SANS

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

VIRGINIA BEACH 2017

August 21 – September 1

Protect Your Business and Advance Your Career

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

CYBER DEFENSE
DETECTION & MONITORING
PENETRATION TESTING
CYBER THREAT INTELLIGENCE
ETHICAL HACKING
DIGITAL FORENSICS
MANAGEMENT

GIAC CERTIFICATIONS

> "You can't beat the quality of SANS courses and instructors. I returned to work with a new malware case and was able to implement the skills learned in class on day one. Invaluable!"
>
> -MELISSA SOKOLOWSKI, XEROX

Core NETWARS EXPERIENCE

SAVE $400

Register and pay by June 28th – Use code **EarlyBird17**

www.sans.org/virginia-beach

SANS Virginia Beach 2017

AUGUST 21 – SEPTEMBER 1

Courses at a Glance (WEEK 1)

	MON 8-21	TUE 8-22	WED 8-23	THU 8-24	FRI 8-25	SAT 8-26
SEC401 **Security Essentials Bootcamp Style**	Page 2 *SIMULCAST*					
SEC501 **Advanced Security Essentials – Enterprise Defender**	Page 3 *SIMULCAST*					
SEC503 **Intrusion Detection In-Depth**	Page 4					
SEC511 **Continuous Monitoring and Security Operations**	Page 7 *SIMULCAST*					
SEC555 **SIEM with Tactical Analytics**	Page 9 *NEW!*					
SEC560 **Network Penetration Testing and Ethical Hacking**	Page 10 *SIMULCAST*					
FOR500 **Windows Forensic Analysis (FORMERLY FOR408)**	Page 11					
MGT512 **SANS Security Leadership Essentials for Managers with Knowledge Compression™**	Page 16					
Core NetWars Experience				Page 19		

Courses at a Glance (WEEK 2)

	SUN 8-27	MON 8-28	TUE 8-29	WED 8-30	THU 8-31	FRI 9-1
SEC504 **Hacker Tools, Techniques, Exploits, and Incident Handling**	Page 5					
SEC505 **Securing Windows and PowerShell Automation**	Page 6					
SEC542 **Web App Penetration Testing and Ethical Hacking**	Page 8					
FOR508 **Advanced Digital Forensics, Incident Response, and Threat Hunting**	Page 12					
FOR572 **Advanced Network Forensics and Analysis**	Page 13					
FOR578 **Cyber Threat Intelligence**		Page 14				
FOR610 **Reverse-Engineering Malware: Malware Analysis Tools and Techniques**	Page 15 *NEW!*					
MGT517 **Managing Security Operations: Detection, Response, and Intelligence**		Page 17 *NEW!*				
Core NetWars Experience				Page 19		

Evening Bonus Sessions

Take advantage of these extra evening presentations
and add more value to your training. Learn more on page 18.

KEYNOTE (WEEK 1): ***Quality Not Quantity: Continuous Monitoring's Deadliest Events***
Eric Conrad

