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

Security East 2019
New Orleans | February 2-9

Protect Your Business | Advance Your Career
30+ hands-on, immersion-style courses taught by real-world practitioners

See inside for courses and GIAC certifications in:
- Cyber Defense
- Ethical Hacking
- Security Management
- Detection & Monitoring
- Incident Response
- ICS/SCADA Security
- Penetration Testing
- Digital Forensics
- Secure Development
- See inside for courses and GIAC certifications in:

PLUS NEW COURSES
- SIEM Design & Implementation
- Defensible Security Architecture
- Managing Security Vulnerabilities: Enterprise and Cloud
- SIEM Design & Implementation
- Defensible Security Architecture
- Managing Security Vulnerabilities: Enterprise and Cloud

“Always relevant and up-to-date information is taught. I always walk away with a better understanding of current risks and mitigation possibilities. SANS courses also seem to spur additional ideas on how to better implement security in our environment.”

-Dan Smith, Raytheon Company

SAVE $350
Register and pay by Dec 12th
Use code EarlyBird19

www.sans.org/security-east
## Courses at a Glance

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

<table>
<thead>
<tr>
<th>Course Title</th>
<th>GIAC Certifications</th>
<th>Page</th>
<th>Available via On Demand</th>
<th>Bundle OnDemand with this course</th>
<th>Needs DoDD 8140 (STIP) Requirements</th>
<th>Instructor</th>
<th>Security East 2019 Training Schedule</th>
</tr>
</thead>
</table>
| SEC401 Security Essentials Bootcamp Style                                    | GSEC                | 12   |                         |                                  |                                     | Dr. Eric Cole                | Sat 2
| SEC440 Critical Security Controls: Planning, Implementing, and Auditing       |                     | 58   |                         |                                  |                                     | Russell Eubanks              | Sun 2-3
| SEC455 SIEM Design and Implementation                                      |                     | 58   |                         |                                  |                                     | John Hubbard                 | Mon 2-5
| SEC503 Intrusion Detection In-Depth                                          | GCA                 | 16   |                         |                                  |                                     | David Hoelzer                | Wed 2-7
| SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling             | GCIB                | 18   |                         |                                  |                                     | Michael Murr                 | Thu 2-8
| SEC511 Continuous Monitoring and Security Operations                        | GMON                | 20   |                         |                                  |                                     | Bryan Simon                  | Fri 2-9
| SEC524 Cloud Security Fundamentals                                          |                     | 58   |                         |                                  |                                     | Jorge Orchilies              | Sat 2-9
| SEC530 Defensible Security Architecture                                      |                     | 10   |                         |                                  |                                     | Ismael Valenzuela            | Sun 2-10
| SEC545 Cloud Security Architecture and Operations                           |                     | 22   |                         |                                  |                                     | Dave Shackelford             | Mon 2-11
| SEC555 SIEM with Tactical Analytics                                         | GCDA                | 24   |                         |                                  |                                     | John Hubbard                 | Tue 2-12
| SEC566 Implementing and Auditing the Critical Security Controls – In-Depth   | GCCC                | 26   |                         |                                  |                                     | James Tarala                 | Wed 2-13
| SEC562 Web App Penetration Testing and Ethical Hacking                      | GWAFT               | 30   |                         |                                  |                                     | Eric Conrad                  | Thu 2-14
| SEC560 Network Penetration Testing and Ethical Hacking                       | GPEN                | 32   |                         |                                  |                                     | Kevin Fiscus                 | Fri 2-15
| SEC564 Red Team Operations and Threat Emulation                             |                     | 59   |                         |                                  |                                     | Joe Vest                     | Sat 2-16
| SEC567 Social Engineering for Penetration Testers                           |                     | 59   |                         |                                  |                                     | Christopher Crowley          | Sun 2-17
| SEC579 Mobile Device Security and Ethical Hacking                           | GMOB                | 34   |                         |                                  |                                     | Joshua Wright                | Mon 2-18
| SEC580 Metasploit Rung Fo for Enterprise Pen Testing                         |                     | 59   |                         |                                  |                                     | Kevin Fiscus                 | Tue 2-19
| SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking    | GXPEN               | 36   |                         |                                  |                                     | Jake Williams                | Wed 2-20
| FOR508 Advanced Digital Forensics, Incident Response, and Threat Hunting     | GCFA                | 38   |                         |                                  |                                     | Rob Lee                      | Thu 2-21
| FOR572 Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response | GNFA            | 40   |                         |                                  |                                     | Philip Hagen                 | Fri 2-22
| FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques    | GREM                | 42   |                         |                                  |                                     | Anuj Soni                    | Sat 2-23
| MGTS44 SANS Training Program for CISSP® Certification                      | GISP                | 44   |                         |                                  |                                     | Seth Misenar                 | Sun 2-24
| MGTS15 A Practical Introduction to Cyber Security Risk Management           |                     | 60   |                         |                                  |                                     | Brian Ventura               | Mon 2-25
| MGTS12 Security Leadership Essentials for Managers                          | GSLC                | 46   |                         |                                  |                                     | G. Mark Hardy                | Tue 2-26
| MGTS14 Security Strategic Planning, Policy, and Leadership                  | GSTRT               | 48   |                         |                                  |                                     | Russell Eubanks              | Wed 2-27
| MGTS16 Managing Security Vulnerabilities: Enterprise and Cloud              |                     | 50   |                         |                                  |                                     | David R. Miller              | Thu 2-28
| MGTS17 Managing Security Operations: Detection, Response, and Intelligence  |                     | 52   |                         |                                  |                                     | Christopher Crowley          | Fri 2-29
| DEV531 Defending Mobile Applications Security Essentials                    |                     | 60   |                         |                                  |                                     | Gregory Leonard              | Sat 2-30
| DEV540 Secure DevOps and Cloud Application Security                          |                     | 54   |                         |                                  |                                     | Gregory Leonard              | Sun 2-31
| IC5410 ICS/SCADA Security Essentials                                        | GCISP               | 56   |                         |                                  |                                     | Paul Piotrowski              | Mon 3-1
| DFR/SCADA ICS/SCADA Security Essentials                                     |                     |      |                         |                                  |                                     |                            | Tue 3-2
| Cyber Defense NetWars Tournament                                            |                     |      |                         |                                  |                                     |                            | Wed 3-3

### Contents

- **About SANS** .......................... 2
- **SANS Faculty** ................. 3
- **Securing Approval & Budget for Training** 4
- **Build a High-Performing Security Organization** 5
- **SANS Training Roadmap** .......... 6-7
- **GIAC Certifications** .......... 28
- **Vendor-Sponsored Events** .......... 62
- **Registration Fees** ............. 65
- **Future SANS Training Events** .......... 63
- **Free Resources** .............. 64
- **Hotel Information** ........... 64
- **Registra** ......... 64

---

Christopher Crowley

G. Mark Hardy

Russell Eubanks

David R. Miller

Russell Eubanks

Jorge Orchilles

Dr. Eric Cole

James Tarala

Eric Conrad

Kevin Fiscus

Jake Williams

Russell Eubanks

David R. Miller
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 65 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 area 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.

**SKILLS VALIDATION**
GIAC exams and certifications ensure that professionals have learned and can apply the real-world knowledge and skills taught in class. More than 30 certifications align with SANS training and ensure mastery in critical, specialized InfoSec domains and job-specific roles. See [www.giac.org](http://www.giac.org) for more information.

**SANS FORMATS**
More than 200 live SANS events are offered each year, featuring 5- and 6-day technical courses taught in classrooms around the world. SANS training events provide an ideal learning environment that includes opportunities to network with other security professionals, SANS instructors, and staff.

SANS training is also 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.

**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.

**HOW TO REGISTER FOR SANS TRAINING**
Students can learn more and register online by visiting [www.sans.org](http://www.sans.org)
SANS Faculty

A revered faculty of cybersecurity specialists author and teach SANS courses, which is why so many professionals choose SANS training again and again, year after year.

Just over 90 individuals are currently qualified to hold the title SANS Certified Instructor. They are the founders of international cybersecurity organizations, authors of top-selling information security books, and developers of the most advanced cyber ranges and Capture-the-Flag challenges. They are called on regularly to share their expertise with government and commercial organizations around the world.

Whether you train with us live at an event or online, SANS guarantees that you will be able to apply what you learn from our instructors and training as soon as you return to work.

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

Ron Foupht, Sirius Computer Solutions

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

Packaging matters

Write a formal request

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

Clearly state the benefits

Be specific

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

Set the context

Establish longer-term expectations

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

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

**Four job roles** typically emerge as organizations grow in size, risk, and/or complexity:

- **Security Monitoring & Detection Professionals** – The detection of what is happening in your environment requires an increasingly sophisticated set of skills and capabilities. Vendor training all too often teaches to the tool, and not how or why the tool works, or how it can be best deployed. Identifying security anomalies requires increased depth of understanding to deploy detection and monitoring tools and interpret their output.

- **Pen Testers & Vulnerability Analysts** – The professional who can find weaknesses is often a different breed than one focused exclusively on building defenses. A basic tenet of red team/blue team deployments is that finding vulnerabilities requires a different way of thinking and different tools, but is essential for defense specialists to improve defenses.

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

- **Security Managers** – With an increasing number of talented technologists, organizations require effective leaders to manage their teams and processes. Those managers will not necessarily perform hands-on work, but they must know enough about the underlying technologies and frameworks to help set strategy, develop appropriate policies, interact with skilled practitioners, and measure outcomes.

Within (or beyond) these four areas, high-performing security organizations will develop individual professionals to either utilize advanced skills generally, or to meet specialized needs. Along the entire spectrum, from Active Defense to Cloud Defense to Python for Pen Testers to Malware Re-engineering, SANS offers more than 30 courses for specialized roles or more advanced topics, meeting the needs of nearly all security professionals at every level.

**Practical strategies for building an information security group, based on SANS research and observations globally:**

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

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

- **Determine the number** and type of professionals you require to perform the hands-on work. Engage in a persistent campaign to develop professionals with the appropriate skills and capabilities. Cybersecurity is a specialized practice area within IT and demands specialized training.
### Training Roadmap | Development Paths

#### Baseline Skills

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

#### Focus Job Roles

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

#### Crucial Skills, Specialized Roles

3. You are a candidate for specialized or advanced training

### Core Skills | Prevent, Defend, Maintain

- **Every Security Professional Should Know**
  - **Security Essentials**
    - SEC401 Security Essentials Bootcamp Style | GIAC
  - **Nuclear Techniques**
    - SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling | GIAC

#### Cyber Defense Operations | Harden Your Defenses

- **Specialized Defense Area**
  - **Advanced Generalist**
    - GIAC Advanced Security Essentials - Enterprise Defender | GIAC
  - **Cloud Security**
    - GIAC Cloud Security Architecture and Operations
  - **Industrial Controls**
    - GIAC Industrial Control Systems Security (ICSS)

- **Other Advanced Defense Courses**
  - **Critical Controls**
    - GIAC Implementing and Auditing the Critical Security Controls – In Depth | GIAC
  - **Security Architecture**
    - GIAC Defensible Security Architecture

#### Incident Response & Threat Hunting | Detect, Defend, Defeat

- **Specialized Penetration Testing | Focused Techniques & Areas**
  - **De-Depth Cognizance**
    - GIAC Enterprise Threat and Vulnerability Assessment
  - **Networks**
    - GIAC Advanced Penetration Testing, Exploit Writing, and Exploitation Techniques | GIAC
  - **Web Apps**
    - GIAC Advanced Web App Penetration Testing and Exploitation Techniques | GIAC

- **Hands-On Ranges**
  - GIAC CyberDefend Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses | GIAC
  - GIAC Advanced Forensic Tools for Investigators | GIAC

#### Host & Network Forensics | Investigate, Defend, Recover

- **Digital Forensics, Malware Analysis, & Threat Intel | Specialized Investigation Skills**
  - **Malware Analysis**
    - GIAC Reverse Engineering Malware: Malware Analysis Tools and Techniques | GIAC
  - **Threat Intelligence**
    - GIAC Cyber Threat Intelligence | GIAC

### Development & Secure Coding | Build, Secure, Maintain


- **Every Security Manager Should Know**
  - **Leadership Essentials**
    - GIAC Security Leadership Essentials for Managers | GIAC
  - **Critical Controls**
    - GIAC Critical Security Controls – In Depth | GIAC

- **Advanced Management | Advanced Leadership, Audit, Legal**
  - **Management Skills**
    - GIAC Security Strategic Planning, Policy, and Leadership | GIAC
  - **Auditing and Monitoring Networks, Protocols & Systems | GIAC
  - **Law & Investigations**
    - GIAC Law of Digital Security and Investigations | GIAC

### Industrial Control Systems

- **ICS Security Professionals Need**
  - GIAC ICS/SCADA Security Essentials | GIAC

### Development Offerings

- **Every Developer Should Know**
  - GIAC220 Wracking Web Applications Security Essentials | GIAC
  - GIAC515 Secure Development and Cloud Application Security

### Language-Specific Courses

- JAVA/RE
  - GIAC Secure Coding in Java (J5): Developing Defensibile Applications | GIAC
- .NET
  - GIAC Secure Coding in .NET: Developing Defensibile Applications | GIAC

---

**Training Roadmap**

- **Baseline Skills**
- **Focus Job Roles**
- **Crucial Skills, Specialized Roles**
- **Core Skills | Prevent, Defend, Maintain**
- **Cyber Defense Operations | Harden Your Defenses**
- **Incident Response & Threat Hunting | Detect, Defend, Defeat**
- **Host & Network Forensics | Investigate, Defend, Recover**
- **Digital Forensics, Malware Analysis, & Threat Intel | Specialized Investigation Skills**
- **Development & Secure Coding | Build, Secure, Maintain**
- **Security Management | Managing Technical Security Operations**
- **Advanced Management | Advanced Leadership, Audit, Legal**

**Key**

- **GIAC**
- **SANS**

---

**SANS Training Program for CISSP® Certification | GIAC**

---

**SANS Training Program for GSEC® Certification | GIAC**
Extend and Validate Your Training

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

**Extend Your Training Experience with an OnDemand Bundle**

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

**OnDemand Bundle price – $769**

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

-ROBERT JONES, TEAM JONES, INC.

