17 Great Courses – 2 Convenient Locations

SANS CAPITAL REGION

Cyber Guardian 2015

Baltimore, MD
March 2-7

Northern Virginia 2015

Reston, VA
March 9-14

Hands-on immersion training:

CYBER GUARDIAN: Baltimore, MD | March 2-7

- SEC401: **Security Essentials Bootcamp Style**
- SEC501: **Advanced Security Essentials – Enterprise Defender**
- SEC505: **Securing Windows with the Critical Security Controls**
- SEC560: **Network Penetration Testing and Ethical Hacking**
- SEC573: **Python for Penetration Testers**
- FOR508: **Advanced Digital Forensics and Incident Response**

REGISTER AT **sans.org/event/cyber-guardian-2015**

NORTHERN VIRGINIA: Reston, VA | March 9-14

- SEC301: **Intro to Information Security**
- SEC401: **Security Essentials Bootcamp Style**
- SEC503: **Intrusion Detection In-Depth**
- SEC504: **Hacker Tools, Techniques, Exploits, and Incident Handling**
- SEC511: **Continuous Monitoring and Security Operations** ***NEW!***
- SEC542: **Web App Penetration Testing and Ethical Hacking**
- SEC561: **Intense Hands-on Pen Testing Skill Development (with SANS NetWars)**
- FOR408: **Windows Forensic Analysis**
- FOR585: **Advanced Smartphone Forensics**
- MGT414: **SANS® +S™ Training Program for the CISSP® Certification Exam**
- MGT512: **SANS Security Leadership Essentials For Managers**
- DEV541: **Secure Coding in Java/JEE: Developing Defensible Applications**

GLOBAL INFORMATION ASSURANCE CERTIFICATION GIAC www.giac.org

GIAC Approved Training

REGISTER AT **sans.org/event/northern-virginia-2015**

SANS Capital Region 2015, two training events in two cities near the DC area. These back-to-back events and their perspective cities are: **SANS Cyber Guardian 2015** in Baltimore from March 2-7, and **SANS Northern Virginia 2015** in Reston from March 9-14. There is not a week that goes by that we don't read of a security breach. Get the training you need to survive a cybersecurity incident at SANS Capital Region 2015. SANS top instructors will ensure you not only learn the material, but that you will be able to apply our information security training the day you get back to the office!

SANS Cyber Guardian 2015 in Baltimore is from March 2-7. This cybersecurity event is the training you need to get you on the path to becoming a Cyber Guardian, and these courses are presented by SANS instructors who have real-world experience including: Jason Fossen, Hal Pomeranz, Ed Skoudis, Paul A. Henry, Mark Baggett, Keith Palmgren, and Jeff McJunkin who will host the two-day NetWars Tournament on March 5-6. The campus location for this event is the **Sheraton Inner Harbor.**

SANS Northern Virginia 2015 in Reston from March 9-14, features 12 comprehensive hands-on cybersecurity training courses from some of our most popular and top industry professional instructors including: Dr. Eric Cole, Mike Poor, John Strand, Joshua Wright, Eric Conrad, Ovie Carroll, G. Mark Hardy, Heather Mahalik, Keith Palmgren, Micah Hoffman, Bryan Simon, Eric Johnson, and Steve Kosten. This event will be held at the **Sheraton Reston**.

Some of our courses in both events are associated with a GIAC Certification, to see how to register for your GIAC Certification attempt and for more information visit www.giac.org.

To further your training experience and advance your career, earn your master's degree through SANS Technology Institute. Take classes in Information Security Engineering or a graduate certificate in Penetration Testing or Incident Response. You can pick the course or courses that will contribute to your specific needs and that are important to you! For more information, visit www.sans.edu.

Please take the time to look through this brochure, you will find information for both events including course descriptions, instructor's bios, evening talks, and hotel registration information with special discounted rates. Select a course from each event to maximize your training in a location convenient to you, and **receive a discount of up to $400 for any full course paid for by January 14, 2015**. Start making your travel plans now and let your colleagues and friends know about **SANS Capital Region 2015**. We look forward to seeing you there!

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

"Very engaging. I was on the edge of my seat the entire time."
-Carol Flamer, Vanguard

"SANS teaches you the logic and how to apply it to the real world."
-Kyle Prather, Heartland Dental

"I was blown away! I learned more in 5 minutes at SANS then I did in weeks of studying MS books. This was a true wake-up call with great, simple solutions, excellent!"
-Sam Cruz, NTT Data Federal Services, Inc.

"The instructor is extremely knowledgeable and able to keep the audience engaged over long periods of time while presenting difficult material. Good examples both planned and off the cuff. Best course I have ever attended!!"
-Gloria McAuley, Health Sciences North

@SANSInstitute *Join the conversation:* #CyberGuardian #SANSNoVA

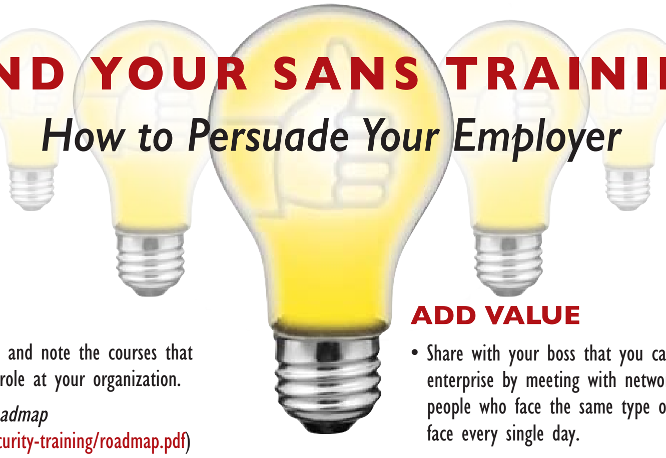
COURSES-AT-A-GLANCE

<table>
<tr><th><strong><em>SANS CYBER GUARDIAN – Baltimore, MD</em></strong></th><th>MON
3/2</th><th>TUE
3/3</th><th>WED
3/4</th><th>THU
3/5</th><th>FRI
3/6</th><th>SAT
3/7</th></tr>
<tr><td>SEC401: <strong>Security Essentials Bootcamp Style</strong></td><td colspan="6">Page 3</td></tr>
<tr><td>SEC501: <strong>Advanced Security Essentials – Enterprise Defender</strong></td><td colspan="6">Page 4</td></tr>
<tr><td>SEC505: <strong>Securing Windows with the Critical Security Controls</strong></td><td colspan="6">Page 7</td></tr>
<tr><td>SEC560: <strong>Network Penetration Testing and Ethical Hacking</strong></td><td colspan="6">Page 10</td></tr>
<tr><td>SEC573: <strong>Python for Penetration Testers</strong></td><td colspan="5">Page 12</td><td></td></tr>
<tr><td>FOR508: <strong>Advanced Digital Forensics and Incident Response</strong></td><td colspan="6">Page 14</td></tr>
</table>