KEYNOTE (WEEK 2): ***Lessons in Incident Response*** – Chad Tilbury

Actionable Detects: Blue Team Cyber Defense Tactics – Seth Misenar

Stuck in the Box, a SIEM's Tale – Justin Henderson

Anti-Ransomware: How to Turn the Tables – G. Mark Hardy

Kill Chain – Paul Henry

Mobile Application Assessment – Chris Crowley

Save $400 when you register and pay by June 28th using code EarlyBird17

Register today for SANS Virginia Beach 2017!
www.sans.org/virginia-beach

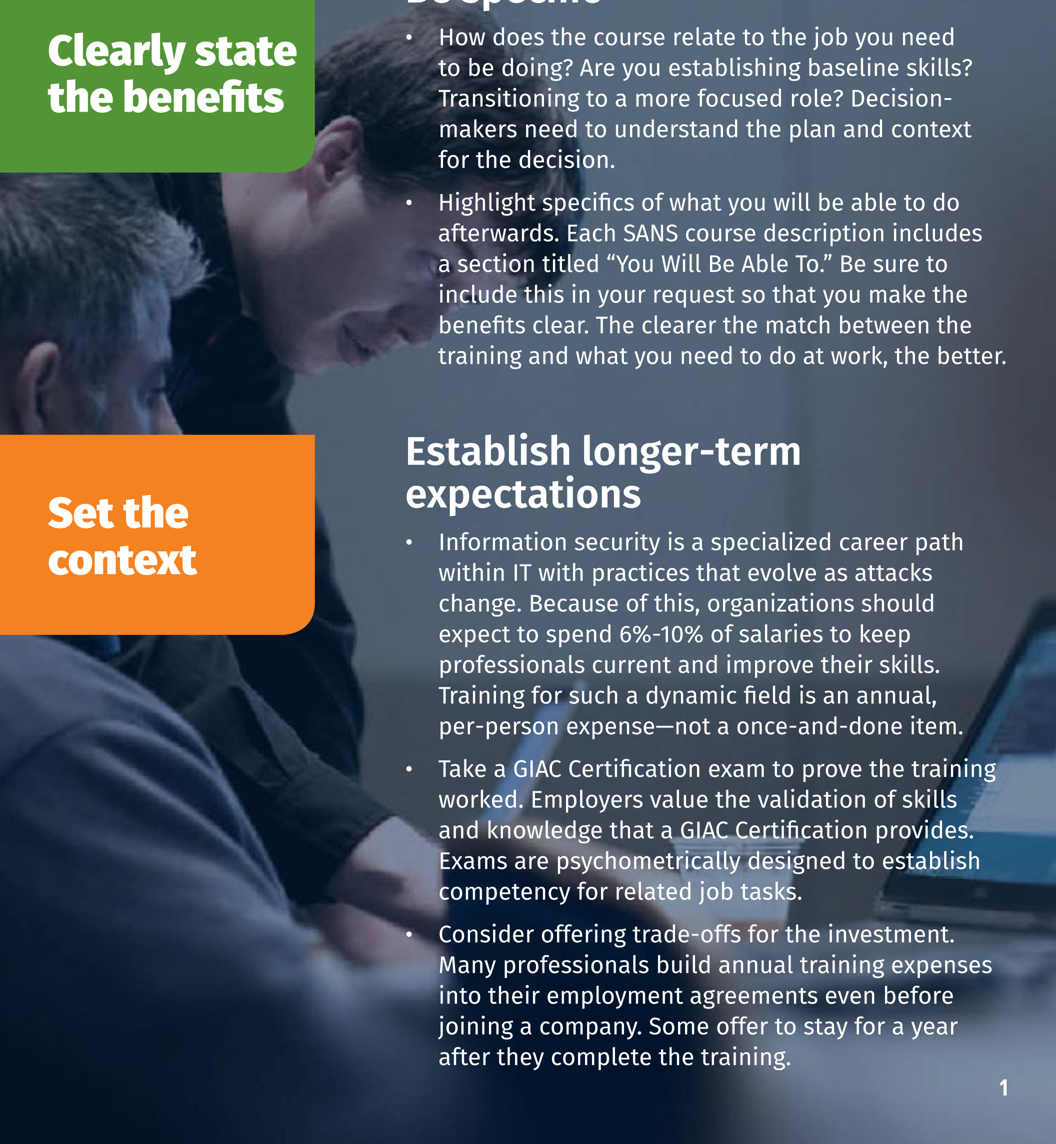
@SANSInstitute
Join the conversation:
#SANSVaBeach

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.

SEC**401**

Security Essentials Bootcamp Style

GSEC Certification
Security Essentials
www.giac.org/gsec

Six-Day Program
Mon, Aug 21 - Sat, Aug 26
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Dr. Eric Cole

Who Should Attend

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

> "SEC401 has opened my eyes to just how important security is, and has given me a deeper understanding on how to protect our systems."
> -Travis Sorensen, Xpress Solutions, Inc.

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

STOP and ask yourself the following questions:

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

If you do not know the answers to these questions, SEC401 will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

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

Prevention Is Ideal but Detection Is a Must

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

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

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

SANS Technology Institute
www.sans.edu

www.sans.org/8140

Bundle OnDemand
with this course
www.sans.org/ondemand

Also available via Simulcast
See page 21 for details.

Dr. Eric Cole *SANS Faculty Fellow*

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. He has experience in information technology with a focus on helping customers focus on the right areas of security by building out a dynamic defense. Dr. Cole 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 was 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 cyber security consulting services, expert witness work, and leads research and development initiatives to advance the state-of-the-art in information systems security. Dr. Cole 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

SEC501

GCED Certification

Certified Enterprise Defender

www.giac.org/gced

Advanced Security Essentials – Enterprise Defender

Six-Day Program
Mon, Aug 21 - Sat, Aug 26
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Paul A. Henry

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

> "SEC501 is the perfect course to immerse enterprise security staff into essential skills. Failing to attend this course is done at the peril of your organization."
> -John N. Johnson, Houston Police Department

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.

> "The content is relevant, the labs were interactive, and the instructor is awesome. I strongly recommend this course for SOC analysts and IR professionals."
> -Brett Smetanka, KeyBank

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.

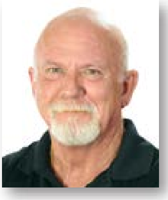
Finally, once an attack is detected we must react quickly and effectively and perform the forensics required. Knowledge gained by understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

SANS Technology Institute
www.sans.edu

www.sans.org/8140

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

Also available via Simulcast
See page 21 for details.



