANDS ON: Web Application Firewall and Filter Bypass

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

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

642.6 HANDS ON: Capture the Flag

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

Six-Day Program
Thu, Dec 14 - Tue, Dec 19
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Stephen Sims

This course has evening Bootcamp Sessions

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

"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

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

Stephen Sims  SANS Senior Instructor

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

@

Register at www.sans.org/cdi | 301-654-SANS (7267)
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 cryptographic 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 NOP; Building NOP 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/cyber-defense-initiative-2017/courses

You Will Be Able To

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

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/ondemand

BUNDLE ONDEMAND
WITH THIS COURSE

www.sans.org/ondemand

45
Voucher Program

The SANS Voucher Program allows organizations to:

- Centrally administer their employee training and budget
- Potentially receive bonus funds based on their investment

$ Training Investment & Bonus Funds

To open a Voucher Account, an organization pays an agreed-upon training investment. Based on the amount of the training investment, that organization could be eligible to receive bonus funds.

**Investment and bonus funds:**
- Can be applied to any live or online SANS training course, SANS Summit, GIAC certification, or certification renewal*
- Can be increased at any time by making additional investments
- Need to be utilized within 12 months; however, the term can be extended by investing additional funds before the end of the 12-month term

*Current exceptions are the Partnership Program, Security Awareness Training, and SANS workshops hosted at events run by other companies.

Flexibility & Control

The online SANS Admin Tool allows organizations to manage their training at any time and from anywhere.

**With the SANS Admin Tool, the Administrator can:**
- Approve and manage student enrollment
- View fund usage in real time
- View students’ certification status and test results
- Obtain OnDemand course progress by student per course

Get Started

Visit www.sans.org/vouchers and submit the contact request form to have a SANS representative in your region call or email you within 24 business hours. Within as little as one week, your employees can begin their training.

www.sans.org/vouchers
Focus Job Roles and Specialized Skills
Incident Response and Enterprise Forensics

Summary: Properly trained Incident Responders can hunt for and identify compromised systems, provide effective containment during a breach, and rapidly remediate an incident. They must have in-depth digital forensics knowledge of both host and network systems within the enterprise as well as know how to apply proactive threat intelligence – skills taught by SANS in FOR508, FOR572, and FOR578.

Specialized incident response and forensics skills are taught in six additional SANS courses, covering everything from Windows forensics to reverse engineering malware. Review the following pages for detailed information about all of these courses.

Who This Path Is For: Incident Responders, Cyber Threat Analysts, Forensic Examiners, Security Analysts and Engineers all utilize this training path to advance their threat hunting and responding skills.

Why This Training Is Important: This training will teach you to detect compromised and affected systems, how and when a breach occurred, what attackers took or changed, and how to contain and remediate incidents. Upon completing your focus path in incident response and enterprise forensics, you will be able to incorporate evidence from different sources such as networks, mobile devices, and more into your investigations, provide better findings, and get the job done faster.

“This material is directly relevant to what our analysts are doing daily. Highly useful.”
-Tom L., U.S. Air Force

“For our industry, you cannot beat the quality of SANS classes and instructors. I came back to work with a new malware case and was able to implement my skills learned in class on day one. Invaluable.”
-Melissa Sokolowski, Xerox
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.

**“FOR508 was a great in-depth dive into memory analysis and event correlation.”**
- JOHN BANGE, MEIJER

---

**Chad Tilbury**  SANS Senior Instructor

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

@chadtilbury
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 and 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 beacons 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
Advanced Network Forensics and Analysis

Six-Day Program
Thu, Dec 14 - Tue, Dec 19
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Philip Hagen

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

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

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

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

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

Whether you are a consultant responding to a client’s site, a law enforcement professional assisting victims of cybercrime and seeking prosecution of those responsible, an on-staff forensic practitioner, or a member of the growing ranks of “threat hunters”, this course offers hands-on experience with real-world scenarios that will help take your work to the next level. Previous SANS SEC curriculum students and other network defenders will benefit from the FOR572 perspective on security operations as they take on more incident response and investigative responsibilities. SANS Forensics alumni from FOR500 (formerly FOR408) and FOR508 can take their existing knowledge and apply it directly to the network-based attacks that occur daily. In FOR572, we solve the same caliber of real-world problems without the use of disk or memory images.

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

Philip Hagen  SANS Certified Instructor

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

“Immediately applicable skills from an active professional in the field.”
- Abe Jones, Spectrum Health
Course Day Descriptions

572.1 HANDS ON: Off the Disk and Onto the Wire

Network data can be preserved, but only if captured directly from the wire. Whether tactical or strategic, packet capture methods are quite basic. You will re-acquaint yourself with tcpdump and Wireshark, the most common tools used to capture and analyze network packets, respectively. However, since long-term full-packet capture is still uncommon in most environments, many artifacts that can tell us about what happened on the wire in the past come from devices that manage network functions. You will learn about what kinds of devices can provide valuable evidence and at what level of granularity. We will walk through collecting evidence from one of the most common sources of network evidence, a web proxy server, then you’ll go hands-on to find and extract stolen data from the proxy yourself. The Linux SIFT virtual machine, which has been specifically loaded with a set of network forensic tools, will be your primary toolkit for the week.

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

572.2 HANDS ON: Core Protocols & Log Aggregation/Analysis

Understanding log data and how to guide the investigative process is an important network forensicators skill. Examining network-centric logs can also fill gaps left by an incomplete or nonexistent network capture. In this section, you will learn various logging mechanisms available to both endpoint and network transport devices. You will also learn how to consolidate log data from multiple sources, providing a broad corpus of evidence in one location. As the volume of log data increases, so does the need to consider automated analytic tools. You’ll use the SOF-ELK platform for post-incident log aggregation and analysis, bringing quick and decisive insight to a compromise investigation.


572.3 HANDS ON: NetFlow and File Access Protocols

In this section, you will learn the contents of typical NetFlow protocols, as well as common collection architectures and analysis methods. You’ll also learn how to distill full-packet collections to NetFlow records for quick initial analysis before diving into more cumbersome pcap files. In addition, you’ll examine the File Transfer Protocol, including how to reconstruct specific files from an FTP session. While FTP is commonly used for data eXfiltration, it is also an opportunity to refine protocol analysis techniques, due to its multiple-stream nature. Lastly, you’ll explore a variety of the network protocols unique to a Microsoft Windows or Windows-compatible environment. Attackers frequently use these protocols to “live off the land” within the victim’s environment. By using existing and expected protocols, adversaries can hide in plain sight and avoid deploying malware that could tip off the investigators to their presence and actions.

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

572.4 HANDS ON: Commercial Tools, Wireless, and Full-Packet Hunting

Commercial tools hold clear advantages in some situations a forensicators may typically encounter. Most commonly, this centers on scalability. Many open-source tools are designed for tactical or small-scale use. Whether they are used for large-scale deployments or for specific niche functionalities, these tools can immediately address many investigative needs. You’ll look at the typical areas where commercial tools in the network forensic realm tend to focus, and discuss the value each may provide for your organizational requirements or those of your clients. Additionally, we will address the forensic aspects of wireless networking.

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

572.5 HANDS ON: Encryption, Protocol Reversing, OPSEC, and Intel

Encryption is frequently cited as the most significant hurdle to effective network forensics, and for good reason. When properly implemented, encryption can be a brick wall in between an investigator and critical answers. However, technical and implementation weaknesses can be used to our advantage. Even in the absence of these weaknesses, the right analytic approach to encrypted network traffic can still yield valuable information about the content. We will discuss the basics of encryption and how to approach it during an investigation. The section will also cover flow analysis to characterize encrypted conversations.