**Get Certified with GIAC Certifications**

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

**GIAC bundle price – $769**

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

-CHRISTINA FORD, DEPARTMENT OF COMMERCE

---

**More Information**

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

*GIAC and OnDemand Bundles are only available for certain courses.*
Training Events
Live SANS training events feature SANS top instructors teaching multiple courses at a single location. These events feature:

- Focused, immersive learning without the distractions of your office environment
- Direct access to SANS Certified Instructors
- Interactions with and learning from other professionals
- SANS@Night events, NetWars, vendor presentations, industry receptions, and many other activities

Our live training events in North America, serving thousands of students, are held in Orlando, Washington DC, Las Vegas, New Orleans, and San Diego. Regional events with hundreds of students are held in most major metropolitan areas during the year.

Summits
SANS Summits focus one or two days on a single topic of particular interest to the community. Speakers and talks are curated to ensure the greatest applicability to participants. Closely aligned SANS courses are offered before or after each Summit to give attendees a convenient way to enhance their Summit experience with in-depth training.

Community SANS Courses
Same SANS courses, courseware, and labs, taught by up-and-coming instructors in a regional area. Smaller classes allow for more extensive instructor interaction. No need to travel; commute each day to a nearby location.

Private Classes
Have a SANS Certified Instructor train your staff privately on site so that you can incorporate insights, stories, and questions pertinent to your business objectives. Private training allows you to freely discuss sensitive issues and spend additional time on topics relevant to your organization.

Online Training
SANS Online Training delivers the same world-renowned instructors, content, and learning results as SANS live training options, with several unique and valuable benefits. Students who train online enjoy subject-matter-expert support throughout the course, online access to all course labs, and the ability to revisit content without limits.

No matter where you are or when you can train, SANS has courses that will fit around your life.

Top Reasons to Take SANS Training Online:

- **Rewind** your training, so you can review complex details or topics
- **Revisit** content to ensure you master key concepts
- **Reinforce** your learning with subject-matter experts and labs
- **Retain** your knowledge of course content with four months of access

Our SANS OnDemand, vLive, Simulcast, and SelfStudy formats are backed by nearly 100 professionals who ensure we deliver the same quality instruction online (including support) as we do at live training events.

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

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

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

“The course content and OnDemand delivery method have both exceeded my expectations.”
—R/o.sc/b.sc/e.sc/r.sc/t.sc J/o.sc/n.sc/e.sc/s.sc, T/e.sc/a.sc/m.sc J/o.sc/n.sc/e.sc/s.sc

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

“GIAC is the only certification that proves you have hands-on technical skills.”
—C/h.sc/r.sc/i.sc/s.sc/t.sc/i.sc/n.sc/a.sc F/o.sc/r.sc/d.sc, D/e.sc/p.sc/a.sc/r.sc/t.sc/m.sc/e.sc/n.sc/t.sc /o.sc/f.sc C/o.sc/m.sc/m.sc/e.sc/r.sc/c.sc/e.sc

Special Pricing
GIAC bundle price – $769
OnDemand Bundle price – $769

“Extend your Training Experience with an OnDemand Bundle”
Get Certifed with GIAC Certifcations
Add an OnDemand Bundle OR GIAC Certification Attempt to your course within seven days of this event to get bundle pricing.*

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

Extended and Validate Your Training Experience with an OnDemand Bundle
- Get Certifed with GIAC Certifcations
- Add an OnDemand Bundle OR GIAC Certification Attempt to your course within seven days of this event to get bundle pricing.*

Special Pricing
GIAC bundle price – $769
OnDemand Bundle price – $769

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

Ismael Valenzuela
SANS Certified Instructor

SEC530: Defensible Security Architecture

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

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

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

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

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

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

“SANS training addresses the most relevant security issues and practices that immediately increase my work capabilities.”
- Steven Launius, Discover Financial Services

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

Register at www.sans.org/security-east | 301-654-SANS (7267)
Adversaries Already in Our Networks

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/security-east-2019/courses

This course is available via Simulcast. See page 64 for more information.

Day 1: Defensible Security Architecture

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

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

Day 2: Network Security Architecture

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

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

Day 3: Architecting Application Layer Security

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

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

Day 4: Data and Application Security Architecture

Day 4 continues hardening the infrastructure and moves on to layer six: data-centric security. We will progress through multiple levels and missions designed to ensure mastery of the modern cyber defense techniques promoted throughout the course. Powered by NetWars, day six provides a full day of hands-on work applying the principles taught throughout the week. Your team will progress through multiple levels and missions designed to ensure mastery of the modern cyber defense techniques promoted throughout this course. Teams will assess, design, and secure a variety of computer systems and devices, leveraging all seven layers of the OSI model.

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

Day 5: Zero Trust Architecture: Addressing the Adversaries Already in Our Networks

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

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

Day 6: Hands-On Secure-the-Flag Challenge

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

Topics: Capstone – Design/Detect/Defend

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/security-east-2019/courses
You Will Be Able To

- Apply what you learned directly to your job when you go back to work
- Design and build a network architecture using VLANs, NAC, and 802.1x based on advanced persistent threat indicators of compromise
- Run Windows command line tools to analyze the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat, etc.) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Install VMWare and create virtual machines to create a virtual lab to test and evaluate tools/security of systems
- Create an effective policy that can be enforced within an organization and design a checklist to validate security and create metrics to tie into training and awareness
- Identify visible weaknesses of a system using various tools and, once vulnerabilities are discovered, cover ways to configure the system to be more secure
- Build a network visibility map that can be used for hardening of a network — validating the attack surface and covering ways to reduce that surface by hardening and patching
- Sniff open protocols like telnet and ftp and determine the content, passwords, and vulnerabilities using WireShark

Dr. Eric Cole
SANS Faculty Fellow

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

Is SEC401: Security Essentials Bootcamp Style the right course for you?

STOP and ask yourself the following questions:

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

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

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

Prevention is ideal but detection is a must.

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

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

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

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole has experience in information technology with a focus on helping customers focus on the right areas of security by building out a dynamic defense. He has a master’s degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. He served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is the author of several books, including Advanced Persistent Threat, Hackers Beware, Hiding in Plain Sight, Network Security Bible 2nd Edition, and Insider Threat. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Dr. Cole is the founder and an executive leader at Secure Anchor Consulting where he provides leading-edge cybersecurity consulting services, expert witness work, and leads research and development initiatives to advance the state-of-the-art in information systems security. He was the lone inductee into the InfoSec European Hall of Fame in 2014. Dr. Cole is actively involved with the SANS Technology Institute (STI) and is a SANS faculty Fellow and course author who works with students, teaches, and develops and maintains courseware. @drericcole
D1: Network Security Essentials
A key way that attackers gain access to a company’s resources is through a network connected to the Internet. A company wants to try to prevent as many attacks as possible, but in cases where it cannot prevent an attack, it must detect it in a timely manner. Therefore, an understanding and ability to create and identify the goals of building a defensible network architecture are critical. It is just as important to know and understand the architecture of the system, types of designs, communication flow and how to protect against attacks using devices such as routers and firewalls. These essentials, and more, will be covered during this first day in order to provide a firm foundation for the consecutive days of training.


D2: Defense-In-Depth and Attacks
To secure an enterprise network, you must understand the general principles of network security. On this second course day, we look at threats to our systems and take a “big picture” look at how to defend against them. You will learn that protections need to be layered – a principle called defense-in-depth. We explain some principles that will serve you well in protecting your systems. You will also learn about key areas of network security.


D3: Threat Management
Whether targeting a specific system or just searching the Internet for an easy target, an attacker uses an arsenal of tools to automate finding new systems, mapping out networks, and probing for specific, exploitable vulnerabilities. This phase of an attack is called reconnaissance, and it can be launched by an attacker any amount of time before exploiting vulnerabilities and gaining access to systems and networks. In fact, evidence of reconnaissance activity can be a clue that a targeted attack is on the horizon.


D4: Cryptography, Risk Management, and Response
There is no silver bullet when it comes to security. However, there is one technology that would help solve a lot of security issues, though few companies deploy it correctly. This technology is cryptography. Concealing the meaning of a message can prevent unauthorized parties from reading sensitive information. This course section looks at various aspects of encryption and how it can be used to secure a company’s assets. A related area called steganography, or information hiding, is also covered.


D5: Windows Security
Remember when Windows was simple? Windows XP desktops in a little workgroup...what could be easier? A lot has changed over time. Now, we have Windows tablets, Azure, Active Directory, PowerShell, Office 365, Hyper-V, Virtual Desktop Infrastructure (VDI), and so on. Microsoft is battling Google, Apple, Amazon.com, and other cloud giants for supremacy. The trick is to do it securely, of course. Windows is the most widely-used and targeted operating system on the planet. At the same time, the complexities of Active Directory, PKI, BitLocker, Applocker, and User Account Control represent both challenges and opportunities. This section will help you quickly master the world of Windows security while showing you the tools that can simplify and automate your work. You will complete the day with a solid grounding in Windows security by looking at automation, auditing and forensics.


D6: Linux Security
While organizations do not have as many Unix/Linux systems, those that they do have are often some of the most critical systems that need to be protected. This final course day provides step-by-step guidance to improve the security of any Linux system. The course combines practical “how to” instructions with background information for Linux beginners, as well as security advice and best practices for administrators of all levels of expertise. This module discusses the foundational items that are needed to understand how to configure and secure a Linux system. It also provides an overview of the operating system and mobile markets. To lay a foundation, it provides an overview of the different operating systems that are based on Linux.

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

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

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

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

You Will Be Able To

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

Who Should Attend

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

“You will be able to...

- [List of skills]

Who Should Attend

- [List of roles]

Paul A. Henry
SANS Senior Instructor

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

@phenrycissp
### DAY 1: Defensive Network Architecture

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

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

### DAY 2: Penetration Testing

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

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

### DAY 3: Network Detection and Packet Analysis

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

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

### DAY 4: Digital Forensics and Incident Response

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

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

### DAY 5: Malware Analysis

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

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

### DAY 6: Enterprise Defender Capstone

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

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

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

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

“SEC503 is fundamental for anyone performing blue team/defensive operations.”


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.

@it_audit
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. Traffic is discussed and displayed using the two open-source tools, Wireshark and tcpdump.