Paul A. Henry *SANS Senior Instructor*

Paul is one of the world's foremost global information security and computer forensic experts, with more than 20 years' experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principal at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security. Throughout his career, Paul has played a key strategic role in launching new network security initiatives to meet our ever-changing threat landscape. 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 and telecommunications projects throughout Southeast Asia. Paul is frequently cited by major publications as an expert on perimeter security, incident response, computer forensics, and general security trends, and serves as an expert commentator for network broadcast outlets such as FOX, NBC, CNN, and CNBC. In addition, Paul regularly authors thought leadership articles on technical security issues, and his expertise and insight help shape the editorial direction of key security publications such as the *Information Security Management Handbook*, to which he is a consistent contributor. Paul is a featured speaker at seminars and conferences worldwide, delivering presentations on diverse topics such as anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, perimeter security, and incident response. **@phenrycissp**

SEC**503**

Intrusion Detection In-Depth

GCIA Certification
Certified Intrusion Analyst
www.giac.org/gcia

Six-Day Program
Mon, Aug 21 - Sat, Aug 26
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Dr. Johannes Ullrich

Who Should Attend

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

> "This training directly correlates to my agency's mission of conducting network forensics/ intrusion investigations."
> -Chris G., U.S. Air Force Office of Special Investigations

> "This course met my expectations, providing clear and concise information from an instructor who did an excellent job keeping the material and course interesting – well done."
> -David Holland, Stroz Friedberg

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 determine if it is noteworthy or a false indication.

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

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

www.sans.org/8140

▶❚❚ Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

Dr. Johannes Ullrich *SANS Senior Instructor*

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

SEC504

GCIH Certification
Incident Handler

www.giac.org/gcih

Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program
Sun, Aug 27 - Fri, Sep 1
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
(If your laptop supports only wireless, please bring a USB Ethernet adapter.)
Instructor: Kevin Fiscus

Who Should Attend

- Incident handlers
- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack

"It fills the gap of 'here's what adversaries do and the evidence they leave.'"
-Kevin Heithaus, JPMorgan Chase

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or 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.**

"A real eye opener on the Web attack section. Windows command line bootcamp section was excellent."-Terrence Randell, JPMorgan Chase

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 those attacks. Additionally, 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!**

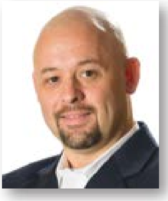
The course is particularly well-suited to individuals who lead or are a part of an incident handling team. General security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

www.sans.org/8140

▶II Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand



Kevin Fiscus *SANS Certified Instructor*

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. He currently holds the CISA, GPEN, GREM, GMOB, GCED, GCFA-Gold, GCIA-Gold, GCIH, GAWN, GPPA, GCWN, GCSC-Gold, GSEC, SCSA, RCSE, and SnortCP certifications and is proud to have earned the top information security certification in the industry, the GIAC Security Expert. Kevin has also achieved the distinctive title of SANS Cyber Guardian for both red team and blue team. Kevin has taught many of SANS' most popular classes including SEC401, SEC464, SEC503, SEC504, SEC542, SEC560, SEC561, SEC575, FOR508, and MGT414. **@kevinbfiscus**

SEC505

Securing Windows and PowerShell Automation

GCWN Certification
Windows Security Administrator
www.giac.org/gcwn

Six-Day Program
Sun, Aug 27 - Fri, Sep 1
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jason Fossen

Who Should Attend

- Security Operations engineers
- Windows endpoint and server administrators
- Anyone who wants to learn PowerShell automation
- Anyone implementing the NSA Top 10 Mitigations
- Anyone implementing the CIS Critical Security Controls
- Those deploying or managing a Public Key Infrastructure or smart cards
- Anyone who needs to reduce malware infections

> "Most excellent, content-packed, skills-enhancement course."
> -Jesus Perez, Texas A&M University

> "Really great course for anyone involved in the administration or securing of Windows environments."
> -David Hazar, Oracle

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

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

For the assume breach mindset, we must carefully delegate limited administrative powers so that the compromise of one administrator account is not a catastrophe across the board. Managing administrative privileges is a tough problem, so this course devotes an entire day to just this one critical task.

Learning PowerShell is also useful for another kind of security: *job security*. Employers are looking for people with these skills. You don't have to know any PowerShell to attend the course, we will learn it together. About half the labs during the week are PowerShell, while the rest use graphical security tools. PowerShell is free and open-source on GitHub for Linux and Mac OS, too.

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

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

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

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

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

Jason Fossen *SANS Faculty Fellow*

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

SEC**511**

GMON Certification
Continuous Monitoring

GIAC CONTINUOUS MONITORING CERTIFICATION GMON
www.giac.org/gmon

Continuous Monitoring and Security Operations

Six-Day Program
Mon, Aug 21 - Sat, Aug 26
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Eric Conrad

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)

"This course has been awesome at teaching me how to use tools and existing architecture in ways I haven't thought of before!"
-John Hubbard, GlaxoSmithKline

We continue to underestimate the tenacity of our adversaries! Organizations are investing significant time and financial and human resources trying 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, 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.

"Keep on giving real-life scenarios to spice up the class. This class was perfect."
-Genevieve Opaye-Tetteh, eProcess Int SA

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.

SANS Technology Institute
www.sans.edu

▶❚❚ Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

ALSO AVAILABLE VIA SIMULCAST
See page 21 for details.

