THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH

SANS

Baltimore Spring 2016

Baltimore, MD May 9-14

SANS Offers Hands-On, Immersion-Style Security Training Courses Taught by Real-World Practitioners

Choose from these popular courses:

- Cyber Threat Intelligence – **NEW!**
- Security Essentials Bootcamp Style
- Hacker Tools, Techniques, Exploits, and Incident Handling
- Windows Forensic Analysis
- SANS Security Leadership Essentials for Managers with Knowledge Compression™
- SANS Training Program for CISSP® Certification
- Securing Windows with PowerShell and the Critical Security Controls
- Advanced Security Essentials – Enterprise Defender
- IT Security Strategic Planning, Policy, and Leadership
- Continuous Monitoring and Security Operations

> *"SANS lived up to its reputation. This is the best training I have ever attended!"*
>
> -Ryan O'Connor, Atlantic Health

GLOBAL INFORMATION ASSURANCE CERTIFICATION GIAC www.giac.org

GIAC Approved Training

SAVE $400

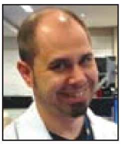
by registering and paying early!

See page 13 for more details.

sans.org/baltimore-spring-2016

SANS Instructors

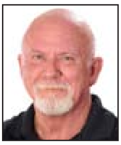
SANS Instructors are real-world practitioners who specialize in the subjects they teach. All SANS instructors undergo rigorous training and testing. This guarantees that what you learn in class will be up-to-date and relevant to your job. The SANS Baltimore Spring 2016 line-up of instructors includes:


Mike Cloppert
SANS Instructor

Christopher Crowley
Certified Instructor

Jason Fossen
Faculty Fellow

G. Mark Hardy
Certified Instructor

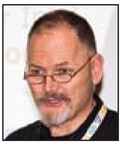

Paul A. Henry
Senoir Instructor

David R. Miller
SANS Instructor

Michael Murr
Principal Instructor

Keith Palmgren
Certified Instructor

Mike Pilkington
Certified Instructor


Mark Williams
SANS Instructor

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 11.

What's New for Security in Windows 10 and Server 2016 – Jason Fossen
Evolving Threats – Paul A. Henry
SANS' 8 Mobile Device Security Steps – Chris Crowley
How to Build a Cybersecurity Platform the Easy Way – Keith Palmgren
Privileged Domain Account Protection: How to Limit Credentials Exposure – Mike Pilkington
Card Fraud 101 – G. Mark Hardy
Security Without Exception – Mark Williams

Be sure to register and pay by March 16th for a $400 tuition discount!

Courses-at-a-Glance

<table>
<tr><th></th><th>MON 5-9</th><th>TUE 5-10</th><th>WED 5-11</th><th>THU 5-12</th><th>FRI 5-13</th><th>SAT 5-14</th></tr>
<tr><td>SEC401 Security Essentials Bootcamp Style</td><td colspan="6">Page 1</td></tr>
<tr><td>SEC501 Advanced Security Essentials – Enterprise Defender</td><td colspan="6">Page 2</td></tr>
<tr><td>SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling</td><td colspan="6">Page 3</td></tr>
<tr><td>SEC505 Securing Windows with PowerShell & the Critical Security Controls</td><td colspan="6">Page 4</td></tr>
<tr><td>SEC511 Continuous Monitoring and Security Operations</td><td colspan="6">Page 5</td></tr>
<tr><td>FOR408 Windows Forensic Analysis</td><td colspan="6">Page 6</td></tr>
<tr><td>FOR578 Cyber Threat Intelligence <em>NEW!</em></td><td colspan="5">Page 7</td><td></td></tr>
<tr><td>MGT414 SANS Training Program for CISSP® Certification</td><td colspan="6">Page 8</td></tr>
<tr><td>MGT512 SANS Security Leadership Essentials for Managers with Knowledge Compression™</td><td colspan="5">Page 9</td><td></td></tr>
<tr><td>MGT514 IT Security Strategic Planning, Policy, and Leadership</td><td colspan="5">Page 10</td><td></td></tr>
</table>

Register today for SANS Baltimore Spring 2016!
sans.org/baltimore-spring-2016

@SANSInstitute
Join the conversation:
#SANSBaltimore

SEC401:

Security Essentials Bootcamp Style

Six-Day Program
Mon, May 9 - Sat, May 14
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Paul A. Henry

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

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

"This course was fantastic! The content, instructor, and books are nicely detailed, interesting, and complete!"
-Dave Rozzi, New York Post

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

Learn to build a security roadmap that can scale today and into the future.