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

572.6 HANDS ON: Network Forensics Capstone Challenge

Students will test their understanding of network evidence and their ability to articulate and support hypotheses through presentations made to the instructor and class. The audience will include senior-level decision-makers, so all presentations must include executive summaries as well as technical details. Time permitting, students should also include recommended steps that could help to prevent, detect, or mitigate a repeat compromise.

Topics: Network Forensic Case

You Will Be Able To

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

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/cyber-defense-initiative-2017/courses
Ovie Carroll  SANS Principal Instructor

Ovie Carroll has 31 years of law enforcement experience and over 20 years of cyber investigative experience. He is the Director of the Cybercrime Lab of the Computer Crime and Intellectual Property Section (CCIPS) at the Department of Justice (DOJ). The lab provides advanced computer forensics, cybercrime investigation, and other technical assistance to DOJ prosecutors to support implementation of the department’s national strategies for digital evidence and to combat electronic penetration, data theft, and cyberattacks on critical information systems. At SANS he teaches FOR500: Windows Forensic Analysis, a course he also co-authored. Prior to joining the DOJ, Ovie was a special agent in charge of overseeing the Technical Crimes Unit of the Postal Inspector General’s Office, where he was responsible for all computer intrusion investigations within the postal service network infrastructure and for providing all digital forensic analysis in support of criminal investigations and audits. He also served as a special agent in the Air Force Office of Special Investigations, investigating computer intrusions and working both general crimes and counterintelligence as well as conducting investigations into offenses including murder, rape, fraud, bribery, theft, and gangs and narcotics.  

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

Proper analysis requires real data for students to examine. The completely updated FOR500 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7/8/10, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows XP systems to just-discovered Windows 10 artifacts. FOR500 is continually updated. This course utilizes a brand-new intellectual property theft and corporate espionage case that took over six months to create. You work in the real world and your training should include real practice data. Our development team used incidents from their own experiences and investigations and created an incredibly rich and detailed scenario designed to immerse students in a true investigation. The case demonstrates the latest artifacts and technologies an investigator might encounter while analyzing Windows systems. The incredibly detailed step-by-step workbook details the tools and techniques that each investigator should follow to solve a forensic case.

“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 really knew, but in a good way.”

-Lance Freeman, BCBSLA

“It’s the best Windows forensic class in the world.”

-Bob A. Akim, SALC
500.1 HANDS ON: Windows Digital Forensics and Advanced Data Triage

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

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

500.2 HANDS ON: CORE WINDOWS FORENSICS PART 1 –

Windows Registry Forensics and Analysis

Our journey continues with the Windows Registry, where the digital forensic investigator will learn how to discover critical user and system information pertinent to almost any investigation. Each examiner will learn how to navigate and examine the Registry to obtain user-profile data and system data. The course teaches forensic investigators how to prove that a specific user performed key word searches, ran specific programs, opened and saved files, perused folders, and used removable devices.

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

500.3 HANDS ON: CORE WINDOWS FORENSICS PART 2 –

USB Devices And Shell Items

Being able to show the first and last time a file was opened is a critical analysis skill. Utilizing shortcut (LNK) and jumplist databases, we are able to easily pinpoint which file was opened and when. We will demonstrate how to examine the pagefile, system memory, and unallocated space — all difficult-to-access locations that can offer the critical data for your case.

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

500.4 HANDS ON: CORE WINDOWS FORENSICS PART 3 –

Email, Key Additional Artifacts, and Event Logs

This section discusses what types of information can be relevant to an investigation, where to find email files, and how to use forensic tools to facilitate the analysis process. We will find that the analysis process is similar across different types of email stores, but the real work takes place in the preparation — finding and extracting the email files from a variety of different sources. The last part of the section will arm each investigator with the core knowledge and capability to maintain this crucial skill for many years to come.

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

500.5 HANDS ON: CORE WINDOWS FORENSICS PART 4 –

Web Browser Forensics: Firefox, Internet Explorer, and Chrome

Throughout the section, investigators will use their skills in real hands-on cases, exploring evidence created by Chrome, Firefox, and Internet Explorer along with Windows Operating System artifacts.

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

500.6 HANDS ON: Windows Forensic Challenge

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

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

---

**You Will Be Able To**

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

“Labs walk through practical steps that will teach how the applications work. Love it!”

- Jonathan Singer, GuidePoint Security
FOR526: Memory Forensics In-Depth

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

“This course is totally awesome, relevant, and eye opening. I want to learn more every day.”
- Matthew Britton, Blue Cross Blue Shield of Louisiana

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

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

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

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

MALWARE CAN HIDE, BUT IT MUST RUN

FOR526: Memory Forensics In-Depth will teach you:
- Proper Memory Acquisition: Demonstrate targeted memory capture ensuring data integrity and overcoming obstacles to acquisition/anti-acquisition behaviors
- How to Find Evil in Memory: Detect rogue, hidden, and injected processes, kernel-level rootkits, Dynamic Link Libraries (DLL) hijacking, process hollowing, and sophisticated persistence mechanisms
- Effective Step-by-Step Memory Analysis Techniques: Use process timelining, high-low level analysis, and walking the Virtual Address Descriptors (VAD) tree to spot anomalous behavior
- Best Practice Techniques: Learn when to implement triage, live system analysis, and alternative acquisition techniques and how to devise custom parsing scripts for targeted memory analysis

Alissa Torres  SANS Certified Instructor

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

@sibertor
Course Day Descriptions

526.1 HANDS ON: Foundations in Memory Analysis and Acquisition
Simply put, memory analysis has become a required skill for all incident responders and digital forensics examiners. Regardless of the type of investigation, system memory and its contents often expose the first piece of the evidential thread that, when pulled, unravels the whole picture of what happened on the target system. Where is the malware? How did the machine get infected? Where did the attacker move laterally? Or what did the disgruntled employee do on the system? What lies in physical memory can provide answers to all of these questions and more.

Topics: Why Memory Forensics?; Investigative Methodologies; The Ubuntu SIFT and Windows 8.1 Workstations; The Volatility Framework; System Architectures; Triage versus Full Memory Acquisition; Physical Memory Acquisition

526.2 HANDS ON: Unstructured Analysis and Process Exploration
Structured memory analysis using tools that identify and interpret operating system structures is certainly powerful. However, many remnants of previously allocated memory remain available for analysis, and they cannot be parsed through structure identification. What tools are best for processing fragmented data? Unstructured analysis tools! They neither know nor care about operating system structures. Instead, they examine data, extracting findings using pattern matching. You will learn how to use Bulk Extractor to parse memory images and extract investigative leads such as email addresses, network packets, and more.

Topics: Unstructured Memory Analysis; Page File Analysis; Exploring Process Structures; List Walking and Scanning; Pool Memory; Exploring Process Relationships; Exploring DLLs; Kernel Objects

526.3 HANDS ON: Investigating the User via Memory Artifacts
An incident responder (IR) is often asked to triage a system because of a network intrusion detection system alert. The Security Operations Center makes the call and requires more information due to outbound network traffic from an endpoint and the IR team is asked to respond. In this section, we cover how to enumerate active and terminated TCP connections — selecting the right plugin for the job based on the OS version.

Topics: Network Connections; Virtual Address Descriptors; Detecting Injected Code; Analyzing the Registry via Memory Analysis; User Artifacts in Memory

526.4 HANDS ON: Internal Memory Structures
Day 4 focuses on introducing some internal memory structures (such as drivers), Windows memory table structures, and extraction techniques for portable executables. As we come to the final steps in our investigative methodology, “Spotting Rootkit Behaviors” and “Extracting Suspicious Binaries,” it is important to emphasize again the rootkit paradox. The more malicious code attempts to hide itself, the more abnormal and seemingly suspicious it appears. We will use this concept to evaluate some of the most common structures in Windows memory for hooking, the IDTs and SSDTs.