Eric Conrad *SANS Senior Instructor*

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 GIAC GPEN, GCIH, GCIA, GCFA, GAWN, and GSEC certifications. Eric also blogs about information security at ericconrad.com. **@eric_conrad**

SEC542

GWAPT Certification
Web Application Penetration Tester
www.giac.org/gwapt

Web App Penetration Testing and Ethical Hacking

Six-Day Program
Sun, Aug 27 - Fri, Sep 1
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Moses Hernandez

Who Should Attend

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

> "This course taught me to truly focus on the methodology while performing a pen test. During the Capture the Flag event, I realized how much time can be wasted if you fail to respect your methodology."
>
> -Sean Rosado, RavenEye

> "As a developer, this course has taught me many ways my website could be hacked and has exposed me to tools I've never heard of before."
>
> -Linus Christian, Magellan Midstream

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.

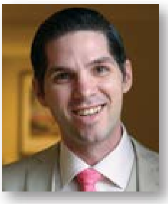
In addition to high-quality course content, SEC542 focuses heavily on in-depth, hands-on labs to ensure that students can immediately apply all they learn.

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.

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

▶❚❚ Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand



Moses Hernandez *SANS Instructor*

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

SEC555

SIEM with Tactical Analytics *NEW!*

Six-Day Program
Mon, Aug 21 - Sat, Aug 26
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructors: Seth Misenar,
Justin Henderson

Who Should Attend

- Security analysts
- Security architects
- Senior security engineers
- Technical security managers
- SOC analysts
- SOC engineers
- SOC managers
- CND analysts
- Security monitoring personnel
- System administrators
- Cyber threat investigators
- Individuals working to implement Continuous Security Monitoring or Network
- Individuals working in a hunt team capacity

Many organizations have logging capabilities but lack the people and processes to analyze logging systems. These systems collect vast amounts of data from a variety of sources, so proper analysis requires an understanding of those data sources. This class is designed to provide students with the training, methods, and processes to enhance existing logging solutions. The class will also provide an understanding of the when, what, and why behind the logs. This is a lab-heavy course that utilizes SOF-ELK – a SANS-sponsored free Security Incident and Events Management (SIEM) solution – to provide the hands-on experience and mindset needed 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. Add to this the daunting challenge that there is an infinite list of systems from which one can collect logs. It is easy to get lost in the perils of data saturation. This class is the switch from the typical churn-and-burn log systems to 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 data are collected, the student will be shown how to present the gathered input into usable formats to aid in eventual correlation. Students will then iterate through the log data and events to analyze key components that will allow them to learn how rich this information is, how to correlate the data, start investigating based on the aggregate data, and finally, how to go hunting with this newly gained knowledge. They will also learn how to deploy internal post-exploitation tripwires and breach canaries to nimbly detect sophisticated intrusions. Throughout the course, the text and labs will not only show how to manually perform these actions, but also how to automate many of the processes mentioned so students 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.

Seth Misenar *SANS Senior Instructor*

Seth Misenar is the founder of and now the lead consultant for Jackson, Mississippi-based Context Security, which 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 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**

Justin Henderson *SANS Instructor*

Justin Henderson has been in the information technology field since 2005. He specializes in technical platforms including operating systems, networking, security, storage, and virtualization, but has also applied himself in governance, project management, and service management. Justin holds a bachelor's degree of science in network design and administration from Western Governors University and has over 40 certifications Some of Justin's achievements include mentoring individuals in the information technology field as well as developing the virtual dojo, a fully automated Cloud Computing solution showcase environment.

SEC560

GPEN Certification
Penetration Tester
www.giac.org/gpen

Network Penetration Testing and Ethical Hacking

Six-Day Program
Mon, Aug 21 - Sat, Aug 26
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Kevin Fiscus

Who Should Attend

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

"I learned more in one class than in years of self-study!"
-Bradley Milhorn, Compucom Inc.

"It introduces the whole process of pen testing from start of engagement to end."
-Barry Tsang, Deloitte

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.

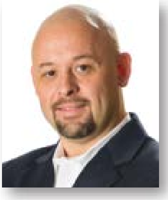
You will learn how to perform detailed reconnaissance, studying a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won't just cover 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.

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

▶II Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

Also available via Simulcast
See page 21 for details.



Kevin Fiscus *SANS Certified Instructor*

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 for the past 12 years on information security. Kevin currently holds the CISA, GPEN, GREM, GMOB, GCED, GCFA-Gold, GCIA-Gold, GCIH, GAWN, GPPA, GCWN, GCSC-Gold, GSEC, SCSA, RCSE, and SnortCP certifications and is proud to have earned the top information security certification in the industry, the GIAC Security Expert. Kevin has also achieved the distinctive title of SANS Cyber Guardian for both red team and blue team. @kevinbfiscus

FOR500 (Formerly FOR408)

Windows Forensic Analysis

GCFE Certification
Forensic Examiner
www.giac.org/gcfe

Six-Day Program
Mon, Aug 21 - Sat, Aug 26
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Rob Lee

Who Should Attend

- Information security professionals
- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Anyone interested in a deep understanding of Windows forensics

> "This is a fantastic course! Rob is a fantastic instructor with real-world application experience. This is a must for any investigator."
>
> -Eddie Sky, Forsythe

SANS Technology Institute
www.sans.edu

▶❚❚ Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

MASTER WINDOWS FORENSICS – YOU CAN'T PROTECT WHAT YOU DON'T KNOW ABOUT

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

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

Proper analysis requires real data for students to examine. The completely updated FOR500 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7, Windows 8/8.1, Windows 10, Office and Office365, cloud storage, SharePoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques, prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows 7 systems to just-discovered Windows 10 artifacts.

