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

SANS Boston 2017

August 7-12

PROTECT YOUR COMPANY AND ADVANCE YOUR CAREER
WITH HANDS-ON, IMMERSION-STYLE

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

10 courses in:

- CYBER DEFENSE
- PENETRATION TESTING
- ETHICAL HACKING
- DETECTION & MONITORING
- CYBER THREAT INTELLIGENCE
- MANAGEMENT

GIAC CERTIFICATIONS
GIAC-Approved Training

> "The combination of coursework relevant to the real world, exceptionally knowledgeable instructors, and networking opportunities with others in the field really helped me get a grasp on the tools and skills I need to stay on top of security threats and trends."
>
> -Dustin Lee, Centene

SAVE $400
Register and pay by June 14th – Use code **EarlyBird17**

Core NETWARS EXPERIENCE

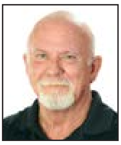
www.sans.org/boston

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 Boston 2017 lineup of instructors includes:

Eric Conrad
Senior Instructor
@eric_conrad

Adrien de Beaupre
Certified Instructor
@adriendb



Paul A. Henry
Senior Instructor
@phenrycissp

David Hoelzer
Faculty Fellow
@it_audit

Micah Hoffman
Certified Instructor
@WebBreacher

Frank Kim
Certified Instructor
@fykim

Rob Lee
Faculty Fellow
@robtlee
@sansforensics

Robert M. Lee
Certified Instructor
@RobertMLee

David R. Miller
Certified Instructor
@DRM_CyberDude

Bryan Simon
Certified Instructor
@BryanOnSecurity

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 12.

KEYNOTE: ***Exploitation Throughout the Ages: Stacks, Canaries, ASLR, ROP and More!***
David Hoelzer

