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

SANS NORTHERN VIRGINIA Reston 2016

Reston, VA April 4-9

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

- Cyber Threat Intelligence – **NEW!**
- Network Penetration Testing and Ethical Hacking – **NEW!**
- Security Essentials Bootcamp Style
- Continuous Monitoring and Security Operations
- Advanced Digital Forensics and Incident Response
- Intrusion Detection In-Depth
- Defending Web Applications Security Essentials
- Reverse-Engineering Malware: Malware Analysis Tools and Techniques
- CyberCity Hands-on Kinetic Cyber Range Exercise

"SANS was excellent! Not only were there good instructors, but this was a great networking experience."

-Leslie Morse, Department of the Treasury

GIAC Approved Training

SAVE $400

by registering and paying early!

See page 13 for more details.

sans.org/reston-2016

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 become SANS Certified Instructors. This guarantees that what you learn in class will be up-to-date and relevant to your job. The SANS Reston 2016 line-up of instructors includes:

Dr. Eric Cole
Faculty Fellow

Eric Conrad
Senior Instructor

Adrien de Beaupre
Certified Instructor

Kevin Fiscus
Certified Instructor

Tim Medin
Certified Instructor

Anuj Soni
Certified Instructor

Alissa Torres
Certified Instructor

Dr. Johannes Ullrich
Senoir Instructor

Jake Williams
Certified Instructor

Evening Bonus Sessions

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

Why Your Incident Response Plan Sucks And What To Do About It – Jake Williams

Complete App Pwnage with multi-POST XSRF – Adrien de Beaupre

DLP FAIL!!! Using Encoding, Steganography, and Covert Channels to Evade DLP and Other Critical Controls – Kevin Fiscus

Under the Dome with Windows 10 – Alissa Torres

Be sure to register and pay by Feb 10th for a $400 tuition discount!

Courses-at-a-Glance

	MON 4-4	TUE 4-5	WED 4-6	THU 4-7	FRI 4-8	SAT 4-9
SEC401 Security Essentials Bootcamp Style	Page 2					
SEC503 Intrusion Detection In-Depth	Page 3					
SEC511 Continuous Monitoring and Security Operations	Page 4					
SEC560 Network Penetration Testing and Ethical Hacking *NEW!*	Page 5					
SEC562 CyberCity Hands-on Kinetic Cyber Range Exercise	Page 6					
FOR508 Advanced Digital Forensics and Incident Response	Page 7					
FOR578 Cyber Threat Intelligence *NEW!*	Page 8					
FOR610 REM: Malware Analysis Tools and Techniques	Page 9					
DEV522 Defending Web Applications Security Essentials	Page 10					

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.

SEC401:
Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Apr 4 - Sat, Apr 9
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Dr. Eric Cole

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

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

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

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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

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

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

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

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks

"Eric did an awesome job explaining Diffie-Hellman key exchange, and overall, it was the best quality of instruction ever!"
-Kevin K, U.S. Army

Dr. Eric Cole *SANS Faculty Fellow*

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

SEC503:
Intrusion Detection In-Depth

SANS

Six-Day Program
Mon, Apr 4 - Sat, Apr 9
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Kevin Fiscus

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

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.

Preserving the security of your site in today's threat environment is more challenging than ever before. The security landscape is continually changing from what was once only perimeter protection to protecting exposed and mobile systems that are almost always connected and often vulnerable. Security-savvy employees who can help detect and prevent intrusions are therefore in great demand. Our goal in **SEC503: Intrusion Detection In-Depth** is to acquaint you with the core knowledge, tools, and techniques to defend your networks. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

Bundle OnDemand
with this course
sans.org/ondemand

"The material was presented in a way that facilitates understanding rather than just memorization."
-Edward Dunnahoe, CRIF Lending Solutions

"Excellent exposure and training for all skill levels. Thanks for the in-depth analysis combined with real-life scenarios."
-Art Mason, Rackspace ISOC