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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

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

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

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

giac.org

SANS Technology Institute
sans.edu

sans.org/cyber-guardian

sans.org/8570

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

Paul A. Henry *SANS Senior Instructor*

Paul Henry is one of the world's foremost global information security and computer forensic experts, with more than 20 years' 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 U.S. Department of Defense's Satellite Data Project, and both government and telecommunications projects throughout Southeast Asia. Paul is frequently cited by major publications as an expert in perimeter security, incident response, computer forensics, and general security trends, and serves as an expert commentator for network broadcast outlets such as FOX, NBC, CNN, and CNBC. In addition, Paul regularly authors thought leadership articles on technical security issues, and his expertise and insight help shape the editorial direction of key security publications such as the *Information Security Management Handbook*, to which he is a consistent contributor. Paul is a featured speaker at seminars and conferences worldwide, delivering presentations on diverse topics such as anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, perimeter security, and incident response. @phenrycissp

SANS

SEC501:

Advanced Security Essentials – Enterprise Defender

Six-Day Program
Mon, May 9 - Sat, May 14
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: Keith Palmgren

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

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

Who Should Attend

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

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

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

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

"I can't stress enough how important the SEC501 course is for today's network defenders. It's a hostile world, so why settle for anything less than the best? SANS is simply the best!"
-John J., Houston PD

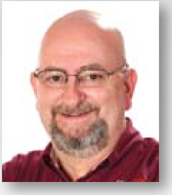
"SEC501 has a nice balance between courseware, labs, and lectures that include examples, reviews, and interesting tidbits of current events to keep everyone involved."
-Debra S., Naval Supply Systems Command FLCSD

GIAC Certified Enterprise Defender GCED
giac.org

SANS Technology Institute
sans.edu

sans.org/8570

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



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 and 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 17 training courses. Keith currently holds the CISSP, GSEC, CEH, Security+, Network+, A+, and CTT+ certifications. @kpalmgren

SANS

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling

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

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

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

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

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

Who Should Attend

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

"It was another excellent day and the course was crammed-packed full of outstanding information. The instructor has all the information at his fingertips and is a remarkable teacher. Thanks!"
-Jim Carroll, MOD

"This training provides actual hands-on experience with the labs, and you get great perspective from people in the industry.
-Michael H., U.S. Navy

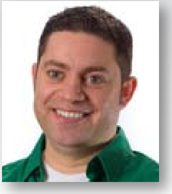
giac.org

SANS Technology Institute
sans.edu

sans.org/cyber-guardian

sans.org/8570

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



Michael Murr *SANS Principal Instructor*

Michael has been a forensic analyst with Code-X Technologies for over five years, conducted numerous investigations and computer forensic examinations, and performed specialized research and development. Michael has taught SANS SEC504: Hacker Techniques, Exploits, and Incident Handling; SANS FOR508: Advanced Digital Forensics and Incident Response; and SANS FOR610: Reverse-Engineering Malware. He has also led SANS@Home courses and is a member of the GIAC Advisory Board. Currently, Michael is working on an open-source framework for developing digital forensics applications. He holds the GCIH, GCFA, and GREM certifications and has a degree in computer science from California State University at Channel Islands. Michael also blogs about digital forensics on his forensic computing blog (www.forensicblog.org). @mikemurr

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/baltimore-spring-2016/courses

SEC505:

Securing Windows with PowerShell and the Critical Security Controls

Six-Day Program
Mon, May 9 - Sat, May 14
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jason Fossen

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

What is Windows Hello in Windows 10? 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 that lead to advanced persistent threat malware infections? We tackle these tough problems in **SEC505: Securing Windows with PowerShell and the Critical Security Controls**.

Understanding how penetration testers and hackers break into networks is not the same as knowing how to design defenses against them, especially when you work in a large and complex Active Directory environment. Knowing about tools like Metasploit, Cain, Netcat, and Poison Ivy is useful, but there is no simple patch against their abuse. The goal of this course is to show you ways to defend against both current Windows attack techniques and the likely types of attacks we can expect in the future. This requires more than just reactive patch management – we need to proactively design security into our systems and networks. That is what SEC505 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 and PowerShell scripting.