HTTPDeux – Adrien de Beaupre

Collecting and Exploiting Your "Private" Internet Data Using OSINT
Micah Hoffman

Quality Not Quantity: Continuous Monitoring's Deadliest Events – Eric Conrad

Birds of a Feather or... – Mark Williams

Save $400 when you register and pay by June 14th using code EarlyBird17

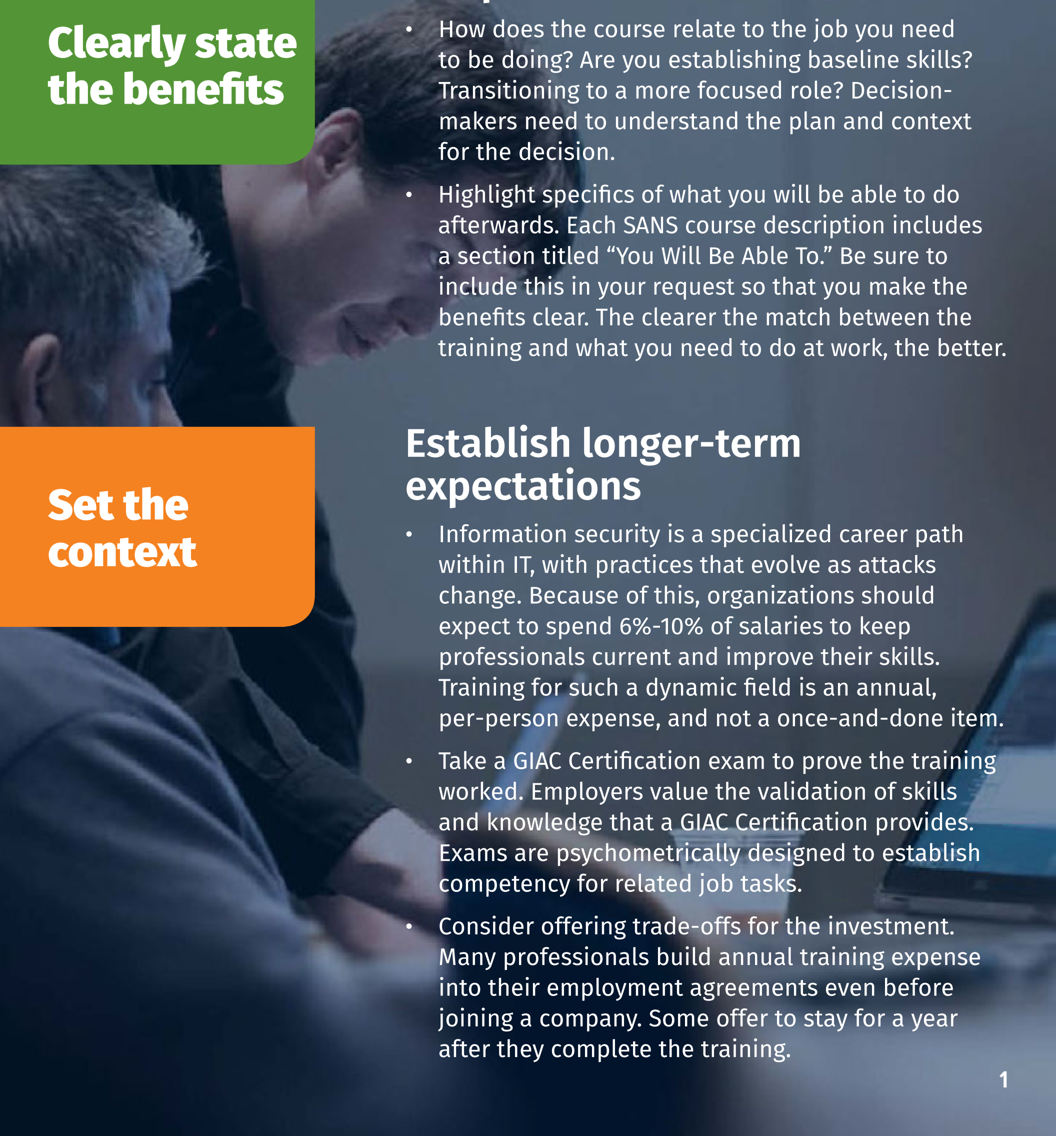
Courses at a Glance

		MON 8-7	TUE 8-8	WED 8-9	THU 8-10	FRI 8-11	SAT 8-12
SEC401	Security Essentials Bootcamp Style	Page 2	■	■	■	■	■
SEC501	Advanced Security Essentials – Enterprise Defender	Page 3	■	■	■	■	■
SEC503	Intrusion Detection In-Depth	Page 4	■	■	■	■	■
SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling	Page 5	■	■	■	■	■
SEC511	Continuous Monitoring and Security Operations	Page 6	■	■	■	■	■
SEC542	Web App Penetration Testing and Ethical Hacking	Page 7	■	■	■	■	■
FOR500	Windows Forensic Analysis (FORMERLY FOR408)	Page 8	■	■	■	■	■
FOR578	Cyber Threat Intelligence	Page 9	■	■	■	■	
MGT414	SANS Training Program for CISSP® Certification	Page 10	■	■	■	■	■
MGT514	IT Security Strategic Planning, Policy, and Leadership	Page 11	■	■	■	■	

Register today for SANS Boston 2017!
www.sans.org/boston

@SANSInstitute
Join the conversation:
#SANSBoston

Securing **Approval** and **Budget** for Training



Packaging matters

Write a formal request

- All organizations are different, but because training requires a significant investment of both time and money, most successful training requests are made via a written document (short memo and/or a few powerpoint slides) that justifies the need and benefit. Most managers will respect and value the effort.
- Provide all the necessary information in one place. In addition to your request, provide all the right context by including the summary pages on Why SANS?, the Training Roadmap, the instructor bio, and additional benefits available at our live events or online.

Clearly state the benefits

Be specific

- How does the course relate to the job you need to be doing? Are you establishing baseline skills? Transitioning to a more focused role? Decision-makers need to understand the plan and context for the decision.
- Highlight specifics of what you will be able to do afterwards. Each SANS course description includes a section titled “You Will Be Able To.” Be sure to include this in your request so that you make the benefits clear. The clearer the match between the training and what you need to do at work, the better.