<table>
<tr><th><strong><em>SANS NORTHERN VIRGINIA – Reston, VA</em></strong></th><th>MON
3/9</th><th>TUE
3/10</th><th>WED
3/11</th><th>THU
3/12</th><th>FRI
3/13</th><th>SAT
3/14</th></tr>
<tr><td>SEC301: <strong>Intro to Information Security</strong></td><td colspan="5">Page 2</td><td></td></tr>
<tr><td>SEC401: <strong>Security Essentials Bootcamp Style</strong></td><td colspan="6">Page 3</td></tr>
<tr><td>SEC503: <strong>Intrusion Detection In-Depth</strong></td><td colspan="6">Page 5</td></tr>
<tr><td>SEC504: <strong>Hacker Tools, Techniques, Exploits & Incident Handling</strong></td><td colspan="6">Page 6</td></tr>
<tr><td>SEC511: <strong>Continuous Monitoring and Security Operations <em>NEW!</em></strong></td><td colspan="6">Page 8</td></tr>
<tr><td>SEC542: <strong>Web App Penetration Testing and Ethical Hacking</strong></td><td colspan="6">Page 9</td></tr>
<tr><td>SEC561: <strong>Intense Hands-on Pen Testing Skill Development</strong></td><td colspan="6">Page 11</td></tr>
<tr><td>FOR408: <strong>Windows Forensic Analysis</strong></td><td colspan="6">Page 13</td></tr>
<tr><td>FOR585: <strong>Advanced Smartphone Forensics</strong></td><td colspan="6">Page 15</td></tr>
<tr><td>MGT414: <strong>SANS® +S™ Training Program for the CISSP® Cert Exam</strong></td><td colspan="6">Page 16</td></tr>
<tr><td>MGT512: <strong>SANS Security Leadership Essentials For Managers</strong></td><td colspan="5">Page 17</td><td></td></tr>
<tr><td>DEV541: <strong>Secure Coding in Java/JEE: Developing Defensible Apps</strong></td><td colspan="4">Page 18</td><td></td><td></td></tr>
</table>

FUND YOUR SANS TRAINING:

How to Persuade Your Employer



EXPLORE

- Read this brochure and note the courses that will enhance your role at your organization.
- Use the *Career Roadmap* (sans.org/media/security-training/roadmap.pdf) to arm yourself with all the necessary materials to make a good case for attending a SANS training event.

RELATE

- Show how recent problems or issues will be solved with the knowledge you gain from the SANS course.
- Describe how your knowledge will allow you to become an expert resource for the rest of your team.

VALIDATE

- Earn a GIAC certification, proving to your employer that you gained the expertise they paid for!
- Hone your skills at NetWars and report your competitive score (free with 5- or 6-day courses at select live training events).

SAVE

- The earlier you sign up and pay, the more you save, so explain the benefit of paying early.
- Save even more with group discounts, or bundled course packages! See inside for details.

ADD VALUE

- Share with your boss that you can add value to your enterprise by meeting with network security experts – people who face the same type of challenges that you face every single day.
- Explain how you will be able to get and share great ideas on improving your IT productivity and efficiency.
- Enhance your training experience with *SANS@Night* talks. They are free and included at every live training event.
- Attend the *Vendor Expo* at select live training events to learn about some of the best security solutions available.

ALTERNATIVES

- If time out of the office is limited, pitch *SANS OnDemand*, *Event Simulcast*, or *Live Online Training*.
- Highlight that students in our online courses earn the same GIAC scores as those who take training live!

ACT

- With the fortitude and initiative you have demonstrated thus far, you can confidently seek approval to attend SANS training!

OFFERED AT
Northern Virginia

SECURITY 301
Intro to Information Security

Five-Day Program
Mon, Mar 9 - Fri, Mar 13
9:00am - 5:00pm
Laptop Required
30 CPEs
Instructor: Keith Palmgren
‣ GIAC Cert: GISF

This introductory certification course is the fastest way to get up to speed in information security. Written and taught by battle-scarred security veterans, this entry-level course covers a broad spectrum of security topics and is liberally sprinkled with real-life examples. A balanced mix of technical and managerial issues makes this course appealing to attendees who need to understand the salient facets of information security and the basics of risk management.

Who Should Attend

- Persons new to information technology who need to understand the basics of information assurance, computer networking, cryptography, and risk evaluation
- Managers and Information Security Officers who need a basic understanding of risk management and the tradeoffs between confidentiality, integrity, and availability
- Managers, administrators, and auditors who need to draft, update, implement, or enforce policy

Organizations often tap someone who has no information security training and say, "Congratulations, you are now a security officer." If you need to get up to speed fast, Security 301 is the course for you!

We begin by covering basic terminology and concepts, and then move to the basics of computers and networking as we discuss Internet Protocol, routing, Domain Name Service, and network devices. We cover the basics of cryptography, security management, and wireless technology, then we look at policy as a tool to effect change in your organization. On the final day of the course, we put it all together with an implementation of defense in-depth.

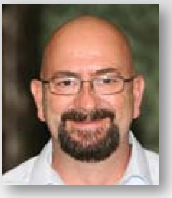
If you're a newcomer to the field of information security, this course will start you off with a solid foundation. SEC301 will help you develop the skills to bridge the gap that often exists between managers and system administrators, and learn to communicate effectively with personnel in all departments and at all levels within your organization.

NOTICE: This course has been revised to incorporate practical hands-on exercises and a short practice certification test on the last day. This course will require a laptop for all classes.

giac.org

"Really interesting course – I feel as if I'm getting a great overview of security, and I now know the areas where I need more training to best get my job done."
Rachel Shaw,
Qualcomm Incorporated

"Very engaging course. I was on the edge of my seat the entire time."
-Carol Flamer, Vanguard



Keith Palmgren *SANS Certified Instructor*

Keith Palmgren is an IT security professional with 26 years of experience in the field. He began his career with the U.S. Air Force working with cryptographic keys & codes management. He also worked in, what was at the time, the newly-formed computer security department. Following the Air Force, Keith worked as an MIS director for a small company before joining AT&T/Lucent as a senior security architect working on engagements with the DoD and the National Security Agency. As security practice manager for both Sprint and Netigy, Keith built and ran the security consulting practice – responsible for all security consulting world-wide and for leading dozens of security professionals on many consulting engagements across all business spectrums. For the last several years, Keith has run his own company, NetIP, Inc. He divides his time between consulting, training, and freelance writing projects. As a trainer, Keith has satisfied the needs of nearly 5,000 IT professionals and authored a total of 17 training courses. Keith currently holds the CISSP, GSEC, CEH, Security+, Network+, A+, and CTT+ certifications. @kpalmgren

SECURITY 401

Security Essentials Bootcamp Style

Six-Day Program
Mon, Mar 2 - Sat, Mar 7
&
Mon, Mar 9 - Sat, Mar 14
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Keith Palmgren (CG)
(Keith's bio – page 2)
Instructor: Bryan Simon (NV)

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

OFFERED AT
Cyber Guardian
&
Northern Virginia

This course 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 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:

1. What is the risk?
2. Is it the highest priority risk?
3. Is it the most cost-effective way of reducing 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.

Who Should Attend

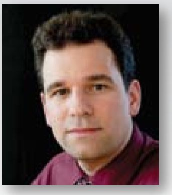
- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding 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 analysts, penetration testers, and auditors who need a solid foundation of security principles so they can be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

"Anyone tasked with the security of their company needs this training and knowledge."
-Brendan Flanning, Fandango

"This course is a must for anyone who is responsible for managing security in an enterprise."
-Bradley Hoover, ExxonMobil

"Even if you are not a security professional this course is filled with invaluable information on how to protect yourself!"
-David Billingly, Sandia National Labs

giac.org   sans.org/cyber-guardian   sans.edu   DoD 8570 REQUIRED sans.org/8570



Bryan Simon *SANS Instructor*

With more than 20 years of experience in information technology and infosec, Bryan Simon is an internationally recognized expert in cybersecurity. Over the course of his career, Bryan has held various technical and managerial positions in the education, environmental, accounting, and financial services sectors. Bryan speaks on a regular basis at international conferences and with the press on matters of cybersecurity, and has instructed individuals from organizations such as the FBI, NATO, and the UN in matters of cybersecurity, on two continents. Bryan has specialized expertise in defensive and offensive capabilities. Bryan has received recognition for his work in I.T. Security, and was most recently profiled by McAfee (part of Intel Security) as an I.T. Hero. Bryan's scholastic achievements have resulted in the honour of sitting as a current member of the Advisory Board for the SANS Institute, and his acceptance into the prestigious SANS Cyber Guardian program.