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

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

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

Day 3 introduces the versatile packet crafting tool Scapy. It is a very powerful Python-based tool that allows for the manipulation, creation, reading, and writing of packets. Scapy can be used to craft packets to test the detection capability of an IDS/IPS, especially important when a new user-created IDS rule is added, for instance for a recently announced vulnerability. The examination of TCP/IP culminates with a deeper look into the capabilities 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

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

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

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

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

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

**Topics:** NetWars: IDS Version

---

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

---

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

-Alphonse Wichrowski, Allegiant Air
SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling

You Will Be Able To
- Apply incident handling processes in-depth, including preparation, identification, containment, eradication, and recovery, to protect enterprise environments
- Analyze the structure of common attack techniques in order to evaluate an attacker’s spread through a system and network, anticipating and thwarting further attacker activity
- Utilize tools and evidence to determine the kind of malware used in an attack, including rootkits, backdoors, and trojan horses, choosing appropriate defenses and response tactics for each
- Use built-in command-line tools such as Windows tasklist, wmic, and reg as well as Linux netstat, ps, and lsof 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

Michael Murr
SANS Principal Instructor

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection and one or two disgruntled employees (and whose does not!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth. As defenders, it is essential we understand these hacking tools and techniques.

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

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

“The training offered at SANS is the best in the industry, and the SEC504 course is a must for any IT security professional – highly recommended.”
- Michael Hoffman, Shell Oil Products US

Michael has been a forensic analyst with Code-X Technologies for over five years, conducted numerous investigations and computer forensic examinations, and performed specialized research and development. In addition to teaching SEC504, Michael has taught FOR508: Computer Forensics, Investigation, and Response, and FOR610: Reverse-Engineering Malware. He has led SANS Online Training courses and is a member of the GIAC Advisory Board. Currently, Michael is working on an open-source framework for developing digital forensics applications. Michael 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

Register at www.sans.org/security-east | 301-654-SANS (7267)
Hacker Exploits – Part 4

This course day covers the fourth and fifth phases of many hacker attacks: maintaining access and cover their tracks. Computer attackers install tools that manipulate the underlying kernel itself to hide backdoors, apply rootkits, and sometimes even take over systems from the network level up to the application level. In this course, we will analyze the access. Attackers employ a variety of strategies to take over systems from the network level up to the application level. This section covers the attacks in depth, from the details of buffer overflow and format string attack techniques to the latest in session hijacking of supposedly secure protocols.

Topics: Network-level attacks; gathering and parsing packets; operating system and application-level attacks; Nettac: the attacker’s best friend; hands-on exercises with a list of tools.

DAY 4: Computer and Network Hacker Exploits – Part 3

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

Topics: Password cracking; web application attacks; denial of service attacks; hands-on exercises with a list of tools.

DAY 5: Computer and Network Hacker Exploits – Part 4

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

Topics: Maintaining access; covering the tracks; putting it all together; hands-on exercises with a list of tools.

DAY 6: Hacker Tools Workshop

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

Topics: Hands-on analysis.

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/security-east-2019/courses
You Will Be Able To

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

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

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

The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM) taught in this course will best position your organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach will be early detection of an intrusion, or successfully thwarting the efforts of attackers altogether.

The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and this course will greatly increase your understanding and enhance your skills in implementing CM utilizing the NIST framework.

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

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

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

Topics: Current State Assessment, SOCs, and Security Architecture; Modern Security Architecture Principles; Frameworks and Enterprise Security Architecture; Security Architecture – Key Principles; Frameworks and Enterprise Security Architecture; Security Operations Center Principles Applied

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

Topics: SOCs/Security Architecture – Key Principles Applied; Frameworks and Enterprise Security Architecture; Security Architecture – Key Principles Applied

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

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

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

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

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

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

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

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

“SEC511 provides lots of knowledge in a short period of time. I am confident this course will teach me more than several years of experience!”

-Erich Nieskes, Johnson Financial Group

Who Should Attend
- Security architects
- Senior security engineers
- Technical security managers
- Security Operations Center (SOC) analysts, engineers, and managers
- CND analysts
- Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)
SEC545: Cloud Security Architecture and Operations

You Will Be Able To

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

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

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

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

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

“SEC545 directly relates to every aspect of my job. It also touches on things I had not even thought of!”

-Bill Pirone, EY

Who Should Attend

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

Dave Shackleford is the owner and principal consultant of Voodoo Security and a SANS analyst and course author. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering and is a VMware VExpert with extensive experience designing and configuring secure virtualized infrastructures. He has previously worked as CSO for Configuresoft, CTO for the Center for Internet Security, and as a security architect, analyst, and manager for several Fortune 500 companies. Dave is the author of the Sybex book Virtualization Security: Protecting Virtualized Environments as well as the co-author of Hands-On Information Security from Course Technology. Recently Dave co-authored the first published course on virtualization security for the SANS Institute. Dave currently serves on the Board of Directors at the SANS Technology Institute and helps lead the Atlanta chapter of the Cloud Security Alliance. 
@daveshackleford
DAY 1: Cloud Security Foundations
The first day of the course starts out with an introduction to the cloud, including terminology, taxonomy, and basic technical premises. We also examine what is happening in the cloud today, and cover the spectrum of guidance available from the Cloud Security Alliance, including the Cloud Controls Matrix, the 14 major themes of cloud security, and other research available. Next we spend time on cloud policy and planning, delving into the changes an organization needs to make for security and IT policy to properly embrace the cloud. After all the legwork is done, we’ll start talking about some of the main technical considerations for the different cloud models. We’ll start by breaking down Software-as-a-Service (SaaS) and some of the main types of security controls available. A specialized type of Security-as-a-Service (SecaaS) known as Cloud Access Security Brokers (CASBs) will also be explained, with examples of what to look for in such a service. We’ll wrap up with an introduction to Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) controls, which will set the stage for the rest of the course.
Topics: Introduction to the Cloud and Cloud Security Basics; Cloud Security Alliance Guidance; Cloud Policy and Planning; SaaS Security; Cloud Access Security Brokers (CASBs), Intro to PaaS and IaaS Security Controls

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

DAY 3: Cloud Security Architecture and Design
Instead of focusing on individual layers of the 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 any cloud security strategy. We then look at architecture and design for data security, touching on encryption technologies, key management, and what the different options are today. We wrap up our third day with another crucial topic: availability. Redundant and available design is as important as ever, but we need to use cloud provider tools and geography to our advantage. At the same time, we need to make sure we evaluate the cloud provider’s disaster recovery and continuity, and so this is covered as well.
Topics: Cloud Security Architecture Overview; Cloud Architecture and Security Principles; Infrastructure and Core Component Security; Access Controls and Compartmentalization; Confidentiality and Data Protection; Availability

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

DAY 5: Cloud Security Automation and Orchestration
On our final day, we’ll focus explicitly on how to automate security in the cloud, both with and without scripting techniques. We will use tools like the AWS CLI and AWS Lambda to illustrate the premises of automation, then turn our attention toward SecDevOps principles. We begin by explaining what 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

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/security-east-2019/courses
Many organizations have logging capabilities but lack the people and processes to analyze them. In addition, logging systems collect vast amounts of data from a variety of data sources that require an understanding of the sources for proper analysis. This class is designed to provide students with the training, methods, and processes to enhance existing logging solutions. This class will also help you understand the when, what, and why behind the logs. This is a lab-heavy course that utilizes SOF-ELK, a SANS-sponsored free Security Information and Event Management (SIEM) solution, to provide hands-on experience and the mindset for large-scale data analysis.

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

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

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

“This course uses real-world events and hands-on training to allow me to immediately improve my organization’s security stance.

Day one back in the office I was implementing what I learned.”

-Frank Giachino, Bechtel

John Hubbard
SANS Instructor

John is a dedicated blue-teamer and is driven to help develop defensive talent around the world. Through his years of experience as the SOC Lead for GlaxoSmithKline, he has real-world, first-hand knowledge of what it takes to defend an organization against advanced cyber-attacks and is eager to share these lessons with his students. As a SANS Cyber Defense curriculum instructor and course author of SEC455, John specializes in threat hunting, network security monitoring, SIEM design and optimization, and constructing defensive postures that allow organizations to protect their most sensitive data. Throughout class, he works with students to explain difficult concepts in relatable and clear language, illustrates important ideas with stories and demonstrations, and encourages students to push themselves beyond the limit of what they thought possible. John holds degrees in electrical and computer engineering and his past research ranges from malware reverse-engineering to car hacking, mobile app security, and IoT devices. In his free time, John enjoys catching every InfoSec conference he can attend, FPV drone racing, coffee roasting, and slowly turning his home into a data center. @SecHubb
**Course Day Descriptions**

**Mon, Feb 4 - Sat, Feb 9**

**9:00am - 7:00pm** (Days 1-5)  
**9:00am - 5:00pm** (Day 6)  
Evening bootcamp sessions; hands-on labs

### DAY 1: SIEM Architecture and SOF-ELK

This section will introduce free logging and analysis tools and focus on techniques to make sense of and augment traditional logs. It also covers how to handle the big data problem of handling billions of logs and how advances in free tools are starting to give commercial solutions a run for their money. Day one is designed to bring all students up to speed on SIEM concepts and to bring all students to a base level to carry them through the rest of the class. It is designed to also cover SIEM best practices. During day one we will be introducing Elasticsearch, Logstash, and Kibana within SOF-ELK and immediately go into labs to get students comfortable with ingesting, manipulating, and reporting on log data.

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

### DAY 2: Service Profiling with SIEM

This section covers how to collect and handle this massive amount of data. Methods for collecting these logs through service logs such as from DNS servers will be covered, as will be passive ways of pulling the same data from the network itself. Techniques will be demonstrated to augment and add valuable context to the data as they are collected. Finally, analytical principles will be covered for finding the needles in the stack of needles. We will cover how, even if we have the problem of searching through billions of logs, we can surface only meaningful items of interest. Active dashboards will be designed to quickly find the logs of interest and to provide analysts with additional context for what to do next.

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

### DAY 3: Advanced Endpoint Analytics

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

**Topics:** Endpoint Logs

### DAY 4: Baselining and User Behavior Monitoring

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

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

### DAY 5: Tactical SIEM Detection and Post-Mortem Analysis

This section focuses on combining multiple security logs for central analysis. More importantly, we will cover methods for combining multiple sources to provide improved context to analysts. We will also show how providing context with asset data can help prioritize analyst time, saving money and addressing risks that matter. After covering ways to optimize traditional security alerts, we will jump into new methods to utilize logging technology to implement virtual trippers. While it would be ideal to prevent attackers from gaining access to your network, it is a given that at some point you will be compromised. However, preventing compromise is the beginning, not the end goal. Adversaries will crowd your systems and network to achieve their own ends. Knowing this, we will implement logging-based tripswires—and if a single one is stepped on, we can quickly detect it and respond to the adversary.

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

### DAY 6: Capstone: Design, Detect, Defend

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

**Topics:** Defend-the-Flag Challenge – Hands-on Experience

“**This course is as practical and real-world as it gets. SEC555 provides numerous quick wins and really stimulates thinking about the relative value of numerous ways to defend your organization.**”

-Mikhale Vitebskiy, Lexington Partners

---

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/security-east-2019/courses](http://www.sans.org/event/security-east-2019/courses)
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

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

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches? This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS).

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

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

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

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

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

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

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

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

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

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

**Topics:**

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

---

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

**Topics:**

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

---

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

**Topics:**

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

---

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

**Topics:**

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

---

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

**Topics:**

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

---

**Who Should Attend**

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

---

"SEC566 will help directly in my work to implement better security controls for the organization."

- Tan Toh Hwee, Merck
Job-Specific, Specialized Focus

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

Deep, Real-World Knowledge

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

Most Trusted Certification Design

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

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

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

ce NetWars at

Security East 2019

Play solo or in a team of up to five players

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

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

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

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

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

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

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

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

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

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

In addition to high-quality course content, SEC542 focuses heavily on in-depth, hands-on labs to ensure that students can immediately apply all they learn. In addition to having more than 30 formal hands-on labs, the course culminates in a web application pen test tournament, powered by the SANS NetWars Cyber Range. This Capture-the-Flag event on the final day brings students into teams to apply their newly acquired command of web application penetration testing techniques in a fun way that hammers home lessons learned.

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

@eric_conrad
**Course Day Descriptions**

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

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

---

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

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

---

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

**Topics:** Python for Web App Penetration Testing; Web App Vulnerabilities and Manual Verification Techniques; 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

---

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

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

---

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

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

---

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

---

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

---

“SEC542 shows a hands-on way of doing web app penetration testing – not just how to use this tool or that tool.”