Topics: Interrupt Descriptor Tables; System Service Descriptor Tables; Drivers; Direct Kernel Object Manipulation; Module Extraction; Hibernation Files; Crash Dump Files

526.5 HANDS ON: Memory Analysis on Platforms Other than Windows
Windows systems may be the most prevalent platform encountered by forensic examiners today, but most enterprises are not homogeneous. Forensic examiners and incident responders are best served by having the skills to analyze the memory of multiple platforms, including Linux and Mac — that is, platforms other than Windows.

Topics: Linux Memory Acquisition and Analysis; Mac Memory Acquisition and Analysis

526.6 HANDS ON: Memory Analysis Challenges
This final section provides students with a direct memory forensics challenge that makes use of the SANS NetWars Tournament platform. Your memory analysis skills are put to the test with a variety of hands-on scenarios involving hibernation files, Crash Dump files, and raw memory images, reinforcing techniques covered in the first five sections of the course. These challenges strengthen students’ ability to respond to typical and atypical memory forensics challenges from all types of cases, from investigating the user to isolating the malware. By applying the techniques learned earlier in the course, students consolidate their knowledge and can shore up skill areas where they feel they need additional practice.

Topics: Malware and Rootkit Behavior Detection; Persistence Mechanism Identification; Code Injection Analysis; User Activity Reconstruction; Linux Memory Image Parsing; Mac OS X Memory Image Parsing; Windows Hibernation File Conversion and Analysis; Windows Crash Dump Analysis (Using Windows Debugger)

What You Will Receive

>SIFT Workstation 3
This course extensively uses the SIFT Workstation 3 to teach incident responders and forensic analysts how to respond to and investigate sophisticated attacks. SIFT contains hundreds of free and open-source tools, easily matching any modern forensic and incident response commercial tool suite.

- Ubuntu LTS base
- 64 bit-based system
- Better memory utilization
- Auto-DFIR package update and customizations
- Latest forensic tools and techniques
- VMware Appliance ready to tackle forensics
- Cross-compatibility between Linux and Windows
- Expanded filesystem support (NTFS, HFS, EXFAT, and more)

Windows 8.1 Workstation with license
- 64 bit-based system
- A licensed virtual machine loaded with the latest forensic tools
- VMware Appliance ready to tackle forensics

32 GB Course USB 3.0
- USB loaded with memory captures, SIFT workstation 3, tools, and documentation
- SANS Memory Forensics Exercise Workbook
- Exercise book is over 200 pages long with detailed step-by-step instructions and examples to help you become a master incident responder

SANS DFIR cheat sheets to help use the tools
- MP3 audio files of the complete course lecture
- Alissa is an excellent instructor!
- Memory forensics is one of the very best classes that SANS has to offer!”
  -David Bernal, SCITIUM

“I cannot wait to try these techniques out on some recent cases.”
- Greg Barnett, CHCIM

BUNDLE ONDEMAND WITH THIS COURSE
www.sans.org/ondemand

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/cyber-defense-initiative-2017/courses
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

### Five-Day Program

**Thu, Dec 14 - Mon, Dec 18**  
9:00am - 5:00pm  
30 CPEs  
Laptop Required  
Instructor: Jake Williams

### Who Should Attend

- Incident response team members  
- Threat hunters  
- Experienced digital forensic analysts  
- Security Operations Center personnel and information security practitioners  
- Federal agents and law enforcement officials  
- SANS FOR500 (formerly FOR408), FOR572, FOR508, or FOR610 graduates looking to take their skills to the next level

“\[This training very well summarizes CTI and connects all the dots. On the training, one will get clear answers to the following questions: what is CTI, how important is it, what is it built up on, and how can it be applied in practice?\]”  
- Nikita Martynov, NNIT A/S

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.

\[THERE IS NO TEACHER BUT THE ENEMY!\]

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
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-level attribution from previously identified campaigns and take away a more holistic view of the cyber threat intelligence industry to date. The class will finish with a discussion on consuming threat intelligence and actionable takeaways for students to make significant changes in their organizations.

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
Who Should Attend

- Experienced digital forensic analysts who want to extend their knowledge and experience to forensic analysis of mobile devices, especially smartphones
- Media exploitation analysts who need to master Tactical Exploitation or Document and Media Exploitation operations on smartphones and mobile devices by learning how individuals used their smartphones, who they communicated with, and what files they accessed
- Information security professionals who respond to data breach incidents and intrusions
- Incident response teams tasked with identifying the role that smartphones played in a breach
- Law enforcement officers, federal agents, and detectives who want to master smartphone forensics and expand their investigative skills beyond traditional host-based digital forensics
- Accident reconstruction investigators who need to determine how a phone was accessed or used during specific periods of time
- IT auditors who want to learn how smartphones can expose sensitive information
- Graduates of SANS SEC575, SEC563, FOR500 (formerly FOR408), FOR508, FOR572, FOR526, FOR610, or FOR518 who want to take their skills to the next level

Heather Mahalik  SANS Senior Instructor

Heather has worked on high-stress and high-profile cases, investigating everything from child exploitation to Osama Bin Laden’s media. She has helped law enforcement, ediscovery firms, and the federal government extract and manually decode artifacts used in solving investigations around the world. All told she has more than 14 years of experience in digital forensics, including eight years focused on mobile forensics – there’s hardly a device or platform she hasn’t researched or examined or a commercial tool she hasn’t used. These days Heather is the Director of Forensic Engineering at ManTech CARD. Heather previously led the mobile device team for Basis Technology, where she focused on mobile device exploitation in support of the federal government. She also worked as a forensic examiner at Stroz Friedberg and the U.S. State Department Computer Investigations and Forensics Lab, where she handled a number of high-profile cases. She has also developed and implemented forensic training programs and standard operating procedures.

This in-depth smartphone forensic course provides examiners and investigators with advanced skills to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. The course features 20 hands-on labs that allow students to analyze different datasets from smart devices and leverage the best forensic tools, methods, and custom scripts to learn how smartphone data hide and can be easily misinterpreted by forensic tools. Each lab is designed to teach you a lesson that can be applied to other smartphones. You will gain experience with the different data formats on multiple platforms and learn how the data are stored and encoded on each type of smart device. The labs will open your eyes to what you are missing by relying 100% on your forensic tools.

FOR585 is continuously updated to keep up with the latest malware, smartphone operating systems, third-party applications, and encryption. This intensive six-day course offers the most unique and current instruction on the planet, and it will arm you with mobile device forensic knowledge you can immediately apply to cases you’re working on the day you leave the course.

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

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

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

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

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

“This is the most advanced mobile device training that I know of and is greatly needed. It is currently the only course being taught at this level!”  - SCOTT MCNAMEE, DOD/CACI
Course Day Descriptions

585.1 HANDS ON: Malware Forensics, Smartphone Overview, and SQLite Introduction

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

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

585.2 HANDS ON: Android Forensics

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

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

585.3 HANDS ON: Android Backups and iOS Device Forensics

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

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

585.4 HANDS ON: iOS Backups, Windows, and BlackBerry Forensics

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

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

585.5 HANDS ON: Third-Party Application and Knock-Off Forensics

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

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

585.6 HANDS ON: Smartphone Forensics Capstone Exercise

This final course day will test all that you have learned during the course. Working in small groups, students will examine three smartphone devices and solve a scenario relating to a real-world smartphone forensic investigation. Each group will independently analyze the three smartphones, manually decode data, answer specific questions, form an investigation hypothesis, develop a report, and present findings.
Learn to turn malware inside out! This popular course explores malware analysis tools and techniques in depth. FOR610 training has helped forensic investigators, incident responders, security engineers, and IT administrators acquire the practical skills to examine malicious programs that target and infect Windows systems.

