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

SANS Minneapolis 2016

July 18-23

SANS OFFERS HANDS-ON, IMMERSION-STYLE

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

Protect your company and advance your career with information security training this summer from SANS!

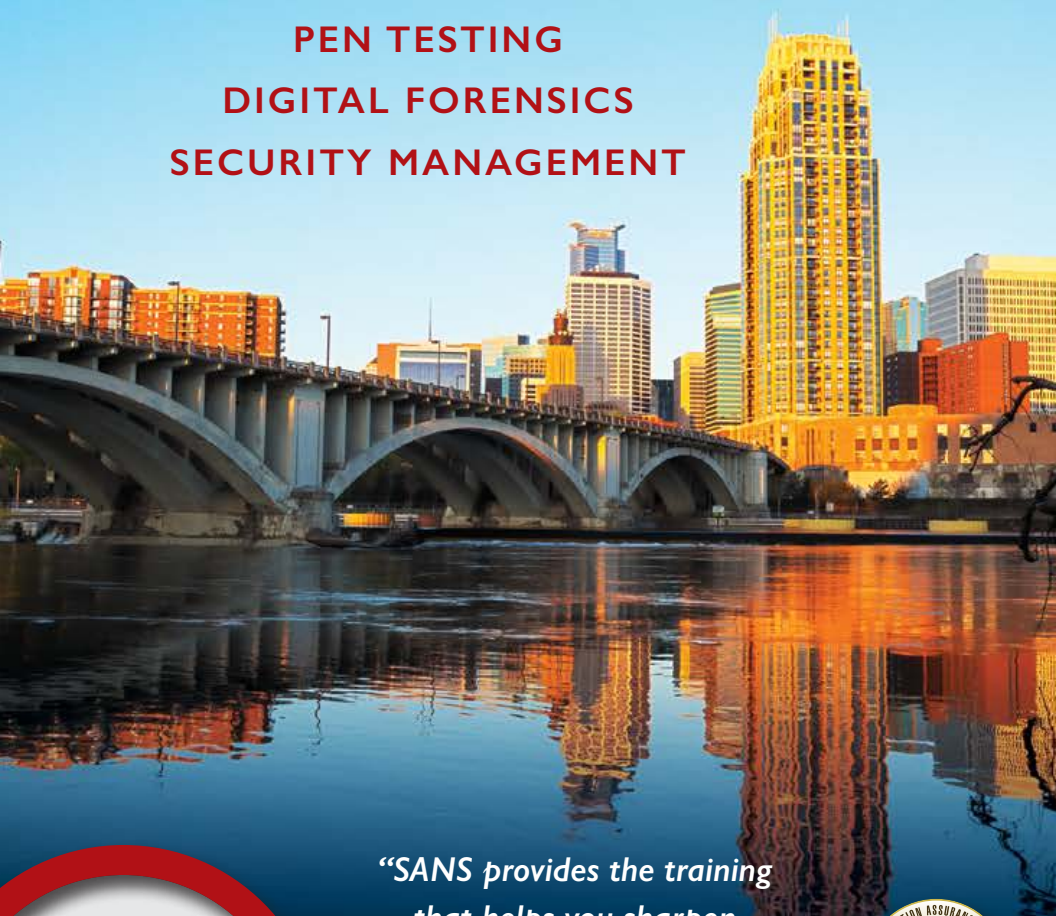
Eight courses on

CYBER DEFENSE

PEN TESTING

DIGITAL FORENSICS

SECURITY MANAGEMENT



"SANS provides the training that helps you sharpen your skill set or obtain a new set of skills that you can apply right away."

-Todd Russell, Magellan LP

GIAC-Approved Training

SAVE $400

by registering and paying early!

See page 13 for more details.

sans.org/minneapolis

SANS Instructors

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

Jason Fossen
Faculty Fellow

Paul A. Henry
Senior Instructor

Michael Murr
Principal Instructor

Chris Pizor
SANS Instructor

Bryan Simon
Certified Instructor

Johannes Ullrich
Senior Instructor

Jake Williams
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 9.

KEYNOTE: ***What's New for Security in Windows 10 and Server 2016?*** – Jason Fossen

InfoSec Potpourri – Jake Williams

Continuous Ownage: Why You Need Continuous Monitoring – Bryan Simon

Threat Intelligence: Neighborhood Watch for Your Networks – Matthew J. Harmon

Evolving Threats – Paul A. Henry

Be sure to register and pay by May 25th for a $400 tuition discount!