Kevin Fiscus *SANS Certified Instructor*

Kevin Fiscus is the founder of and lead consultant for Cyber Defense Advisors where he performs security and risk assessments, vulnerability and penetration testing, security program design, policy development and security awareness with a focus on serving the needs of small and mid-sized organizations. Kevin has over 20 years of IT experience and has focused exclusively for the past 12 years on information security. Kevin currently holds the CISA, GPEN, GREM, GMOB, GCED, GCFA-Gold, GCIA-Gold, GCIH, GAWN, GPPA, GCWN, GCSC-Gold, GSEC, SCSA, RCSE, and SnortCP certifications and is proud to have earned the top information security certification in the industry, the GIAC Security Expert. Kevin has also achieved the distinctive title of SANS Cyber Guardian for both red team and blue team. @kevinbfiscus

SEC511:

Continuous Monitoring and Security Operations

New in 2016 to Enhance Your Skills — Extended-Hours Bootcamp

SANS

Six-Day Program
Mon, Apr 4 - Sat, Apr 9
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Laptop Required
Instructor: Eric Conrad

- 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

"SEC511 is a practical approach to continue security monitoring using free and open-source tools either alone or in conjunction with existing tools and devices. This course is a must for anyone responsible for monitoring networks for security."
-Brad Milhorn, CompuCom

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.

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)

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.

GMON
giac.org

SANS Technology Institute
sans.edu

Bundle OnDemand
with this course
sans.org/ondemand

Eric Conrad *SANS Senior Instructor*

Eric Conrad is the lead author of SANS MGT414: SANS Training Program for CISSP® Certification, and coauthor of both SANS SEC511: Continuous Monitoring and Security Operations and SANS SEC542: Web App Penetration Testing and Ethical Hacking. He is also the lead author of the *CISSP Study Guide*, and the *Eleventh Hour CISSP: Study Guide*. Eric's career began in 1991 as a UNIX systems administrator for a small oceanographic communications company. He gained information security experience in a variety of industries, including research, education, power, Internet, and healthcare. He is now CTO of Backshore Communications, a company focusing on hunt teaming, intrusion detection, incident handling, and penetration testing. He is a graduate of the SANS Technology Institute with a master of science degree in information security engineering. In addition to the CISSP, he holds the prestigious GIAC Security Expert (GSE) certification as well as the GIAC GPEN, GCIH, GCIA, GCFA, GAWN, and GSEC certifications. Eric also blogs about information security at www.ericconrad.com. @eric_conrad

SEC560:
Network Penetration Testing and Ethical Hacking

NEW

SANS

Six-Day Program
Mon, Apr 4 - Sat, Apr 9
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Adrien de Beaupre

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

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

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.

Equipping 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.

giac.org

sans.edu

sans.org/cyber-guardian

Bundle OnDemand
with this course
sans.org/ondemand

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

"This course has a direct correlation to my job duties. The insight, real-world references, and the use of various tools will make my job a lot easier. You will learn skills and ways your systems are vulnerable."
-Roland T., USAF

Adrien de Beaupre *SANS Certified Instructor*

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

SEC562:

CyberCity Hands-on Kinetic Cyber Range Exercise

SANS

Six-Day Program
Mon, Apr 4 - Sat, Apr 9
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Tim Medin

Computers, networks, and programmable logic controllers operate most of the physical infrastructure of our modern world, ranging from electrical power grids, water systems, and traffic systems all the way down to HVAC systems and industrial automation. Increasingly, security professionals need the skills to assess and defend this important infrastructure. In this innovative and cutting-edge course based on the SANS CyberCity kinetic range, you will learn how to analyze and assess the security of control systems and related infrastructure, finding vulnerabilities that could result in significant kinetic impact.

Who Should Attend

- Red and blue team members
- Cyber warriors
- Incident handlers
- Penetration testers
- Ethical hackers
- Other security personnel who are first responders when systems come under attack.