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

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

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

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

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

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

“As 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, GMOB, GCED, GCFA-Gold, GClA-Gold, GCIH, GAWN, GPPA, GCWN, GCSC-Gold, GSEC, SCtSA, RCSE, 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

Kevin Fiscus
SANS Principal Instructor
**Course Day Descriptions**

**DAY 1: 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

**DAY 2: 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
- Tcudpump 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

**DAY 3: Exploitation**

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

**Topics:**
- Comprehensive Metasploit Coverage with Exploits/Stagers/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

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

This section of the course zooms in on pilaging target environments and building formidable hands-on command line skills. We’ll cover Windows command line skills in-depth, including PowerShell’s awesome abilities for post-exploitation. We’ll see how we can leverage malicious services and the incredible WMIC toolset to access and pivot through a target organization. We’ll then turn our attention to password guessing attacks, discussing how to avoid account lockout, as well as numerous options for plundering password hashes from target machines including the great Mimikatz Kiwi tool. Finally, we’ll look at Metasploit’s fantastic features for pivoting, including the msfconsole route command.

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

**DAY 5: 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 pentesting, covering the most powerful and common web app attack techniques with hands-on labs for every topic we address. We’ll cover finding and exploiting cross-site scripting (XSS), cross-site request forgery (CSRF), command injection, and SQL injection flaws in applications such as online banking, blog sites, and more.

**Topics:**
- Password Cracking with John the Ripper
- Sniffing and Cracking Windows Authentication Exchanges Using Cain
- Using Rainbow Tables to Maximize 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

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

This lively session represents the culmination of the network penetration testing and ethical hacking course. You’ll apply all of the skills mastered in the course 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

“**The hacker perspective in SEC560 allows new penetration testers and cyber defenders to identify security posture gaps and holes by adapting to a diverse skillset.”**

- Ryan Guest, Southern Company

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/security-east-2019/courses](http://www.sans.org/event/security-east-2019/courses)
Imagine an attack surface that is spread across your organization and in the hands of every user. It moves from place to place regularly, stores highly sensitive and critical data, and sports numerous different wireless technologies all ripe for attack. Such a surface already exists today: mobile devices. These devices are the biggest attack surface in most organizations, yet these same organizations often don’t have the skills needed to assess them.

SEC575 NOW COVERS ANDROID OREO and iOS 11

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

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

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

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

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

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

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

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

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

@joswr1ght
DAY 1: Device Architecture and Common Mobile Threats
The first module of SEC575 quickly looks at the significant threats affecting mobile device deployments, highlighted by a hands-on exercise evaluating network traffic from a vulnerable mobile banking application. As a critical component of a secure deployment, we will examine the architectural and implementation differences and similarities between Android (including Android Marshmallow), Apple iOS 11, and the Apple Watch and Google Wear platforms. We will also look at the specific implementation details of popular platform features such as iBeacon, AirDrop, App Verification, and more. Hands-on exercises will be used to interact with mobile devices running in a virtualized environment, including low-level access to installed application services and application data. We’ll examine the tools used to evaluate mobile devices as part of establishing a lab environment for mobile device assessments, including the analysis of mobile malware affecting Android and non-jailbroken iOS devices. Finally, we will address the threats of lost and stolen devices (and opportunities for a pen tester), including techniques to bypass mobile device lock screens.

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

DAY 2: Mobile Platform Access and Application Analysis
Continuing our look at ethical hacking and penetration testing, we turn our focus on analyzing mobile devices and infrastructure from the perspective of an attacker, identifying and exploiting flaws that deliver unauthorized access to data or supporting networks. By identifying these flaws we can evaluate the mobile phone deployment risk to the organization with practical and useful risk metrics. Whether your role is to implement the penetration test, or to source and evaluate the penetration tests of others, understanding these techniques will help your organization identify and resolve vulnerabilities before they become incidents.

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

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

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

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

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

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

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

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

“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
You Will Be Able To

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

Who Should Attend

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

This course is designed as a logical progression point for those who have completed SEC650: Network Penetration Testing and Ethical Hacking, or for those with existing penetration testing experience. Students with the prerequisite knowledge to take this course will walk through dozens of real-world attacks used by the most seasoned penetration testers. The methodology of a given attack is discussed, followed by exercises in a real-world lab environment to solidify advanced concepts and allow for the immediate application of techniques in the workplace. Each day includes a two-hour evening bootcamp to allow for additional mastery of the techniques discussed and even more hands-on exercises. A sample of topics covered includes weaponizing Python for penetration testers, attacks against network access control (NAC) and VLAN manipulation, network device exploitation, breaking out of Linux and Windows restricted environments, IPv6, Linux privilege escalation and exploit-writing, testing cryptographic implementations, fuzzing, defeating modern OS controls such as ASLR and DEP, return-oriented programming (ROP), Windows exploit-writing, and much more!

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

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

Jake Williams
SANS Senior Instructor

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

@MalwareJake
**Course Day Descriptions**

**DAY 1: Network Attacks for Penetration Testers**
Day one serves as an advanced network attack module, building on knowledge gained from SEC560. The focus will be on obtaining access to the network; manipulating the network to gain an attack position for eavesdropping and attacks, and for exploiting network devices; leveraging weaknesses in network infrastructure; and taking advantage of client frailty.

**Topics:** Bypassing Network 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 Evingrade to Attack Software Updates; Overcoming SSL Transport Encryption Security with SSLstrip; Remote Cisco Router Configuration File Retrieval; IPv6 for Penetration Testers

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

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

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

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

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

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

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

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

**DAY 6: Capture-the-Flag Challenge**
This day will serve as a real-world challenge for students by requiring them to utilize skills they have learned throughout the course, think outside the box, and solve a range of problems from simple to complex. A web server scoring system and Capture-the-Flag engine will be provided to score students as they capture flags. More difficult challenges will be worth more points. This day will serve as a real-world challenge for students by requiring them to utilize skills they have learned throughout the course, think outside the box, and solve a range of problems from simple to complex. A web server scoring system 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 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.

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

- Anton Ebertzeder, Siemens AG

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/security-east-2019/courses](http://www.sans.org/event/security-east-2019/courses)
FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting

You Will Be Able To

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

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.

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

“For508 analyzes Advanced Persistent Threat samples that are affecting our industry today. This training can’t get any better!”

-Neel Mehta, Chevron

Rob Lee is an entrepreneur and consultant in the Washington, DC area and currently the Curriculum Lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 15 years’ experience in computer forensics, vulnerability and exploit development, intrusion detection/prevention, and incident response. Rob graduated from the U.S. Air Force Academy and earned his MBA from Georgetown University. He served in the U.S. Air Force as a member of the 690th Information Warfare Squadron (IWS), the first U.S. military operational unit focused on information warfare. Later, he was a member of the Air Force Office of Special Investigations (AFOSI), where he led crime investigations and an incident response team. Over the next seven years, he worked directly with a variety of government agencies in the law enforcement, U.S. Department of Defense, and intelligence communities as the technical lead for vulnerability discovery and exploit development teams, lead for a cyber-forensics branch, and lead for a computer forensic and security software development team. Most recently, Rob was a Director for MANDIANT, a commercial firm focusing on responding to advanced adversaries such as the APT. Rob co-authored the book Know Your Enemy, 2nd Edition. Rob is also co-author of the MANDIANT threat intelligence report “M-Trends: The Advanced Persistent Threat.”

@robtlee

Register at www.sans.org/security-east | 301-654-SANS (7267)
DAY 1: Advanced Incident Response and Threat Hunting
Incident responders and threat hunters should be armed with the latest tools, memory analysis techniques, and enterprise methodologies to identify, track, and contain advanced adversaries and to remediate incidents. Incident response and threat hunting analysts must be able to scale their analysis across thousands of systems in their enterprise. This section examines the six-step incident response methodology as it applies to 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

DAY 2: Memory Forensics in Incident Response and Threat Hunting
Now a critical component of many incident response and threat hunting teams that detect advanced threats in their organization, memory forensics has come a long way in just a few years. Memory forensics can be extraordinarily effective at finding evidence of worms, rootkits, and advanced malware used by an APT group of attackers. 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

DAY 3: Intrusion Forensics
Cyber defenders have a wide variety of tools and artifacts available to identify, hunt, and track adversary activity in a network. Each attacker’s action leaves a corresponding artifact, and understanding what is left behind as footprints can be critical to both red and blue team members. Attacks follow a predictable pattern, and we focus our detective efforts on immutable portions of that pattern. In this section, we cover common attacker tradecraft and discuss the various data sources and forensic tools you can use to identify malicious activity in the enterprise.

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

DAY 4: Timeline Analysis
Learn advanced incident response and hunting techniques uncovered via timeline analysis directly from the authors who pioneered timeline analysis tradecraft. This section will step you through the two primary methods of building and analyzing timelines created during advanced incident response, threat hunting, and forensic cases. Exercises will show analysts how to create a timeline and also how to introduce the key methods to help you use those timelines effectively in your cases.

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

DAY 5: Incident Response and Hunting Across the Enterprise – Advanced Adversary and Anti-Forensics Detection
Over the years, we have observed that many incident responders and threat hunters have a challenging time finding threats without pre-built indicators of compromise or threat intelligence gathered before a breach. This is especially true in APT adversary intrusions. This advanced session will demonstrate techniques used by first responders to identify malware or forensic artifacts when very little information exists about their capabilities or hidden locations. We will discuss techniques to help funnel possibilities down to the candidates most likely to be evil malware trying to hide on the system.

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

DAY 6: The APT Incident Response Challenge
This incredibly rich and realistic enterprise intrusion exercise is based on a real-world advanced persistent threat (APT) group. It brings together techniques learned earlier in the week and tests your newly acquired skills in a case that simulates an attack by an advanced adversary. The challenge brings it all together using a real intrusion into a complete Windows enterprise environment. You will be asked to uncover how the systems were compromised in the initial intrusion, find other systems the adversary moved 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 hactivist groups.

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

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

“Great class! It shows you how to handle forensics from an incident response perspective vs. law enforcement, which helps corporate employees.”
- Brandon B., RSA

“This class gives me a refresher on items I should have been looking for, also new insights I had never thought of.”
- Calvin Raphile, Americasource Bergen
FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

You Will Be Able To

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

Philip Hagen
SANS Senior Instructor

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

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

Whether you are a consultant responding to a client’s site, a law enforcement professional assisting victims of cybercrime and seeking prosecution of those responsible, an on-staff forensic practitioner, or a member of the growing ranks of “threat hunters,” this course offers hands-on experience with real-world scenarios that will help take your work to the next level. 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 nfldump, tcpextract, tcpflow, and more. Newly added tools in the course include the SOF-ELK platform—a VMware appliance pre-configured with the ELK stack. This “big data” platform includes the Elasticsearch storage and search database, the Logstash ingest and parse utility, and the Kibana graphical dashboard interface. Together with the custom SOF-ELK configuration files, the platform gives forensicators a ready-to-use platform for log and NetFlow analysis. For full-packet analysis and hunting at scale, the Moloch platform is also used. Through all of the in-class labs, your shell scripting abilities will also be used to make easy work of ripping through hundreds and thousands of data records.

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

@PhilHagen

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

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

---

**Day 2: Core Protocols & Log Aggregation/Analysis**
Understanding log data and how it can guide the investigative process is an important network forensicator 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.

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

---

**Day 3: NetFlow and File Access Protocols**
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

---

**Day 4: Commercial Tools, Wireless, and Full-Packet Hunting**
Commercial tools hold clear advantages in some situations a forensicator 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

---

**Day 5: 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

---

**Day 6: 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

---

### 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

---

“This course is fantastic. It has prepared me with new ideas to take back to work.”

-Ryan Fletcher, Fulton Financial Corp

“This course is next-level in developing top-notch incident response and a network analysis professional.”

-Tom L., U.S. Air Force
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 executables. 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.

Who Should Attend

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

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

@asoni

You Will Be Able To

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

Anuj Soni
SANS Certified Instructor

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques

6 Day Program | 36 CPES | Laptop Required

Register at www.sans.org/security-east | 301-654-SANS (7267)
DAY 1: Malware Analysis Fundamentals
Section one lays the groundwork for malware analysis by presenting the key tools and techniques useful for examining malicious programs. You will learn how to save time by exploring Windows malware in two phases. Behavioral analysis focuses on the program’s interactions with its environment, such as the registry, the network, and the file system. Code analysis focuses on the specimen’s code and makes use of a disassembler and debugger tools such as IDA Pro and OllyDbg. You will learn how to set up a flexible laboratory to perform such analysis in a controlled manner, and set up such a lab on your laptop using the supplied Windows and Linux (REMnux) virtual machines. You will then learn how to use the key analysis tools by examining a malware sample in your lab—with guidance and explanations from the instructor—to reinforce the concepts discussed throughout the day.

