THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS

Virginia Beach 2015

Virginia Beach, VA Aug 24 – Sept 4

> *"SANS course work is the most thorough learning available anywhere. What you learn is not only conceptual, but also hands-on showing you what you do, why you do it, and how you can apply what you learn to real-world solutions."*
>
> -Duane Tucker, Baymark Partners

Choose from these popular courses:

- Security Essentials Bootcamp Style
- Hacker Tools, Techniques, Exploits & Incident Handling
- Network Penetration Testing and Ethical Hacking
- Windows Forensic Analysis
- Intrusion Detection In-Depth
- SANS Security Leadership Essentials For Managers with Knowledge Compression™
- Reverse-Engineering Malware: Malware Analysis Tools and Techniques
- Advanced Digital Forensics and Incident Response
- Advanced Security Essentials – Enterprise Defender
- Mobile Device Security and Ethical Hacking
- Continuous Monitoring and Security Operations
- Mac Forensic Analysis
- Advanced Network Forensics and Analysis

Save $400

Register & pay early!
See page 17 for
more details.

Register at
sans.org/event/virginia-beach-2015

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

GIAC Approved Training

SANS Virginia Beach 2015 from August 24–September 4 offers a rare opportunity to take two full weeks of the intense cybersecurity training you need to protect your critical information. The news reports on cyber-attacks almost every day, so there's no time to waste: SANS immersion training is the best way to prevent and thwart the full range of today's cyber threats.

The expanded format for SANS Virginia Beach 2015 will enable you to take two of our 13 courses in IT security, security management, and computer forensics – and then relax on the beach at this popular resort area! You will return home with hands-on security skills (and maybe even a nice tan!) Take a look at the catalog for more detailed course descriptions, instructor bios, and course schedules.

SANS courses are taught by experienced industry practitioners considered to be among the best cybersecurity instructors in the world. At SANS Virginia Beach 2015 you can take courses with some of our top instructors, including Dr. Eric Cole, Rob Lee, Mike Poor, Chad Tilbury, Seth Misenar, Christopher Crowley, Adrien de Beaupre, Sarah Edwards, Philip Hagen, G. Mark Hardy, Heather Mahalik, Michael Murr, Jeff McJunkin, and Anuj Soni.

Virginia Beach 2015 will also offer bonus evening talks with keynote presentations. These unique, late-breaking presentations by our expert instructors will add to your learning experience at no additional cost. Another feature at Virginia Beach 2015 will by the ever-popular **NetWars Tournament** on August 27-28 and September 2-3. **CORE NetWars** is a hands-on computer and network security challenge that presents real-world security concerns but is accessible to a broad level of player skills.

SANS GIAC offers some 20 specialized information security certifications, so why not complement your training and register for a certification exam? See **giac.org** for details. Some GIAC certificates may be applied toward a Master's of Science in Information Security Engineering (MSISE) or Information Security Management (MSISM) at the accredited **SANS Technology Institute** also offering graduate certificates in cybersecurity. For the most up-to-date information visit **sans.edu**. Finally, you can supplement your SANS training with an **OnDemand Bundle** option that provides you with additional training and four months of online access to our OnDemand e-learning platform. Go to **sans.org/ondemand/bundles** for details.

Our campus for this event will be the **Hilton Virginia Beach Oceanfront** located along the city's renowned boardwalk and conveniently located just 20 minutes from Norfolk International Airport. With 35 miles of beaches, the Virginia Beach area is an outdoor enthusiast's paradise. You can rent a bike and cycle along the three-mile boardwalk, explore over 4,000 acres of parks and national refuges, go on a fresh or salt water adventure, take in some carnival rides, or just walk the hub. A special discounted room rate of $199 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. These rates include high-speed Internet in your room and are only available through July 24, 2015.

Save $400 by entering the discount code "**EarlyBird15**" on the registration page and paying for any 4-6 day course by July 1. This event has a history of filling up fast, so tell your colleagues and friends about Virginia Beach 2015 and start making your training and travel plans as early as possible. We'll see you on the waterfront at Virginia Beach!

SANS

Here's what SANS alumni have said about the value of SANS training:

"After years of imaging and analysis I learned more in one day then 6 months in this field."

-Don Malone, Beyond Inc.

"SANS training has given me a better understanding on security essentials that will not only help at work but at home."

-Star Brown, ADM

"The hands-on lab approach is a great way to make sense of what is being taught, and working with other classmates helped expand our knowledge and brought cohesion."

-Rachel Weiss, UPS Inc.