"This course is the greatest! I've taken over 14 SANS training courses and have been been waiting for this type of course. I would like to take this course again in a few years."
-Masashi Fujiwara, Hitachi, LTD

"Tim is a great instructor, I really enjoyed the live demos and the style of his teaching. He really keeps you engaged."
-Drew Davis, Rook Security

NetWars CyberCity

NetWars CyberCity, our most in-depth and ambitious offering, is designed to teach warriors and infosec pros that cyber action can have significant kinetic impact in the physical world. As computer technology, networks, and industrial control systems permeate nearly every aspect of modern life, military, government, and commercial organizations are realizing an increasing need for skilled defenders of critical infrastructure. We engineered and built CyberCity to help organizations grow these capabilities in their teams.

CyberCity is a 1:87 scale miniaturized physical city that features SCADA-controlled electrical power distribution, as well as water, transit, hospital, bank, retail, and residential infrastructure. CyberCity engages participants to defend the city's components from terrorist cyber attacks, as well as to utilize offensive tactics to retake or maintain control of critical assets.

The main objectives of CyberCity are to:

- Teach cyber warriors and their leaders the potential kinetic impacts of cyber attacks
- Provide a hands-on, realistic kinetic cyber range with engaging missions to conduct defensive and offensive actions
- Develop capabilities for defending and controlling critical infrastructure components to mitigate or respond to cyber attacks
- Demonstrate to senior leaders and planners the potential impacts of cyber attacks and cyber warfare

Tim Medin *SANS Certified Instructor*

Tim Medin is a senior technical analyst at Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through the course of his career, Tim has performed penetration tests on a wide range of organizations and technologies. Prior to Counter Hack, Tim was a Senior Security Consultant for FishNet Security where the majority of his focus was on penetration testing. He gained information security experience in a variety of industries including previous positions in control systems, higher education, financial services, and manufacturing. Tim regularly contributes to the SANS Penetration Testing Blog (pen-testing.sans.org/blog/) and the Command Line Kung Fu Blog (blog.commandlinekungfu.com). He is also project lead for the Laudanum Project, a collection of injectable scripts designed to be used in penetration testing. @timmedin

FOR508:

Advanced Digital Forensics and Incident Response

SANS

Six-Day Program
Mon, Apr 4 - Sat, Apr 9
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Alissa Torres

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

digital-forensics.sans.org

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

"Wow! What a course, and one of the best I have attended in my learning career."
-Srinath Kannan, Accenture

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.

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

giac.org

sans.edu

sans.org/
cyber-guardian

sans.org/8570

Bundle OnDemand
with this course
sans.org/ondemand

Alissa Torres *SANS Certified Instructor*

Alissa Torres specializes in teaching advanced computer forensics and incident response. Her industry experience includes serving in the trenches as part of the Mandiant Computer Incident Response Team (MCIRT) as an incident handler and working on a internal security team as a digital forensic investigator. She has extensive experience in information security, spanning government, academic, and corporate environments and holds a Bachelors degree from the University of Virginia and a Masters from the University of Maryland in Information Technology. Alissa has taught at the Defense Cyber Investigations Training Academy (DCITA), delivering incident response and network basics to security professionals entering the forensics community. She has presented at various industry conferences and numerous B-Sides events. In addition to being a GIAC Certified Forensic Analyst (GCFA), she holds the GCFE, GPEN, CISSP, EnCE, CFCE, MCT, and CTT+ certifications. @sibertor

FOR578:
Cyber Threat Intelligence

NEW

SANS

Five-Day Program
Mon, Apr 4 - Fri, Apr 8
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Jake Williams
▸ OnDemand Bundle

DFIR
digital-forensics.sans.org

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 detect, scope, and select resilient courses of action in response to such intrusions and data breaches.

THERE IS NO TEACHER BUT THE ENEMY!

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

"Fantastic class! I love the way the terminology was covered. I will be making index cards to ensure I have them memorized."
-Nate DeWitt, eBay, Inc.

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

FOR610:

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

SANS

Six-Day Program
Mon, Apr 4 - Sat, Apr 9
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Anuj Soni

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

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

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

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

You will also learn how to analyze malicious documents that take the form of Microsoft Office and Adobe PDF files. Such documents act as a common infection vector and may need to be examined when dealing with large-scale infections as well as targeted attacks. The course also explores memory forensics approaches to examining malicious software, especially useful if it exhibits rootkit characteristics.