FOR500: Windows Forensic Analysis will teach you to:

- **Conduct in-depth forensic analysis of Windows operating systems and media exploitation focusing on Windows 7, Windows 8/8.1, Windows 10, and Windows Server 2008/2012/2016**
- **Identify artifact and evidence locations to answer critical questions, including application execution, file access, data theft, external device usage, cloud services, geolocation, file download, anti-forensics, and detailed system usage**
- **Focus your capabilities on analysis instead of on how to use a particular tool**
- **Extract critical answers and build an in-house forensic capability via a variety of free, open-source, and commercial tools provided within the SANS Windows SIFT Workstation**

Rob Lee *SANS Faculty Fellow*

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

FOR508

Advanced Digital Forensics, Incident Response, and Threat Hunting

GCFA Certification
Forensic Analyst
www.giac.org/gcfa

Six-Day Program
Sun, Aug 27 - Fri, Sep 1
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Chad Tilbury

Who Should Attend

- Incident response team members
- Threat hunters
- Experienced digital forensic analysts
- Information security professionals
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- SANS FOR500 (formerly FOR408) and SEC504 graduates

> "This is, by far, the best training I have ever had. My forensic knowledge increased more in the last five days than in the last year."
> -Vito Rocco, University of Nevada Las Vegas

> "Come prepared to learn a lot!"
> -Todd Black Lee, Golden 1 Credit Union

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!

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

www.sans.org/8140

▶❚❚ Bundle OnDemand with this course
www.sans.org/ondemand

Chad Tilbury *SANS Senior Instructor*

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

FOR572

GNFA Certification
Network Forensic Analyst
www.giac.org/gnfa

Advanced Network Forensics and Analysis

Six-Day Program
Sun, Aug 27 - Fri, Sep 1
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Ryan Johnson

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

"Great training course that is exposing me to new networking concepts."
-John McDonald, Florida Dept. of Law Enforcement

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 prove useful even in definitively proving a crime actually occurred.

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

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

Whether you are a consultant responding to a client's site, a law enforcement professional assisting victims of cybercrime and seeking prosecution of those responsible, an on-staff forensic practitioner, or a member of the growing ranks of "threat hunters," this course offers hands-on experience with real-world scenarios that will help take your work to the next level. Previous SANS Security 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.

Ryan Johnson *SANS Instructor*

As a globe-trotting cyber sleuth, Ryan Johnson is always looking to find the bad guy, and to share his enthusiasm and knowledge about digital forensics along the way. Ryan started out performing digital forensic exams for local law enforcement in Durham, N.C., assisting in homicide, fraud, narcotics, and child exploitation cases. He quickly saw the importance of digital evidence in ensuring that guilty parties are held accountable and innocent parties go free. That work led Ryan to join a team of media exploitation analysts working for the U.S. Army in Iraq. During his year in Iraq he helped gather actionable intelligence, streamline processes, and enhance equipment resources for in-country teams. When he returned stateside, Ryan began to work on computer intrusion cases. Since then he's traveled the globe teaching digital forensics for the U.S. State Department's Anti-Terrorism Assistance Program and served as a digital forensics analyst and consultant. Ryan co-authored several of the State Department's digital forensics courses as well as the book *Mastering Windows Network Forensics and Investigations*, Second Edition. Ryan also currently serves as the Global Head of CSIRT at PricewaterhouseCoopers, where he leads the response, readiness and investigations functions. In addition, based on his background, practical forensic experience, and government clearance, Ryan has been regularly called upon to train U.S.-based government departments, international governments, and corporations in the areas of network and digital forensics. Ryan earned a master's of science degree from Dalhousie University and two bachelor's degrees from Queen's University. He has taught college students, professionals, law enforcement, attorneys, and judges. Ryan knows that teaching the process, not the tool, is what gives students information they can put into practice outside of the classroom, and he works tirelessly to ensure every student understands the concepts he's teaching. **@ForensicRJ**

FOR578

Cyber Threat Intelligence

GIAC Certification Available Late 2017

Five-Day Program
Mon, Aug 28 - Fri, Sep 1
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor:
Peter Szczepankiewicz

Who Should Attend

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

"Great course which provided a good overview and understanding of different levels of intel, defeating APTs, and the use of IOCs."

-Scott R., U.S. Marine Corps

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

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

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

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

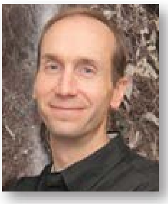
Cyber threat intelligence thus represents a force multiplier for organizations looking to update their response and detection programs to deal with increasingly sophisticated advanced persistent threats. Malware is an adversary's tool but the real threat is the human one, and cyber threat intelligence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

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

THERE IS NO TEACHER BUT THE ENEMY!

"This course gives a very smart and structured approach to CTI, something that the global community has been lacking to date."