Set the context

Establish longer-term expectations

- Information security is a specialized career path within IT, with practices that evolve as attacks change. Because of this, organizations should expect to spend 6%-10% of salaries to keep professionals current and improve their skills. Training for such a dynamic field is an annual, per-person expense, and not a once-and-done item.
- Take a GIAC Certification exam to prove the training worked. Employers value the validation of skills and knowledge that a GIAC Certification provides. Exams are psychometrically designed to establish competency for related job tasks.
- Consider offering trade-offs for the investment. Many professionals build annual training expense into their employment agreements even before joining a company. Some offer to stay for a year after they complete the training.

SEC401

GSEC Certification
Security Essentials
www.giac.org/gsec

Security Essentials Bootcamp Style

Six-Day Program
Mon, Aug 7 - Sat, Aug 12
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Bryan Simon

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks
- Administrators responsible for building and maintaining systems that are being targeted by attackers
- Forensic specialists, penetration testers, and auditors who need a solid foundation of security principles to be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

> "This training answers the 'why' of my work practices, and asks the 'why not' for the practices my company doesn't follow."
>
> -Thomas Petro, Southern California Edison

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

STOP and ask yourself the following questions:

- **Do you fully understand why some organizations get compromised and others do not?**
- **If there were compromised systems on your network, are you confident you would be able to find them?**
- **Do you know the effectiveness of each security device and are you certain they are all configured correctly?**
- **Are proper security metrics set up and communicated to your executives to drive security decisions?**

If you do not know the answers to these questions, SEC401 will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

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. Our course will show you how to prevent your organization's security problems from being headline news in the *Wall Street Journal*!

Prevention Is Ideal but Detection Is a Must

With the rise in 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:

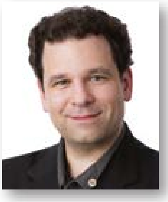
- **What is the risk?**
- **Is it the highest priority risk?**
- **What is the most cost-effective way to reduce the risk?**

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 will need if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security instructors in the industry.

SANS Technology Institute
www.sans.edu

www.sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand



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, Bryan has held various technical and managerial positions in the education, environmental, accounting, and financial services sectors. Bryan speaks on a regular basis at international conferences and with the press on matters of cybersecurity. He has instructed individuals from organizations such as the FBI, NATO, and the UN in matters of cybersecurity on two continents. Bryan has specialized expertise in defensive and offensive capabilities. 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 12 GIAC certifications including the GSEC, GCWN, GCIH, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, GCUX, and GISF. 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**

SEC501

GCED Certification
Certified Enterprise Defender
www.giac.org/gced

Advanced Security Essentials – Enterprise Defender

Six-Day Program
Mon, Aug 7 - Sat, Aug 12
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Paul A. Henry

Who Should Attend

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

> "SEC501 is the perfect course to immerse enterprise security staff into essential skills. Failing to attend this course is done at the peril of your organization."
> -John N. Johnson, Houston Police Department

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

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

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

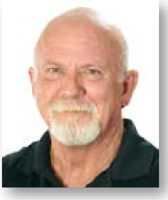
Despite an organization's best efforts to prevent network attacks and protect its critical data, some attacks will still be successful. Therefore, organizations need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks, looking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

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

SANS Technology Institute
www.sans.edu

www.sans.org/8140

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



Paul A. Henry *SANS Senior Instructor*

Paul is one of the world's foremost global information security and computer forensic experts, with more than 20 years' experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principal at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security. Throughout his career, Paul has played a key strategic role in launching new network security initiatives to meet our ever-changing threat landscape. He also advises and consults on some of the world's most challenging and high-risk information security projects, including the National Banking System in Saudi Arabia, the Reserve Bank of Australia, the U.S. Department of Defense's Satellite Data Project, and both government and telecommunications projects throughout Southeast Asia. Paul is frequently cited by major publications as an expert on perimeter security, incident response, computer forensics, and general security trends and serves as an expert commentator for network broadcast outlets such as FOX, NBC, CNN, and CNBC. In addition, Paul regularly authors thought leadership articles on technical security issues, and his expertise and insight help shape the editorial direction of key security publications such as the *Information Security Management Handbook*, to which he is a consistent contributor. Paul is a featured speaker at seminars and conferences worldwide, delivering presentations on diverse topics such as anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, perimeter security, and incident response. **@phenrycissp**