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

DAY 2: Reversing Malicious Windows 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, Drovers); Extending Assembly Knowledge to Include x64 Code Analysis

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

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

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

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

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

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

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

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

“This is truly a step-by-step mentorship course. The content is immediately applicable to DFIR job roles.”
- Chad Reams, Parsons, Inc.
MGT414: **SANS Training Program for CISSP® Certification**

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

**After completing the course students will have:**
- Detailed coverage of the eight domains of knowledge
- The analytical skills required to pass the CISSP® exam
- The technical skills required to understand each question
- The foundational information needed to become a 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.

"The MGT414 class prepared me for the CISSP® certification, which will increase my professional credibility, and our firm's credibility in our industry."

- Phillip Woosley, KirkpatrickPrice, LLC

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

**DAY 1: Introduction; Security and Risk Management**
On the first day of training for the CISSP® exam, MGT414 introduces the specific requirements needed to obtain certification. The exam update will be discussed in detail. We will cover the general security principles needed to understand the eight domains of knowledge, with specific examples for each domain. The first of the eight domains, Security and Risk Management, is discussed using real-world scenarios to illustrate the critical points.

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

---

**DAY 2: Asset Security and Security Engineering – Part 1**
Understanding asset security is critical to building a solid information security program. The Asset Security domain, the initial focus of today’s course section, describes data classification programs, including those used by both governments and the military as well as the private sector. We will also discuss ownership ranging from business/mission owners to data and system owners. We will examine data retention and destruction in detail, including secure methods for purging data from electronic media. We then turn to the first part of the Security Engineering domain, including new topics for the 2018 exam such as the Internet of Things, Trusted Platform Modules, Cloud Security, and much more.

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

---

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

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

---

**DAY 4: Identity and Access Management**
Controlling access to data and systems is one of the primary objectives of information security. Domain 5, Identity and Access Management, strikes at the heart of access control by focusing on identification, authentication, and authorization of accounts. Password-based authentication represents a continued weakness, so Domain 5 stresses multi-factor authentication, biometrics, and secure credential management. The CISSP® exam underscores the increased role of external users and service providers, and mastery of Domain 5 requires an understanding of federated identity, SSO, SAML, and third-party identity and authorization services like OAuth and OpenID.

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

---

**DAY 5: Security Assessment and Testing; Security Operations**
This course section covers Domain 6 (Security Assessment and Testing) and Domain 7 (Security Operations). Security Assessment covers types of security tests, testing strategies, and security processes. Security Operations covers investigatory issues, including discovery, logging and monitoring, and provisioning. We will discuss cutting-edge technologies such as the cloud, and we’ll wrap up day five with a deep dive into disaster recovery.

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

---

**DAY 6: Software Development Security**
Domain 8 (Software Development Security) describes the requirements for secure software. Security should be “baked in” as part of network design from day one, since it is always less effective when it is added later to a poor design. We will discuss classic development models, including waterfall and spiral methodologies. We will then turn to more modern models, including agile software development methodologies. New content for the CISSP® exam update will be discussed, including DevOps. We will wrap up this course section by discussing security vulnerabilities, secure coding strategies, and testing methodologies.

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

---

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

---

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

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

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

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

This approach prepares you to:

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

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

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

-Brian Harris, Jackson EMC

G. Mark Hardy
SANS Principal Instructor

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

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

@g_mark
**Course Day Descriptions**

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

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

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

**Topics:** Data Protection; Privacy Primer; Network Security

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

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

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

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

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

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

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

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

-Frank Kim

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

-Rick Derks, FCS Financial
Russell Eubanks is Vice President and Chief Information Security Officer for the Federal Reserve Bank of Atlanta. He is responsible for developing and executing the Information Security strategy for both the Retail Payments Office and the Atlanta Reserve Bank. Russell has developed information security programs from the ground up and actively seeks opportunities to measurably increase their overall security posture. Russell is a Handler for the SANS Internet Storm Center, serves on the Editorial Panel for the Critical Security Controls and maintains securityeverafter.com. He holds a bachelor’s degree in computer science from the University of Tennessee at Chattanooga.

@russelleubanks

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:

<table>
<thead>
<tr>
<th>Develop Strategic Plans</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Create Effective Information Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Develop Management and Leadership Skills</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

You Will Be Able To

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

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

-Mike Parkin, Chapters Health System

Russell Eubanks
SANS Certified Instructor

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 |

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:

<table>
<thead>
<tr>
<th>Develop Strategic Plans</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Create Effective Information Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Develop Management and Leadership Skills</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

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 |

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:

<table>
<thead>
<tr>
<th>Develop Strategic Plans</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Create Effective Information Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Develop Management and Leadership Skills</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

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 |

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:

<table>
<thead>
<tr>
<th>Develop Strategic Plans</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Create Effective Information Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Develop Management and Leadership Skills</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

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 |

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:

<table>
<thead>
<tr>
<th>Develop Strategic Plans</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Create Effective Information Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Develop Management and Leadership Skills</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

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 |

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:

<table>
<thead>
<tr>
<th>Develop Strategic Plans</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Create Effective Information Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Develop Management and Leadership Skills</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

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 |
**Course Day Descriptions**

**DAY 1: Strategic Planning Foundations**
On this first day we will introduce the key elements of strategic security plans and lay the groundwork for the rest of the course. Creating strategic plans for security requires a fundamental understanding of the business and a deep understanding of the threat landscape.

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

**DAY 2: Strategic Roadmap Development**
With a firm understanding of business drivers as well as the threats facing the organization, you will develop a plan to analyze the current situation, identify the target situation, perform gap analysis, and develop a prioritized roadmap. In other words, you will be able to determine (1) what you do today, (2) what you should be doing in the future, (3) what you don’t do, and (4) what you should do first. With this plan in place you will learn how to build and execute your plan by developing a business case, defining metrics for success, and effectively marketing your security program.

**Topics:** Historical Analysis; Values and Culture; SWOT Analysis; Vision and Innovation; Security Framework; Gap Analysis; Roadmap Development; Business Case Development; Metrics and Dashboards; Marketing and Executive Communications

**DAY 3: Security Policy Development and Assessment**
Policy is one of the key tools that security leaders have to influence and guide the organization. Security managers must understand how to review, write, assess, and support security policy and procedure. Using an instructional delivery methodology that balances lecture, exercises, and in-class discussion, this course section will teach techniques to create successful policy that users will read and follow and business leaders will accept. Learn key elements of policy, including positive and negative tone, consistency of policy bullets, how to balance the level of specificity to the problem at hand, the role of policy, awareness and training, and the SMART approach to policy development and assessment.

**Topics:** Purpose of Policy; Policy Gap Analysis; Policy Development; Policy Review; Awareness and Training

**DAY 4: Leadership and Management Competencies**
Learn the critical skills you need to lead, motivate, and inspire your teams to achieve the goal. By establishing a minimum standard for the knowledge, skills, and abilities required to develop leadership you will understand how to motivate employees and develop from a manager into a leader.

**Topics:** Leadership Building Blocks; Creating and Developing Teams; Coaching and Mentoring; Customer Service Focus; Conflict Resolution; Effective Communication; Leading Through Change; Relationship Building; Motivation and Self-Direction; Teamwork; Leadership Development

**DAY 5: Strategic Planning Workshop**
Using the case study method, students will work through real-world scenarios by applying the skills and knowledge learned throughout the course. Case studies are taken directly from Harvard Business School, the pioneer of the case-study method, and focus specifically on information security management and leadership competencies. The Strategic Planning Workshop serves as a capstone exercise for the course, allowing students to synthesize and apply concepts, management tools, and methodologies learned in class.

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

---

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

---

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

- Alyssa DeVita, Marriott
Christopher Crowley has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. His work experience includes penetration testing, computer network defense, incident response, and forensic analysis. He is the course author for SANS MGT535: 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 MGT535; 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

52 Day Program 30 CPEs Laptop Required

You Will Be Able To
- Design security operations to address all needed functions for the organization
- Select technologies needed to implement the functions for a Security Operations Center (SOC)
- Maintain appropriate business alignment with the security capability and the organization
- Develop and streamline security operations processes
- Strengthen and deepen capabilities
- Collect data for metrics, report meaningful metrics to the business, and maintain internal SOC performance metrics
- Hire appropriate SOC staff and keep existing SOC staff up to date

Who Should Attend
- Information security managers
- SOC managers, analysts, and engineers
- Information security architects
- IT managers
- Operations managers
- Risk management professionals
- IT/System administration/Network administration professionals
- IT auditors
- Business continuity and disaster recovery staff

Christopher Crowley
SANS Principal Instructor

“MGT517 is a good assurance we are heading in the right direction for SOC/IR development while plugging/identifying the gaps and being introduced to new ideas.”

-Nate Poirier, Staples, Inc.

This course covers the design, operation, and ongoing growth of all facets of the security operations capabilities in an organization. An effective Security Operations Center (SOC) has many moving parts and must be designed so that it can be adjusted to work within the context and constraints of the organization. To run a successful SOC, managers need to provide tactical and strategic direction and inform staff of the changing threat environment and provide them with guidance and training. This course covers design, deployment, and operation of the security program to empower leadership through technical excellence.

The course covers the functional areas of Communications, Network Security Monitoring, Threat Intelligence, Incident Response, Forensics, and Self-Assessment. We discuss establishing Security Operations governance for:
- Business alignment and ongoing adjustment of capabilities and objectives
- Designing the SOC and the associated objectives of functional areas
- Software and hardware technology required for performance of functions
- Knowledge, skills, and abilities of staff as well as staff hiring and training
- Execution of ongoing operations

You will walk out of this course armed with a roadmap to design and operate an effective SOC tailored to the needs of your organization.
Course Day Descriptions

**DAY 1: Design the Security Operations Center**
This course section will focus on how to align and deploy a Security Operations Center (SOC). We will lay the foundational aspects of the SOC by discussing the functional areas that form the basis of the build and operate days that follow. The first issue to address is how the SOC will serve the business. To understand what is to be built, we explore the business drivers for SOCs. Each company has its own circumstances and needs, but there are common drivers for setting out to build a SOC. From business alignment, systems analysis performed shows all the things that need to be done. This is an elaborate and substantial effort to undertake. Knowing what components are available and how the pieces fit together is critical. This analysis will be followed with design and build on day 2.

**Topics:** SOC Fundamentals; SOC Components; Sizing and Scoping; SOC Program

**DAY 2: Build the Security Operations Center**
Once a clear picture of what should be done to secure the organization is produced from analysis of what the needs are, and what resources are available, we set out to build the SOC. The build-out starts with an operating plan decided on by the key stakeholders from the organization. The interactions, inputs, outputs, and actions within each of the process components are identified. Each functional area needs specific hardware and software to accomplish each process, so alternatives are discussed for all of these. Open-source, inexpensive, and enterprise-level solutions are presented for each need. We will discuss the available solutions in-depth, and help focus the budget available on the necessary tools. The output of this day is on all the procurement necessary for building out a SOC.

**Topics:** Governance Structure; Process Engineering; Technical Components

**DAY 3: Operate and Mature the Security Operations Center**
Designing and building-out a SOC are considered projects. Operation is an ongoing and perpetual effort. If the design of the system is insufficient or short-sighted, then operating the system will be difficult and inefficient. The overriding challenge of management is discussed in terms of organizational dimensions. The analytical processes of competing hypotheses, the kill chain, and the diamond model are discussed to provide a context for the analytical currency of the SOC. We will evaluate the staffing structure, how to hire, and how to keep those staff continually trained and updated. A schedule of meetings, specific metrics to report, and specific metrics to use to measure the relationship within the functional areas of the SOC are shown. Specific processes and the data relationships when performing the processes are discussed to depict the standard operating procedures that the SOC must carry out.

**Topics:** People and Processes; Measurements and Metrics; Process Development

**DAY 4: Incident Response Management – Part 1**
Further detail on incident response is developed to show the operation of the SOC. Since the response component is the action of defense, the operation of the incident response team is addressed in great detail. An examination of cloud-based systems shows a special case of incident response. The preparation of response capability in the cloud is insufficient because the contractual negotiations of the service rarely address incident response adequately. We discuss appropriate preparation and response action within cloud services. User training and awareness is developed as a basis for corrective action when incident response is required.

**Topics:** The Cloud; Incident Response Process; Creating Incident Requirements; Training, Education, and Awareness

**DAY 5: Incident Response Management – Part 2**
Continuing the operation of incident response, we discuss the staffing requirements in detail. Common caveats of incidence response operations are discussed, and tabletop exercises are developed to mitigate those caveats. Communication requirements are laid out and incident tracking methods are discussed. We also look at how to make the most out of a response and damage control task. Tools for estimating and tracking costs associated with incidents are demonstrated, and overall recommendations are presented on how to interface with law enforcement. The final topic addressed is the development of appropriate response techniques for APT-style actors, including strategies for quickly differentiating APT-style compromise using threat intelligence, sufficient scope identification, and eradication of the current wave of compromise.