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

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

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

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

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.

Lenny Zeltser  SANS Senior Instructor

Aptly called the “Yoda” of malware analysis by his students, Lenny Zeltser keeps his eye on the big picture and focuses on the sum of events rather than individual occurrences. He lives by that philosophy and brings it to his job and classroom. A seasoned business and technology leader with extensive information security expertise, Lenny started his professional journey in a variety of technical Infosec roles before serving as the national lead of the U.S. security consulting practice at a major cloud services provider. Later in his career he oversaw a portfolio of security services at a Fortune 500 technology company. Today, as VP of Products at Minerva Labs, Lenny designs and builds creative anti-malware products. Lenny also developed the Linux toolkit REMnux to make it easier to use a variety of freely available malware analysis tools, many of which run well on Linux but can be difficult to find and install. Lenny earned the prestigious GIAC Security Expert professional designation, and he currently serves on the Board of Directors of the SANS Technology Institute. Lenny holds a bachelor’s degree in computer science from the University of Pennsylvania and a master’s in business administration from MIT Sloan and is the co-author of four books on malware, network security, and digital forensics. @lennyzeltser
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 (REMemory) 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, Droppers); 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 executables. The section begins by discussing how to examine suspicious websites that might host client-side exploits. Next, you will learn how to de-obfuscate malicious scripts with the help of script debuggers and interpreters, examine Microsoft Office macros, and assess the threats associated with PDF and RTF files using several techniques.

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

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 Obfuscation; PDF Document Analysis; Office Document Analysis; Memory Analysis

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

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/cyber-defense-initiative-2017/courses
Securing Approval and Budget for Training

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.
Summary: Professional security managers need broad and proven knowledge of policy, standards and practices in order to provide the greatest level of security to their organizations. They also need to speak their technicians’ language, and design security plans that withstand attack from all angles. SANS’s specialized management, audit, and legal courses deliver the tools and techniques required to lead with confidence.

More than 10 advanced and specialized training options in this practice area are detailed on the following pages.

Who This Path Is For: CISOs, IT directors, or others with responsibility for managing their organization’s security operations benefit from the experience-rich instruction in SANS management, audit, and legal courses. Security, system, and network administrators who are pursuing a CISSP® or a new management role should also prepare themselves for this type of training.

Why This Training Is Important: Professionals who train and certify in these skills are the leaders of cybersecurity. They master the specific techniques and tools needed to implement and audit the Critical Security Controls, they have a firm understanding of the eight domains of knowledge covered in the CISSP®, they can communicate information security best practices to executives and technical teams, and they are designing the Security Operation Centers of the future.

Software Security  |  Industrial Control System Security

Specialists in software security or industrial control system security can find detailed information about four additional SANS courses available for SANS Cyber Defense Initiative 2017 on page 70.

“SANS offers the best security training available.”

-David M., U.S. Air Force
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 masters in strategic studies, and holds the GSLC, CISSP, CISM and CISA certifications.  @g_mark
Course Day Descriptions

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.

You Will Be Able To
▶ Speak the same language as a manager or auditor as system, security, and network administrators
▶ Establish a minimum standard for IT management knowledge, skills, and abilities. I keep running into managers who don’t know TCP/IP, and that is OK; but then they don’t know how to calculate total cost of ownership (TCO), leaving me quietly wondering what they do know
▶ Save the up-and-coming generation of senior and rapidly advancing managers a world of pain by sharing the things we wish someone had shared with us. As the saying goes, it is OK to make mistakes, just make new ones

“Offers management insight and resources to help foster growth.”
—STEVEN BERNSTEIN, USAA

“Excellent material geared directly to general management principles that can be applied in any organization.”
—TOM KLEIS, DON

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/cyber-defense-initiative-2017/courses

65
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.

“Best security training I have ever received and just the right amount of detail for each domain.”
-Tony Barnes, United States Sugar Corporation

“Awesome! One of the best classes and experiences I have had.” -R. Glen Carl, Leidos

“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 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
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 do three things:

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

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

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

### 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.

---

**Frank Kim**  
*SANS Certified Instructor*

As CISO at the SANS Institute, Frank leads the security risk function for the most trusted source of computer security training, certification, and research in the world. He also helps shape, develop, and support the next generation of security leaders by teaching, developing courseware, and leading the management and software security curricula. Prior to the SANS Institute, Frank was Executive Director of Cyber Security at Kaiser Permanente with responsibility for delivering innovative security solutions to meet the unique needs of the nation’s largest not-for-profit health plan and integrated health care provider with annual revenue of $55 billion, 9.5 million members, and 175,000 employees. In recognition of his work, Frank was a two-time recipient of the CIO Achievement Award for business-enabling thought leadership. Frank holds degrees from the University of California at Berkeley and is the author of popular SANS courseware on strategic planning, leadership, and application security. @fykim
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

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

“Excellent training with encyclopedic coverage of the topic.”
-ALEXANDER KOTKOV, ERNST AND YOUNG

“MTG514 targets the exact information needs of my organization.”
-TIM HOFFMAN, UCSF

“Frank was an excellent instructor who had a solid grasp of the material and provided unique insight into real-world scenarios and practice of examples faced by senior cybersecurity leaders in the work place.”
-DAVE ODIN, BECHTEL

“Excellent training with encyclopedic coverage of the topic.”
-ALEXANDER KOTKOV, ERNST AND YOUNG

“MTG514 targets the exact information needs of my organization.”
-TIM HOFFMAN, UCSF

“Frank was an excellent instructor who had a solid grasp of the material and provided unique insight into real-world scenarios and practice of examples faced by senior cybersecurity leaders in the work place.”
-DAVE ODIN, BECHTEL

“This training was valuable because it helped me examine myself from an outside point of view.”
-DI, ZOETIS
This is the course to take if you have to defend web applications!

The quantity and importance of data entrusted to web applications is growing, and defenders need to learn how to secure these web applications. Traditional network defenses, such as firewalls, fail to secure web applications. DEV522 covers the OWASP Top 10 Risks and will help you better understand web application vulnerabilities, thus enabling you to properly defend your organization’s web assets.

Mitigation strategies from an infrastructure, architecture, and coding perspective will be discussed alongside real-world applications that have been proven to work. The testing aspect of vulnerabilities will also be covered so that you can ensure your application is tested for the vulnerabilities discussed in class.

To maximize the benefit for a wider range of audiences, the discussions in this course will be programming language agnostic. Focus will be maintained on security strategies rather than coding-level implementation.

DEV522: Defending Web Applications Security Essentials is intended for anyone tasked with implementing, managing, or protecting web applications. It is particularly well suited to application security analysts, developers, application architects, pen testers, auditors who are interested in recommending proper mitigations for web security issues, and infrastructure security professionals who have an interest in better defending their web applications.

The course will also cover additional issues the authors have found to be important in their day-to-day web application development practices. The topics that will be covered include:

- Infrastructure security
- Server configuration
- Authentication mechanisms
- Application language configuration
- Application coding errors like SQL injection and cross-site scripting
- Cross-site request forging
- Authentication bypass
- Web services and related flaws
- Web 2.0 and its use of web services
- XPATH and XQUERY languages and injection
- Business logic flaws
- Protective HTTP headers

The course will make heavy use of hands-on exercises and conclude with a large defensive exercise that reinforces the lessons learned throughout the week.