OFFERED AT
Cyber Guardian

SECURITY 501

Advanced Security Essentials – Enterprise Defender

Six-Day Program
Mon, Mar 2 - Sat, Mar 7
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: Paul A. Henry
▸ GIAC Cert: GCED
▸ Master's Program

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.

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.

giac.org sans.edu

Who Should Attend

- Students who have taken Security Essentials and want a more advanced 500-level course similar to SEC401
- Students who have foundational knowledge covered in SEC401, do not want to take a specialized 500-level course, and still want broad, advanced coverage of the core areas to protect their systems
- Anyone looking for detailed technical knowledge on how to protect against, detect, and react to the new threats that will continue to cause harm to an organization

"Good introduction and hands-on experience with a variety of tools!"
-Carrie Crot, DOJ

"A very good thoughtful and practical understanding of security, something everyone in IT should get."
-Paul Godard, OPC

"I enjoyed real-life business cases that were discussed in SEC501 to make the material relevant."
-Lorelei Duff, Lockheed Martin

Paul A. Henry *SANS Senior Instructor*

Paul Henry is a Senior Instructor with the SANS Institute and 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. Paul 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 Department of Defense's Satellite Data Project (USA), and both government as well as telecommunications projects throughout Southeast Asia. @phenrycissp

SECURITY 503

Intrusion Detection In-Depth

OFFERED AT
Northern Virginia

Six-Day Program
Mon, Mar 9 - Sat, Mar 14
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: Mike Poor
- GIAC Cert: GCIA
- Master's Program
- Cyber Guardian
- DoDD 8570

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?

Who Should Attend

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

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.

"This course provides real-world content and perspectives, data, and tools. The instructor is very knowledgeable and is a great educator."
-George Diolamou, Jacob's Engineering

"Awesome course! Thanks for the in-depth analysis combined with real-life scenarios."
-Art Mason, Rackspace ISOC

"The amount of knowledge and experience that Mike has, I don't think you could get that from any other organization other than SANS."
-Hayley Roberts, MOD

giac.org

sans.org/cyber-guardian

sans.edu

DoD 8570
REQUIRED

sans.org/8570

Mike Poor *SANS Senior Instructor*

Mike Poor is a founder and senior security analyst for the Washington, DC firm InGuardians, Inc. In the past he has worked for Sourcefire as a research engineer and for SANS leading its 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 on 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

OFFERED AT
Northern Virginia

SECURITY 504
Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program
Mon, Mar 9 - Sat, Mar 14
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: John Strand

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

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

"SEC504 is awesome! Everything included in this course is very useful in my job as a security professional!"
-Vereleo Bateo, KCG Holdings, Inc.

"John made me feel more confident and less stressed at the beginning of the course by making it clear that he's here to help."
-Bruno Leblanc, Ubisoft

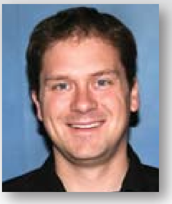
"This course is very beneficial and will sharpen your skills and then some."
-Robert Delizio, Federal Reserve Bank of New York

giac.org

sans.org/cyber-guardian

sans.edu

DoD 8570 REQUIRED
sans.org/8570



John Strand *SANS Senior Instructor*

Along with SEC504, John Strand also teaches SEC560: Network Penetration Testing and Ethical Hacking; SEC580: Metasploit Kung Fu for Enterprise Pen Testing; and SEC464: Hacker Detection for System Administrators. John is the course author for SEC464 and the co-author for SEC580. When not teaching for SANS, John co-hosts PaulDotCom Security Weekly, the world's largest computer security podcast. He also is the owner of Black Hills Information Security, specializing in penetration testing and security architecture services. He has presented for the FBI, NASA, the NSA, and at DefCon. In his spare time he writes loud rock music and makes various futile attempts at fly-fishing. @strandjs

OFFERED AT
Cyber Guardian

SECURITY 505

Securing Windows with the Critical Security Controls

Six-Day Program
Mon, Mar 2 - Sat, Mar 7
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jason Fossen

- GIAC Cert: GCWN
- Master's Program
- Cyber Guardian

This course is the defense-only mirror image of the penetration testing courses at SANS: we talk about how to block or mitigate those attacks. SEC505 also covers the Critical Security Controls which directly apply to Windows clients and servers. It includes topics like deploying a Microsoft PKI, IPSec policies, PowerShell scripting, Dynamic Access Control, BitLocker, AppLocker and more. The course aims to thwart the lateral movement of hackers inside our networks and to reduce the client-side exploits used for Advanced Persistent Threat (APT) malware.

How can we defend against pass-the-hash attacks, administrator account compromise, and the lateral movement of hackers inside our networks? How do we actually implement the Critical Security Controls on Windows in a large environment? How can we significantly reduce the client-side exploits which lead to APT malware infections? These are tough problems, but we tackle them in this course.

Understanding how penetration testers and hackers break into networks is not the same thing as knowing how to design defenses against them, especially when you work in a large, complex Active Directory environment. Knowing about tools like Metasploit, Cain, Netcat, and Poison Ivy is very useful, but there is no simple patch against their abuse. The goal of this course is to provide a defense or mitigation for the Windows attack techniques known today and the new ones that will be discovered tomorrow. This requires more than just reactive patch management; we need to proactively design security into our systems and networks. That is what this course is about.

Your adversaries want to elevate their privileges to win control over your servers and domain controllers, so a major theme of this course is controlling administrative powers through Group Policy hardening and PowerShell scripting.

Learning PowerShell is probably the single best new skill for Windows people to acquire, especially with the trend towards cloud computing. Because most of your competition lacks scripting skills, it is a great way to make your resume stand out. This course devotes an entire day to PowerShell, but you do not need any prior scripting experience, we will start with the basics.

Who Should Attend

- Windows security engineers and system administrators
- Anyone who wants to learn PowerShell
- Anyone who wants to implement the 20 Critical Security Controls
- Anyone implementing the Australian Directorate's Four Controls
- Those who must enforce security policies on Windows hosts
- Anyone who needs a whole drive encryption solution
- Those deploying or managing a PKI or smart cards
- Anyone who needs to prevent malware infections

"SEC505 course content is excellent. In-class activities were very valuable. Very good teaching skills and knowledge."
-Jesus Perez,
Texas A&M University

"I have been to other windows training, but never one with a focus on security — this has been an eye-opening experience. I hope to attend more events like this in the future."
-Dewayne Wasson,
Kellogg Company

giac.org sans.org/cyber-guardian sans.edu

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. Jason blogs about Windows Security Issues on the SANS Windows Security Blog. http://blogs.sans.org/windows-security

SECURITY 511

Continuous Monitoring and Security Operations

NEW

OFFERED AT
Northern Virginia

Six-Day Program
Mon, Mar 9 - Sat, Mar 14
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Eric Conrad

SEC511: Continuous monitoring in the Security Operations Center (SOC). 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

Eric Conrad *SANS Principal 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 health care. 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 www.ericconrad.com. @eric_conrad

SECURITY 542

Web App Penetration Testing and Ethical Hacking

OFFERED AT
Northern Virginia

Six-Day Program
Mon, Mar 9 - Sat, Mar 14
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Micah Hoffman

- GIAC Cert: GWAPT
- Cyber Guardian
- Master's Program

Web applications play a vital role in every modern organization. This becomes apparent when adversaries compromise these applications, damage business functionality and steal data.

Who Should Attend

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

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 penetration testing to professional web application penetration testing that finds flaws before the adversaries discover and abuse them.

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 tools within any organization. Unfortunately, there is no "patch Tuesday" for custom web applications, so, not surprisingly, every major industry study finds 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.

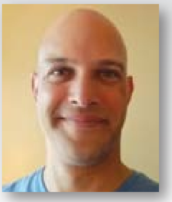
Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but web application penetration testing requires something deeper. SEC542 will enable students to capably assess a web application's security posture and convincingly demonstrate the impact of inadequate security that plagues most organizations. Students will come to understand major web application flaws and their exploitation and, most importantly, learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organizations.