**Topics:** Staffing Considerations; Setting Up Operations; Managing Daily Operations; Cost Considerations; Legal and Regulatory Issues; Advanced Threat Response

“This course touches on the art and science of cybersecurity operations management.”

-Joanne Lim, Citibank

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/security-east-2019/courses](http://www.sans.org/event/security-east-2019/courses)
DEV540: Secure DevOps and Cloud Application Security

DEV540 gives developers and security professionals the tools needed to build and deliver secure software using DevOps and cloud services, specifically Amazon Web Services (AWS). It explains how the principles, practices, and tools of DevOps and AWS can improve the reliability, integrity, and security of applications.

The first two days of the course examine the implementation of Secure DevOps using lessons from successful DevOps security programs. Using popular open-source tools such as GitLab, Puppet, Jenkins, Vault, Graphana, and Docker, you will create a secure DevOps CI/CD toolchain that can automatically build, test, and deploy infrastructure and applications. In a series of labs, you will inject security into your CI/CD toolchain using a variety of security tools, patterns, and techniques.

The final three days of the course will teach you to shift your DevOps workloads to the cloud and secure software using AWS. With your CI/CD toolchain, you will build a cloud infrastructure that can deploy applications and microservices to the cloud, instead of to local servers. You’ll also analyze and fix cloud infrastructure and application vulnerabilities using AWS security services and tools such as API Gateway, IAM, CloudFront Signed URLs, Security Token Service, KMS, encryption, WAF, Lambda for Serverless computing, CFN NAG scanner, AWS Security Benchmark, and much more.

DEV540 makes extensive use of open-source materials and tooling for automated configuration management (“Infrastructure as Code”), Continuous Integration, Continuous Delivery, Continuous Deployment, containerization, micro-segmentation, automated compliance (“Compliance as Code”), and Continuous Monitoring. It also uses Jenkins and AWS developer tools such as CloudFormation, CodeCommit, CodeBuild, CodePipeline, and other cloud application services, so you can experience the use of these services when securing infrastructure and applications.

**You Will Be Able To**
- Build a DevSecOps control framework within your organization
- Communicate DevSecOps security controls to auditors, managers, and engineers
- Configure open-source DevSecOps tools to perform automated security scanning
- Manage security vulnerabilities in CI/CD tools for audit reporting
- Review cloud infrastructure and applications for security issues
- Leverage cloud security automation for continuous monitoring, active defense, and compliance

**“The training was a valuable centralized collection of resources to the ever-evolving DevSecOps world.”**
- Almahdi Sahad, CoStar

Gregory Leonard has more than 17 years of experience in software development, with an emphasis on writing large-scale enterprise applications. Greg’s responsibilities over the course of his career have included application architecture and security, performing infrastructure design and implementation, providing security analysis, conducting code reviews and evaluating performance diagnostics. He is currently employed as an application security consultant at Optiv Security, Inc.

@appsegreg

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

**MON, FEB 4 - FRI, FEB 8**
9:00am - 5:00pm

### DAY 1: Introduction to Secure DevOps

The first course section introduces DevOps practices, principles, and tooling. We will examine how DevOps works, how work is done in DevOps, and the importance of culture, collaboration, and automation. Using case studies of DevOps “Unicorns”—the Internet tech leaders who’ve created the DevOps DNA—we’ll consider how and why these leaders succeeded, and examine the keys to their DevOps security programs. We’ll then look at Continuous Delivery, the DevOps automation engine. We’ll explore how to build up a Continuous Delivery or Continuous Deployment pipeline, including how to fold or wire security controls into the CD pipeline, and how to automate security checks and tests in CD.

**Topics:** Introduction to DevOps; Case Studies on DevOps Unicorns; Working in DevOps; Security Challenges in DevOps; Building a CD Pipeline; DevOps Deployment Kata; Secure Continuous Delivery, Security in Pre-Commit; Security in Commit; Security in Acceptance

### DAY 2: Moving to Production

Building on the ideas and frameworks developed in Section 1, and using modern automated configuration management tools like Puppet, Chef, and Ansible, you’ll learn how secure Infrastructure as Code allows you to quickly and consistently deploy new infrastructure and manage configurations. Because the automated CD pipeline is so critically important to DevOps, you’ll also learn to secure the pipeline, including RASP and other run-time defense technologies. As the infrastructure and application code moves to production, we’ll spend the second half of the day exploring container security issues associated with tools such as Docker and Kubernetes, as well as how to protect secrets using Vault and how to build continuous security monitoring using Graphana, Graphite, and StatsD. Finally, we’ll discuss how to build compliance into Continuous Delivery, using the security controls and guardrails that have been built in the DevOps toolchain.

**Topics:** Secure Infrastructure as Code; Building Security Policies into Infrastructure Code; Security with Puppet Lab; Securing Your CD Pipeline; Threat Modeling and Locking Down Your Build and Deployment Environment; Run-time Defense: RASP, IAST and other run-time security solutions; Container Security: Introduction to Containers, Docker, and Docker Security Risks and Tools; Security in Monitoring; Using Production Metrics and Insight to Drive Improvements in Your Security Program; Red Teaming, Bug Bounties, and Blameless Postmortems; Managing Secrets: The Problem of Secrets in an Automated Environment; Patterns and Anti-patterns for Managing Secrets; Compliance as Code: How to Satisfy Compliance Requirements Using Continuous Delivery and Continuous Deployment

### DAY 3: Moving to the Cloud

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

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

### DAY 4: Cloud Application Security

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

**Topics:** Data Protection; Secure Content Delivery; Microservice Security; Serverless Security

### DAY 5: Cloud Security Automation

Expanding on the foundation of the previous sections, we’ll now focus on leveraging cloud services to automate security tasks such as deploying application patches to blue/green environments, deploying and configuring cloud web application firewalls, enabling cloud security monitoring, and automating cloud compliance scanning.

**Topics:** Blue/Green Deployment Options; Security Automation; Security Monitoring; Cloud Compliance

---

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

---

“Extremely relevant to our DevOps/CICD journey.”

- Devon D., USAA

---

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/security-east-2019/courses](www.sans.org/event/security-east-2019/courses)
ICS410: ICS/SCADA Security Essentials

You Will Be Able To

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

Paul Piotrowski
SANS Instructor

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

The course will provide you with:

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

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

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

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

Paul Piotrowski is currently an Automation Engineer in Shell’s Global PCD Integrity Organization (Process Control Domain). Paul consults on global capital projects and supports Shell’s operated and non-operated assets across all business units. Paul has spent over 16 years with Shell in various security roles including network operations, risk governance and compliance, audit, incident management, forensics, pen testing and project management. His extensive travel for Shell has given him the opportunity to work across diverse sets of cultures and landscapes that have shaped his worldview. Paul possesses the valuable hybrid skill set of Operations Technology (OT) and Information Technology (IT). By visiting and working at over 50 Shell operations globally, he understands how to embed practical solutions between operations and corporate IT that reduce an organization’s cybersecurity risk while minimizing operational impact. Paul was involved in the initial development of the Global Industrial Cyber Security Professional (GICSP) course curriculum. He holds a B.Sc degree in computer science with a minor in management. He holds several certifications including the GICSP and GIAPP®. In addition, he has participated in several executive development programmes. He is based in Calgary, Canada.

www.giac.org/gicsp

GICSP: Industrial Cyber Security Professional

Paul Piotrowski is currently an Automation Engineer in Shell’s Global PCD Integrity Organization (Process Control Domain). Paul consults on global capital projects and supports Shell’s operated and non-operated assets across all business units. Paul has spent over 16 years with Shell in various security roles including network operations, risk governance and compliance, audit, incident management, forensics, pen testing and project management. His extensive travel for Shell has given him the opportunity to work across diverse sets of cultures and landscapes that have shaped his worldview. Paul possesses the valuable hybrid skill set of Operations Technology (OT) and Information Technology (IT). By visiting and working at over 50 Shell operations globally, he understands how to embed practical solutions between operations and corporate IT that reduce an organization’s cybersecurity risk while minimizing operational impact. Paul was involved in the initial development of the Global Industrial Cyber Security Professional (GICSP) course curriculum. He holds a B.Sc degree in computer science with a minor in management. He holds several certifications including the GICSP and GIAPP®. In addition, he has participated in several executive development programmes. He is based in Calgary, Canada.

Paul Piotrowski is currently an Automation Engineer in Shell’s Global PCD Integrity Organization (Process Control Domain). Paul consults on global capital projects and supports Shell’s operated and non-operated assets across all business units. Paul has spent over 16 years with Shell in various security roles including network operations, risk governance and compliance, audit, incident management, forensics, pen testing and project management. His extensive travel for Shell has given him the opportunity to work across diverse sets of cultures and landscapes that have shaped his worldview. Paul possesses the valuable hybrid skill set of Operations Technology (OT) and Information Technology (IT). By visiting and working at over 50 Shell operations globally, he understands how to embed practical solutions between operations and corporate IT that reduce an organization’s cybersecurity risk while minimizing operational impact. Paul was involved in the initial development of the Global Industrial Cyber Security Professional (GICSP) course curriculum. He holds a B.Sc degree in computer science with a minor in management. He holds several certifications including the GICSP and GIAPP®. In addition, he has participated in several executive development programmes. He is based in Calgary, Canada.

Paul Piotrowski is currently an Automation Engineer in Shell’s Global PCD Integrity Organization (Process Control Domain). Paul consults on global capital projects and supports Shell’s operated and non-operated assets across all business units. Paul has spent over 16 years with Shell in various security roles including network operations, risk governance and compliance, audit, incident management, forensics, pen testing and project management. His extensive travel for Shell has given him the opportunity to work across diverse sets of cultures and landscapes that have shaped his worldview. Paul possesses the valuable hybrid skill set of Operations Technology (OT) and Information Technology (IT). By visiting and working at over 50 Shell operations globally, he understands how to embed practical solutions between operations and corporate IT that reduce an organization’s cybersecurity risk while minimizing operational impact. Paul was involved in the initial development of the Global Industrial Cyber Security Professional (GICSP) course curriculum. He holds a B.Sc degree in computer science with a minor in management. He holds several certifications including the GICSP and GIAPP®. In addition, he has participated in several executive development programmes. He is based in Calgary, Canada.
**Course Day Descriptions**

**DAY 1: ICS Overview**

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

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

---

**DAY 2: Field Devices and Controllers**

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

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

---

**DAY 3: Supervisory Systems**

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

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

---

**DAY 4: Workstations and Servers**

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

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

---

**DAY 5: ICS Security Governance**

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

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

---

**Who Should Attend**

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

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

“"The course is informative and relevant to anyone working with or alongside industrial control systems.""  
-Abrael Delgado,  
Compuquip Technologies

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/security-east-2019/courses](http://www.sans.org/event/security-east-2019/courses)
Cyber Defense | Short Courses

SEC440: Critical Security Controls: Planning, Implementing, and Auditing

This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS). These Critical Security Controls are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all serious and sensitive organizations. These controls were selected and defined by the U.S. military and other government agencies (including 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.

SEC455: SIEM Design and Implementation NEW!

Security Information and Event Management (SIEM) can be an extraordinary benefit to an organization’s security posture, but understanding and maintaining it can be difficult. Many solutions require complex infrastructure and software that necessitate professional services for installation. The use of professional services can leave security teams feeling as if they do not truly own or understand how their SIEM operates. Combine this situation of complicated solutions with a shortage of available skills, a lack of simple documentation, and the high costs of software and labor, and it is not surprising that deployments often fail to meet expectations. A SIEM can be the most powerful tool a cyber defense team can wield, but only when it is used to its fullest potential. This course is designed to address this problem by demystifying SIEMs and simplifying the process of implementing a solution that is usable, scalable, and simple to maintain.

The goal of this course is to teach students how to build a SIEM from the ground up using the Elastic Stack. Throughout the course, students will learn about the required stages of log collection. We will cover endpoint agent selection, logging formats, parsing, enrichment, storage, and alerting, and we will combine these components to make a flexible, high-performance SIEM solution. Using this approach empowers SIEM engineers and analysts to understand the complete system, make the best use of technology purchases, and supplement current underperforming deployments. This process allows organizations to save money on professional services, increase the efficiency of internal labor, and develop a nimbler solution than many existing deployments. For example, many organizations pay thousands of dollars in consulting fees when a unique log source needs a custom parser. This course will train students how to easily parse any log source without requiring consulting services, saving their organizations both time and money, and facilitating faster collection and use of new log sources.