Johannes Ullrich, Ph.D.  SANS Senior Instructor

As Dean of Research for the SANS Technology Institute, Johannes is currently responsible for the SANS Internet Storm Center (ISC) and the GIAC Gold program. He founded DShield.org in 2000, which is now the data collection engine behind the ISC. His work with the ISC has been widely recognized, and in 2004, Network World named him one of the 50 most powerful people in the networking industry. Prior to working for SANS, Johannes worked as a lead support engineer for a web development company and as a research physicist. Johannes holds a PhD in Physics from SUNY Albany and is based in Jacksonville, Florida. His daily podcast summarizes current security news in a concise format.  @johullrich
Course Day Descriptions

522.1 HANDS ON: Web Basics and Authentication Security
We begin day one with an overview of recent web application attack and security trends, then follow up by examining the essential technologies that are at play in web applications. You cannot win the battle if you do not understand what you are trying to defend. We arm you with the right information so you can understand how web applications work and the security concepts related to them.

Topics: HTTP Basics; Overview of Web Technologies; Web Application Architecture; Recent Attack Trends; Authentication Vulnerabilities and Defense; Authorization Vulnerabilities and Defense

522.2 HANDS ON: Web Application Common Vulnerabilities & Mitigations
Since the Internet does not guarantee the secrecy of information being transferred, encryption is commonly used to protect the integrity and secrecy of information on the web. This course day covers the security of data in transit or on disk and how encryption can help with securing that information in the context of web application security.

Topics: SSL Vulnerabilities and Testing; Proper Encryption Use in Web Application; Session Vulnerabilities and Testing; Cross-site Request Forgery; Business Logic Flaws; Concurrent Execution; Insecure Code Flaws and Related Defenses; SQL Injection Vulnerabilities, Testing, and Defense

522.3 HANDS ON: Proactive Defense and Operation Security
Day three begins with a detailed discussion on cross-site scripting and related mitigation and testing strategies, as well as HTTP response splitting. The code in an application may be totally locked down, but if the server setting is insecure, the server running the application can be easily compromised. Locking down the web environment is essential, so we cover this basic concept of defending the platform and host. To enable any detection of intrusion, logging and error handling must be done correctly. We will discuss the correct approach to handling incidents and logs, then dive even further to cover the intrusion detection aspect of web application security. In the afternoon we turn our focus to the proactive defense mechanism so that we are ahead of the bad guys in the game of hack and defend.

Topics: Cross-site Scripting Vulnerability and Defenses; Web Environment Configuration Security; Intrusion Detection in Web Applications; Incident Handling; Honeytokens

522.4 HANDS ON: AJAX and Web Services Security
Day four is dedicated to the security of asynchronous JavaScript and XML (AJAX) and web services, which are currently the most active areas in web application development. Security issues continue to arise as organizations dive head first into insecurely implementing new web technologies without first understanding them. We will cover security issues, mitigation strategies, and general best practices for implementing AJAX and web services. We will also examine real-world attacks and trends to give you a better understanding of exactly what you are protecting against. Discussion focuses on the web services in the morning and AJAX technologies in the afternoon.

Topics: Web Services Overview; Security in Parsing of XML; XML Security; AJAX Technologies Overview; AJAX Attack Trends and Common Attacks; AJAX Defense

522.5 HANDS ON: Cutting-Edge Web Security
Day five focuses on cutting-edge web application technologies and current research areas. Topics such as clickjacking and DNS re-binding are covered. These vulnerabilities are difficult to defend and multiple defense strategies are needed for their defense to be successful. Another topic of discussion is the new generation of single-sign-on solutions such as OpenID. We cover the implications of using these authentication systems and the common “gotchas” to avoid. With the Web2.0 adoption, the use of Java applet, Flash, ActiveX, and Silverlight are on the increase. The security strategies of defending these technologies are discussed so that these client-side technologies can be locked down properly.

Topics: Clickjacking; DNS Rebinding; Flash Security; Java Applet Security; Single-Sign-On Solution and Security; IPv6 Impact on Web Security

522.6 HANDS ON: Capture and Defend the Flag Exercise
Day six starts with an introduction to the secure software development life cycle and how to apply it to web development. But the focus is a large lab that will tie together the lessons learned during the week and reinforce them with hands-on applications. Students will be provided with a virtual machine to implement a complete database-driven dynamic website. In addition, they will use a custom tool to enumerate security vulnerabilities and simulate a vulnerability assessment of the website. Students will then have to decide which vulnerabilities are real and which are false positives, and then mitigate the vulnerabilities. The scanner will score the student as vulnerabilities are eliminated or checked off as false positives. Advanced students will be able to extend this exercise and find vulnerabilities not presented by the scanner. Students will learn through these hands-on exercises how to secure the web application, starting with the operating system, the web server, finding configuration problems in the application language setup, and finding and fixing coding problems in the site.

Topics: Mitigation of Server Configuration Errors; Discovering and Mitigating Coding Problems; Testing Business Logic Issues and Fixing Problems; Web Services Testing and Security Problem Mitigation

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/cyber-defense-initiative-2017/courses

You Will Be Able To
> Understand the major risks and common vulnerabilities related to web applications through real-world examples
> Mitigate common security vulnerabilities in web applications using proper coding techniques, software components, configurations, and defensive architecture
> Understand the best practices in various domains of web application security such as authentication, access control, and input validation
> Fulfill the training requirement as stated in PCI DSS 6.5
> Deploy and consume web services (SOAP and REST) in a more secure fashion
> Proactively deploy cutting-edge defensive mechanisms such as the defensive HTTP response headers and Content Security Policy to improve the security of web applications
> Strategically roll out a web application security program in a large environment
> Incorporate advanced web technologies such as HTML5 and AJAX cross-domain requests into applications in a safe and secure manner
> Develop strategies to assess the security posture of multiple web applications

“This course has been excellent and will directly benefit me upon my return to work.”

-Darrell Marsh, ATFS, LLC
ICS410: ICS/SCADA Security Essentials

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

The course will provide you with:

- An understanding of 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 cybersecure-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

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 is informative and relevant to anyone working with or alongside industrial control systems.”

-Abrael Delgado,
Compquip Technologies

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 is informative and relevant to anyone working with or alongside industrial control systems.”

-Abrael Delgado,
Compquip Technologies

Bundled OnDemand

With this course:

- 30 CPEs
- Laptop Required
- Instructor: Billy Rios

Bundle OnDemand

With this course:

- 30 CPEs
- Laptop Required
- Instructor: Billy Rios

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

This course will empower students to understand their networked industrial control system environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security. This process of monitoring, responding to, and learning from threats internal to the network is known as active defense. An active defense is the approach needed to counter advanced adversaries targeting ICS, as has been seen with malware such as Stuxnet, Havex, and BlackEnergy2. Students can expect to come out of this course with the ability to deconstruct targeted ICS attacks and fight these adversaries and others. The course uses a hands-on approach and real-world malware to break down cyber attacks on ICS from start to finish. Students will gain a practical and technical understanding of leveraging active defense concepts such as using threat intelligence, performing network security monitoring, and utilizing malware analysis and incident response to ensure the safety and reliability of operations. The strategy and technical skills presented in this course serve as a basis for ICS organizations looking to show that defense is do-able.