"Web app assessment is currently what I do. SEC542 really fills in the gaps in on-the-job training."
-James Kelly,
Blue Canopy LLP

"With the infinite tools used for web app penetration, SEC542 helps you understand/use the best tools for your environment."
-Linh Sithihao, UT
Southwestern Medical Center

"SEC542 is an essential course for application security professionals."
-John Yamich, Exact Target

giac.org   sans.org/cyber-guardian   sans.edu



Micah Hoffman *SANS Instructor*

Micah Hoffman has been working in the information technology field since 1998 supporting federal government, commercial, and internal customers in their searches to discover and quantify information security weaknesses within their organizations. He leverages years of hands-on, real-world penetration testing and incident response experience to provide unique solutions to his customers. Micah holds GIAC's GAWN, GWAPT, and GPEN certifications as well as the CISSP. Micah is an active member in the NoVAHackers group, has written Recon-ng and Nmap testing tool modules and enjoys tackling issues with the Python scripting language. When not working, teaching, or learning, Micah can be found hiking or backpacking on Appalachian Trail or the many park trails in Maryland. @WebBreacher

OFFERED AT
Cyber Guardian

SECURITY 560

Network Penetration Testing and Ethical Hacking

Six-Day Program
Mon, Mar 2 - Sat, Mar 7
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Ed Skoudis

- GIAC Cert: GPEN
- Cyber Guardian
- Master's Program

As a cyber security 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.

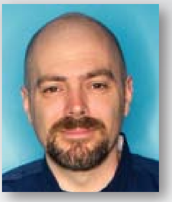
Who Should Attend

- 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

"I had a great time. SEC560 has tons of useful material and techniques. As with all SANS training, I leave knowing that I can apply this as soon as I am back at work."
-Benjamin Bagby, XE.Com

"Ed Skoudis successfully combines expertise, real-world experiences, and even humor to deliver an incredibly effective learning experience."
-George Huang, Nationwide Insurance

giac.org   sans.org/cyber-guardian   sans.edu



Ed Skoudis *SANS Faculty Fellow*

Ed Skoudis is the founder of Counter Hack, an innovative organization that designs, builds, and operates popular infosec challenges and simulations including CyberCity, NetWars, Cyber Quests, and Cyber Foundations. As director of the CyberCity project, Ed oversees the development of missions which help train cyber warriors in how to defend the kinetic assets of a physical, miniaturized city. Ed's expertise includes hacker attacks and defenses, incident response, and malware analysis, with over fifteen years of experience in information security. Ed authored and regularly teaches the SANS courses on network penetration testing (SEC560) and incident response (SEC504), helping over three thousand information security professionals each year improve their skills and abilities to defend their networks. He has performed numerous security assessments; conducted exhaustive anti-virus, anti-spyware, Virtual Machine, and IPS research; and responded to computer attacks for clients in government, military, financial, high technology, healthcare, and other industries. Previously, Ed served as a security consultant with InGuardians, International Network Services (INS), Global Integrity, Predictive Systems, SAIC, and Bell Communications Research (Bellcore). Ed also blogs about command line tips and penetration testing. @edskoudis

OFFERED AT
Northern Virginia

SECURITY 561

Intense Hands-on Pen Testing Skill Development (with SANS NetWars)

Six-Day Program
Mon, Mar 9 - Sat, Mar 14
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Joshua Wright

To be a top penetration testing professional, you need fantastic hands-on skills for finding, exploiting and resolving vulnerabilities. Top instructors at SANS engineered SEC561: Intense Hands-on Pen Testing Skill Development from the ground up to help you get good fast. The course teaches in-depth security capabilities through 80%+ hands-on exercises, maximizing keyboard time on in-class labs and making this SANS' most hands-on course ever. With over 30 hours of intense labs, students experience a leap in their capabilities, as they come out equipped with the practical skills needed to handle today's pen test and vulnerability assessment projects in enterprise environments. Throughout the course, an expert instructor coaches students as they work their way through solving increasingly demanding real-world information security scenarios using skills that they will be able to apply the day they get back to their jobs.

People often talk about these concepts, but this course teaches you how to actually do them hands-on and in-depth. SEC561 shows penetration testers, vulnerability assessment personnel, auditors, and operations personnel how to leverage in-depth techniques to get powerful results in every one of their projects. The course is overflowing with practical lessons and innovative tips, all with direct hands-on application. Throughout the course, students interact with brand new and custom-developed scenarios built just for this course on the innovative NetWars challenge infrastructure, which guides them through the numerous hands-on labs providing questions, hints, and lessons learned as they build their skills.

Who Should Attend

- Security professionals who want to expand their hands-on technical skills in new analysis areas such as packet analysis, digital forensics, vulnerability assessment, system hardening and penetration testing.
- Systems and network administrators who want to gain hands-on experience in information security skills to become better administrators.
- Incident response analysts who want to better understand system attack and defense techniques.
- Forensic analysts who need to improve their skills through experience with real-world attacks.
- Penetration testers seeking to gain practical hands-on experience for use in their own assessments.
- Red team members who want to build their hands-on skills, and blue team members who want to better understand attacks and defend their environments.

> "This class really forces you to think and the format rewards your hard work and dedication to finding the solutions."
> -Michael Nutbrown, Solers, Inc

> "80% hands-on is intense and the best way to build on previous pen-testing-focused SANS courses."
> -Timothy McKenzie, Dell/SecureWorks

> "Great challenge – it forces you to use skills you might not otherwise use."
> -Brian Thompson, Avista

Joshua Wright *SANS Senior Instructor*

Joshua Wright is a senior technical analyst with Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through his experiences as a penetration tester, Josh has worked with hundreds of organizations on attacking and defending mobile devices and wireless systems, ethically disclosing significant product and protocol security weaknesses to well-known organizations. As an open-source software advocate, Josh has conducted cutting-edge research resulting in several software tools that are commonly used to evaluate the security of widely deployed technology targeting WiFi, Bluetooth, and ZigBee wireless systems, smart grid deployments, and the Android and Apple iOS mobile device platforms. As the technical lead of the innovative CyberCity, Josh also oversees and manages the development of critical training and educational missions cyber warriors in the U.S. military, government agencies, and critical infrastructure providers. @joswr1ght

SECURITY 573

Python for Penetration Testers

OFFERED AT
Cyber Guardian

Five-Day Program
Mon, Mar 2 - Fri, Mar 6
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Mark Baggett

Who Should Attend

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

"Great course — very advanced thinking required and challenges are excellent."
-Kevin Nicholson, Motorola Solutions

"SEC573 gave me exposure to tools and techniques I would not have normally considered, but now are part of my arsenal."
-Allen Cox, DoD

Your target has been well hardened. So far, your every attempt to compromise their network has failed. But, you did find evidence of a vulnerability, a lucky break in their defensive posture. Sadly, all of your tools have failed to successfully exploit it. Your employers demand results. What do you do when off-the-shelf tools fall short? You write your own tool.

The best penetration testers can customize existing open source tools or develop their own tools. The ability to read, write, and customize software is what distinguishes the good penetration tester from the great penetration tester. This course is designed to give you the skills you need for tweaking, customizing, or outright developing your own tools to put you on the path of becoming a great penetration tester. Again and again, organizations serious about security emphasize their need for skilled tool builders. There is a huge demand for people who can understand a problem and then rapidly develop prototype code to attack or defend against it. Join us and learn Python in-depth and fully weaponized.