Courses-at-a-Glance

		MON 8/24	TUE 8/25	WED 8/26	THU 8/27	FRI 8/28	SAT 8/29	SUN 8/30	MON 8/31	TUE 9/1	WED 9/2	THU 9/3	FRI 9/4
SEC401	**Security Essentials Bootcamp Style**	Page 2											
SEC501	**Advanced Security Essentials – Enterprise Defender**							Page 3					
SEC503	**Intrusion Detection In-Depth**	Page 4											
SEC504	**Hacker Tools, Techniques, Exploits & Incident Handling**	Page 5											
SEC511	**Continuous Monitoring and Security Operations**	Page 6											
SEC560	**Network Penetration Testing and Ethical Hacking**							Page 7					
SEC575	**Mobile Device Security and Ethical Hacking**							Page 8					
FOR408	**Windows Forensic Analysis**	Page 9											
FOR508	**Advanced Digital Forensics and Incident Response**							Page 10					
FOR518	**Mac Forensic Analysis**	Page 11											
FOR572	**Advanced Network Forensics and Analysis**	Page 12											
FOR610	**REM: Malware Analysis Tools and Techniques**							Page 13					
MGT512	**SANS Security Leadership Essentials For Managers**	Page 14											

@SANSInstitute *Join the conversation:* **#SANSVaBeach**

The CORE NetWars Tournament will be held at SANS Virginia Beach 2015!

CORE NETWARS TOURNAMENT

SANS CORE NetWars Tournament is a computer and network security challenge designed to test your experience and skills in a safe, controlled environment while having a little fun with your fellow IT security professionals. Many enterprises, government agencies, and military bases are using NetWars to help identify skilled personnel and as part of extensive hands-on training. With CORE NetWars Tournament, you'll build a wide variety of skills while having a great time.

Who Should Attend:

- ▶ Security professionals
- ▶ System administrators
- ▶ Network administrators
- ▶ Ethical hackers
- ▶ Penetration testers
- ▶ Incident handlers
- ▶ Security auditors
- ▶ Vulnerability assessment personnel
- ▶ SOC staff members
- ▶ Forensic Analysts

In-Depth, Hands-On InfoSec Skills
Embrace the Challenge
CORE NetWars

Two separate NetWars competitions will be held at the event. The first one runs August 27-28 and the second runs September 2-3.

Prizes will be awarded at the conclusion of each tournament.

REGISTRATION IS FREE BUT SPACE IS LIMITED
for students attending any long course at SANS Virginia Beach 2015
(NON-STUDENT ENTRANCE FEE IS $1,249).

Register at sans.org/event/virginia-beach-2015

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Aug 24 - Sat, Aug 29
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Dr. Eric Cole

- GIAC Cert: GSEC
- STI Master's Program
- Cyber Guardian
- DoDD 8570
- OnDemand Bundle

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.

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. This 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 advanced persistent threat, 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'll 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.

giac.org

SANS Technology Institute
sans.edu

sans.org/cyber-guardian

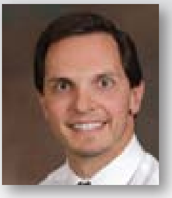
sans.org/8570

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

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

"Really good foundational stuff! I have been working with TCP/IP for many years, but felt like today really clarified my understanding of what happens behind the scenes."
-John Hanes, Apparatus



Dr. Eric Cole *SANS Faculty Fellow*

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole currently performs leading-edge security consulting and works in research and development to advance the state of the art in information systems security. Dr. Cole has experience in information technology with a focus on perimeter defense, secure network design, vulnerability discovery, penetration testing, and intrusion detection systems. He has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. Dr. Cole is the author of several books, including *Hackers Beware*, *Hiding in Plain Site*, *Network Security Bible*, 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 Cybersecurity for the 44th President and several executive advisory boards. Dr. Cole is founder of Secure Anchor Consulting, where he provides state-of-the-art security services and expert witness work. He also served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is actively involved with the SANS Technology Institute (STI) and SANS, working with students, teaching, and maintaining and developing courseware. @drericcole

SANS

SECURITY 501

Advanced Security Essentials – Enterprise Defender

Six-Day Program
Sun, Aug 30 - Fri, Sep 4
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: Dr. Eric Cole

- GIAC Cert: GCED
- STI Master's Program
- OnDemand Bundle

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.

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

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.

Of course, 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.

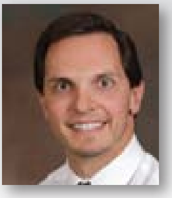
GCED
giac.org

SANS Technology Institute
sans.edu

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

"Love the content, course, and instructor. It is great to hear about the instructor's past experiences and real-world cases. This course will greatly enhance my effectiveness upon my return to the office."
-Andrew D'Albor, CB&I

"This course is fun and fast paced! I'm really enjoying the class, plus the time is going by so fast! Great information and tools."
-Danielle Perchert, Sandia National Labs



Dr. Eric Cole *SANS Faculty Fellow*

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole currently performs leading-edge security consulting and works in research and development to advance the state of the art in information systems security. Dr. Cole has experience in information technology with a focus on perimeter defense, secure network design, vulnerability discovery, penetration testing, and intrusion detection systems. He has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. Dr. Cole is the author of several books, including *Hackers Beware*, *Hiding in Plain Site*, *Network Security Bible*, 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 Cybersecurity for the 44th President and several executive advisory boards. Dr. Cole is founder of Secure Anchor Consulting, where he provides state-of-the-art security services and expert witness work. He also served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is actively involved with the SANS Technology Institute (STI) and SANS, working with students, teaching, and maintaining and developing courseware. @drericcole

SECURITY 503

Intrusion Detection In-Depth

Six-Day Program
Mon, Aug 24 - Sat, Aug 29
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: Mike Poor

- GIAC Cert: GCIA
- STI Master's Program
- Cyber Guardian
- DoDD 8570
- OnDemand Bundle

Who Should Attend

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

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

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 HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You'll get plenty of practice learning to configure and master different open-source tools like tcpdump, Wireshark, Snort, Bro, and many more. 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. In addition, most exercises include an "extra credit" stumper question intended to challenge even the most advanced student.