**This course will prepare you to:**

- Examine ICS networks and identify the assets and their data flows in order to understand the network baseline information needed to identify advanced threats
- Use active defense concepts such as threat intelligence consumption, network security monitoring, malware analysis, and incident response to safeguard the ICS
- Build your own Programmable Logic Controller using a CYBATIworks Kit and keep it after the class ends
- Gain hands-on experience with samples of Havex, BlackEnergy2, and Stuxnet through engaging labs while de-constructing these threats and others
- Leverage technical tools such as Shodan, Security Onion, TCPDump, NetworkMiner, Foremost, Wireshark, Snort, Bro, SGUIL, ELSA, Volatility, Redline, FTK Imager, PDF analyzers, malware sandboxes, and more
- Create indicators of compromise (IOCs) in OpenIOC and YARA while understanding sharing standards such as STIX and TAXII
- Take advantage of models such as the Sliding Scale of Cybersecurity, the Active Cyber Defense Cycle, and the ICS Cyber Kill Chain to extract information from threats and use it to encourage the long-term success of ICS network security

**Who Should Attend**

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**

---

**Robert M. Lee**  
**SANS Certified Instructor**

Robert M. Lee is the CEO and founder of the critical infrastructure cybersecurity company Dragos Security LLC, where he has a passion for control system traffic analysis, incident response, and threat intelligence research. He is the course author of SANS ICS515: Active Defense and Incident Response and the co-author of SANS FOR578: Cyber Threat Intelligence. Robert is also a non-resident National Cyber Security Fellow at New America focusing on policy issues relating to the cybersecurity of critical infrastructure and a PhD candidate at Kings College London. For his research and focus areas, he was named one of Passcode’s Influencers and awarded EnergySec’s 2015 Cyber Security Professional of the Year. Robert obtained his start in cybersecurity in the U.S. Air Force, where he served as a Cyber Warfare Operations Officer. He has performed defense, intelligence, and attack missions in various government organizations, and he established a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Robert routinely writes articles in publications such as *Control Engineering* and the *Christian Science Monitor’s* Passcode and speaks at conferences around the world. He is also the author of *SCADA and Me* and the weekly web-comic (www.LittleBobbyComic.com) @RobertMLee

---

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/cyber-defense-initiative-2017/courses](www.sans.org/event/cyber-defense-initiative-2017/courses)
Critical Security Controls: Planning, Implementing, and Auditing

This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS). These Critical Security Controls are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all serious and sensitive organizations. These controls were selected and defined by the U.S. military and other government agencies (including NSA, DHS, GAO, and many others) and private organizations that are the most respected experts on how attacks actually work and what can be done to stop them. They defined these controls as their consensus for the best way to block known attacks and find and mitigate damage from the attacks that get through. For security professionals, the course enables you to see how to put the controls in place in your existing network through effective and widespread use of cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the controls are effectively implemented. SEC440 does not contain any labs. Students looking for hands-on labs involving the Critical Controls should take SEC566.

IPv6 Essentials

We are out of IPv4 addresses. ISPs worldwide will have to rapidly adopt IPv6 in the years ahead in order to grow, particularly because mobile devices require more and more address space. Already, modern operating systems implement IPv6 by default. Windows 7, for example, ships with Teredo enabled by default. This course is designed not just for implementers of IPv6, but also for those who just need to learn how to detect IPv6 and defend against threats that unintentional IPv6 use may bring about.

IPv6 is currently being implemented rapidly in Asia in response to the exhaustion of IPv4 address space, which is most urgently felt in fast-growing networks in China and India. Even if you do not feel the same urgency of IP address exhaustion, you may have to connect to these IPv6 resources as they become more important to global commerce.

The Security Impact of IPv6

Implementing IPv6 should not happen without carefully considering the security impact of the new protocol. Even if you haven’t implemented it yet, the ubiquitous IPv6 support in modern operating systems easily leads to unintentional IPv6 implementation, which may put your network at risk. In this course, we will start out by introducing the IPv6 protocol, explaining in detail many of its features like the IPv6 header, extension headers and auto configuration. Only by understanding the design of the protocols in depth will it be possible to appreciate the various attacks and mitigation techniques. The course will address how to take advantage of IPv6 to re-think how to assign addresses in your network and how to cope with what some suggest is the biggest security problem in IPv6: no more NAT! IPv6 doesn’t stop at the network layer. Many application layer protocols change in order to support IPv6, and we will take a close look at protocols like DNS, DHCPv6 and more.

What You Will Learn

The course covers various security technologies like firewalls and Intrusion Detection and Prevention Systems (IDS/IPS). It also addresses the challenges in adequately configuring these systems and makes suggestions as to how apply existing best practices to IPv6. Upcoming IPv6 attacks are discussed using tools like the THC IPv6 attack suite and others as an example.

This course will introduce network administrators and security professionals to the basic concepts of IPv6. While it is an introduction to IPv6, it is not an introduction to networking concepts. You should understand and be aware of the basic concepts of IPv4, and networking in general. It is an ideal refresher if you took SEC503 Intrusion Detection in Depth. However, you do not need to know IPv4 in the full detail in which it is presented in SEC503. The networking and IPv4 principles taught in SEC401 Security Essentials should prepare you for this course.
Social Engineering for Penetration Testers

SEC567 provides the blend of knowledge required to add social engineering skills to your penetration testing portfolio. Successful social engineering utilizes psychological principles and technical techniques to measure your success and manage the risk. SEC567 covers the principles of persuasion and the psychological foundations required to craft effective attacks, then bolsters this with many examples of what works, drawing on the work of cyber criminals as well as the experience of the instructor in combating them. On top of these principles we provide a number of tools (produced in our engagements over the years and now available in the course) as well as labs centered around the key technical skills required to measure your social engineering success and report it to your company or client.

You’ll learn how to perform recon on targets using a wide variety of sites and tools, create and track phishing campaigns, and develop media payloads that effectively demonstrate compromise scenarios. You’ll also learn how to conduct pretexting exercises, and we wrap the course with a fun “Capture the Human” exercise to put what you’ve learned into practice. This is the perfect course to open up new attack possibilities, to better understand the human vulnerability in attacks, and to let you practice snares that have proven themselves in tests time and time again.

Red Team Operations and Threat Emulation

SEC564 This course provides the foundation needed to manage and operate a Red Team and conduct Red Team engagements. What is Red Teaming? Red Teaming is the process of using tactics, techniques, and procedures (TTPs) to emulate a real-world threat with the goals of training and measuring the effectiveness of people, processes and technology used to defend an environment.

Red Teaming is built on the fundamentals of penetration testing, yet focuses on specific scenarios and goals used to evaluate and measure an organization’s overall security defense posture. That posture includes people, processes, and technology. This course will explore Red Teaming concepts in depth to provide a clear understanding of what a Red Team is and its role in security testing.

Organizations spend a great deal of time and money on the security of their systems. Red Teaming uses a comprehensive approach to gain insight into an organization’s overall security. Red Teams have a unique goal of testing an organization’s ability to detect, respond to, and recover from an attack. When properly conducted, Red Team activities significantly improve an organization’s security controls, help hone defensive capabilities, and measure the effectiveness of security operations.

The Red Team concept requires a different approach from a typical security test, and it relies heavily on well-defined TTPs. These are critical if a Red Team is to successfully emulate a realistic threat or adversary. Red Team results exceed a typical list of penetration test vulnerabilities, provide a deeper understanding of how an organization would perform against an actual threat, and identify where security strengths and weaknesses exist.

Metasploit Kung Fu for Enterprise Pen Testing

SEC580 Many enterprises today face regulatory or compliance requirements that mandate regular penetration testing and vulnerability assessments. Commercial tools and services for performing such tests can be expensive. While really solid free tools such as Metasploit are available, many testers do not understand the comprehensive feature sets of such tools and how to apply them in a professional-grade testing methodology. Metasploit was designed to help testers confirm vulnerabilities using an open-source and easy-to-use framework. This course will help students get the most out of this free tool.