Unfortunately, many penetration testers do not have these skills today. The time and effort required to develop programming skills may seem overwhelming. But it is not beyond your reach. This course is designed to meet you at your current skill level, appealing to a wide variety of backgrounds ranging from people without a drop of coding experience all the way up to skilled Python developers looking to increase their expertise and map their capabilities to penetration testing. Because you can't become a world-class tool builder by merely listening to lectures, the course is chock full of hours of hands-on labs every day that will teach you the skills required to develop serious Python programs and how to apply those skills in penetration testing engagements.

The course begins with an introduction to SANS pyWars. pyWars is a 4-day Capture the Flag competition that runs parallel to the course material. It will challenge your existing programming skills and help you develop new skills at your own individualized pace. This allows experienced programmers to quickly progress to more advanced concepts while novice programmers spend time building a strong foundation. This individualized approach allows everyone to hone their current skills making them the most lethal weapon they can be.

Mark Baggett *SANS Certified Instructor*

Mark Baggett is the owner of Indepth Defense, an independent consulting firm that offers incident response and penetration testing services. He has served in a variety of roles from software developer to Chief Information Security Officer. Mark is the author of SANS Python for Penetration testers course (SEC573) and the pyWars gaming environment. Mark teaches several classes in SANS Penetration Testing curriculum including SEC504 (Incident Handing), SEC560 (Penetration Testing) and his Python course. Mark is very active in the information security community. Mark is the founding president of The Greater Augusta ISSA (Information Systems Security Association) chapter which has been extremely successful in bringing networking and educational opportunities to Augusta Information Technology workers. As part of the Pauldotcom Team, Mark generates blog content for the "pauldotcom.com" podcast . In January 2011, Mark assumed a new role as the Technical Advisor to the DoD for SANS. Today he assists various government branches in the development of information security training programs. @MarkBaggett

FORENSICS 408

Windows Forensic Analysis

Six-Day Program
Mon, Mar 9 - Sat, Mar 14
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Ovie Carroll

- GIAC Cert: GCFE
- Master's Program

OFFERED AT
Northern Virginia

DFIR
digital-forensics.sans.org

Master Computer Forensics.
What Do You Want to Uncover Today?

Every organization will deal with cyber-crime occurring on the latest Windows operating systems. Analysts will investigate crimes including fraud, insider threats, industrial espionage, traditional crimes, and computer hacking. Government agencies use media exploitation of Windows systems to recover key intelligence available on adversary systems. To help solve these cases, organizations are hiring digital forensic professionals, investigators, and agents to uncover what happened on a system.

FOR408: Windows Forensic Analysis focuses on critical knowledge of the Windows OS that every digital forensic analyst must know in order to investigate computer incidents successfully. You will learn how computer forensic analysts collect and analyze data from computer systems to track user-based activity that could be used internally or in civil/criminal litigation.

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 8.1, Office365, Skydrive, Sharepoint, Exchange Online, and Windows Phone). This will ensure that students are prepared to investigate the latest trends and capabilities they might encounter. In addition, students will have labs that cover both Windows XP and Windows 7 artifacts.

This course utilizes a brand-new Windows 8.1-based realistic case exercise for which it took over 6 months to create the data. The example case is a Windows 8.1 based image that has the subject utilize Windows Phone, Office 365, Sharepoint, MS Portal Online, Skydrive/Onedrive, Dropbox, and USB external devices. Our development team has created an incredibly realistic scenario. The case demonstrates the latest technologies an investigator would encounter analyzing a Windows operating system. The new case workbook will detail step-by-step what each investigator needs to know to examine the latest Windows 8.1.

FIGHT CRIME.
UNRAVEL INCIDENTS...
ONE BYTE AT A TIME

Who Should Attend

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

giac.org

sans.edu

"FOR408 is based on real scenarios that are likely to occur again. The most up-to-date training I have received."
-Martin Heyde,
UK Ministry of Defence

"FOR408 provides in-depth knowledge of the best forensic practices that can be applied directly to investigations."
-Nathan Lewis, KPMG

Ovie Carroll *SANS Certified Instructor*

Ovie Carroll has over 20 years of federal law enforcement experience. Ovie was a special agent for the Air Force Office of Special Investigations (AFOSI) and Chief of the Washington Field Office Computer Investigations and Operations Branch responsible for investigating all national level computer intrusions into USAF computer systems. Following his career with the AFOSI he was the Special Agent in Charge of the Postal Inspector General's computer crimes unit where he was responsible for all computer intrusion investigations and for providing all computer forensic analysis in support of USPS-OIG investigations. Ovie is currently the Director for the Cybercrime Lab at the Department of Justice, Computer Crime and Intellectual Property Section (CCIPS) and an adjunct professor at George Washington University teaching computer crime investigations. In addition to his career fighting computer crime, Ovie has conducted investigations into a variety of offenses including murder, fraud, bribery, theft, gangs and narcotics.

FORENSICS 508

Advanced Digital Forensics and Incident Response

OFFERED AT
Cyber Guardian

Six-Day Program
Mon, Mar 2 - Sat, Mar 7
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Hal Pomeranz

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

DFIR
digital-forensics.sans.org

DAY 0: A 3-letter government agency contacts you to say critical information was stolen from 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.

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.

Who Should Attend

- IT professionals
- 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

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 remediate the incident rapidly.

FOR508: will help your incident response team to determine:

- How did the breach occur?
- What systems were compromised and affected?
- What did they take? What did they change?
- How do we contain and 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. The completely up to date incident response course (FOR508) addresses today's incidents by providing real-life, hands-on incident response tactics and techniques that elite responders are successfully using in real-world breach cases.

During a targeted attack, an organization needs the best incident response team in the field. F**OR508: Advanced Digital Forensics and Incident Response** will train you and your team to be ready to respond, detect, scope, and stop intrusions and data breaches.

GATHER YOUR INICDENT RESPONSE TEAM – IT'S TIME TO GO HUNTING

giac.org

sans.org/cyber-guardian

sans.edu

DoD 8570 REQUIRED
sans.org/8570

> "Extremely valuable course overall, and brings essential topics into one. The course covers an extensive amount of topics with excellent reference material."
> -Edgar Zayas, U.S. Securities and Exchange Commission

> "This course [FOR508] really takes you from 0-60 in understanding the core concepts of forensics, especially the file system."
> -Matthew Harvey, U.S. DoJ

Hal Pomeranz *SANS Faculty Fellow*

Hal Pomeranz is an independent digital forensic investigator who has consulted on cases ranging from intellectual property theft, to employee sabotage, to organized cybercrime and malicious software infrastructures. He has worked with law enforcement agencies in the US and Europe and global corporations. While equally at home in the Windows or Mac environment, Hal is recognized as an expert in the analysis of Linux and Unix systems. His research on EXT4 file system forensics provided a basis for the development of Open Source forensic support for this file system. His EXT3 file recovery tools are used by investigators worldwide. Hal is a SANS Faculty Fellow and Lethal Forensicator, and is the creator of the SANS Linux/Unix Security track (GCUX). He holds the GCFA and GREM certifications and teaches the related courses in the SANS Forensics curriculum. He is a respected author and speaker at industry gatherings worldwide. Hal is a regular contributor to the SANS Computer Forensics blog and co-author of the Command Line Kung Fu blog. @hal_pomeranz

FORENSICS 585

Advanced Smartphone Forensics

OFFERED AT
Northern Virginia

Six-Day Program
Mon, Mar 9 - Sat, Mar 14
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Heather Mahalik

It is rare to conduct a digital forensics investigation that does not include a smartphone or mobile device. Such a device may be the only source of digital evidence tracing an individual's movements and motives, and may provide access to the who, what, when, where, why and how behind a case. **FOR585: Advanced Smartphone Forensics** teaches real-life, hands-on skills that enable digital forensics examiners, law enforcement officers and information security professionals to handle investigations involving even the most complex smartphones available today.