Industry expert Mike Poor has created a VMware distribution, Packetrix, specifically for this course. As the name implies, Packetrix contains many of the tricks of the trade to perform packet and traffic analysis. It is supplemented with demonstration "pcaps," which are files that contain network traffic. This allows students to follow along on their laptops with the class material and demonstrations. The pcaps also provide a good library of network traffic to use when reviewing the material, especially for certification.

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 often 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. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

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

"I am enjoying the course and liking the focus on community, tools sharing, and different points of views. It's great to share scenarios so we can grow in our field and as an industry."
-Zaeem Zahid, Betfair

"I loved this course. I had big expectations, because I have also taken SEC401 Security Essentials course and it was amazing too."
-Diana Moldovan, Betfair

Mike Poor *SANS Senior Instructor*

Mike is a founder and senior security analyst for the DC firm InGuardians, Inc. In the past he has worked for Sourcefire as a research engineer and for SANS leading their intrusion analysis team. As a consultant, Mike conducts incident response, breach analysis, penetration tests, vulnerability assessments, security audits, and architecture reviews. His primary job focus, however, is in intrusion detection, response, and mitigation. Mike currently holds the GCIA certification and is an expert in network engineering and systems and network and web administration. Mike is an author of the international best selling Snort series of books from Syngress, a member of the Honeynet Project, and a handler for the SANS Internet Storm Center. @Mike_Poor

SECURITY 504

Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program
Mon, Aug 24 - Sat, Aug 29
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Michael Murr

- GIAC Cert: GCIH
- STI Master's Program
- Cyber Guardian
- DoDD 8570
- OnDemand Bundle

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.

By helping you understand attackers' 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, this course helps you turn the tables on computer attackers. 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, 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 for, exploiting, and defending systems. It 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.

Who Should Attend

- Incident handlers
- Penetration testers
- Ethical hackers
- 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

"This course gave me a better understanding of what a hacker can do and how he does it — which will help me with incident handling."
-Jill Gallagher, HSBC

"This course provides a dual perspective when it comes to threats: offensive and defensive. The mentality of one lends itself to the other. The stress emphasizes this, and demonstrates the need for knowledge."
-Michael Jedrey,
Commonwealth of Virginia

giac.org

sans.edu

sans.org/
cyber-guardian

sans.org/8570

▶II
Bundle OnDemand
with this course
sans.org/ondemand

Michael Murr *SANS Certified Instructor*

Michael has been a forensic analyst with Code-X Technologies for over five years, has conducted numerous investigations and computer forensic examinations, and has performed specialized research and development. Michael has taught SANS SEC504 (Hacker Techniques, Exploits, and Incident Handling), SANS FOR508 (Computer Forensics, Investigation, and Response), and SANS FOR610 (Reverse-Engineering Malware); has led SANS@Home 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. www.forensicblog.org @mikemurr

SECURITY 511

Continuous Monitoring and Security Operations

Six-Day Program
Mon, Aug 24 - Sat, Aug 29
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Seth Misenar
- OnDemand Bundle

We continue to underestimate the tenacity of our adversaries! Organizations are investing a significant amount of 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.

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 would 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 Day five will greatly increase your understanding and enhance your skills in implementing Continuous Monitoring utilizing NIST framework.

Who Should Attend

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

"When students walk out, they have a list of action items in hand for making their organization one of the most effective vehicles for frustrating adversaries."
-Eric Conrad and Seth Misenar, SANS

"The material in SEC511 is excellent, and I appreciate the background/pen test material build up to defense. Good defense understands offense."
-Kenneth Hall, BCBSMS

Seth Misenar *SANS Senior Instructor*

Seth Misenar serves as lead consultant and founder of Jackson, Mississippi-based Context Security, which provides information security though 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 HIPAA and information security officer for a state government agency. Prior to becoming a security geek, Seth received a BS 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 which include, but are not limited to, the following: CISSP, GPEN, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE. @sethmisenar

SECURITY 560

Network Penetration Testing and Ethical Hacking

Six-Day Program
Sun, Aug 30 - Fri, Sep 4
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Adrien de Beaupre

- GIAC Cert: GPEN
- STI Master's Program
- Cyber Guardian
- OnDemand Bundle

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 duty head-on.

SEC560 is the must-have course for every well-rounded security professional.

This course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks and wireless and web apps, with over 30 detailed hands-on labs throughout.

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

Chock full of practical, real-world tips from some of the world's best penetration testers, SEC560 prepares you to perform detailed reconnaissance by examining a target's infrastructure and mining blogs, search engines, social networking sites and other Internet and intranet infrastructure. You will be equipped to scan target networks using best-of-breed tools. We will not just cover run-of-the-mill options and configurations, we will also go over the less-known but highly useful capabilities of the best pen test toolsets available today. After scanning, you will learn dozens of methods for exploiting target systems to gain access and measure real business risk, then examine post-exploitation, password attacks, wireless and web apps, pivoting through the target environment to model the attacks of real-world bad guys.