Learning PowerShell is probably the single best new skill for Windows administrators, especially with the trend toward cloud computing. Most of your competition in the job market lacks scripting skills, so knowing PowerShell is a great way to make your résumé stand out. This course devotes the entire first day to PowerShell, then we do more PowerShell exercises throughout the rest of the week. Don't worry, you don't need any prior scripting experience to attend.

This is a fun course and a real eye-opener, even for Windows administrators with years of experience. Come have fun learning PowerShell and Windows security!

Who Should Attend

- Anyone who wants to learn PowerShell
- Windows security engineers and system administrators
- Anyone implementing the Critical Security Controls
- Those who must enforce security policies on Windows hosts
- Those deploying or managing a PKI or smart cards
- Anyone who needs to reduce APT malware infections

"As auditors, we are always being accused of not understanding the technology and not empathizing with our clients when we challenge the control decisions they make. This course allows me to understand the technology and the available controls so I can effectively audit it."
-Susan Chiutsi, Canadian Imperial Bank of Commerce

"This training was an excellent balance between theory and practical applications, extremely relevant to current trends, concepts, and technologies."
-Chris S., Naval Surface Warfare Center

GCWN
giac.org

SANS Technology Institute
sans.edu

sans.org/cyber-guardian

sans.org/8570

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

Jason Fossen *SANS Faculty Fellow*

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

SEC511:

Continuous Monitoring and Security Operations

New in 2016 to Enhance Your Skills Extended-Hours Bootcamp

Six-Day Program
Mon, May 9 - Sat, May 14
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Laptop Required
Instructor:
Christopher Crowley

- GIAC Cert: GMON
- Master's Program
- OnDemand Bundle

> "SEC511 delivers the practical methodologies and granular information that can help bridge the communications gaps that may exist between analysts, engineers, and operations."
> -Patrick Nolan, Intel Security Foundstone

> "The focus on methodologies was superb because the techniques taught are applicable to every environment regardless of tools that are utilized."
> -Conrad B., DSS

Who Should Attend

- Security architects
- Senior security engineers
- Technical security managers
- Security Operations Center (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)

We continue to underestimate the tenacity of our adversaries! Organizations are investing a significant amount of time and financial and human resources trying to prevent and combat 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 is early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and this course will greatly increase your understanding and enhance your skills in implementing CM utilizing the NIST framework.

giac.org

SANS Technology Institute
sans.edu

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

Christopher Crowley *SANS Certified Instructor*

Christopher has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. His work experience includes penetration testing, computer network defense, incident response, and forensic analysis. He is the course author for SANS MGT535: Incident Response Team Management and holds the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GREM, GMOB, and CISSP certifications. His teaching experience includes SEC401, SEC503, SEC504, SEC560, SEC575, SEC580, FOR585, and MGT535; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor Year Award, which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities. @CCrowMontance

FOR408:

Windows Forensic Analysis

SANS

Six-Day Program
Mon, May 9 - Sat, May 14
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Mike Pilkington

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

DFIR
digital-forensics.sans.org

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

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

Who Should Attend

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

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

Proper analysis requires real data for students to examine. The completely updated FOR408 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7/8/10, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows XP systems to just-discovered Windows 10 artifacts.

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

GIAC CERTIFIED FORENSIC EXAMINER GCFE
giac.org

SANS Technology Institute
sans.edu

▶‖
BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

> "Awesome content, awesome instructor! Everyone needs this course, not just forensics, but any security personnel."
> -Thomas Farley, Raytheon

> "I like the fact that the whole course is centered around the same data and that there is so much data available. I can't wait to try this out at work!"
> -Greg Dub, National Center for Policy Analysis

Mike Pilkington *SANS Certified Instructor*

Mike Pilkington is the technical incident response lead for a Fortune 500 company in the oil and gas industry. In his role, Mike regularly works malware and intrusion cases, evaluates and implements both commercial and open-source forensic tools, and consults with various groups within the organization. Over the years, Mike has accumulated a broad range of technical expertise, having spent significant time performing software quality assurance, Windows systems administration, LAN and WAN network administration, firewall and IDS/IPS security administration, computer forensic analysis, and incident response. As a forensic analyst, he worked numerous human resources investigations, including cases involving intellectual property theft, inappropriate use of the Internet, employee hacking, IT administrator privilege abuse, and illegal downloading of copyright materials. Mike holds a B.S. in Mechanical Engineering from the University of Texas, as well as numerous IT security certifications, including the CISSP, EnCE, GCFE, GCFA, and GREM. @mikepilkington