The course focuses on smartphones as sources of evidence, providing the necessary skills to handle mobile devices in a forensically sound manner, understand the different technologies, discover malware and analyze the results for use in digital investigations by diving deeper into the file systems of each smartphone. Students will be able to obtain actionable intelligence and recover and analyze data that commercial tools often miss for use in internal investigations, criminal and civil litigation and security breach cases.

The hands-on exercises in this course cover the best tools currently available to conduct smartphone and mobile device forensics, and provide detailed instructions on how to manually decode data that tools sometimes overlook. The course will prepare you to recover and reconstruct events relating to illegal or unauthorized activities, determine if a smartphone has been compromised with malware or spyware, and provide your organization the capability to use evidence from smartphones.

This intensive six-day course will take your mobile device forensics knowledge and abilities to the next level. Smartphone technologies are new and the data formats are unfamiliar to most forensics professionals. It is time for the good guys to get smarter and for the bad guys to know that their texts and apps can and will be used against them!

***YOUR TEXTS AND APPS
CAN AND WILL BE USED AGAINST YOU!***

Who Should Attend

- Experienced digital forensic analysts who want to extend their knowledge and experience to forensic analysis of mobile devices, especially smartphones
- Media exploitation analysts who need to master Tactical Exploitation or Document and Media Exploitation (DOMEX) operations on smartphones and mobile devices by learning how individuals used their smartphones, who they communicated with, and files they accessed
- Information security professionals who respond to data breach incidents and intrusions
- Incident response teams tasked with identifying the role that smartphones played in a breach
- Law enforcement officers, federal agents, or detectives who want to master smartphone forensics and expand their investigative skills beyond traditional host-based digital forensics
- IT auditors who want to learn how smartphones can expose sensitive information
- SANS SEC575, FOR563, FOR408, and FOR508 graduates looking to take their skills to the next level

DFIR
digital-forensics.sans.org

"Examiners who are tasked with acquiring and analyzing data, this course is a must!"
-Helena Polend,
VA Dept of Forensic Science

"This is the most advanced mobile device training that I know of and is greatly needed. It is currently the only course being taught at this level!"
-Scott McNamee DoS/CACI

Heather Mahalik *SANS Certified Instructor*

Heather Mahalik is a project manager for Ocean's Edge, where she uses her experience to manage projects focused on wireless cyber security and mobile application development. Heather has over 12 years of experience in digital forensics, vulnerability discovery of mobile devices, application reverse engineering and manual decoding. She is currently a certified instructor for the SANS Institute and is the course lead for FOR585, Advanced Smartphone Forensics. Previously, Heather led the mobile device team for Basis Technology, where she led the mobile device exploitation efforts in support of the U.S. Government. She also worked as a forensic examiner at Stroz Friedberg and the U.S. State Department Computer Investigations and Forensics Lab, where she focused her efforts on high profiles cases. Heather co-authored Practical Mobile Forensics and various white papers, presented at leading conferences, and instructed classes focused on Mac forensics, mobile device forensics, and computer forensics to practitioners in the field. Heather maintains www.smarterforensics.com where she blogs and hosts work from the digital forensics community. @HeatherMahalik

MANAGEMENT 414

SANS® +S™ Training Program for the CISSP® Certification Exam

OFFERED AT
Northern Virginia

Six-Day Program
Mon, Mar 9 - Sat, Mar 14
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPEs
Laptop NOT Needed
Instructor: Dr. Eric Cole
- GIAC Cert: GISP
- DoDD 8570

This course will cover the security concepts needed to pass the CISSP® exam. This is an accelerated review course that assumes the student has a basic understanding of networks and operating systems and focuses solely on the 10 domains of knowledge of the CISSP®:

Domain 1:	Access Controls
Domain 2:	Telecommunications and Network Security
Domain 3:	Information Security Governance & Risk Management
Domain 4:	Software Development Security
Domain 5:	Cryptography
Domain 6:	Security Architecture and Design
Domain 7:	Security Operations
Domain 8:	Business Continuity and Disaster Recovery Planning
Domain 9:	Legal, Regulations, Investigations and Compliance
Domain 10:	Physical (Environmental) Security

Each domain of knowledge is dissected into its critical components. Every component is discussed in terms of its relationship to other components and other areas of network security. After completion of the course, the student will have a good working knowledge of the 10 domains of knowledge and, with proper preparation, be ready to take and pass the CISSP® exam.

You Will Receive With This Course:

Free "CISSP® Study Guide" by Eric Conrad, Seth Misenar, and Joshua Feldman.

Note: CISSP® exams are not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam.

Take advantage of SANS CISSP® Get Certified Program currently being offered.
sans.org/special/cissp-get-certified-program

> "MGT414 offers a good top-level look at the information — it helps to know what to focus on."
> -Paul Gunnerson, U.S. Army

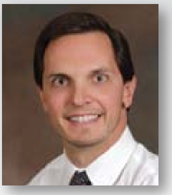
> "Great course and well worth it if you are considering taking the CISSP exam."
> -David Raymond, U.S. Army

Who Should Attend

- Security professionals who are interested in understanding the concepts covered in the CISSP® exam as determined by (ISC)²
- Managers who want to understand the critical areas of network security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® 10 domains
- Security professionals and managers looking for practical ways the 10 domains of knowledge can be applied to the current job
- In short, if you desire a CISSP® or your job requires it, MGT414 is the training for you to get GISP certified

DoD 8570 REQUIRED

giac.org   sans.org/8570



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 Cyber Security 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. He is a SANS faculty Fellow and course author. @drericcole

OFFERED AT
Northern Virginia

MANAGEMENT 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program
Mon, Mar 9 - Fri, Mar 13
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
- Master's Program
- DoDD 8570

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.

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

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.

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

> "MGT512 gives a good understanding of what knowledge our employees need to have to be successful."
> -Teddie Steele,
> State Department of FCU

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!

GIAC SECURITY LEADERSHIP CERTIFICATION GSLC
giac.org

SANS TECHNOLOGY INSTITUTE KNOWLEDGE FOR PEACE
sans.edu

DoD 8570
REQUIRED

sans.org/8570

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

OFFERED AT
Northern Virginia

DEVELOPER 541

Secure Coding in Java/JEE: Developing Defensible Applications

Four-Day Program
Mon, Mar 9 - Thu, Mar 12
9:00am - 5:00pm
24 CPEs
Laptop Required
Instructors: Eric Johnson
Steve Kosten

- GIAC Cert: GSSP-JAVA
- Master's Program

This secure coding course will teach students how to build secure Java applications and gain the knowledge and skills to keep a website from getting hacked, counter a wide range of application attacks, prevent critical security vulnerabilities that can lead to data loss, and understand the mindset of attackers.

The course teaches you the art of modern web defense for Java applications by focusing on foundational defensive techniques, cutting-edge protection, and Java EE security features you can use in your applications as soon as you return to work. This includes learning how to:

- Identify security defects in your code
- Fix security bugs using secure coding techniques
- Utilize secure HTTP headers to prevent attacks
- Secure your sensitive representational state transfer (REST) services
- Incorporate security into your development process
- Use freely available security tools to test your applications

Great developers have traditionally distinguished themselves by the elegance, effectiveness and reliability of their code. That is still true, but the security of the code now needs to be added to those other qualities. This unique SANS course allows you to hone the skills and knowledge required to prevent your applications from getting hacked.

giac.org   sans.edu

Who Should Attend

- Developers who want to build more secure applications
- Java Enterprise Edition (JEE) programmers
- Software engineers
- Software architects
- Developers who need to be trained in secure coding techniques to meet PCI compliance
- Application security auditors
- Technical project managers
- Senior software QA specialists
- Penetration testers

"The instruction is well versed in subject and this makes the complex issues more understandable."
-Mason Jackson, NGIS

"The content and more importantly the instructor's presentation of SEC541 was exactly what I was looking for."
-Gilbert Lappano, Northrop Grumman IS