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

After building your skills in challenging labs over five days, the course culminates with a full-day, real-world network penetration test scenario. You will conduct an end-to-end penetration test, applying the knowledge, tools and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization.

Who Should Attend

- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Red team members
- Blue team members

giac.org

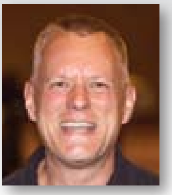
sans.edu

sans.org/cyber-guardian

Bundle OnDemand
WITH THIS COURSE
sans.org/ondemand

"This course does a great job of condensing an overwhelming amount of information down to what an IT professional needs for a solid foundation."
-JD Holcomb

"The course material in SEC560 is presented very well and is excellent. All the labs worked for me and the instructor is very engaging."
-Marilyn Moux,
Knowledge Consulting Group



Adrien de Beaupre *SANS Certified Instructor*

Adrien de Beaupre is a certified SANS instructor and works as an independent consultant in beautiful Ottawa, Ontario. His work experience includes technical instruction, vulnerability assessment, penetration testing, intrusion detection, incident response and forensic analysis. He is a member of the SANS Internet Storm Center (isc.sans.edu). He is actively involved with the information security community, and has been working with SANS since 2000. Adrien holds a variety of certifications including the GXPN, GPEN, GWAPT, GCIH, GCIA, GSEC, CISSP, OPST, and OPSA. When not geeking out he can be found with his family, or at the dojo. @adriendb

SANS

SECURITY 575

Mobile Device Security and Ethical Hacking

Six-Day Program
Sun, Aug 30 - Fri, Sep 4
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor:
Christopher Crowley

- GIAC Cert: GMOB
- STI Master's Program
- OnDemand Bundle

Mobile phones and tablets have become essential to enterprise and government networks ranging from small organizations to Fortune 500 companies and large agencies. Often, mobile phone deployments grow organically, adopted by multitudes of end-users for convenient email access, as well as by managers and executives who need access to sensitive organizational resources from their favored personal mobile devices. In other cases, mobile phones and tablets have become critical systems for a wide variety of production applications from enterprise resource planning (ERP) to project management.

For all of its convenience, however, the ubiquitous use of mobile devices in the work place and beyond has brought new security risks. As reliance on these devices has grown exponentially, organizations have quickly recognized that mobile phones and tablets need greater security implementations than a simple screen protector and clever password. Whether an Apple iPhone or iPad, a Windows Phone, or an Android or BlackBerry phone or tablet, these devices have become hugely attractive and vulnerable targets for nefarious attackers. The use of such devices poses an array of new risks to organizations, including:

- Distributed sensitive data storage and access mechanisms
- Lack of consistent patch management and firmware updates
- High probability of the device being hacked, lost or stolen

Mobile code and apps are also introducing new avenues for malware and data leakage, exposing critical enterprise secrets, intellectual property, and personally identifiable information assets to attackers. To further complicate matters, today there simply are not enough people with the security skills needed to manage mobile phone and tablet deployments.

Who Should Attend

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

GMOB
giac.org

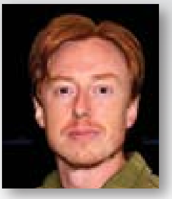
SANS Technology Institute
sans.edu

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

"This course is helping me consolidate my network knowledge in a mobile environment."
-Tony Maurer, DIBP

"I really enjoyed the last android exercise and the iPhone backup analysis, and we applied what was discussed in class."
-Katrina Howard, BAH

"The course material was well organized, the instructor explained the material thoroughly, and the ending lab was enjoyable."
-Lyle Sutton, BAH



Christopher Crowley *SANS Certified Instructor*

Mr. 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. Mr. Crowley 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. The Mentor of the Year Award is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities. @CCrowMontance

FORENSICS 408

Windows Forensic Analysis

Six-Day Program
Mon, Aug 24 - Sat, Aug 29
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructors: Rob Lee
Heather Mahalik

- GIAC Cert: GCFE
- STI Master's Program
- OnDemand Bundle

Master Windows Forensics – You can't protect what you don't know about.

Every organization must prepare for cyber-crime occurring on their computer systems and within their networks. Demand has never been higher for analysts who can investigate crimes like fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover key 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 masters capable of piecing together what happened on computer systems second by second.

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

FOR408: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can't protect what you don't know about, and understanding forensic capabilities and artifacts is a core component of information security. Learn to recover, analyze, and authenticate forensic data on Windows systems. Understand how to track detailed user activity on your network and how to organize findings for use in incident response, internal investigations, and civil/criminal litigation. Use your new skills for validating security tools, enhancing vulnerability assessments, identifying insider threats, tracking hackers, and improving security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR408 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR408 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, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook,). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out - attendees learn to analyze everything from legacy Windows XP systems to just discovered Windows 8.1 artifacts.

giac.org

sans.edu

"I have been doing forensic investigations for several years, and would highly recommend this course."
-Robert Galarza, JP Morgan Chase

digital-forensics.sans.org

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Heather Mahalik

SANS Certified Instructor

Heather Mahalik is leading the forensic effort for Ocean's Edge as a project manager. Heather's extensive experience in digital forensics began in 2003. She is currently a certified instructor for the SANS Institute and is the course lead for FOR585: Advanced Smartphone Forensics. Most of Heather's experience includes smartphone, mobile, smartphone, computer, and Mac forensics. She is co-author of "Practical Mobile Forensics" – currently a best seller from Pack't Publishing. Heather is the technical editor for "Learning Android Forensics" from Pack't Publishing. Previously, Heather led the mobile device team for Basis Technology, where she focused on mobile device exploitation in support of the U.S. Government.