Courses-at-a-Glance

		MON 7-18	TUE 7-19	WED 7-20	THU 7-21	FRI 7-22	SAT 7-23
SEC401	Security Essentials Bootcamp Style	Page 1					
SEC503	Intrusion Detection In-Depth	Page 2					
SEC504	Hacker Tools, Techniques, Exploits and Incident Handling	Page 3					
SEC505	Securing Windows with PowerShell and the Critical Security Controls	Page 4					
SEC560	Network Penetration Testing and Ethical Hacking	Page 5					
FOR508	Advanced Digital Forensics and Incident Response	Page 6					
MGT414	SANS Training Program for CISSP® Certification	Page 7					
MGT514	IT Security Strategic Planning, Policy, and Leadership	Page 8					

SEC401:
Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Jul 18 - Sat, Jul 23
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Bryan Simon

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8140

Bundle OnDemand
with this course
sans.org/ondemand

"The success of this course rides on the delivery of the instructor. Bryan makes a 10-hour day go by very fast, and his teaching is stellar and his knowledge is amazing."
-Carroll Anne Smith, Analyst at DHS

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*!

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
- 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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

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

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

Security is all about making sure you focus on the right areas of defense. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you'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.

Bryan Simon *SANS Certified Instructor*

Bryan Simon is an internationally recognized expert in cybersecurity and has been working in the information technology and security field since 1991. Over the course of his career, he 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 cybersecurity issues. He has instructed individuals from the FBI, NATO, and the UN in matters of cybersecurity, on two continents. Bryan has specialized expertise in defensive and offensive capabilities. He has received recognition for his work in IT security, and was most recently profiled by McAfee (part of Intel Security) as an IT Hero. Bryan holds 11 GIAC certifications including GSEC, GCWN, GCIH, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, and GCUX. Bryan's scholastic achievements have resulted in the honor of sitting as a current member of the Advisory Board for the SANS Institute, and his acceptance into the prestigious SANS Cyber Guardian program. Bryan is a SANS instructor for SEC401, SEC501, SEC505, and SEC511. @BryanOnSecurity

SEC503:
Intrusion Detection In-Depth

SANS

Six-Day Program
Mon, Jul 18 - Sat, Jul 23
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor:
Johannes Ullrich, PhD

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8140

Bundle OnDemand
with this course
sans.org/ondemand

"This training allowed me to gain the knowledge to better defend systems and understand the underlying concept, communication, and means of analysis."
-Ryan Hunt, Alert Logic

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 analysts (all levels)
- Network engineers
- System, security, and network 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 will 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.

"The threats to our businesses and government agencies are ever increasing. We need to focus our IDS/IPS on our critical data and SEC503 helps us achieve that."
-Ed Brewster, SAIC, Inc.

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.

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

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, Jul 18 - Sat, Jul 23
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Chris Pizor

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8140

Bundle OnDemand
with this course
sans.org/ondemand

"SEC504 is practical and can be utilized immediately."
-Abraham Rivera, Morgan Stanley

Who Should Attend

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

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, exploiting, and defending systems. This 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.

"This course is foundational and core strength building in the most critical areas of incident handling. It reinforces and develops understanding around roles and TTPs of both adversary and defender." -Araceli Ari Gomes, Dell Secureworks

Chris Pizor *SANS Instructor*

Chris Pizor is a civilian employee working for the U.S. Air Force as the lead curriculum designer for cyber warfare operations training. Chris served on active duty in the USAF as a Network Intelligence Analyst before retiring in 2010. He was part of the initial cadre of the NSA Threat Operations Center and helped develop tactics to discover and eradicate intrusions into U.S. government systems. Chris has worked for 20 years in the intelligence community, with 12 years focused on cybersecurity. Over the course of his active duty career, Chris received multiple individual and team awards. Chris is passionate about security and helping others advance their security knowledge. He is continuously researching and refining his own skills so he can prepare U.S. airman and other professionals to defend their vital networks and critical infrastructure. Chris earned a Bachelor's Degree in Intelligence Studies and Information Operations, and is pursuing a Master's Degree in cybersecurity. He holds the GSEC, GCIA, GCIH, GPEN, GXPN, and GCFA certifications.