SEC503

Intrusion Detection In-Depth

GCIA Certification
Certified Intrusion Analyst
www.giac.org/gcia

Six-Day Program
Mon, Aug 7 - Sat, Aug 12
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: David Hoelzer

Who Should Attend

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

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

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 sometimes vulnerable. Security-savvy employees who can help detect and prevent intrusions are therefore in great demand. Our goal in SEC503 is to acquaint you with the core knowledge, tools, and techniques to defend your networks with insight and awareness. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

Mark Twain said, "It is easier to fool people than to convince them that they've been fooled." Too many IDS/IPS solutions provide a simplistic red/green, good/bad assessment of traffic and too many untrained analysts accept that feedback as the absolute truth. This course emphasizes the theory that a properly trained analyst uses an IDS alert as a starting point for examination of traffic, not as a final assessment. SEC503 imparts the philosophy that the analyst must have access and the ability to examine the alerts to give them meaning and context. You will learn to investigate and reconstruct activity to deem if it is noteworthy or a false indication.

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 DNS and HTTP, so you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to master different open-source tools like tcpdump, Wireshark, Snort, Bro, tshark, and SiLK. Daily hands-on exercises suitable for all experience levels reinforce the course book material so 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.

> "This training directly correlates to my agency's mission of conducting network forensics/ intrusion investigations."
>
> -Chris G., U.S. Air Force Office of Special Investigations

> "Thank you SANS! I have doubled my security knowledge."
>
> -Jerome Joseph, Nationwide Insurance

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

www.sans.org/8140

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

David Hoelzer *SANS Faculty Fellow*

David Hoelzer is a high-scoring SANS instructor and author of more than 20 sections of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past 25 years. Recently, David was called upon to serve as an expert witness for the Federal Trade Commission for ground-breaking GLBA Privacy Rule litigation. David has been highly involved in governance at the SANS Technology Institute, serving as a member of the Curriculum Committee, as well as Audit Curriculum Lead. As a SANS instructor, David has trained security professionals from organizations including the NSA, DHHS, Fortune 500 companies, various Department of Defense sites, national laboratories, and many colleges and universities. David is a Research Fellow at the Center for Cybermedia Research as well as the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC). He also is an Adjunct Research Associate for the UNLV Cybermedia Research, Lab and a Research Fellow with the Internet Forensics Lab. David has written and contributed to more than 15 peer-reviewed books, publications, and journal articles. Currently, David serves as the principal examiner and director of research for Enclave Forensics, a New York/Las Vegas based incident response and forensics company. He also serves as the chief information security officer for Cyber-Defense, an open-source security software solution provider. In the past, David served as the director of the GIAC Certification program, bringing the GIAC Security Expert certification to life. David holds a BS in IT, Summa Cum Laude, having spent time either attending or consulting for Stony Brook University, Binghamton University, and American Intercontinental University. @it_audit

SEC504

Hacker Tools, Techniques, Exploits, and Incident Handling

GCIH Certification
Incident Handler
www.giac.org/gcih

Six-Day Program
Mon, Aug 7 - Sat, Aug 12
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
(If your laptop supports only wireless, please bring a USB Ethernet adapter.)
Instructor: Adrien de Beaupre

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

"SANS offers very valuable, practical training which makes it possible to return to the workplace and immediately implement improvements and strategies."
-Jill Stuart,
Reserve Bank of Australia

"SEC504 helped me put many pieces of the puzzle together."
-Ian Trimble,
Blue Cross Blue Shield

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection and 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.

"[This course is a] good foundation for security incidents. It's a must-have for security incident handlers/managers."-Wu Peihui, Citibank

This course enables you to turn the tables on computer attackers by helping you understand their 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. 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 for, detect, and respond to those attacks. 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 course 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.