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 a vulnerability discovery and an exploit development team, 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

FORENSICS 508

Advanced Digital Forensics and Incident Response

Six-Day Program
Sun, Aug 30 - Fri, Sep 4
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Chad Tilbury

- GIAC Cert: GCFA
- STI Master's Program
- Cyber Guardian
- DoDD 8570
- OnDemand Bundle

SANS

FOR508: Advanced Digital Forensics and Incident Response will help you determine:

- How the breach occured
- Compromised and affected systems
- What attackers took or changed
- Incident containment and remediation

DAY 0: A 3-letter government agency contacts you to say critical information was stolen through a targeted attack on your organization. They won't tell how they know, but they identify several breached systems within your enterprise. An Advanced Persistent Threat adversary, aka an APT, is likely involved – the most sophisticated threat you are likely to face in your efforts to defend your systems and data.

Who Should Attend

- Security Operations Center (SOC) personnel and information security practitioners
- System administrators
- Incident response team members
- Experienced digital forensic analysts
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- SANS FOR408 and SEC504 graduates looking to take their skills to the next level

Over 80% of all breach victims learn of a compromise from third-party notifications, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years.

Incident response tactics and procedures have evolved rapidly over the past several years. Data breaches and intrusions are growing more complex. Adversaries are no longer compromising one or two systems in your enterprise; they are compromising hundreds. Your team can no longer afford antiquated incident response techniques that fail to properly identify compromised systems, provide ineffective containment of the breach, and ultimately fail to rapidly remediate the incident.

This in-depth incident response course provides responders with advanced skills to hunt down, counter, and recover from a wide range of threats within enterprise networks, including APT adversaries, organized crime syndicates, and hactivism. Constantly updated, the incident response course (FOR508) addresses today's incidents by providing hands-on incident response tactics and techniques that elite responders are successfully using in real-world breach cases.

THE ADVANCED PERSISTENT THREAT IS IN YOUR NETWORK – TIME TO GO HUNTING!

DFIR
digital-forensics.sans.org

"The final challenge is excellent and really brought home all the lessons learned."
-Alexandros Papadopoulos, Dell SecureWorks

"This course was incredibly challenging and realistic! The final challenge is intense and really puts you in your place!"
-Reza Salari, DRS Technologies

GCFA
giac.org

SANS Technology Institute
sans.edu

sapere aude
sans.org/cyber-guardian

sans.org/8570

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

Chad Tilbury *SANS Senior Instructor*

Chad Tilbury has been responding to computer intrusions and conducting forensic investigations since 1998. His extensive law enforcement and international experience stems from working with a broad cross-section of Fortune 500 corporations and government agencies around the world. During his service as a Special Agent with the U.S. Air Force Office of Special Investigations, he investigated and conducted computer forensics for a variety of crimes, including hacking, abduction, espionage, identity theft, and multi-million dollar fraud cases. He has led international forensic teams and was selected to provide computer forensic support to the United Nations Weapons Inspection Team. Chad has worked as a computer security engineer and forensic lead for a major defense contractor and 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. Chad is a graduate of the U.S. Air Force Academy and holds a B.S. and M.S. in Computer Science as well as GCFA, GCIH, GREM, and ENCE certifications. He is currently a consultant specializing in incident response, corporate espionage, and computer forensics. @chadtilbury

SANS

FORENSICS 518

Mac Forensic Analysis

Six-Day Program
Mon, Aug 24 - Sat, Aug 29
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Sarah Edwards
▸ OnDemand Bundle

Digital forensic investigators have traditionally dealt with Windows machines, but what if they find themselves in front of a new Apple Mac or iDevice? The increasing popularity of Apple devices can be seen everywhere, from coffee shops to corporate boardrooms, yet most investigators are familiar with Windows-only machines.

Times and trends change and forensic investigators and analysts need to change with them. The new **FOR518: Mac Forensic Analysis** course provides the tools and techniques necessary to take on any Mac case without hesitation. The intense hands-on forensic analysis skills taught in the course will enable Windows-based investigators to broaden their analysis capabilities and have the confidence and knowledge to comfortably analyze any Mac or iOS system.

Who Should Attend

- Experienced digital forensic analysts
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Incident response team members
- Information security professionals
- SANS FOR408, FOR508, FOR526, FOR610, FOR585 Alumni looking to round out their forensic skills

FOR518: Mac Forensic Analysis will teach you:

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

FOR518: Mac Forensic Analysis aims to form a well-rounded investigator by introducing Mac forensics into a Windows-based forensics world. This course focuses on topics such as the HFS+ file system, Mac specific data files, tracking user activity, system configuration, analysis and correlation of Mac logs, Mac applications, and Mac exclusive technologies. A computer forensic analyst who successfully completes the course will have the skills needed to take on a Mac forensics case.