SEC505:

Securing Windows with PowerShell and the Critical Security Controls

SANS

Six-Day Program
Mon, Jul 18 - Sat, Jul 23
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jason Fossen

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"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

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

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

For the assume breach mindset, we must carefully delegate *limited* administrative powers so that the compromise of one administrator account is not a total catastrophe. Managing administrative privileges is a tough problem, so this course devotes an entire day to just this one critical task (in fact, this is one of the top five Critical Security Controls).

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

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

If you are an IT manager or CIO, the aim is for this course to pay for itself 10 times over within two years. Automation isn't just good for SecOps/DevOps; it saves money, too. And PowerShell is also just plain fun!

The Critical Security Controls are not just for auditors and managers. This course is designed for systems engineers, security architects, and the Security Operations team. The focus of the course is on how to automate those Windows-related Critical Security Controls that are the most effective, but also the most difficult to implement, especially in large environments.

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

Who Should Attend

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

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

SEC560:
Network Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, Jul 18 - Sat, Jul 23
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Michael Murr

giac.org

sans.edu

sans.org/cyber-guardian

Bundle OnDemand
with this course
sans.org/ondemand

"SEC560 has helped me have a more in-depth knowledge of penetration testing. The instructor's flow and method made it easier to understand."
-Mithra Ravendran, BAE Systems Applied Intel

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

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

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

Who Should Attend

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

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

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

This course equips security organizations with comprehensive penetration testing and ethical hacking know-how.

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

Michael Murr *SANS Principal Instructor*

Michael has been a forensic analyst with Code-X Technologies for over five years. He has 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 (Computer Forensics, Investigation, and 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. Michael holds the GCIH, GCFA, and GREM certifications and has a degree in computer science from California State University at Channel Islands. Michael also blogs about digital forensics on his forensic computing blog (www.forensicblog.org). @mikemurr

FOR508:

Advanced Digital Forensics and Incident Response

SANS

Six-Day Program
Mon, Jul 18 - Sat, Jul 23
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jake Williams

DFIR
digital-forensics.sans.org

GCFA
giac.org

SANS Technology Institute
sans.edu

sans.org/cyber-guardian

sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

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

- How the breach occurred
- How systems were affected and compromised
- What attackers took or changed
- How to contain and mitigate the incident

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

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.

"The instructor was beyond qualified and excellent! He took the time to answer questions and help the students, and the exercises flowed very well with the instruction." -Wilfredo Hernandez, FL Dept. of Law Enforcement

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

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

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

Who Should Attend

- Incident response team leaders and members
- Security Operations Center personnel and information security practitioners
- Experienced digital forensic analysts
- System administrators
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- SANS FOR408 and SEC504 graduates

Jake Williams *SANS Certified Instructor*

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

MGT414:

SANS Training Program for CISSP® Certification

SANS

Six-Day Program
Mon, Jul 18 - Sat, Jul 23
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: Paul A. Henry

giac.org

sans.org/8140

Bundle OnDemand
WITH THIS COURSE
sans.org/ondemand

"This course has been fantastic in terms of boiling down years of IT security trends and best practices into a week of learning."
-Eric Pavlov, InnoMark

MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that has been specifically updated to prepare you to pass the 2015 version of the CISSP® exam.

Course authors Eric Conrad and Seth Misenar have revised MGT414 to take into account the 2015 updates to the CISSP® exam and prepare students to navigate all types of questions included in the new version.

MGT414 focuses solely on the eight 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® eight domains
- Security professionals and managers looking for practical ways to apply the eight domains of knowledge to their current activities

You Will Be Able To:

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

"I would recommend this class for anyone wanting to get a CISSP. I feel it gave me the tools to be confident to take the test."
-Matthew Trummer, Lincoln Electric Systems

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.

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

Paul A. Henry *SANS Senior Instructor*
Paul Henry is one of the foremost global information security and computer forensic experts in the world 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 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 (United States), and both government as well as telecommunications projects throughout Southeast Asia. @phenrycissp

MGT514:

IT Security Strategic Planning, Policy, and Leadership

SANS

Five-Day Program
Mon, Jul 18 - Fri, Jul 22
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: Mark Williams

SANS Technology Institute
sans.edu

Bundle OnDemand
with this course
sans.org/ondemand

"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

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:

Who Should Attend

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

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.

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

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

Windows 8 was a flop, worse than Vista, so will Windows 10 be successful? The return of the Start Menu, touch screen integration, the faster Edge browser, and Cortana should make Windows 10 popular with users. Windows 10 also includes significant changes for security and manageability in large organizations, such as "Windows as a Service" rolling updates and deeper integration with Azure Active Directory. In this lively talk, Jason Fossen, author of the Securing Windows (SEC505) course at SANS, will lay out what to love and fear in Windows 10 and Windows Server 2016. We will also talk about some of the epic changes going on at Microsoft, now that CEO Steve Ballmer is gone. Is it really a new era for Microsoft? Come join the presentation and see what Microsoft is betting its future on!