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

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

Who Should Attend

- Individuals who have dealt with incidents involving malware and want to learn how to understand key aspects of malicious programs
- Technologists who have informally experimented with aspects of malware analysis prior to the course and are looking to formalize and expand their expertise in this area
- Forensic investigators and IT practitioners looking to expand their skillsets and learn how to play a pivotal role in the incident response process

"Wow! What a course, and one of the best I have attended in my learning career."

-Srinath Kannan, Accenture

GREM
giac.org

SANS Technology Institute
sans.edu

Bundle OnDemand
with this course
sans.org/ondemand

Anuj Soni *SANS Certified Instructor*

Anuj Soni is a Senior Incident Responder at Booz Allen Hamilton, where he leads forensic, malware, and network analysis efforts to investigate security incidents. Since entering the information security field in 2005, Anuj has performed numerous intrusion investigations to help government and commercial clients mitigate attacks against the enterprise. His malware hunt skills and technical analysis abilities have resulted in the successful identification, containment, and remediation of multiple threat actor groups. Anuj has analyzed over 400 malware samples to assess function, purpose, and impact, and his recommendations have improved the security posture of the organizations he supports. @asoni

DEV522:

Defending Web Applications Security Essentials

SANS

Six-Day Program
Mon, Apr 4 - Sat, Apr 9
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor:
Johannes Ullrich, Ph.D.

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

This is the course to take if you have to defend web applications!

The quantity and importance of data entrusted to web applications is growing, and defenders need to learn how to secure them. Traditional network defenses, such as firewalls, fail to secure web applications. DEV522 covers the OWASP Top 10 Risks and will help you better understand web application vulnerabilities, thus enabling you to properly defend your organization's web assets.

Mitigation strategies from an infrastructure, architecture, and coding perspective will be discussed alongside real-world implementations that really work. The testing aspect of vulnerabilities will also be covered so you can ensure your application is tested for the vulnerabilities discussed in class.

Who Should Attend

- Application developers
- Application security analysts or managers
- Application architects
- Penetration testers who are interested in learning about defensive strategies
- Security professionals who are interested in learning about web application security
- Auditors who need to understand defensive mechanisms in web applications
- Employees of PCI-compliant organizations who need to be trained to comply with PCI requirements

To maximize the benefit for a wider range of audiences, the discussions in this course will be programming language agnostic. Focus will be maintained on security strategies rather than coding-level implementation.

DEV522: Defending Web Applications Security Essentials is intended for anyone tasked with implementing, managing, or protecting web applications. It is particularly well suited for application security analysts, developers, application architects, pen testers, and auditors who are interested in recommending proper mitigations to web security issues and for infrastructure security professionals who have an interest in better defending their web applications.

The course will also cover additional issues the authors have found to be important in their day-to-day web application development practices. The topics that will be covered include:

- Infrastructure security
- Server configuration
- Authentication mechanisms
- Application language configuration
- Application coding errors like SQL Injection and cross-site scripting
- Cross-site request forging
- Authentication bypass
- Web services and related flaws
- Web 2.0 and its use of web services
- XPATH and XQUERY languages and injection
- Business logic flaws
- Protective HTTP headers

The course will make heavy use of hands-on exercises and will conclude with a large defensive exercise, reinforcing the lessons learned throughout the week.

GWEB
giac.org

SANS Technology Institute
sans.edu

Bundle OnDemand
with this course
sans.org/ondemand

"This training has been very helpful in making me more aware and have a better understanding of vulnerabilities and what can be done to minimize them in future development projects."
-Lerma Winchell, VyStar Credit Union

"SANS has always provided exceptional training using solid coursework to labs, ratios, and formats."
-Darrell Marsh, ATFS, LLC

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 working for 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 located in Jacksonville, Florida. His daily podcast summarizes current security news in a concise format. @johullrich

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.