FOR578:

Cyber Threat Intelligence

NEW

SANS

Five-Day Program
Mon, May 9 - Fri, May 13
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Mike Cloppert

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

FOR578: Cyber Threat Intelligence will help network defenders and incident responders:

- Construct and exploit threat intelligence to detect, respond, and defeat advanced persistent threats (APTs)
- Fully analyze successful and unsuccessful intrusions by advanced attackers
- Piece together intrusion campaigns, threat actors, and nation-state organizations
- Manage, share, and receive intelligence on APT adversary groups
- Generate intelligence from their own data sources and share it accordingly
- Identify, extract, and leverage intelligence from APT intrusions
- Expand upon existing intelligence to build profiles of adversary groups
- Leverage intelligence to better defend against and respond to future intrusions

Conventional network defenses such as intrusion detection systems and anti-virus tools focus on the vulnerability component of risk, and traditional incident response methodology pre-supposes a successful intrusion. However, the evolving sophistication of computer network intrusions has rendered these approaches insufficient to address the threats faced by modern networked organizations. Today's adversaries accomplish their goals using advanced tools and techniques designed to circumvent most conventional computer network defense mechanisms, go undetected during the intrusion, and then remain undetected on networks over long periods of time.

The collection, classification, and exploitation of knowledge about adversaries – collectively known as cyber threat intelligence – gives network defenders information superiority that can be used to reduce the adversary's likelihood of success with each subsequent intrusion attempt. Responders need accurate, timely, and detailed information to monitor new and evolving attacks, as well as methods to exploit this information to put in place an improved defensive posture. Threat intelligence thus represents a force multiplier for organizations looking to update their response and detection programs to deal with increasingly sophisticated advanced persistent threats.

During a targeted attack, an organization needs a top-notch and cutting-edge incident response armed with the critical intelligence necessary to understand how adversaries operate and to combat the threat. FOR578 will train you and your team to identify, scope, and select resilient courses of action in response to such intrusions and data breaches.

THERE IS NO TEACHER BUT THE ENEMY!

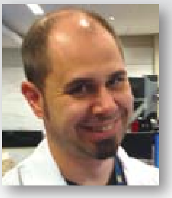
DFIR
digital-forensics.sans.org

Who Should Attend

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

"I absolutely loved this class! Mike provided a great framework for CTI that I will use to be more effective."

-Nate DeWitt, eBay



Mike Cloppert *SANS Instructor*

Michael is the lead analyst for Lockheed Martin CIRT's Intel Fusion team, charged with collecting and managing intelligence on adversaries intent on stealing the organization's intellectual property, and with developing new detection and analysis techniques. Michael has worked as a security analyst in various sectors including the financial industry, federal government, and defense industry. He has an undergraduate degree in Computer Engineering from the University of Dayton and an MS in Computer Science from George Washington University. He holds numerous industry certifications including the GCIA, GREM, and GCFA, and is a SANS Forensics and Incidence Response blog contributor. Michael's past speaking engagements include the DC3 Cybercrime Conference and the IEEE, along with various SANS events. @mikecloppert

SANS

MGT414:

SANS Training Program for CISSP® Certification

Six-Day Program
Mon, May 9 - Sat, May 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: David R. Miller

- GIAC Cert: GISP
- DoDD 8570
- OnDemand Bundle

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that has been specifically updated to prepare you to pass the 2016 version of the CISSP® exam.

Course authors Eric Conrad and Seth Misenar have revised MGT414 to take into account the 2016 updates to the CISSP® exam and prepare students to navigate all types of questions included in the new version.

MGT414 focuses solely on the 8 domains of knowledge as determined by (ISC)^2 that form a critical part of the CISSP® exam. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

Who Should Attend

- Security professionals who want to understand 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® 8 domains
- Security professionals and managers looking for practical ways to apply the 8 domains of knowledge to their current activities

You Will Be Able To:

- Understand the 8 domains of knowledge that are covered on the CISSP® exam
- Analyze questions on the exam and be able to select the correct answer
- Apply the knowledge and testing skills learned in class to pass the CISSP® exam
- Understand and explain all of the concepts covered in the 8 domains of knowledge
- Apply the skills learned across the 8 domains to solve security problems when you return to work

GISP
giac.org

sans.org/8570

BUNDLE ONDEMAND WITH THIS COURSE
sans.org/ondemand

Note:
The CISSP® exam itself is not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam. Please note as well that the GISP exam offered by GIAC is NOT the same as the CISSP® exam offered by (ISC)^2.