InfoSec Potpourri *– Jake Williams*

At the time this went to print, Jake, like everyone in the industry, lacked a crystal ball to know what would be hot, hip, and happening in InfoSec. But odds are good that something completely awesome has happened in the last few weeks that we can get together and talk about in depth. And if nothing interesting is happening in the field, Jake and his company are constantly doing exciting research in DFIR and offensive methodologies that he would love to share with you. One thing is for sure, you won't be bored. So bring an adult beverage and come unwind after a long day of class and learn something hip and new.

Continuous Ownage: Why You Need Continuous Monitoring

– Bryan Simon

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 explain 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 the new course designed by Seth Misenar and Eric Conrad: SANS SEC511: Continuous Monitoring and Security Operations.

Threat Intelligence: Neighborhood Watch for Your Networks

– Matthew J. Harmon

Matthew will dive into threat intelligence and show participants how to use high-confidence indicators of compromise to detect threats and prevent them from adversely affecting their network. This will help peers prevent the same attacks through information sharing.

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 on attempting to outwit attackers' delivery methods. This leaves us woefully exposed and according to a recent Data Breach Report has resulted in 3,765 incidents, 806 million records exposed, and $157 billion in data breach costs in only the past six years. This presentation will highlight recent/current developments in the evolution of both attacks and defenses.

Build Your Best Career

WITH

SANS

Add an

OnDemand Bundle & GIAC Certification Attempt*

to your course within seven days of this event for just $659 each.

SPECIAL PRICING

OnDemand Bundle

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

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

-Robert Jones, Team Jones, Inc.

GIAC Certification

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

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

-Christina Ford, Department of Commerce

MORE INFORMATION

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

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

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

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

Baltimore Spring 2016
Baltimore, MD | May 9-14

Houston 2016
Houston, TX | May 9-14

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

SANSFIRE 2016
Washington, DC | Jun 11-18

Digital Forensics & Incident Response
SUMMIT & TRAINING 2016
Austin, TX | Jun 23-30

Salt Lake City 2016
Salt Lake City, UT | Jun 27 - Jul 2

Rocky Mountain 2016
Denver, CO | Jul 11-16

San Antonio 2016
San Antonio, TX | Jul 18-23

ICS Security & Training – Houston 2016
Houston, TX | Jul 25-30

San Jose 2016
San Jose, CA | Jul 25-30

Boston 2016
Boston, MA | Aug 1-6

Security Awareness
SUMMIT & TRAINING 2016
San Francisco, CA | Aug 1-10

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

SANS MINNEAPOLIS 2016

Hotel Information

Training Campus
Hilton Minneapolis

1001 Marquette Avenue South
Minneapolis, MN 55403
612-376-1000
sans.org/event/minneapolis-2016/location

This 25-story, Victorian-style brick high-rise boasts a fantastic location in the center of Minneapolis' financial center and is within minutes of many attractions. Conveniently connected to the Minneapolis Convention Center, the hotel is a world-class convention and leisure destination located near theaters, shops, restaurants and other cultural attractions, and is just steps from Target Center and Target Field. The Mall of America, Minnesota Zoo, and TCF Bank Stadium are just a short drive away.

Special Hotel Rates Available

A special discounted rate of $189.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through 5:00pm CST on June 24, 2016.

Top 5 reasons to stay at Hilton Minneapolis

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

SANS MINNEAPOLIS 2016

Registration Information

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

Register online at sans.org/minneapolis-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	**5-25-16**	**$400.00**	**6-15-16**	**$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 June 29, 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

Open a **SANS Portal Account** today to enjoy these FREE resources:

WEBCASTS

Ask The Expert Webcasts – SANS experts bring current and timely information on relevant topics in IT Security.

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

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

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

NEWSLETTERS

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

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

@RISK: The Consensus Security Alert – A reliable weekly summary of (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) how recent attacks worked, and (4) other valuable data

OTHER FREE RESOURCES

- InfoSec Reading Room
- Top 25 Software Errors
- 20 Critical Controls
- Security Policies
- Intrusion Detection FAQ
- Tip of the Day
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

sans.org/security-resources