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

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

In this course students will learn the practical skills necessary to perform regular risk assessments for their organizations. The ability to perform a risk assessment is crucial for organizations hoping to defend their systems. There are simply too many threats, too many potential vulnerabilities, and not enough resources to create an impregnable security infrastructure. Therefore every organization, whether it does so in an organized manner or not, will make priority decisions on how best to defend its valuable data assets. Risk assessment should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.

You Will Learn:

- How to perform a risk assessment step by step
- How to map an organization’s business requirements to implemented security controls
- The elements of risk assessment and the data necessary for performing an effective risk assessment
- In-depth risk management models for implementing a deeper risk management program in your organization

Two-Day Program
Tue, Dec 12 - Wed, Dec 13
9:00am - 5:00pm
12 CPEs
Laptop Required
Instructor: James Tarala

Drawing on lessons from successful DevOps security programs, students will build up a DevOps CI/CD toolchain and learn how code is automatically built, tested and deployed, using popular open-source tools including git, Puppet, Jenkins, and Docker.

In a series of labs students will inject security into a CI/CD toolchain, and learn about the tools, patterns and techniques to do this.

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

You Will Learn:

- Foundations and principles of DevOps, Continuous Delivery and Continuous Deployment
- The security risks and challenges that DevOps introduces
- The keys to successful DevOps security programs
- How to build security into Continuous Delivery and Continuous Deployment, including tools, patterns and techniques of security automation in DevOps
- How to secure your build-and-deployment environment and tool chain
- How to leverage infrastructure as code for secure configuration management and provisioning
- How manual security practices (risk assessments, audits and pen tests) can be adapted to continuously changing environments, and the important role that they still play
- Security risks and challenges that containers introduce, and how to secure container technology
- How to automate compliance in DevOps, using the DevOps Audit Defense Toolkit

Two-Day Program
Tue, Dec 12 - Wed, Dec 13
9:00am - 5:00pm
12 CPEs
Laptop Required
Instructor: Eric Johnson

Management SHORT COURSES

Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program

Organizations have invested a tremendous amount of money and resources into securing technology, but little if anything into securing their employees and staff. As a result, people, not technology, have become their weakest link in cybersecurity. The most effective way to secure the human element is to establish a high-impact security awareness program that goes beyond just compliance and changes behaviors. This intense two-day course will teach you the key concepts and skills needed to build, maintain, and measure just such a program. All course content is based on lessons learned from hundreds of security awareness programs from around the world. You will learn not only from your instructor, but from extensive interaction with your peers as well. Please bring example materials from your security awareness program that you can show and share with other students during the course. Finally, through a series of labs and exercises, you will develop your own custom security awareness plan that you can implement as soon as you return to your organization.

Who Should Attend

- Security awareness officers
- Chief security officers and security management officials
- Security auditors, and governance and compliance officers
- Training, human resources, and communications staff
- Representatives from organizations regulated by industries such as HIPAA, FISMA, FERPA, PCI-DSS, ISO/IEC 27001 SOX, NERC, or any other compliance-driven standard
- Anyone involved in planning, deploying or maintaining a security awareness program

Two-Day Program
Tue, Dec 12 - Wed, Dec 13
9:00am - 5:00pm
12 CPEs
Laptop Not Needed
Instructor: Lance Spitzner

www.sans.edu

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

#### Network Security
- **Las Vegas, NV**
  - **Sep 10-17**
- **Baltimore Fall**
  - **Baltimore, MD**
  - **Sep 25-30**
- **Rocky Mountain Fall**
  - **Denver, CO**
  - **Sep 25-30**
- **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 Virginia Winter**
  - **Reston, VA**
  - **Jan 15-20, 2018**
- **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**

#### Future Summit Events
- **Data Breach**
  - **Chicago, IL**
  - **Sep 25 - Oct 2**
- **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**
  - **Washington DC**
  - **Jan 29 - Feb 6, 2018**

### Future Community SANS Events
Local, single-course events are also offered throughout the year via SANS Community. Visit [www.sans.org/community](http://www.sans.org/community) for up-to-date Community course information.
Enrich your SANS training experience! Evening talks by our instructors and selected subject-matter experts help you broaden your knowledge, hear from the voices that matter in computer security, and get the most for your training dollar.

**KEYNOTE: Exploitation 101: Stacks, NX/DEP, ASLR and ROP!**

**David Hoelzer**

In this two-hour talk we will begin with basic stack overflows, then introduce the various protections one at a time and demonstrate how they are defeated. The talk will cover stack overflows, bypassing DEP/NX (non-executable stacks), defeating ASLR, and defeating code signing with ROP. While the talk covers technical topics, even those with less of a technical background will walk away with an appreciation of just how easy exploit development actually is!

**Women’s CONNECT Event**

**Hosted by SANS COINS Program and ISSA WIS SIG**

Joins SANS and the ISSA International Women In Security Special Interest Group (WIS SIG) as we partner with local association chapters and groups to foster an evening of connections. Group representatives will be on hand to discuss their activities and the benefits of membership. From Jean Jennings Bartik to Diane Greene, women have always been a driving force in the field of information technology. Their stories are ones not only of overcoming challenges but of innovation and inspiration. Enjoy the connection building and camaraderie of your peers while discussing the recent successes relating to local luminaries such as Joann Maguire, Sandra Rothenberg, Pam Shockley-Zalabak, Judith Wagner, among MANY others.

**Malware Analysis for Incident Responders: Getting Started**

**Lenny Zeltser**

Knowing how to analyze malware has become a critical skill for incident responders and forensic investigators. A good way to get started is to examine how malicious software behaves in a controlled laboratory environment. In this 90-minute briefing, Lenny Zeltser demonstrates key aspects of this process, walking you through behavioral analysis of a malware specimen by using several free tools and even peeking into the world of code analysis. You will see practical techniques in action and understand how malware analysis will help you triage the incident to assess key capabilities of the malicious software. You will also learn how to determine ways of identifying this malware on systems in your environment by establishing indicators of compromise. This presentation will help you start learning how to turn malware inside out.

**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 they face. 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.

**Building an Effective Security Monitoring Program**

**Jake Williams**

Security monitoring is hard, really hard. So hard that we fail at it regularly. Most breaches aren’t detected for months, many aren’t detected for years. This isn’t surprising since most defenders implement monitoring programs that are geared towards achieving compliance rather than catching attackers. But those goals need not be mutually exclusive. In this talk, Jake will share his years of experience architecting monitoring programs to help you build one that doesn’t suck, catches attackers, and will virtually guarantee your next promotion.

**The Security Impact of IPv6**

**Johannes Ullrich, Ph.D.**

IPv6 is more than just lots of addresses. IPv6 is protocol moving IP into the modern world of gigabit networks connecting billions of machines with gigabytes of RAM. In many ways, this transition is similar to the “DC” to “AC” power conversion in the late 1890s. While we still use DC in many places, AC has shown to be more flexible and scalable. Its initial adoption was hindered by security concerns, and DC supporters like Edison went to great lengths to demonstrate the security problems by stealing pets and electrocuting them in public displays. The fear of IPv6 is in many ways a fear of the unknown. IPv6 has some inherent risks, in particular if the protocol’s opportunities are not well understood, and if IPv4 thinking is applied to its deployment. We will discuss the impact of IPv6 on security architecture, intrusion detection, and network forensics, without harming anybody’s pet.