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

www.sans.org/8140

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

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

SEC**511**

GMON Certification
Continuous Monitoring
www.giac.org/gmon

Continuous Monitoring and Security Operations

Six-Day Program
Mon, Aug 7 - Sat, Aug 12
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Eric Conrad

Who Should Attend

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

> "This course has been awesome at teaching me how to use tools and existing architecture in ways I haven't thought of before!"
> -John Hubbard, GlaxoSmithKline

We continue to underestimate the tenacity of our adversaries! Organizations are investing significant time and financial and human resources trying to combat cyber threats and prevent cyber attacks, but despite this tremendous effort organizations are still getting compromised. The traditional perimeter-focused, prevention-dominant approach to security architecture has failed to prevent intrusions. No network is impenetrable, a reality that business executives and security professionals alike have to accept. Prevention is crucial, and we can't lose sight of it as the primary goal. However, a new proactive approach to security is needed to enhance the capabilities of organizations to detect threats that will inevitably slip through their defenses.

> "Keep on giving real-life scenarios to spice up the class. This class was perfect."
> -Genevieve Opaye-Tetteh, eProcess Int SA

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 will be early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and this course will greatly increase your understanding and enhance your skills in implementing CM utilizing the NIST framework.

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

Eric Conrad *SANS Senior Instructor*

Eric Conrad is lead author of the book *The CISSP® Study Guide*. Eric's career began in 1991 as a UNIX systems administrator for a small oceanographic communications company. He gained information security experience in a variety of industries, including research, education, power, Internet, and healthcare. He is now president of Backshore Communications, a company focusing on intrusion detection, incident handling, information warfare, and penetration testing. He is a graduate of the SANS Technology Institute with a Master of Science degree in information security engineering. In addition to the CISSP®, he holds the prestigious GIAC Security Expert (GSE) certification, as well as the GIAC GPEN, GCIH, GCIA, GCFA, GAWN, and GSEC certifications. Eric also blogs about information security at ericconrad.com. @eric_conrad

SEC542

GWAPT Certification
Web Application Penetration Tester

GIAC WEB APPLICATION PENETRATION TESTER GWAPT
www.giac.org/gwapt

Web App Penetration Testing and Ethical Hacking

Six-Day Program
Mon, Aug 7 - Sat, Aug 12
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Micah Hoffman

Who Should Attend

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

Web applications play a vital role in every modern organization. However, if your organization doesn't properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

SEC542 helps students move beyond push-button scanning to professional, thorough, and high-value web application penetration testing.

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organization. Unfortunately, there is no "patch Tuesday" for custom web applications, and major industry studies find that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but effective web application penetration testing requires something deeper.

SEC542 enables students to assess a web application's security posture and convincingly demonstrate the impact of inadequate security that plagues most organizations.

In this course, students will come to understand major web application flaws and their exploitation. Most importantly, they'll learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organizations. Even technically gifted security geeks often struggle with helping organizations understand risk in terms relatable to business. Much of the art of penetration testing has less to do with learning how adversaries are breaking in than it does with convincing an organization to take the risk seriously and employ appropriate countermeasures. The goal of SEC542 is to better secure organizations through penetration testing, and not just show off hacking skills. This course will help you demonstrate the true impact of web application flaws through exploitation.

In addition to high-quality course content, SEC542 focuses heavily on in-depth, hands-on labs to ensure that students can immediately apply all they learn.

In addition to having more than 30 formal hands-on labs, the course culminates in a web application pen test tournament, powered by the SANS NetWars Cyber Range. This Capture-the-Flag event on the final day brings students into teams to apply their newly acquired command of web application penetration testing techniques in a fun way that hammers home lessons learned.

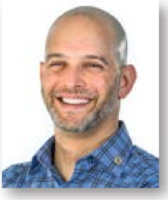
> "SEC542 is a step-by-step introduction to testing and penetrating web applications – a must for anyone who builds, maintains, or audits web systems."
> -Brad Milhorn, ii2P LLC

> "This training boosted my thoughts and perspective on IT. Taught me how to think outside of the box."
> -Ephraim P., U.S. Air Force

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

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



Micah Hoffman *SANS Certified Instructor*

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

FOR500 (Formerly FOR408)

Windows Forensic Analysis

GCFE Certification
Forensic Examiner

www.giac.org/gcfe

Six-Day Program
Mon, Aug 7 - Sat, Aug 12
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Rob Lee

Who Should Attend

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

> "This is a fantastic course! Rob is a fantastic instructor with real-world application experience. This is a must for any investigator."
>
> -Eddie Sky, Forsythe

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

FOR500: Windows Forensic Analysis (Formerly FOR408) focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can't protect what you don't understand, and understanding forensic capabilities and artifacts is a core component of information security. You'll learn to recover, analyze, and authenticate forensic data on Windows systems. You'll understand how to track detailed user activity on your network and how to organize findings for use in incident response, internal investigations, and civil/criminal litigation. You'll be able to use your new skills to validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR500 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR500 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7/8/10, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows XP systems to just-discovered Windows 10 artifacts.