-John Geary, Citigroup



Peter Szczepankiewicz *SANS Certified Instructor*

Peter responded to network attacks and worked with both defensive and offensive red teams during his work with the U.S. military. Currently, he is a senior security engineer with IBM. People lead technology, not the other way around, so Peter works daily to bring actionable intelligence out of disparate security devices for customers, making systems interoperable. "Putting together networks only to tear them apart is just plain fun," explains Peter, "and it allows students to take the information learned from books and this hands-on experience back to their particular work place." @_s14

FOR610

GREM Certification
Reverse Engineering Malware

www.giac.org/grem

Reverse-Engineering Malware: Malware Analysis Tools and Techniques *NEW!*

Six-Day Program
Sun, Aug 27 - Fri, Sep 1
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructors: Lenny Zeltser,
Evan Dygert

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

Learn to turn malware inside out! This popular course explores malware analysis tools and techniques in depth. FOR610 training has helped forensic investigators, incident responders, security engineers, and IT administrators acquire the practical skills to examine malicious programs that target and infect Windows systems. Understanding the capabilities of malware is critical to an organization's ability to derive threat intelligence, respond to information security incidents, and fortify defenses. This course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and many other freely available tools.

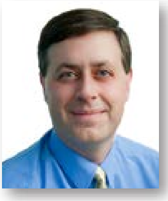
The course begins by establishing the foundation for analyzing malware in a way that dramatically expands upon the findings of automated analysis tools. You will learn how to set up a flexible laboratory to examine the inner workings of malicious software, and how to use the lab to uncover characteristics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

Malware is often obfuscated to hinder analysis efforts, so the course will equip you with the skills to unpack executable files. You will learn how to dump such programs from memory with the help of a debugger and additional specialized tools, and how to rebuild the files' structure to bypass the packer's protection. You will also learn how to examine malware that exhibits rootkit functionality to conceal its presence on the system, employing code analysis and memory forensics approaches to examining these characteristics. FOR610 malware analysis training also teaches how to handle malicious software that attempts to safeguard itself from analysis. You will learn how to recognize and bypass common self-defensive measures, including code injection, sandbox evasion, flow misdirection, and other measures.

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

Lenny Zeltser *SANS Senior Instructor*

Aptly called the "Yoda" of malware analysis by his students, Lenny Zeltser keeps his eye on the big picture and focuses on the sum of events rather than individual occurrences. He lives by that philosophy and brings it to his job and classroom. A seasoned business and technology leader with extensive information security expertise, Lenny started his professional journey in a variety of technical InfoSec roles before serving as the national lead of the U.S. security consulting practice at a major cloud services provider. Later in his career he oversaw a portfolio of security services at a Fortune 500 technology company. Today, as VP of Products at Minerva Labs, Lenny designs and builds designs creative anti-malware products. Lenny also developed the Linux toolkit REMnux to make it easier to use a variety of freely available malware analysis tools, many of which run well on Linux but can be difficult to find and install. Lenny earned the prestigious GIAC Security Expert professional designation, and he currently serves on the Board of Directors of SANS Technology Institute. Lenny holds a bachelor's degree in computer science from the University of Pennsylvania and a master's in business administration from MIT Sloan and is the co-author of four books on malware, network security, and digital forensics. **@LennyZeltser**



Evan Dygert *SANS Instructor*

Evan Dygert is a consultant (Dygert Consulting, Inc.) with over 30 years of experience in software development in areas including compilers, databases, finance, insurance, computer networking and security, and software security. He is experienced in many computer languages including Java, Pascal, C/C++, assembly language, and Python. Since 2005, Evan has also performed digital forensics, computer security and expert witness work. Evan has written expert reports, affidavits, and declarations and testified in multiple depositions, a federal hearing, and a trial. He has presented at BSides Orlando and SANS@Night, and has earned 14 GIAC certifications, including the prestigious GSE. In addition he holds the CISSP, CCE, and CEHv8 certifications. Evan enjoys teaching others about security and has mentored high school CyberPatriot teams for the last four years and his teams have competed in the CyberPatriot National Finals for the last three years in a row. Evan earned a B.S. in computer science from Brigham Young University, an MBA from Rollins College, and has completed the coursework for a Ph.D. in computer information systems.

MGT512

GSLC Certification
Security Leadership

www.giac.org/gslc

SANS Security Leadership Essentials for Managers with Knowledge Compression™

Five-Day Program
Mon, Aug 21 - Fri, Aug 25
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop Recommended
Instructor: G. Mark Hardy

Who Should Attend

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

This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to manage security. Lecture sections are intense; the most common student comment is that it's like drinking from a fire hose. The diligent manager will gain the vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to U.S. government managers and supporting contractors.

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

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

Knowledge Compression™

Maximize your learning potential!