**Securing Your Kids**

**Lance Spitzner**

Technology is an amazing tool. It allows our kids to access a tremendous amount of information, meet new people, and communicate with friends around the world. For them to be successful in the 21st century they have to know and understand how to leverage these new tools. However, with all these capabilities come a variety of new risks that as parents you may not understand or even be aware of. In this one-hour presentation we cover the top three risks to kids online and the top steps you can take to protect them.
Learn how the most effective organizations are overcoming these common obstacles to a successful awareness program, what we found about three challenges and how you can apply their lessons learned to your own security awareness program.

The Three C's to Building a Mature Awareness Program
Lance Spitzner
After working with hundreds of organizations, we have found three common obstacles to a successful awareness program, what we call the three C's: Communication, Collaboration and Culture. Learn how the most effective organizations are overcoming these three challenges and how you can apply their lessons learned to your own security awareness program.

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.

Introducing DeepBlueCLI, a PowerShell Module for Hunt Teaming Via Windows Event Logs
Eric Conrad
A number of events are triggered in Windows environments during virtually every successful breach, including service creation events and errors, user creation events, extremely long command lines, compressed and base64 encoded PowerShell functions, and more. Microsoft has added a wealth of BlueTeam tools to its operating systems, including native support of logging the full command line used to launch all processes, without requiring third-party tools (or Sysmon). KB3004375 adds this feature to Windows 7 and Server 2008R2. DeepBlueCLI can automatically determine events that are typically triggered during most successful breaches, including use of malicious command lines including PowerShell.

When IoT Attacks: Understanding the Safety Risks Associated With Connected Devices
Billy Rios
The Internet of Things (IoT) is all around us, making our lives more convenient. However, we've seen IoT devices being taken over to conduct DDoS attacks. We've heard about connected refrigerators being used to SPAM users and baby monitors being used to scream obscenities at infants. But could an IoT device be re-purposed to physically attack an unsuspecting user? Let's find out.

Control Things Platform
Justin Searle
SamuraiSTFU was a great start to help electric utilities do penetration testing of their DCS and SCADA networks. However, it just wasn't enough. SamuraiSTFU has expanded its goals to include all control systems and IoT devices, thus requiring a name change and a complete rebuild of the pentest distribution. Come check out the new Control Things Platform, a pentesting platform to help you learn, calibrate, and perform security testing of control networks in any ICS organization.

The 14 Absolute Truths of Security
Keith Palmgren
Keith Palmgren has identified 14 absolute truths of security – things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these 14 absolute truths and how they affect a security program can lead to the success of that program. Failing to recognize these truths will spell almost certain doom. Here we will take a non-technical look at each of the 14 absolute truths in turn, examine what they mean to the security manager, what they mean to the security posture, and how understanding them will lead to a successful security program.

SIEM and Threat Intelligence
Robert M. Lee
Industrial control systems (ICS) are some of the most defensible environments on the planet. Sure, ICS tend to have legacy equipment and numerous vulnerabilities, but if you really want to make the lights blink, it’s going to take more than an exploit. In this presentation, the course author for ICS515: ICS Active Defense and Incident Response and FOR578: Cyber Threat Intelligence, will talk about what it means to make a defensible environment a defended one by leveraging active defense best practices such as threat hunting and network security monitoring. In addition, what types of threat intelligence are applicable to such environments will be covered with use-cases highlighting lessons learned for both good and bad practices. Ultimately, defending these industrial environments requires a human focus.

Coffee & Donuts with the Graduate Students
Hosted by SANS Technology Institute
Get the inside scoop on what it’s like to pursue a graduate degree in cybersecurity from SANS from like-minded information security professionals currently enrolled in SANS graduate programs. SANS’s regionally accredited graduate program, the SANS Technology Institute, combines SANS technical training and certifications with leadership and management curriculum specifically designed for the unique needs of aspiring leaders. Find out how the class you’re taking this week may be applied towards a master’s degree or graduate certificate program. Visit www.sans.edu for complete information on curriculum, admissions, and funding options.
NULL
## Job-Based Long Courses

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Name</th>
<th>Paid before 10-18-17</th>
<th>Paid before 11-8-17</th>
<th>Paid after 11-8-17</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></td>
<td></td>
<td></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>SEC501</td>
<td>Advanced Security Essentials — Enterprise Defender</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 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>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>SEC505</td>
<td>Securing Windows and PowerShell Automation</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 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>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>SEC545</td>
<td>Cloud Security Architecture and Operations NEW!</td>
<td>$4,980</td>
<td>$5,180</td>
<td>$5,380</td>
<td></td>
<td></td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC550</td>
<td>Active Defense, Offensive Countermeasures, and Cyber Deception</td>
<td>$4,980</td>
<td>$5,180</td>
<td>$5,380</td>
<td></td>
<td></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></td>
<td></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>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>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>SEC642</td>
<td>Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation 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>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>FOR500</td>
<td>Windows Forensic Analysis (formerly FOR408)</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>FOR526</td>
<td>Memory Forensics 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>FOR572</td>
<td>Advanced Network Forensics and Analysis</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>FOR585</td>
<td>Advanced Smartphone Forensics</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>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>DEV522</td>
<td>Defending Web Applications Security Essentials</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>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>
<tr>
<td>ICS515</td>
<td>ICS Active Defense and Incident Response</td>
<td>$5,580</td>
<td>$5,780</td>
<td>$5,980</td>
<td>$729</td>
<td>$729</td>
<td>$1,260</td>
</tr>
</tbody>
</table>

## Skill-Based Short 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>SEC440</td>
<td>Critical Security Controls: Planning, Implementing, and Auditing</td>
<td>$1,860</td>
<td>$2,480</td>
</tr>
<tr>
<td>SEC546</td>
<td>IPv6 Essentials</td>
<td>$1,860</td>
<td>$2,480</td>
</tr>
<tr>
<td>SEC564</td>
<td>Red Team Operations and Threat Emulation NEW!</td>
<td>$1,860</td>
<td>$2,480</td>
</tr>
<tr>
<td>SEC567</td>
<td>Social Engineering for Penetration Testers</td>
<td>$1,860</td>
<td>$2,480</td>
</tr>
<tr>
<td>SEC580</td>
<td>Metasploit Kung Fu for Enterprise Pen Testing</td>
<td>$1,860</td>
<td>$2,480</td>
</tr>
<tr>
<td>MGT415</td>
<td>A Practical Introduction to Cybersecurity Risk Management.</td>
<td>$1,860</td>
<td>$2,480</td>
</tr>
<tr>
<td>MGT433</td>
<td>Securing The Human: How to Build, Maintain &amp; Measure a High-Impact Awareness Program</td>
<td>$1,860</td>
<td>$2,480</td>
</tr>
<tr>
<td>DEV534</td>
<td>Secure DevOps: A Practical Introduction NEW!</td>
<td>$1,860</td>
<td>$2,480</td>
</tr>
<tr>
<td>SPECIAL</td>
<td>Core NetWars Experience – Tournament Entrance Fee</td>
<td>FREE</td>
<td>$1,959</td>
</tr>
<tr>
<td>SPECIAL</td>
<td>DFIR NetWars Tournament – Tournament Entrance Fee</td>
<td>FREE</td>
<td>$1,959</td>
</tr>
<tr>
<td>SPECIAL</td>
<td>Cyber Defense NetWars Tournament – Tournament Entrance Fee</td>
<td>FREE</td>
<td>$1,959</td>
</tr>
</tbody>
</table>

### Pay for any long course using the code EarlyBird17 at checkout by October 18th to get $400 OFF* or by November 8th 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