Why Your Incident Response Plan Sucks And What To Do About It

Jake Williams

If you have an incident response (IR) plan at all, you're already ahead of the pack. But most IR plans leave out critical points that need to be covered. A good IR plan is like a good mosquito net – you hope you don't need it but you always have it there to protect you just in case. Just like a mosquito net full of holes can't do the job, an IR plan full of holes can't do the job either. In this talk, Jake will share his experience from the field on where he sees most IR plans fall short so your organization can be better prepared when the inevitable breach comes.

Complete App Pwnage with multi-POST XSRF

Adrien de Beaupre

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

DLP FAIL!!! Using Encoding, Steganography, and Covert Channels to Evade DLP and Other Critical Controls

Kevin Fiscus

It's all about the information! Two decades after the movie Sneakers, the quote remains as relevant, if not more so. The fact that someone hacks into an environment is interesting but not that relevant. What is important is what happens after the compromise. If the data is destroyed or modified, organizations are negatively impacted but the benefits to an attacker for destruction or alteration are somewhat limited. Stealing information however, is highly profitable. Identity theft, espionage, and financial attacks involve the exfiltration of sensitive data. As a result, organizations deploy tools to detect and/or stop that data exfiltration. While these tools can be extremely valuable, many have serious weaknesses; attackers can encode, hide, or obfuscate the data, or can use secret communication channels. This session will talk about and demonstrate a range of these methods.

Under the Dome with Windows 10

Alissa Torres

Windows 10 brings some game changers to memory forensic investigations. It is only a matter of time before this OS version makes up the majority of your casework. Will you have the skills and know-how required to get the job done? AND will your memory forensic tools keep up? Come hear about the Windows 10 memory advances that very well may change your IR procedures.

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 East 2016
New Orleans, LA | Jan 25-30

Cyber Threat Intelligence
SUMMIT & TRAINING 2016
Alexandria, VA | Feb 3-10

Scottsdale 2016
Scottsdale, AZ | Feb 8-13

McLean 2016
McLean, VA | Feb 15-20

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

Anaheim 2016
Anaheim, CA | Feb 22-27

Philadelphia 2016
Philadelphia, PA | Feb 29 - Mar 5

SANS 2016
Orlando, FL | Mar 12-21

Atlanta 2016
Atlanta, GA | Apr 4-9

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

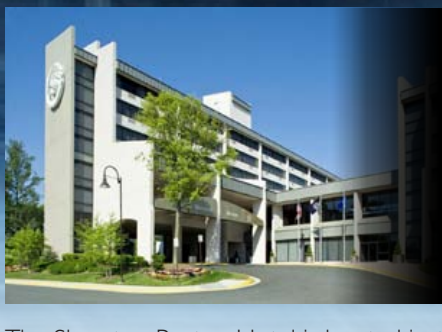
Pen Test Austin 2016
Austin, TX | Apr 18-23

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

Baltimore Spring 2016
Baltimore, MD | May 9-14

Houston 2016
Houston, TX | May 9-14

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



SANS RESTON 2016

Hotel Information

Training Campus
Sheraton Reston Hotel

11810 Sunrise Valley Drive
Reston, VA 20191
703-620-9000
sans.org/event/reston-2016/location

The Sheraton Reston Hotel is located just moments from Washington Dulles International Airport and a short drive to Washington, D.C. The hotel is family- and pet-friendly, dedicated to green practices and assuring your stay includes all the familiar comforts of home. Whatever your plans are, you'll find a feeling of welcome unlike any other at the Sheraton Reston Hotel.

Special Hotel Rates Available

A special discounted rate of $159.00 S/D will be honored based on space availability.
Should the prevailing Government per diem rate fall below the SANS group rate, 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 March 17, 2016.

Top 5 reasons to stay at the Sheraton Reston Hotel

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

SANS RESTON 2016

Registration Information

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

Register online at sans.org/reston-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	**2-10-16**	**$400.00**	**3-2-16**	**$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 March 16, 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