FORENSICATE DIFFERENTLY!

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

DFIR
digital-forensics.sans.org

> "Best of any course I've ever taken. I love the idea of being able to take the content home to review."
> -Eric Koebelen, Incident Response US

> "Pound for pound, dollar for dollar, there is no other forensic training I have seen, from FTK to EnCase to anything private, that holds a candle to what was presented in this course."
> -Kevin J. Ripa, Computer Evidence Recovery, Inc.

Sarah Edwards *SANS Certified Instructor*

Sarah is a senior digital forensic analyst who has worked with various federal law enforcement agencies. She has performed a variety of investigations including computer intrusions, criminal, counter-intelligence, counter-narcotic, and counter-terrorism. Sarah's research and analytical interests include Mac forensics, mobile device forensics, digital profiling, and malware reverse engineering. Sarah has presented at the following industry conferences; Shmoocon, CEIC, BsidesNOLA, TechnoSecurity, HTCIA, and the SANS DFIR Summit. She has a Bachelor of Science in Information Technology from Rochester Institute of Technology and a Master's in Information Assurance from Capitol College. @iamevltwin

FORENSICS 572

Advanced Network Forensics and Analysis

Six-Day Program
Mon, Aug 24 - Sat, Aug 29
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Philip Hagen

- GIAC Cert: GNFA
- STI Master's Program
- OnDemand Bundle

digital-forensics.sans.org

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

Forensic casework that does not include a network component is a rarity in today's environment. Performing disk forensics will always be a critical and foundational skill, but overlooking the network component of today's computing architecture is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, a data theft case, or an employee misuse scenario, the network often has an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent or even definitively prove that 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.

Who Should Attend

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

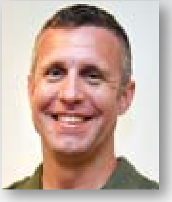
"There is so much information that it will take weeks revisiting before I start to feel comfortable. I really appreciate the labs and examples!"
-Mike McTeague, Brookwood

"This course was everything I've been looking for over the last few years. It covers all of the core attribute topics in today's corporate network environment."
-Troy Wojenroda, Huntington Ingalls Industries

GNFA
giac.org

SANS Technology Institute
sans.edu

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



Philip Hagen *SANS Certified Instructor*

Philip Hagen has been working in the information security field since 1998, running the full spectrum including deep technical tasks, management of an entire computer forensic services portfolio, and executive responsibilities. Currently, Phil is an Evangelist at Red Canary, where he engages with current and future customers of Red Canary's managed threat detection service to ensure their use of the service is best aligned for success in the face of existing and future threats. Phil started his security career while attending the U.S. Air Force Academy, with research covering both the academic and practical sides of security. He served in the Air Force as a communications officer at Beale AFB and the Pentagon. In 2003, Phil became a government contractor, providing technical services for various IT and information security projects. These included systems that demanded 24x7x365 functionality. He later managed a team of 85 computer forensic professionals in the national security sector. He has provided forensic consulting services for law enforcement, government, and commercial clients prior to joining the Red Canary team. Phil is the course lead and co-author of FOR572: Advanced Network Forensics and Analysis. @PhilHagen

FORENSICS 610

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Six-Day Program
Sun, Aug 30 - Fri, Sep 4
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Anuj Soni
- GIAC Cert: GREM
- STI Master's Program
- OnDemand Bundle

This popular malware analysis course helps forensic investigators, incident responders, security engineers and IT administrators acquire practical skills for examining malicious programs that target and infect Windows systems. Understanding the capabilities of malware is critical to an organization's ability to derive the threat intelligence it needs to respond to information security incidents and fortify defenses. The course builds a strong foundation for analyzing malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger and other tools useful for turning malware inside-out.

The course begins by covering fundamental aspects of malware analysis. You will learn how to set up an inexpensive and flexible laboratory to understand the inner workings of malicious software and uncover characteristics of real-world malware samples. Then you will learn to examine the specimens' behavioral patterns and code. The course continues by discussing essential x86 assembly language concepts. You will examine malicious code to understand its key components and execution flow. Additionally, you will learn to identify common malware characteristics by looking at suspicious Windows API patterns employed by bots, rootkits, keyloggers, downloaders, and other types of malware.

You will also learn how to handle self-defending malware, learning to bypass the protection offered by packers, and other anti-analysis methods. In addition, given the frequent use of browser malware for targeting systems, you will learn practical approaches to analyzing malicious browser scripts and deobfuscating JavaScript and VBScript to understand the nature of the attack.

The course culminates with a series of capture-the-flag challenges designed to reinforce the techniques learned in class and provide additional opportunities to learn practical malware analysis skills in a fun setting.