> "SANS does it again! An excellent course (MGT414) for those looking to lead their companies through the next stage of security evolution."
> -Travis Anderson, Pacific Gas and Electric Company

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

David R. Miller *SANS Instructor*

David has been a technical instructor since the early 1980s and has specialized in consulting, auditing, and lecturing on information systems security, legal and regulatory compliance, and network engineering. David has helped many enterprises develop their overall compliance and security program, including policy writing, network architecture design to include security zones, development of incident response teams and programs, design and implementation of public key infrastructures (PKI), security awareness training programs, specific security solution designs like secure remote access and strong authentication architectures, disaster recovery planning and business continuity planning, and pre-audit compliance gap analysis and remediation. He performs as a security lead and forensic investigator on numerous enterprise-wide IT design and implementation projects for Fortune 500 companies, providing compliance, security, technology, and architectural recommendations and guidance. Projects include Microsoft Windows Active Directory enterprise designs, Security Information and Event Management (SIEM) systems, Intrusion Detection and Protection Systems (IDS/IPS), endpoint protection systems, patch management systems, configuration monitoring systems, and enterprise data encryption for data at rest, in transit, in use, and within email systems. David is an author, lecturer and technical editor of books, curriculum, certification exams, and computer-based training videos.

MGT512:

SANS Security Leadership Essentials for Managers with Knowledge Compression™

Five-Day Program
Mon, May 9 - Fri, May 13
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop NOT Needed
Instructor: G. Mark Hardy

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

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

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

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

"The course content is great because it is consistently updated to reflect current IT trends. The instructor was knowledgeable, and very down to earth."
-Terence B., Officer Training Command

"MGT512 was taught on a management level that is informative, but not overly detailed. This training helps you be a better manager of people and security."
-Octavia Howell, New York Life Insurance Company

GSLC
giac.org

SANS Technology Institute
sans.edu

sans.org/8570

Bundle OnDemand with this course
sans.org/ondemand

Knowledge Compression™

Maximize your learning potential!

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

G. Mark Hardy *SANS Certified Instructor*

G. Mark Hardy is founder and president of National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for over 30 years, and is an internationally recognized expert who has spoken at over 250 events world-wide. He 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 U.S. 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 the GSLC, CISSP, CISM, and CISA certifications. @g_mark

MGT514:

IT Security Strategic Planning, Policy, and Leadership

Five-Day Program
Mon, May 9 - Fri, May 13
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: Mark Williams

- STI Master's Program
- OnDemand Bundle

As security professionals we have seen the landscape change. Cybersecurity is now more vital and relevant to the growth of your organization than ever before. As a result, information security teams have more visibility, more budget, and more opportunity. However, with this increased responsibility comes more scrutiny.

This course teaches security professionals how to do three things:

Develop Strategic Plans

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

Create Effective Information Security Policy

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

Develop Management and Leadership Skills

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

Who Should Attend

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

"As I progress in my career within cybersecurity, I find that courses such as MGT514 will allow me to plan and lead organizations forward."
-Eric Burgan, Idaho National Labs

"Mark did a great job engaging the students. This was a tough course, however, he pulled participation out of everyone."
-Todd Wagner, Caterpillar

SANS Technology Institute
sans.edu

Bundle OnDemand
WITH THIS COURSE
sans.org/ondemand

Mark Williams *SANS Instructor*

Mark Williams currently holds the position of Principal Systems Security Officer at BlueCross BlueShield of Tennessee. Mark holds multiple certifications in security and privacy including the CISSP, CISA, CRISC, and CIPP/IT. He has authored and taught courses at undergraduate and graduate levels, as well as public seminars around the world. He has worked in public and private sectors in the Americas, Canada, and Europe in the fields of security, compliance, and management. Mark has more than 20 years of international high-tech business experience working with major multinational organizations, governments, and private firms. During his career Mark has consulted on issues of privacy and security, led seminars, and developed information security, privacy, and compliance-related programs.

SANS@NIGHT EVENING TALKS

Enrich your SANS training experience!

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

KEYNOTE: What's New for Security in Windows 10 and Server 2016

Jason Fossen

The graphical interface of Windows 8 made that OS undeployable, so will users prefer the Windows 10 desktop over Windows 7? This session will lay out what's new in Windows 10, with an emphasis on security and enterprise management, such as Windows Hello biometrics, Passport, and Credential Guard. Windows Server 2016 is also coming out, so we'll cover what's new and interesting on the server side too, such as Virtual TPM chips and Hyper-V containers for Docker. There is a lot more to Windows 10 and Server 2016 than just the return of the Start Menu, so come see!