SEC524: Cloud Security Fundamentals

This course teaches you how to properly evaluate cloud providers, and perform risk assessment and review, with a focus on risk assessment versus technical implementation and operations. The course will discuss architecture and infrastructure fundamentals for private, public and hybrid clouds, including a wide range of topics such as patch and configuration management, virtualization security, application security and change management. Policy, risk assessment, and governance within cloud environments will also be covered, with recommendations for both internal policies and contract provisions. This path leads to a discussion of compliance and legal concerns.
Penetration Testing | 2-Day Courses

SEC564: Red Team Operations and Threat Emulation
Red Teaming is the process of using tactics, techniques, and procedures (TTPs) to emulate real-world threats to train and measure the effectiveness of the people, processes, and technology used to defend environments. Built on the fundamentals of penetration testing, Red Teaming uses a comprehensive approach to gain insight into an organization’s overall security to test its ability to detect, respond to, and recover from an attack. When properly conducted, Red Team activities significantly improve an organization’s security controls, 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 relies heavily on well-defined TTPs, which are critical to successfully emulating a realistic threat or adversary. Red Team results exceed a typical list of penetration test vulnerabilities, provide a deeper understanding of how an organization would perform against an actual threat, and identify where security strengths and weaknesses exist.

Whether you support a defensive or offensive role in security, understanding how Red Teams can be used to improve security is extremely valuable. Organizations spend a great deal of time and money on the security of their systems, and it is critical to have professionals who can effectively and efficiently operate them. SEC564 will provide you with the skills to manage and operate a Red Team, conduct Red Team engagements, and understand the role of a Red Team and its importance in security testing. This two-day course will explore Red Team concepts in-depth, provide the fundamentals of threat emulation, and help you reinforce your organization’s security posture.

SEC567: Social Engineering for Penetration Testers
This course provides the blend of knowledge required to add social engineering skills to your penetration testing portfolio. Successful social engineering utilizes psychological principles and technical methods to measure your success and manage the risk. SEC567 covers the principles of persuasion and the psychological foundations required to craft effective attacks. The course then bolsters this with many examples of what works, drawing on both case studies of cyber criminals as well as on the authors’ experiences in dealing with such cases. On top of these principles the course provides a number of tools (produced in our engagements over the years and now available in the course) and features 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.

SEC580: Metasploit Kung Fu for Enterprise Pen Testing
Many enterprises today face regulatory or compliance requirements that mandate regular penetration testing and vulnerability assessments. Commercial tools and services for performing such tests can be expensive. While really solid free tools such as Metasploit are available, many testers do not understand the comprehensive feature sets of such tools and how to apply them in a professional-grade testing methodology. Metasploit was designed to help testers 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.

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/security-east-2019/courses
Management | 2-Day Courses

MGT415: A Practical Introduction to Cyber Security Risk Management

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

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

“Our company is creating a formal cyber risk and controls assessment program.
This class was a perfect introduction to the topic.”
-Jim Schleske, Ball Aerospace

Developer | Short Course

DEV531: Defending Mobile Applications Security Essentials

Mobile application development is growing exponentially year over year. As of late 2015, over 3 million apps were deployed in the Apple and Google app stores. These apps are consumed by over 700 million users worldwide and account for 33% of the traffic on the Internet. Average users have over 100 mobile apps installed on their device, many of which provide business-critical services to customers and employees.

Unfortunately, these apps are often rushed to market to gain a competitive advantage with little regard for security. As seen in web applications for the past 20 years, software vulnerabilities always exist where code is being written, and mobile apps are no different. Mobile apps are vulnerable to a whole new class of vulnerabilities, as well as most traditional issues that have long plagued web and desktop applications. This problem will only continue to grow unless managers, architects, developers, and QA teams learn how to test and defend their mobile apps.

DEV531: Defending Mobile Applications Security Essentials covers the most prevalent mobile app risks, including those from the OWASP Mobile Top 10. Students will participate in numerous hands-on exercises available in both the Android and iOS platforms. Each exercise is designed to reinforce the lessons learned throughout the course, ensuring that you understand how to properly defend your organization’s mobile applications.

“Mobile DEV security is extremely important and yet very rarely covered in other courses.
Excellent course, and very valuable.”
-Mark Geeslin, Asurion
Kick off your SANS Security East 2019 experience at the Welcome Networking Reception

Date: **Sunday, February 3**  
Time: **6:00pm – 9:00pm**  
Location: **Fulton Alley**, 600 Fulton Street, New Orleans, LA 70130

For all registered SANS Security East 2019 attendees!

Be part of this premier event and join the industry’s most powerful gathering of cybersecurity professionals. Share stories, make connections, and learn how to make the most of your week in New Orleans. Join your peers for a fun evening of bowling, shuffleboard and darts while watching Super Bowl LIII.

Attendees must pick up their event name badge at Registration Sunday, February 3 from 4:00pm-6:00pm. Event name badges are required for admission.

Bonus Sessions

Enrich your SANS training experience! Evening talks led by our instructors and selected subject-matter experts help you broaden your knowledge, hear from the voices that matter in computer security, and get the most for your training dollar.

**General Session – Welcome to SANS**  
Bryan Simon  
Join us for a 30-minute overview to help you get the most out of your SANS training experience. You will receive event information and learn about programs and resources offered by SANS. This brief session will answer many questions and get your training experience off to a great start. This session will be valuable to all attendees but is highly recommended for first-time attendees.

**KEYNOTE:** **OBSESSED: How to Be Wildly Successful**  
Dr. Eric Cole  
Most people want to be successful and achieve their goals, but often struggle getting to the next level. While having technical knowledge in cybersecurity is important, there are other tricks that successful people have learned to truly live the life of their dreams. The cool part is that success leaves clues. Bill Gates and Steve Jobs were not lucky, but they knew about tips and tricks that very few people take advantage of. The good news is that these “secrets” can be learned and used to help you accomplish anything that you want in life. If you want to accomplish anything there are essentially two ways of doing it: 1) make all of the mistakes yourself and slowly excel or, 2) learn from other people’s mistakes and exponentially propel your life more quickly than you ever imagined. It does not take months or years to change your life; it can be done in less than two hours.

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

**So You Think You Want to Be a CISO?**  
Russell Eubanks  
A Chief Information Security Officer role carries an extraordinary amount of influence on the overall information security posture of an organization. What are the keys to be exceptional in fulfilling these duties? How can you level up from being a trusted security advisor to an invited guest in the Boardroom? This presentation will highlight several key tactical and strategic imperatives necessary to be a successful CISO. It might also serve to help you determine this is not the role you are looking for!

Please check for schedule of night talks and updates at www.sans.org/security-east/bonus-sessions
Vendor Showcase
Wednesday, February 6   |   10:30am - 10:50am   |   3:00pm - 3:20pm

Given that virtually everything in security is accomplished with a tool, exposure to those tools is a very important part of the SANS training experience. Leading solution providers will be on hand for a one-day Vendor Expo, an added bonus to registered SANS Security East 2019 attendees. Attendees can visit the showcase during the morning and afternoon breaks.

Blockchain: The New Digital Swiss Army Knife?
G. Mark Hardy
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.

Getting SecOps Foundations Right with Techniques, Tactics and Procedures Zero (TTP0)
Ismael Valenzuela
TTP0 is a new community project created by SecOps practitioners for SecOps practitioners. Just like a blueprint is required to design, build and operate any facility, TTP0 provides the starting point for building or assessing a security program from the ground up. It focuses on resetting the basics of a security program to ensure a solid foundation. In this talk, Ismael Valenzuela, GSE, Certified SANS Instructor and Principal Engineer at McAfee, will discuss how TTP0 provides such a foundation while delivering tactical capabilities through our community templates, wikis, and open-source tools like the newly released DRONE, a custom python client that integrates with various case management platforms to deliver effective Incident Management.

OODA Security: Taking Back the Advantage
Kevin Fiscus
OODA, or Observe, Orient, Decide and Act, is a concept first developed for fighter pilots. The concept states that the adversary who can effectively complete the OODA cycle first will go home while the adversary who takes longer enjoys, at best, a long, slow parachute ride to the ground. This concept can be applied to information security. In theory, we defenders should have the advantage, as it is our “house” the attackers are attacking. Unfortunately, that is rarely the case. Over 50% of organizations find out they have been compromised via notification by a third party, meaning that all too often defenders don’t even start their OODA loop until after the attacker has completed the compromise. Making things worse, traditional security controls are failing us because attackers already know how to circumvent or evade them. Fortunately, there is a solution. By making better use of our existing technology and by using some of the attackers’ tools and techniques against them, we can deter, distract, delay, disrupt and detect them. Come learn how we can turn the tables on the bad guys and reclaim the OODA loop initiative.

Bonus Sessions (CONTINUED)

Please check for schedule of night talks and updates at www.sans.org/security-east/bonus-sessions

Lunch & Learn Presentations

In conjunction with the Vendor Showcase, on Wednesday, February 6 vendors will provide Lunch & Learn presentations. Take a break and get up-to-date on security technologies!
Future SANS Training Events

San Diego Fall .................................. San Diego, CA .............................. Nov 12-17
Austin ................................................. Austin, TX .............................. Nov 26 - Dec 1
San Francisco Fall .......................... San Francisco, CA ......................... Nov 26 - Dec 1
Nashville ........................................... Nashville, TN ........................ Dec 3-8
Santa Monica .................................. Santa Monica, CA ..................... Dec 3-8

Cyber Defense Initiative®

Washington, DC
Dec 11-18

Sonoma ........................................... Santa Rosa, CA ......................... Jan 14-19, 2019
Miami .............................................. Miami, FL .............................. Jan 21-26
Las Vegas ......................................... Las Vegas, NV ........................ Jan 28 - Feb 2

Security East

New Orleans, LA
Feb 2-9

Anaheim ........................................... Anaheim, CA .......................... Feb 11-16
Northern VA Spring – Tysons ................ McLean, VA ............................. Feb 11-16
Dallas .............................................. Dallas, TX .............................. Feb 18-23
New York Metro Winter ...................... Jersey City, NJ ......................... Feb 18-23
Scottsdale ..................................... Scottsdale, AZ ........................ Feb 18-23
Reno Tahoe ..................................... Reno, NV ............................... Feb 25 - Mar 2
Baltimore Spring ............................ Baltimore, MD ....................... Mar 2-9

Future SANS Summit Events

Pen Test HackFest ............................. Bethesda, MD ......................... Nov 12-19
Tactical Detection & Data Analytics ...... Scottsdale, AZ ..................... Dec 4-11
Cyber Threat Intelligence .................. Arlington, VA ......................... Jan 21-28, 2019
OSINT ............................................. Alexandria, VA .................... Feb 25 - Mar 3

Future Community SANS Events

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

Take SANS Training Anytime, Anywhere with OnDemand

More than 30 of the most popular SANS courses are available in our online training format OnDemand with no travel required. All OnDemand courses include:
• Four months of online access to your course
• Subject-matter-expert support
• Training with SANS top instructors
• All printed books and materials
• Labs and quizzes to reinforce your learning

Visit www.sans.org/ondemand to learn more about your OnDemand training options.
Cancellation & Access Policy
If an attendee must cancel, a substitute may attend instead. Substitution requests can be made at any time prior to the event start date. Processing fees will apply. All substitution requests must be submitted by email to registration@sans.org. If an attendee must cancel and no substitute is available, a refund can be issued for any payments received by January 16, 2019. A credit memo can be requested up to the event start date. All cancellation requests must be submitted in writing by mail or fax and received by the stated deadlines. Payments will be refunded by the method that they were submitted. Processing fees will apply.