Eric Johnson *SANS Instructor*

Eric Johnson is a security consultant at Cypress Data Defense and an instructor and contributing author for the SANS DEV544 Secure Coding in.NET course. He previously spent six years performing web application security assessments for a large financial institution and another four years focusing on ASP .NET web development. Other experience includes developing security tools, secure code review, vulnerability assessment, penetration testing, risk assessment, static source code analysis, and security research. Eric completed a bachelor of science in computer engineering and a master of science in information assurance at Iowa State University. Eric currently holds the GSSP-.NET, GWAPT, and CISSP certifications and is located in West Des Moines, IA. Outside the office, Eric enjoys spending time with his wife and daughter, attending Iowa State athletic events, and golfing on the weekends. @emjohn20

Steve Kosten *SANS Instructor*

Steve Kosten previously performed security work in the defense and financial sectors and headed up the security department for a financial services firm. He is currently the Open Web Application Security Project (OWASP) Denver chapter leader and is on the board for the OWASP AppSec USA conference. He has presented security talks before numerous conferences. He is experienced in secure code review, vulnerability assessment, penetration testing, risk management. He holds a bachelor of science in Aerospace Engineering from the Pennsylvania State University and a Master of Science in Information Security from James Madison University. He currently maintains GSSP-JAVA, GWAPT, CISSP, and CISM certifications. Steve resides in Golden, Colorado. In his spare time, Steve enjoys attending his childrens' sporting events with his wife, road and mountain biking, snowboarding, golfing, volleyball, and paragliding.

CYBER GUARDIAN SPECIAL EVENT

CORE NETWARS TOURNAMENT

CORE NetWars is a computer and network security challenge designed to test a participant's 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 OnSite to help identify skilled personnel and as part of extensive hands-on training. With Core NetWars, you'll build a wide variety of skills while having a great time.

CORE NetWars Tournament Topics:

- Vulnerability Assessment
- Packet and File Analysis
- Penetration Testing
- System Hardening
- Mobile Device Analysis
- Intrusion Detection
- Digital Forensics and Incident Response

Who Should Attend:

- Security professionals
- System administrators
- Network administrators
- Ethical hackers
- Penetration testers
- Incident handlers
- Security auditors
- Vulnerability assessment personnel
- Security Operations Center staff members

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

CORE NetWars Tournament will be played over two evenings: March 5-6, 2015 at Cyber Guardian 2015

Prizes will be awarded at the conclusion of the game.

REGISTRATION IS LIMITED AND IS FREE for students attending any long course at Cyber Guardian 2015

(NON-STUDENTS ENTRANCE FEE IS $1,249).

sans.org/event/cyber-guardian-2015/courses

SPECIAL EVENTS

SANS@Night Evening Talks

Enrich your SANS training experience! Evening talks given 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.

CYBER GUARDIAN

KEYNOTE: Windows Exploratory Surgery with Process Hacker *Jason Fossen*

In this talk we'll rummage around inside the guts of Windows while on the lookout for malware using a free tool named Process Hacker (similar to Process Explorer). Understanding processes, threads, drivers, handles, and other OS internals is important for analyzing malware, doing forensics, troubleshooting, and hardening the OS. If you have a laptop, get Process Hacker from SourceForge.net and together we'll take a peek under the GUI to learn about Windows internals and how to use Process Hacker for combating malware.

CYBER GUARDIAN

Evolving Threats *Paul A. Henry*

For nearly two decades defenders have fallen into the "Crowd Mentality Trap." They have simply settled on doing the same thing everyone else was doing, while at the same time attackers have clearly evolved both in terms of malware delivery vectors and attack methodology. Today our defenses focus primarily on the gateway and upon attempting to outwit attacker's delivery methods. This leaves us woefully exposed and according to a recent Data Breach Report has resulted in 3,765 incidents, 806 million records exposed, and $157 billion (USD) in data breach costs in only the past six years.

CYBER GUARDIAN & NORTHERN VIRGINIA

Debunking the Complex Password Myth *Keith Palmgren*

Perhaps the worst advice you can give a user is "choose a complex password." The result is the impossible-to-remember password requiring the infamous sticky note on the monitor. In addition, that password gets used at a dozen sites at home, AND the very same password gets used at work. The final result ends up being the devastating password compromise. In this one-hour talk we will look at the technical and non-technical (human nature) issues behind passwords. Attendees will gain a more complete understanding of passwords and receive solid advice on creating more easily remembered AND significantly stronger passwords at work and at home, for their users, for themselves, and even for their children.

CYBER GUARDIAN & NORTHERN VIRGINIA

The 13 Absolute Truths of Security *Keith Palmgren*

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

NORTHERN VIRGINIA

KEYNOTE: Offensive Countermeasures, Active Defenses, and Internet Tough Guys *John Strand*

In this presentation John Strand will demonstrate the Active Defense Harbinger Distribution, a DARPA funded, free Active Defense virtual machine. He will debunk many of the myths, outright lies, and subtle confusions surrounding taking active actions against attackers. From this presentation, you will not only know how to take action against attackers, you will learn how to do it legally.

NORTHERN VIRGINIA

Who's Watching the Watchers? *Mike Poor*

We have instrumented our networks to the Nth degree. We have firewalls, IDS, IPS, Next Gen Firewalls, Log correlation and aggregation... but do we know if we have it right? Will we detect the NextGen(TM) attackers? In this talk we will explore ways that we improve the signal/noise ratio in our favor, and help identify the needle in the needlestack.

NORTHERN VIRGINIA

Continuous Ownage: Why you Need Continuous Monitoring

Eric Conrad

Repeat after me, "I will be breached." Most organizations realize this fact too late, usually after a third party informs them months after the initial compromise. Treating security monitoring as a quarterly auditing process means most compromises will go undetected for weeks or months. The attacks are continuous, and the monitoring must match. This talk will help you face this problem and describe how to move your organization to a more defensible security architecture that enables continuous security monitoring. The talk will also give you a hint at the value you and your organization will gain from attending Seth Misenar and Eric Conrad's new course Continuous Monitoring and Security Operations.

NORTHERN VIRGINIA

iOS Game Hacking: How I Ruled the World and Built Skills For AWESOME Mobile App Pen Tests *Josh Wright*

I am a terrible video game player. I lack the skills to competitively arrange words with colleagues, crush jelly beans, or achieve a high score arranging numbers by threes. However, what I lack in video game competition, I make up for in iOS app hacking. In this talk, we'll explore the profitable market of iOS games, looking at several techniques that are used to cheat, hack, or even steal from iOS game developers. You'll be able to apply these techniques to give yourself a leg up on your next gaming experience. Most importantly, each and every technique we'll discuss is also directly applicable to penetration testing and assessing the security of the iOS apps your organization uses each and every day. Learn to pwn games while becoming a better app pen tester! What's not to like?

NORTHERN VIRGINIA

SQL Injection Exploited *Micah Hoffman*

For almost two decades attackers have been exploiting web applications using SQL injection attacks; gaining access to database content and compromising systems. We have probably all seen news reports that thousands or millions of database records were stolen from a company's web application through SQL injection. Or perhaps we have seen a report about attackers breaking into a government organization and compromising their systems through a similar flaw. But how many of us have actually seen what SQL injection looks like? How many of us have seen someone exploit a system using it? That is what this talk and demo are about. Come learn about SQL injection, what it is, and how to prevent it. But mostly, come to this talk to see a demonstration of a web application being exploited using manual and automated SQL injection techniques. Attendees will leave the talk with a better understanding of the vulnerability, attacker capabilities, and appropriate places where they can try exploiting a system using SQL injection themselves!