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

SANS Technology Institute
www.sans.edu

www.sans.org/8140

▶❚❚ Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

G. Mark Hardy *SANS Principal Instructor*

G. Mark Hardy is founder and President of National Security Corporation. He has been providing cyber security expertise to government, military, and commercial clients for over 35 years, and is an internationally recognized expert and keynote who has spoken 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. Mr. Hardy is a retired U.S. Navy captain and was entrusted with nine command assignments, including responsibility for leadership training for 70,000 Sailors. A graduate of Northwestern University, he holds a BS in computer science, a BA in mathematics, a masters in business administration, a masters in strategic studies, and holds the GSLC, CISSP, CISM and CISA certifications. @g_mark

MGT517

Managing Security Operations: Detection, Response, and Intelligence *NEW!*

Five-Day Program
Mon, Aug 28 - Fri, Sep 1
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Christopher Crowley

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

Managing Security Operations 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 with the ability to adjust and work within the context and constraints of an organization. To run a successful SOC, managers need to provide tactical and strategic direction and inform staff of the changing threat environment, as well as provide guidance and training for employees. 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 Author Statement

"The inclusion of all functional areas of security operations is intended to develop a standardized program for an organization and express all necessary capabilities. Admittedly ambitious, the intention of the class is to provide a unified picture of coordination among teams with different skillsets to help the business prevent loss due to poor security practices. I have encountered detrimental compartmentalization in most organizations. There is a tendency for specialists to look only at their piece of the problem, without understanding the larger scope of information security within an organization. Organizations are likely to perceive a Security Operations Center as a tool, and not as the unification of people, processes, and technologies.

"This course provides a comprehensive picture of a Cyber Security Operations Center (CSOC). Discussion on the technology needed to run a SOC is handled in a vendor agnostic way. In addition, technology is addressed in a way that attempts to address both minimal budgets as well as budgets with global scope. The course outlines staff roles, addresses staff training through internal training and information-sharing, and examines the interaction between functional areas and data exchange.

"After attending this class, the participant will have a roadmap for what needs to be done in an organization seeking to implement security operations."

-Christopher Crowley

> "Chris is a fantastic instructor, has great pacing with engaging anecdotes, and he's very insightful."
>
> -Rich Savacool, Nixon Peabody

Christopher Crowley *SANS Principal Instructor*

Christopher has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, 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**

Bonus Sessions

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

KEYNOTE (WEEK 1): Quality Not Quantity: Continuous Monitoring's Deadliest Events

Eric Conrad

Most Security Operations Centers are built for compliance, not security. One well-known retail firm suffered the theft of over a million credit cards. Some 60,000 true positive events were reported to their SOC during that breach, but they were missed, lost in the noise of millions. If you are bragging about how many events your SOC "handles" each day, you are doing it wrong. During this talk we will show you how to focus on quality instead of quantity, and provide an actionable list of the deadliest events that occur during virtually every successful breach. We will also provide an overview of DeepBlueCLI, a PowerShell framework for automatically detecting the deadliest events.

(WEEK 1): Actionable Detects: Blue Team Cyber Defense Tactics

Seth Misenar

This ever-evolving presentation provides you with the knowledge, tactics, techniques, and procedures to once again take pride in your Blue Team cyber capabilities. Not applying these lessons learned could prove costly in the face of adapting threat actors. Dig in and learn to hold your head high when talking about your defensive cyber operations capabilities.

(WEEK 1): Stuck in the Box, a SIEM's Tale

Justin Henderson

This talk is for you if you are looking for techniques and methods to get value out of your current SIEM, or if you are interested in seeing how a new open-source big data solution such as the Elasticsearch Stack (formerly ELK) can most likely beat what you have today.

(WEEK 1): Anti-Ransomware: How to Turn the Tables

G. Mark Hardy

This presentation will demonstrate tools and methodologies that are battle-proven and ACTUALLY WORK, as evidenced by fully contained Ransomware "explosions" that went nowhere. We'll offer insights into the future of this attack vector, and we'll venture predictions on how this "industry" will evolve and what to expect next.

(WEEK 1): Kill Chain

Paul Henry

In this presentation, we examine the kill chain from both a defensive and first responder perspective, which will enable you to better direct your efforts.

KEYNOTE (WEEK 2): Lessons in Incident Response

Chad Tilbury

As more organizations face off against advanced adversaries, classic incident response processes are being adapted and updated to address new threats and speed the recovery process. This talk will cover recent trends and use real-world case studies to illustrate exciting new approaches to incident response. Learn how incident response teams are detecting, responding to, and attributing attacks from targeted attackers and get a taste for the future of incident response.

(WEEK 2): Mobile Application Assessment

Chris Crowley

This presentation will discuss a methodology taught in SEC575 known as the application report card. The methodology enables organizations to look at aspects of Android and iOS mobile applications in order to protect their interests. There are some tools available to perform assessment of mobile applications, but we also need analysts who are competent at wielding those tools. This talk will bring awareness to those who haven't had a peek behind the details of mobile applications. Additionally, it will provide technical specifics to people who want to assess mobile applications.

Core NetWars EXPERIENCE

Test your cybersecurity knowledge and skills LIVE at

SANS Virginia Beach 2017 with 4 free nights of NetWars!