FOR500 is continually updated. This course utilizes a brand-new intellectual property theft and corporate espionage case that took over six months to create. You work in the real world and your training should include real practice data. Our development team used incidents from their own experiences and investigations and created an incredibly rich and detailed scenario designed to immerse students in a true investigation. The case demonstrates the latest artifacts and technologies an investigator might encounter while analyzing Windows systems. The incredibly detailed step-by-step workbook details the tools and techniques that each investigator should follow to solve a forensic case.

**MASTER WINDOWS FORENSICS –
YOU CAN'T PROTECT WHAT YOU DON'T KNOW ABOUT**

Rob Lee *SANS Faculty Fellow*

Rob Lee is an entrepreneur and consultant in the Washington, DC area and currently the Curriculum Lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 15 years' experience in computer forensics, vulnerability and exploit development, intrusion detection/prevention, and incident response. Rob graduated from the U.S. Air Force Academy and earned his MBA from Georgetown University. He served in the U.S. Air Force as a member of the 609th Information Warfare Squadron (IWS), the first U.S. military operational unit focused on information warfare. Later, he was a member of the Air Force Office of Special Investigations (AFOSI), where he led crime investigations and an incident response team. Over the next seven years, he worked directly with a variety of government agencies in the law enforcement, U.S. Department of Defense, and intelligence communities as the technical lead for vulnerability discovery and exploit development teams, lead for a cyber-forensics branch, and lead for a computer forensic and security software development team. Most recently, Rob was a Director for MANDIANT, a commercial firm focusing on responding to advanced adversaries such as the APT. Rob co-authored the book *Know Your Enemy*, 2nd Edition. Rob is also co-author of the MANDIANT threat intelligence report "M-Trends: The Advanced Persistent Threat." **@robtlee** & **@sansforensics**

FOR578

Cyber Threat Intelligence

GIAC Certification
Available
Late 2017

Five-Day Program
Mon, Aug 7 - Fri, Aug 11
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Robert M. Lee

Who Should Attend

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

> "This course [FOR578] gives a very smart and structured approach to cyber threat intelligence, something that the global community has been lacking to date."
>
> -John Geary, Citigroup

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

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

FOR578: Cyber Threat Intelligence will help network defenders, threat hunting teams, and incident responders to:

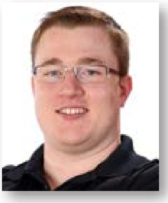
- **Understand and develop skills in tactical, operational, and strategic-level threat intelligence**
- **Generate threat intelligence to detect, respond to, and defeat advanced persistent threats (APTs)**
- **Validate information received from other organizations to minimize resource expenditures on bad intelligence**
- **Leverage open-source intelligence to complement a security team of any size**
- **Create Indicators of Compromise (IOCs) in formats such as YARA, OpenIOC, and STIX**

The collection, classification, and exploitation of knowledge about adversaries – collectively known as cyber threat intelligence – gives network defenders information superiority that is 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.

Cyber 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. Malware is an adversary's tool but the real threat is the human one, and cyber threat intelligence focuses on countering those flexible and persistent human threats with empowered and trained human defenders.

During a targeted attack, an organization needs a top-notch and cutting-edge threat hunting or incident response team armed with the threat intelligence necessary to understand how adversaries operate and to counter the threat. F**OR578: Cyber Threat Intelligence** will train you and your team in the tactical, operational, and strategic-level cyber threat intelligence skills and tradecraft required to make security teams better, threat hunting more accurate, incident response more effective, and organizations more aware of the evolving threat landscape.

THERE IS NO TEACHER BUT THE ENEMY!