SANS SIMULCAST
Nothing beats the SANS live training experience, but if you are unable to attend, learn how you can register for a SANS Security East 2019 Simulcast course. Visit www.sans.org/event/security-east-2019/attend-remotely

SANS Voucher Program
Expand your training budget!
For organizations with multiple employees taking SANS training courses, the SANS Voucher Program is an easy-to-use, flexible training management solution. Based on the number of anticipated students and investment, you may be eligible to receive bonus funds from SANS. Your investment and bonus funds can be used for classroom and online training, and can also be used to pay for GIAC certification exams. Contact SANS for more detailed information about our Voucher Program. www.sans.org/vouchers

Pay Early and Save*
Use code EarlyBird19 when registering early

<table>
<thead>
<tr>
<th>DATE</th>
<th>DISCOUNT</th>
<th>DATE</th>
<th>DISCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec 12</td>
<td>$350</td>
<td>Jan 2</td>
<td>$200</td>
</tr>
</tbody>
</table>

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

SANS Voucher Program
Expand your training budget!
For organizations with multiple employees taking SANS training courses, the SANS Voucher Program is an easy-to-use, flexible training management solution. Based on the number of anticipated students and investment, you may be eligible to receive bonus funds from SANS. Your investment and bonus funds can be used for classroom and online training, and can also be used to pay for GIAC certification exams. Contact SANS for more detailed information about our Voucher Program. www.sans.org/vouchers

It’s all about location in New Orleans, and the Hilton New Orleans Riverside places you at the center of it all. Nestled against the banks of the Mississippi, guests can watch the ships come sailing in or dive into the city life just steps away. Grab a beignet, listen to live jazz, ride a streetcar, or hop into a parade, you never know what you’ll experience in the vibrant culture and excitement of New Orleans just outside the front door.

Special Hotel Rates Available
A special discounted rate of $214 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID. These rates include high-speed Internet in your room and are only available through January 11, 2019.

Top three reasons to stay at the Hilton New Orleans Riverside
1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Hilton New Orleans Riverside, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
3. SANS schedules morning and evening events at the Hilton New Orleans Riverside that you won’t want to miss!

It’s all about location in New Orleans, and the Hilton New Orleans Riverside places you at the center of it all. Nestled against the banks of the Mississippi, guests can watch the ships come sailing in or dive into the city life just steps away. Grab a beignet, listen to live jazz, ride a streetcar, or hop into a parade, you never know what you’ll experience in the vibrant culture and excitement of New Orleans just outside the front door.

Special Hotel Rates Available
A special discounted rate of $214 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID. These rates include high-speed Internet in your room and are only available through January 11, 2019.

Top three reasons to stay at the Hilton New Orleans Riverside
1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Hilton New Orleans Riverside, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
3. SANS schedules morning and evening events at the Hilton New Orleans Riverside that you won’t want to miss!

It’s all about location in New Orleans, and the Hilton New Orleans Riverside places you at the center of it all. Nestled against the banks of the Mississippi, guests can watch the ships come sailing in or dive into the city life just steps away. Grab a beignet, listen to live jazz, ride a streetcar, or hop into a parade, you never know what you’ll experience in the vibrant culture and excitement of New Orleans just outside the front door.

Special Hotel Rates Available
A special discounted rate of $214 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID. These rates include high-speed Internet in your room and are only available through January 11, 2019.

Top three reasons to stay at the Hilton New Orleans Riverside
1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Hilton New Orleans Riverside, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
3. SANS schedules morning and evening events at the Hilton New Orleans Riverside that you won’t want to miss!

SANS SIMULCAST
Nothing beats the SANS live training experience, but if you are unable to attend, learn how you can register for a SANS Security East 2019 Simulcast course. Visit www.sans.org/event/security-east-2019/attend-remotely

SANS Voucher Program
Expand your training budget!
For organizations with multiple employees taking SANS training courses, the SANS Voucher Program is an easy-to-use, flexible training management solution. Based on the number of anticipated students and investment, you may be eligible to receive bonus funds from SANS. Your investment and bonus funds can be used for classroom and online training, and can also be used to pay for GIAC certification exams. Contact SANS for more detailed information about our Voucher Program. www.sans.org/vouchers

Pay Early and Save*
Use code EarlyBird19 when registering early

<table>
<thead>
<tr>
<th>DATE</th>
<th>DISCOUNT</th>
<th>DATE</th>
<th>DISCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec 12</td>
<td>$350</td>
<td>Jan 2</td>
<td>$200</td>
</tr>
</tbody>
</table>

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

SANS SIMULCAST
Nothing beats the SANS live training experience, but if you are unable to attend, learn how you can register for a SANS Security East 2019 Simulcast course. Visit www.sans.org/event/security-east-2019/attend-remotely

SANS Voucher Program
Expand your training budget!
For organizations with multiple employees taking SANS training courses, the SANS Voucher Program is an easy-to-use, flexible training management solution. Based on the number of anticipated students and investment, you may be eligible to receive bonus funds from SANS. Your investment and bonus funds can be used for classroom and online training, and can also be used to pay for GIAC certification exams. Contact SANS for more detailed information about our Voucher Program. www.sans.org/vouchers

Pay Early and Save*
Use code EarlyBird19 when registering early

<table>
<thead>
<tr>
<th>DATE</th>
<th>DISCOUNT</th>
<th>DATE</th>
<th>DISCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec 12</td>
<td>$350</td>
<td>Jan 2</td>
<td>$200</td>
</tr>
</tbody>
</table>

*Some restrictions apply. Early bird discounts do not apply to Hosted courses.
## Courses – 4–6 Days

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Name</th>
<th>Paid before 12-12-18</th>
<th>Paid before 1-2-19</th>
<th>Paid after 1-2-19</th>
<th>Add GIAC Cert</th>
<th>Add OnDemand</th>
<th>Add NetWars Continuous</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
<td>$6,260</td>
<td>$6,410</td>
<td>$6,610</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
</tr>
<tr>
<td>SEC501</td>
<td>Advanced Security Essentials – Enterprise Defender</td>
<td>$6,260</td>
<td>$6,410</td>
<td>$6,610</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
</tr>
<tr>
<td>SEC503</td>
<td>Intrusion Detection In-Depth</td>
<td>$6,260</td>
<td>$6,410</td>
<td>$6,610</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td>$6,260</td>
<td>$6,410</td>
<td>$6,610</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
</tr>
<tr>
<td>SEC531</td>
<td>Continuous Monitoring and Security Operations</td>
<td>$6,260</td>
<td>$6,410</td>
<td>$6,610</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
</tr>
<tr>
<td>SEC530</td>
<td>Defensible Security Architecture NEW!</td>
<td>$6,260</td>
<td>$6,410</td>
<td>$6,610</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
</tr>
<tr>
<td>SEC542</td>
<td>Web App Penetration Testing and Ethical Hacking</td>
<td>$6,260</td>
<td>$6,410</td>
<td>$6,610</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
</tr>
<tr>
<td>SEC545</td>
<td>Cloud Security Architecture and Operations</td>
<td>$5,380</td>
<td>$5,530</td>
<td>$5,730</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
</tr>
<tr>
<td>SEC555</td>
<td>SIEM with Tactical Analytics</td>
<td>$6,260</td>
<td>$6,410</td>
<td>$6,610</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
</tr>
<tr>
<td>SEC560</td>
<td>Network Penetration Testing and Ethical Hacking</td>
<td>$6,260</td>
<td>$6,410</td>
<td>$6,610</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
</tr>
<tr>
<td>SEC566</td>
<td>Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td>$5,380</td>
<td>$5,530</td>
<td>$5,730</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
</tr>
<tr>
<td>SEC575</td>
<td>Mobile Device Security and Ethical Hacking</td>
<td>$6,260</td>
<td>$6,410</td>
<td>$6,610</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
</tr>
<tr>
<td>SEC560</td>
<td>Advanced Penetration Testing, Exploit Writing, and Ethical Hacking</td>
<td>$6,260</td>
<td>$6,410</td>
<td>$6,610</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Digital Forensics, Incident Response, and Threat Hunting</td>
<td>$6,260</td>
<td>$6,410</td>
<td>$6,610</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
</tr>
<tr>
<td>FOR572</td>
<td>Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response</td>
<td>$6,260</td>
<td>$6,410</td>
<td>$6,610</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
</tr>
<tr>
<td>FOR610</td>
<td>Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td>
<td>$6,260</td>
<td>$6,410</td>
<td>$6,610</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
</tr>
<tr>
<td>MGT414</td>
<td>SANS Training Program for CISSP® Certification</td>
<td>$6,260</td>
<td>$6,410</td>
<td>$6,610</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
</tr>
<tr>
<td>MGT512</td>
<td>Security Leadership Essentials for Managers</td>
<td>$5,870</td>
<td>$6,020</td>
<td>$6,220</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
</tr>
<tr>
<td>MGT514</td>
<td>Security Strategic Planning, Policy, and Leadership</td>
<td>$5,870</td>
<td>$6,020</td>
<td>$6,220</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
</tr>
<tr>
<td>MGT516</td>
<td>Managing Security Vulnerabilities: Enterprise and Cloud NEW!</td>
<td>$5,870</td>
<td>$6,020</td>
<td>$6,220</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
</tr>
<tr>
<td>MGT517</td>
<td>Managing Security Operations: Detection, Response, and Intelligence</td>
<td>$5,870</td>
<td>$6,020</td>
<td>$6,220</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
</tr>
<tr>
<td>DEV540</td>
<td>Secure DevOps and Cloud Application Security</td>
<td>$5,380</td>
<td>$5,530</td>
<td>$5,730</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</td>
</tr>
<tr>
<td>ICS410</td>
<td>ICS/SCADA Security Essentials</td>
<td>$5,730</td>
<td>$5,880</td>
<td>$6,080</td>
<td>$769</td>
<td>$769</td>
<td>$1,340</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>
<th>Add OnDemand</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC440</td>
<td>Critical Security Controls: Planning, Implementing, and Auditing</td>
<td>$1,980</td>
<td>$2,640</td>
<td>$279</td>
</tr>
<tr>
<td>SEC455</td>
<td>SIEM Design &amp; Implementation NEW!</td>
<td>$1,980</td>
<td>$2,640</td>
<td>$279</td>
</tr>
<tr>
<td>SEC524</td>
<td>Cloud Security Fundamentals</td>
<td>$1,980</td>
<td>$2,640</td>
<td>$279</td>
</tr>
<tr>
<td>SEC566</td>
<td>Red Team Operations and Threat Emulation</td>
<td>$1,980</td>
<td>$2,640</td>
<td>$279</td>
</tr>
<tr>
<td>SEC567</td>
<td>Social Engineering for Penetration Testers</td>
<td>$1,980</td>
<td>$2,640</td>
<td>$279</td>
</tr>
<tr>
<td>SEC580</td>
<td>Metasploit Kung Fu for Enterprise Pen Testing</td>
<td>$1,980</td>
<td>$2,640</td>
<td>$279</td>
</tr>
<tr>
<td>MGT415</td>
<td>A Practical Introduction to Cyber Security Risk Management</td>
<td>$1,980</td>
<td>$2,640</td>
<td>$279</td>
</tr>
<tr>
<td>DEV531</td>
<td>Defending Mobile Applications Security Essentials</td>
<td>$1,980</td>
<td>$2,640</td>
<td>$279</td>
</tr>
<tr>
<td>SPECIAL</td>
<td>Core NetWars Experience – Tournament Entrance Fee</td>
<td>FREE</td>
<td>$1,695</td>
<td>$279</td>
</tr>
<tr>
<td>SPECIAL</td>
<td>DFIR NetWars Tournament – Tournament Entrance Fee</td>
<td>FREE</td>
<td>$1,695</td>
<td>$279</td>
</tr>
<tr>
<td>SPECIAL</td>
<td>Cyber Defense NetWars Tournament – Tournament Entrance Fee</td>
<td>FREE</td>
<td>$1,695</td>
<td>$279</td>
</tr>
</tbody>
</table>

### Early Bird Discounts

Pay for any long course using the code EarlyBird19 at checkout by December 12th to get $350 OFF or by January 2nd to get $200 OFF.

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

Join the SANS.org community today to enjoy these free resources at www.sans.org/join

**Newsletters**

**NewsBites**
Twice-weekly, high-level executive summary of the most important news relevant to cybersecurity professionals.

**OUCH!**
The world's leading monthly free security awareness newsletter designed for the common computer user.

**Webcasts**

**Ask the Experts Webcasts**
SANS experts bring current and timely information on relevant topics in IT Security.

**Analyst Webcasts**
A follow-on to the SANS Analyst Program, Analyst Webcasts provide key information from our whitepapers and surveys.

**Other Free Resources (SANS.org account not required)**
- InfoSec Reading Room
- Top 25 Software Errors
- 20 Critical Controls
- Security Policies
- Intrusion Detection FAQs
- Tip of the Day

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

WhatWorks Webcasts
The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT Security issues.

Tool Talks
Tool Talks are designed to give you a solid understanding of a problem, and how a vendor’s commercial tool can be used to solve or mitigate that problem.

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

NALT-BRO-SECEAST2019