AUGUST 24-25 & 30-31 6:30-9:30 PM

Come and join us for this exciting event to test your skills in a challenging and fun learning environment. Registration for NetWars is **FREE OF CHARGE TO ALL STUDENTS AT SANS VIRGINIA BEACH 2017**. External participants are welcome to join for an entry fee of $1,520.

SANS NetWars is a dynamic cyber range that allows participants to build, practice, and measure their skills in a real-world environment using defensive, analytic, and offensive tactics. We designed NetWars to appeal to a wide range of participant skill sets by using a system with different levels.

All players start at Level 1, which measures foundational cybersecurity skills. More skilled players can rise rapidly through the ranks to a level suitable for their skill set – top players can make it to Level 4, and only the best of the best can reach level 5.

sans.org/virginia-beach

Future Training Events

Rocky Mountain	Denver, CO	June 12-17
Charlotte	Charlotte, NC	June 12-17
Minneapolis	Minneapolis, MN	June 19-24
Columbia	Columbia, MD	June 26 - July 1
Los Angeles – Long Beach	Long Beach, CA	July 10-15

SANSFIRE	Washington, DC	July 22-29

San Antonio	San Antonio, TX	Aug 6-11
Boston	Boston, MA	Aug 7-12
New York City	New York, NY	Aug 14-19
Salt Lake City	Salt Lake City, UT	Aug 14-19
Chicago	Chicago, IL	Aug 21-26
Virginia Beach	Virginia Beach, VA	Aug 21 - Sep 1
Tampa – Clearwater	Clearwater, FL	Sep 5-10
San Francisco Fall	San Francisco, CA	Sep 5-10

Network Security	Las Vegas, NV	Sep 10-17

Baltimore	Baltimore, MD	Sep 25-30
Rocky Mountain Fall	Denver, CO	Sep 25-30
Phoenix-Mesa	Mesa, AZ	Oct 9-14
Tysons Corner Fall	McLean, VA	Oct 16-21
San Diego Fall	San Diego, CA	Oct 30 - Nov 4
Seattle	Seattle, WA	Oct 30 - Nov 4
Miami	Miami, FL	Nov 6-11
San Francisco Winter	San Francisco, CA	Nov 27 - Dec 2
Austin Winter	Austin, TX	Dec 4-9

Future Summit Events

Digital Forensics	Austin, TX	June 22-29
ICS & Energy	Houston, TX	July 10-15
Security Awareness	Nashville, TN	July 31 - Aug 9
Data Breach	Chicago, IL	Sep 25 - Oct 2
Secure DevOps	Denver, CO	Oct 10-17
SIEM & Tactical Analytics	Scottsdale, AZ	Nov 28 - Dec 5

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.

Hotel Information

Hilton Virginia Beach Oceanfront

3001 Atlantic Avenue
Virginia Beach, VA 23451
Phone: 757-213-3000
www.sans.org/event/virginia-beach-2017/location

Refresh, work and relax at the Hilton Virginia Beach Oceanfront hotel, conveniently located just minutes from Norfolk International Airport and right on Virginia Beach. Wander along the boardwalk or experience great live music for free at Neptune's Park next to the hotel. Enjoy superior views of the Atlantic Ocean and surrounding areas from Sky Bar, located on the 21st floor of the hotel next to Virginia's first rooftop infinity pool. Indulge with gourmet cuisine at Salacia, Virginia's first AAA-4 diamond steakhouse, or be tempted by the freshest oysters at Catch 31.

Special Hotel Rates Available

A special discounted rate of $199.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. All rates include high-speed Internet in your room and are only available through **July 21, 2017**. To make reservations please call 800-445-8667 and ask for the SANS group rate.

Top 5 reasons to stay at the Hilton Virginia Beach Oceanfront

1. All SANS attendees receive complimentary high-speed Internet when booking in the SANS block.
2. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
3. By staying at the Hilton Virginia Beach Oceanfront, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
4. SANS schedules morning and evening events at the Hilton Virginia Beach Oceanfront that you won't want to miss!
5. Everything is in one convenient location!

Registration Information

REGISTER ONLINE AT
www.sans.org/virginia-beach

WE RECOMMEND YOU REGISTER EARLY TO ENSURE YOU GET YOUR FIRST CHOICE OF COURSES.

Select your course and indicate whether you plan to test for GIAC certification. If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

SANS Simulcast

To register for a SANS Virginia Beach 2017 Simulcast course, please visit www.sans.org/event/virginia-beach-2017/attend-remotely

Pay Early and Save*

Use code **EarlyBird17** when registering early

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code by	**6-28-17**	**$400.00**	**7-19-17**	**$200.00**

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

SANS Voucher Program

Expand your training budget!

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

www.sans.org/vouchers

Cancellation & Access Policy

If an attendee must cancel, a substitute may attend instead. Substitution requests can be made at any time prior to the event start date. Processing fees will apply. All substitution requests must be submitted by email to **registration@sans.org**. If an attendee must cancel and no substitute is available, a refund can be issued for any received payments by **July 26, 2017**. A credit memo can be requested up to the event start date. All cancellation requests must be submitted in writing by mail or fax and received by the stated deadlines. Payments will be refunded by the method that they were submitted. Processing fees will apply.