NORTHERN VIRGINIA

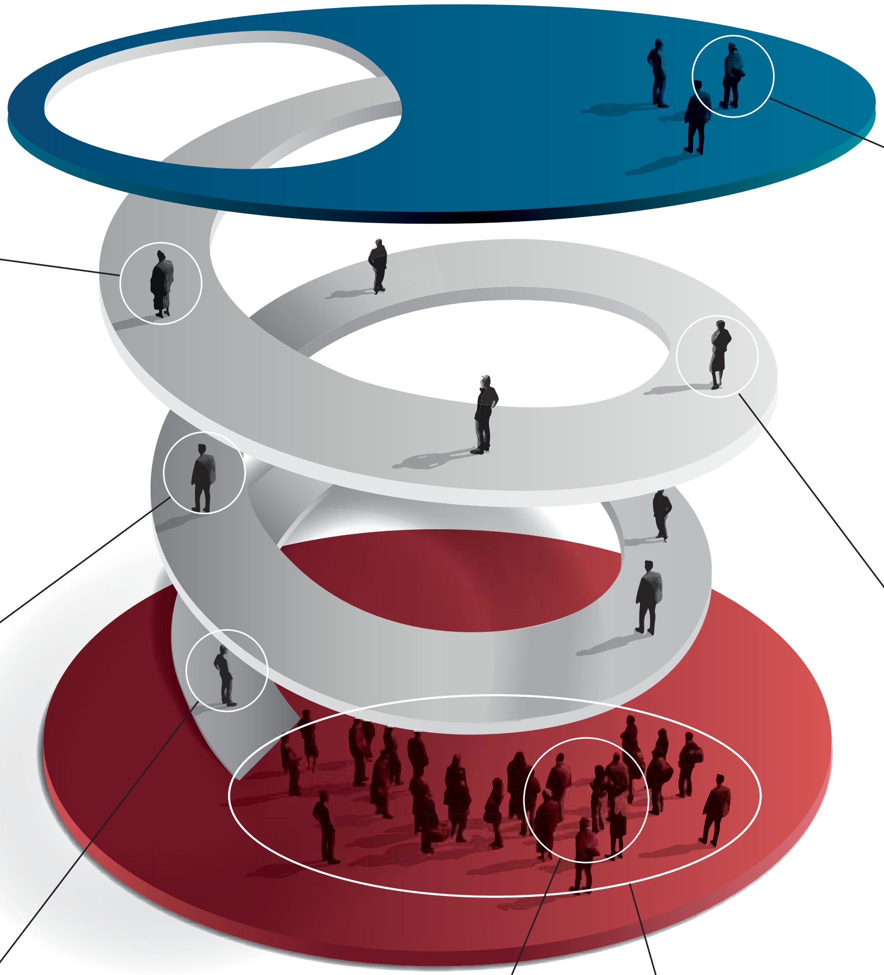
Bitcoin and Crypto and I-Pay, Oh My! *G. Mark Hardy*

Are we finally ready to go mainstream with crypto currency? Bitcoin got off to a slow start but made great gains in 2013, only to fishtail back down last year. Apple jumped on the bandwagon with their Apple Pay offering for the iPhone 6. Plus there's a hundred or more alternative crypto currencies all competing for attention, value, and survival. We'll look at this brave new world of electronic money to understand what it is, how it works, what it can (and cannot) do, and probabilities of success and survival. You'll gain a working knowledge of how to create and use a Bitcoin wallet, how to "invest" in cryptocurrencies, and the mechanics behind electronic payment systems such as Apple Pay, CurrentC, and Softcard.

EDUCATING THE WORLD IN CYBERSECURITY

Protecting data has never been more important. As attackers become more sophisticated and determined, preventing a breach requires information security professionals to own a honed skillset with real-world knowledge and capabilities. SANS is a one-stop education provider for information security, including security awareness program, hands-on training, GIAC certification and graduate programs. SANS world-class instructors and proven curricula will empower you with the ability to protect and defend your vital systems and data.

The SANS family of products includes:



Cyber Guardian

Designed for the elite teams of technical security professionals whose role includes securing systems, reconnaissance, counterterrorism and counter hacks

sans.org/cyber-guardian

SANS NetWars

Testing hands-on technical skills in a safe environment so security professionals are prepared when a real incident occurs

sans.org/netwars

SANS Training

Hands-on security training for professionals just starting in security up to seasoned professionals

Training courses are delivered at live events and online

sans.org

SANS CyberTalent

Assess the skills and aptitude of security professionals so you can feel confident in your hiring decisions

sans.org/cybertalent

SANS Security Awareness

Everything your organization needs for an effective security awareness program

securingthehuman.org

GIAC Certification

Validate the technical skills and knowledge of your security professionals

giac.org

SANS Technology Institute

A regionally accredited postgraduate institution focused solely on information security education for working professionals

sans.edu

FUTURE SANS TRAINING EVENTS

SANS Cyber Defense Initiative 2014
Washington, DC | December 10-19 | #SANSCDI

SANS Security East 2015
New Orleans, LA | January 16-21 | #SecurityEast

SANS Cyber Threat Intelligence SUMMIT & TRAINING 2015
Washington, DC | February 2-9 | #CTISummit

10TH ANNUAL ICS Security SUMMIT – ORLANDO 2015
Orlando, FL | February 23 - March 2 | #SANSICS

SANS DFIR Monterey 2015
Monterey, CA | February 23-28 | #DFIRMonterey

SANS Cyber Guardian 2015
Baltimore, MD | March 2-7 | #CyberGuardian

SANS Northern Virginia 2015
Reston, VA | March 9-14 | #SANSNoVA

SANS 2015
Orlando, FL | April 11-18 | #SANS2015

Visit sans.org for a complete schedule.

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

OnSite sans.org/onsite
Live Training at Your Office Location

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

HOTEL INFORMATION

SANS CYBER GUARDIAN

Training Campus
Sheraton Inner Harbor

300 South Charles Street
Baltimore, MD 21201
sans.org/event/cyber-guardian-2015/location

Special Hotel Rates Available

A special discounted rate of $179.00 S/D will be honored based on space availability. These rates available through February 13, 2015.

You can call the hotel directly at (410) 962-8300 or the Toll Free Starwood Reservation Hot Line at (800) 325-3535 and ask for the SANS group rate.

SANS NORTHERN VIRGINIA

Training Campus
Sheraton Reston

11810 Sunrise Valley Drive
Reston, VA 20191
sans.org/event/northern-virginia-2015/location

Special Hotel Rates Available

A special discounted rate of $145.00 S/D will be honored based on space availability. These rates available through February 7, 2015.

To make reservations please call (703) 620-9000 and ask for the SANS group rate.

Top 5 reasons to stay at the SANS host hotel

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 SANS host hotel, 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 SANS host hotel that you won't want to miss!

5 Everything is in one convenient location!

REGISTRATION INFORMATION

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

SANS CYBER GUARDIAN

REGISTER AT
www.sans.org/event/cyber-guardian-2015/courses

SANS NORTHERN VIRGINIA

REGISTER AT
www.sans.org/event/northern-virginia-2015/courses

Select your course or courses and indicate whether you plan to test for GIAC certification.

How to tell if there is room available in a course:
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.

Look for E-mail Confirmation – It Will Arrive Soon After You Register

We recommend you register and pay early to ensure you get your first choice of courses. An immediate e-mail confirmation is sent to you when the registration is submitted properly. If you have not received e-mail confirmation within two business days of registering, please call the SANS Registration office at 301-654-7267 9am - 8pm ET.

Register Early and Save

SANS CYBER GUARDIAN

Register & Pay By

DATE	DISCOUNT
January 14, 2015	**$400.00**
February 11, 2015	**$200.00**

Cancellation date: February 11, 2015

SANS NORTHERN VIRGINIA

Register & Pay By

DATE	DISCOUNT
January 14, 2015	**$400.00**
February 11, 2015	**$200.00**

Cancellation date: February 18, 2015

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.

**Early-bird rates and/or other discounts cannot be combined with the group discount.*

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 the event's cancellation date – processing fees may apply.