Robert M. Lee *SANS Certified Instructor*

Robert M. Lee is the CEO and founder of the critical infrastructure cybersecurity company Dragos Security LLC, where he has a passion for control system traffic analysis, incident response, and threat intelligence research. He is the course author of SANS ICS515: Active Defense and Incident Response and the co-author of SANS FOR578: Cyber Threat Intelligence. Robert is also a non-resident National Cyber Security Fellow at New America focusing on policy issues relating to the cybersecurity of critical infrastructure and a PhD candidate at Kings College London. For his research and focus areas, he was named one of Passcode's Influencers and awarded EnergySec's 2015 Cyber Security Professional of the Year. Robert obtained his start in cybersecurity in the U.S. Air Force, where he served as a Cyber Warfare Operations Officer. He has performed defense, intelligence, and attack missions in various government organizations, and he established a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Robert routinely writes articles in publications such as *Control Engineering* and the *Christian Science Monitor's Passcode* and speaks at conferences around the world. He is also the author of *SCADA and Me* and the weekly web-comic **www.LittleBobbyComic.com**. **@RobertMLee**

MGT414

SANS Training Program for CISSP® Certification

GISP Certification
Information Security Professional
www.giac.org/gisp

Six-Day Program
Mon, Aug 7 - Sat, Aug 12
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPEs
Laptop NOT Needed
Instructor: David R. Miller

Who Should Attend

- Security professionals who are interested in understanding the concepts covered on the CISSP® exam as determined by (ISC)^2
- Managers who want to understand the critical areas of information 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 the eight domains of knowledge can be applied to their current job

SANS Technology Institute
www.sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that is specifically designed to prepare students to successfully pass the CISSP® exam.

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.

Obtaining Your CISSP® Certification Consists of:

- **Fulfilling minimum requirements for professional work experience**
- **Completing the Candidate Agreement**
- **Review of your résumé**
- **Passing the CISSP® 250 multiple-choice question exam with a scaled score of 700 points or greater**
- **Submitting a properly completed and executed Endorsement Form**
- **Periodic audit of CPEs to maintain the credential**

"Best security training I have ever received and just the right amount of detail for each domain."
-Tony Barnes, United States Sugar Corporation

"It was extremely valuable to have an experienced information security professional teaching the course as he was able to use experiential knowledge in examples and explanations."
-Sean Hoar, Davis Wright Tremaine

"I think the course material and the instructor are very relevant for the task of getting a CISSP. The overall academic exercise is solid."
-Aaron Lewter, Availity

David R. Miller *SANS Certified Instructor*

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

MGT514

GIAC Certification
Available
Late 2017

IT Security Strategic Planning, Policy, and Leadership

Five-Day Program
Mon, Aug 7 - Fri, Aug 11
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: Frank Kim

Who Should Attend

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

> "I moved into management a few years ago and am currently working on a new security strategy/ roadmap and this class just condensed the past two months of my life into a one-week course and I still learned a lot!"
>
> -Travis Evans, SiriusXM

SANS Technology Institute
www.sans.edu

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

This course teaches security professionals how to do three things:

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

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

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

How the Course Works

Using case studies from Harvard Business School, team-based exercises, and discussions that put students in real-world scenarios, students will participate in activities that they can then carry out with their own team members when they return to work.

The next generation of security leadership must bridge the gap between security staff and senior leadership by strategically planning how to build and run effective security programs. After taking this course you will have the fundamental skills to create strategic plans that protect your company, enable key innovations, and work effectively with your business partners.

Frank Kim *SANS Certified Instructor*

As CISO at the SANS Institute, Frank leads the security risk function for the most trusted source of computer security training, certification, and research in the world. He also helps shape, develop, and support the next generation of security leaders by teaching, developing courseware, and leading the management and software security curricula. Prior to the SANS Institute, Frank was Executive Director of Cyber Security at Kaiser Permanente with responsibility for delivering innovative security solutions to meet the unique needs of the nation's largest not-for-profit health plan and integrated health care provider with annual revenue of $55 billion, 9.5 million members, and 175,000 employees. In recognition of his work, Frank was a two-time recipient of the CIO Achievement Award for business-enabling thought leadership. Frank holds degrees from the University of California at Berkeley and is the author of popular SANS courseware on strategic planning, leadership, and application security. **@fykim**

Bonus Sessions

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: Exploitation Throughout the Ages: Stacks, Canaries, ASLR, ROP and More!