Hands-on workshop exercises are a critical aspect of this course and allow you to apply malware analysis techniques by examining malware in a lab that you control. 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

digital-forensics.sans.org

"The course is highly advanced, and the instructor showed us how to perform behavior and code analysis to better understand how malware works."
-David Bernal, Alstom

"Great course especially for people interested in specializing in IR and forensics. I would say this is the core of IR considering today's threat landscape."
-Mudasir Wani, KAUST

GREM
giac.org

SANS Technology Institute
sans.edu

BUNDLE ONDEMAND WITH THIS COURSE
sans.org/ondemand

Anuj Soni *SANS Instructor*

Anuj Soni is a Senior Incident Responder at Booz Allen Hamilton, where he leads forensic, malware, and network analysis efforts to investigate security incidents. 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 hunt skills and technical analysis abilities have resulted in the successful identification, containment, and remediation of multiple threat actor groups. Anuj has analyzed over 400 malware samples to assess function, purpose, and impact, and his recommendations have improved the security posture of the organizations he supports. Sought after as a technical thought leader and adviser, Anuj excels not only in delivering rigorous forensic analysis, but also in process development, knowledge management, and team leadership to accelerate incident response efforts. Anuj shares his knowledge and experience often by teaching for SANS and presenting at events including the U.S. Cyber Crime Conference, SANS DFIR Summit, and the Computer and Enterprise Investigations Conference (CEIC). He received his Bachelors and Masters degrees from Carnegie Mellon University. He also holds the following certifications: GIAC Reverse Engineering Malware (GREM), EnCase Certified Examiner (EnCE), and Certified Information Systems Security Professional (CISSP). @asoni

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/event/virginia-beach-2015/courses

MANAGEMENT 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program
Mon, Aug 24 - Fri, Aug 28
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop NOT Needed
Instructors: G. Mark Hardy

- GIAC Cert: GSLC
- STI Master's Program
- DoDD 8570
- OnDemand Bundle

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

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

Knowledge Compression™

Maximize your learning potential!

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

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

> "Every IT security professional should attend – no matter what their position. This information is important to everyone."
> -John Flood, NASA

> "I've already learned much in this course, and it will greatly assist me in increasing my knowledge base and my interaction with my IT/CS departments."
> -Jon Shadduck, Ameren Missouri

GSLC
giac.org

SANS Technology Institute
sans.edu

sans.org/8570

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

G. Mark Hardy *SANS Certified 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 30 years, and is an internationally recognized expert who has spoken at over 250 events worldwide. G. Mark serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. A retired U.S. Navy Captain, he was privileged to serve in command nine times, including responsibility for leadership training for 70,000 Sailors. He also served as wartime Director, Joint Operations Center for US Pacific Command, and Assistant Director of Technology and Information Management for Naval Logistics in the Pentagon, with responsibility for INFOSEC, Public Key Infrastructure, and Internet security. Captain Hardy was awarded the Defense Superior Service Medal, the Legion of Merit, five Meritorious Service Medals, and 24 other medals and decorations. 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

KEYNOTE: WHY *Dr. Eric Cole*

Cyber security breaches have become a norm and people are no longer surprised when they hear about them on the news, but WHY? Organizations continue to spend a significant amount of money and buy lots of product, however it seems to make little, if any, difference, but WHY? Despite the fact that people are talking more about security and are more aware of the threats, there is little impact on security, but WHY? Startups are creating new technologies, venture capitalist firms continue to dump significant money into this area, and attacks continue, but WHY? In this solution-based talk, Dr. Cole, a world-renowned security expert, will get to the heart of the problem and address WHY the current approach to security is not working. Once the problem is dissected, systematic, provable methods for properly addressing security will be provided. This talk will provide an actionable roadmap to help prepare the next generation of Cyber Defenders to tackle the problems that need to be addressed.

Based on experience gained from responding to many high-profile incidents and engaging with many customers, Dr. Cole will cover solutions that Cyber Defenders can use to increase their security and gain better visibility into what is happening within their organization. If your organization has not detected an attack in the last six months you need to attend this talk. In most cases if you have not detected an attack it is not because it is not happening, but because you are not looking in the right area. This talk will change your vantage point to better understand how to prevent, detect, and respond to advanced attacks. Are you ready to become a Cyber Defender? Are you ready to take a proactive stance against the adversary? Are you ready to take the Dr. Cole Challenge?

The Tap House *Philip Hagen*

Packets move pretty fast. The field of Network Forensics needs to move fast, too. Whether you are investigating a known incident, hunting unidentified adversaries in your environment, or enriching forensic findings from disk- and memory-based examinations, it's critical to stay abreast of the latest developments in the discipline. In this @Night series, Phil Hagen will discuss some of the latest technologies, techniques, and tools that you will want to know in pursuit of forensication nirvana.

Card Fraud 101 *G. Mark Hardy*

Ever get a call from your bank saying your credit card was stolen, but it was still in your wallet? What's going on here? Card fraud costs $16 billion annually, and it's not getting better. Target, PF Changs, Michaels, Home Depot, who's next? Find out how these big card heists are pulled off, why chip-and-pin won't solve the fraud problem, and why Apple Pay is trivial to compromise. See if your bank even bothers to use the security protections it could -- we'll have a mag stripe card reader so you can really see what's in your wallet.