Evolving Threats *Paul A. Henry*

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

SANS' 8 Mobile Device Security Steps *Chris Crowley*

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

How to Build a Cybersecurity Platform the Easy Way *Keith Palmgren*

Building a cybersecurity program is easy, but building one that is effective is seriously hard! When faced with a seemingly insurmountable task, prioritization is vital. Investing time and money in the right place at the right time is the difference between success and being the next cyberbreach headline. Whether you are new to cybersecurity or an old hand, you may feel lost in the storm. If so, this talk is for you.

Privileged Domain Account Protection: How to Limit Credentials Exposure *Mike Pilkington*

In most enterprise networks, there are a number of privileged accounts that are used for maintaining the Windows domain, including accounts for domain administration, configuration management, patch management, vulnerability analysis, and incident response. In all of these cases, the accounts have the ability to log on to most, if not all, Windows hosts in the environment. These accounts therefore become high-value targets for attackers. In order to protect these privileged domain accounts, it is important to have a solid understanding of the various circumstances that can expose domain account credentials. In this presentation, Mike Pilkington discusses what you can and cannot do safely with domain accounts.

Card Fraud 101 *G. Mark Hardy*

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

Security Without Exception *Mark Williams*

As a risk analyst or manager, it is likely that your days are filled with requests for exceptions to policy to permit people to do things wrong. But there is a better way. Permitting exceptions may be a tool in developing a process life cycle, but it is also an easy way to avoid making decisions to upgrade or improve systems, policies or the risk management process. We are all faced daily with decisions on exceptions. This presentation will show you how continuous risk assessment and management can actually avoid the need for exceptions. By using a logical approach to risk identification, categorization, and decision-making, you too can do the "impossible" and say: NO EXCEPTIONS!

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

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

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

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

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

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

ONLINE TRAINING

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

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

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

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

FUTURE SANS TRAINING EVENTS

NORTHERN VIRGINIA
McLean 2016
McLean, VA | Feb 15-20

ICS Security
SUMMIT & TRAINING 2016
Orlando, FL | Feb 16-23

Anaheim 2016
Anaheim, CA | Feb 22-27

RSA Conference 2016
San Francisco, CA | Feb 28-29

Philadelphia 2016
Philadelphia, PA | Feb 29 - Mar 5

SANS 2016
Orlando, FL | Mar 12-21

Atlanta 2016
Atlanta, GA | Apr 4-9

NORTHERN VIRGINIA
Reston 2016
Reston, VA | Apr 4-9

Threat Hunting and Incident Response
SUMMIT & TRAINING 2016
New Orleans, LA | Apr 12-19

Pen Test Austin 2016
Austin, TX | Apr 18-23

Security West 2016
San Diego, CA | April 29 - May 6

Houston 2016
Houston, TX | May 9-14

Security Operations Center
SUMMIT & TRAINING 2016
Crystal City, VA | May 19-26

Information on all events can be found at
sans.org/security-training/by-location/all

SANS BALTIMORE SPRING 2016

Hotel Information

Training Campus

Sheraton Inner Harbor

300 South Charles Street
Baltimore, MD 21201
410-962-8300
sans.org/event/baltimore-spring-2016/location

The Sheraton Inner Harbor Hotel surrounds you with the best of Baltimore. It is steps away from the magnificent Inner Harbor and Oriole Park at Camden Yards. The hotel has everything you need for a comfortable and relaxing stay.

Special Hotel Rates Available

A special discounted rate of $205.00 S/D will be honored based on space availability.

Government per diem rooms will be made available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through April 7, 2016.

Top 5 reasons to stay at the Sheraton Inner Harbor

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 Sheraton Inner Harbor 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 Sheraton Inner Harbor that you won't want to miss!
5. Everything is in one convenient location!

SANS BALTIMORE SPRING 2016

Registration Information

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

Register online at sans.org/baltimore-spring-2016/courses

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

If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

Use code **EarlyBird16** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**3-16-16**	**$400.00**	**4-6-16**	**$200.00**

Some restrictions apply.

Group Savings (Applies to tuition only)

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

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

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

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by April 20, 2016 – processing fees may apply.

SANS Voucher Credit Program

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