Complete Application Pw0nage Via Multi-Post Cross Site Request Forgery (XSRF) *Adrien de Beaupre*

This talk will discuss the risk posed by Cross Site Request Forgery (CSRF or XSRF) which is also known as session riding, or transaction injection. Many applications are vulnerable to XSRF, mitigation is difficult as it often requires re-engineering the entire application, and the threat they pose is often misunderstood. A live demo of identifying the vulnerability, and exploiting it by performing multiple unauthorized transactions in a single POST will be demonstrated.

SANS 8 Mobile Device Security Steps *Chris Crowley*

Every organization is challenged to rapidly deploy mobile device security. The SANS 8 Mobile Device Security Steps is a community-driven project to provide the most up-to-date information on the most effective strategies for securing mobile infrastructure. Chris Crowley will discuss the guidance provided in the 8 Steps, including: user authentication and restricting unauthorized access, OS and application management, device monitoring, and key operational components for mobile device management.

Preparing for PowerShellmageddon – Investigating Windows Command Line Activity *Chad Tilbury*

There is a reason hackers use the command line, and it isn't to impress you with their prowess. Throughout the history of Windows, the command line has left far fewer forensic artifacts than equivalent operations via the GUI. To make matters worse, the transition to Windows 7 and 8 has spread PowerShell throughout the enterprise. While it makes our lives easier as defenders, it does the same for our adversaries. Every time you marvel at the capabilities of PowerShell, you should fear how your adversaries may use that power against you. This talk will demonstrate how incident responders are countering the command line threat with real-world examples. Learn to identify when it is in play, extract command history, and see what is new on the horizon from Microsoft to make tracking command line and PowerShell activity easier.

Need for Speed: Malware Edition *Anuj Soni*

Performing malware analysis can be a thrilling activity, but it can also be time-consuming and tedious. During this talk, I'll use real malware samples to propose strategies to accelerate the malicious code analysis process. Whether you're new to this topic area or familiar with its challenges, this discussion will give you an appreciation for reverse engineering and equip you with tips and tricks to speed up your investigation.

FUTURE SANS TRAINING EVENTS

SANSFIRE 2015
Baltimore, MD | June 13-20 | #SANSFIRE

SANS **Rocky Mountain** 2015
Denver, CO | June 22-27 | #SANSRockyMtn

SANS **Capital City** 2015
Washington, DC | July 6-11 | #SANSDC

SANS **Digital Forensics & Incident Response** SUMMIT & TRAINING
Austin, TX | July 7-14 | #DFIRSummit

SANS **San Jose** 2015
San Jose, CA | July 20-25 | #SANSSJ

SANS **Minneapolis** 2015
Minneapolis, MN | July 20-25 | #SANSmpls

SANS **Boston** 2015
Boston, MA | August 3-8 | #SANSBoston

SANS **Cyber Defense** SUMMIT & TRAINING
Nashville, TN | August 11-18 | #CyberDefenseSummit

SANS **San Antonio** 2015
San Antonio, TX | August 17-22 | #SANSSATX

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events sans.org/security-training/by-location/all
Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with Your Peers

Community SANS sans.org/community
Live Training in Your Local Region with Smaller Class Sizes

Private Training sans.org/private-training
Live Onsite Training at Your Office Location. Both in Person and Online Options Available

Mentor sans.org/mentor
Live Multi-Week Training with a Mentor

Summit sans.org/summit
Live IT Security Summits and Training

ONLINE TRAINING

OnDemand sans.org/ondemand
E-learning Available Anytime, Anywhere, at Your Own Pace

vLive sans.org/vlive
Online, Evening Courses with SANS' Top Instructors

Simulcast sans.org/simulcast
Attend a SANS Training Event without Leaving Home

OnDemand Bundles sans.org/ondemand/bundles
Extend Your Training with an OnDemand Bundle Including Four Months of E-learning

SANS VIRGINIA BEACH 2015

Hotel Information

Training Campus

Hilton Virginia Beach Oceanfront

3001 Atlantic Avenue
Virginia Beach, VA 23451
757-213-3000
sans.org/event/virginia-beach-2015/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. These rates include high-speed Internet in your room and are only available through July 24, 2015.

Top 5 reasons to stay at the Hilton Virginia Beach

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 Hilton Virginia Beach, 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 Hilton Virginia Beach that you won't want to miss!
5. Everything is in one convenient location!

SANS VIRGINIA BEACH 2015

Registration Information

We recommend you register early to ensure you get your first choice of courses.

Register online at sans.org/event/virginia-beach-2015/courses

Select your course or courses 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.

Use code **EarlyBird15** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**7/1/15**	**$400.00**	**7/29/15**	**$200.00**

Some restrictions apply.

Group Savings (Applies to tuition only)

10% discount if 10 or more people from the same organization register at the same time

5% discount if 5-9 people from the same organization register at the same time

To obtain a group discount, complete the discount code request form at sans.org/security-training/discounts prior to registering.

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by August 5, 2015 – processing fees may apply.

SANS Voucher Credit Program

Expand your training budget! Extend your Fiscal Year. The SANS Voucher Discount Program pays you credits and delivers flexibility.
sans.org/vouchers