David Hoelzer

This two-hour keynote will look at the cybersecurity arms race of exploitation and the resulting defenses. The discussion starts back in the 1990s with Aleph One and his seminal paper and ends with the most modern defenses available today. However, we're not just going to talk about exploitation, we're going to demonstrate it! David Hoelzer will discuss and demonstrate how attacks and defenses have evolved over the last 20 years, illustrating the work of a security researcher or hacker engaged in zero-day exploitation. Even though sections of the talk and the demonstrations can be quite technical, even non-technical attendees will leave with very useful takeaways that can be applied to vulnerability remediation within their enterprises right away.

HTTPDeux

Adrien de Beaupre

This talk will discuss the relatively newly approved and published HTTP/2 protocol. The agenda will include reasons for the new protocol to be developed, how it is implemented, tools that can use it, and challenges it presents to penetration testers.

Collecting and Exploiting Your "Private" Internet Data Using OSINT

Micah Hoffman

Have you ever wondered how an attacker gets access to the data you, your family and friends post to the Internet? What could they do with it? Could they find your spouse and family members from your profile information? What tools and techniques do they leverage in their Open-Source Intelligence (OSINT) research on potential victims? If any of these questions raise concerns, you need to come to this talk. We will walk through how an attacker can leverage Burp Suite, Recon-ng and a variety of Internet resources to perform OSINT gathering on potential targets. We will use search engines to locate target homes, learn about the psychology behind why people share what they do, and learn some effective methods of protecting your private Internet data.

Quality Not Quantity: Continuous Monitoring's Deadliest Events

Eric Conrad

Most Security Operations Centers (SOCs) are built for compliance, not security. One well-known retail firm suffered the theft of over a million credit cards. Some 60,000 true positive events were reported to their SOC during that breach, but they were missed, lost in the noise of millions. If you are bragging about how many events your SOC "handles" each day, you are doing it wrong. During this talk we will show you how to focus on quality instead of quantity, and provide an actionable list of the deadliest events that occur during virtually every successful breach. We will also provide an overview of DeepBlueCLI, a PowerShell framework for automatically detecting the deadliest events.

Birds of a Feather or...

Mark Williams

Privacy and security are clearly close cousins if not siblings. However, there are certain "truths" that are immutable with regard to the differences between the two. In this talk, Mark Williams will explore this divide, and how it has influenced structure within Security and Privacy Programs. We will also discuss what is needed to move ahead in a world where privacy and security must not only coexist, but do so by way of a more synergistic relationship that enables us to accomplish both objectives.

Core NETWARS EXPERIENCE

Test your cybersecurity knowledge and skills LIVE at

SANS Boston 2017 with 2 free nights of NetWars!

AUGUST 10-11 6:30-9:30 PM

Come and join us for this exciting event to test your skills in a challenging and fun learning environment. Registration for NetWars is **FREE OF CHARGE TO ALL STUDENTS AT SANS BOSTON 2017**. External participants are welcome to join for an entry fee of $1,520.

SANS NetWars is a dynamic cyber range that allows participants to build, practice, and measure their skills in a real-world environment using defensive, analytic, and offensive tactics. We designed NetWars to appeal to a wide range of participant skill sets by using a system with different levels.

All players start at Level 1, which measures foundational cybersecurity skills. More skilled players can rise rapidly through the ranks to a level suitable for their skill set – top players can make it to Level 4, and only the best of the best can reach level 5.

sans.org/boston

Enhance Your Training Experience

Add an
OnDemand Bundle & GIAC Certification Attempt*
to your course within seven days
of this event for just $689 each.

SPECIAL PRICING

Extend Your Training Experience with an
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.

Get Certified with
GIAC Certifications

- Distinguish yourself as an information security leader
- 30+ GIAC cybersecurity certifications available
- 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

Whether you choose to attend a training class live or online, the entire SANS team is dedicated to ensuring your training experience exceeds expectations.

Live Classroom Instruction

Premier Training Events

Our most recommended format, live SANS training events feature SANS' top instructors teaching multiple courses at a single time and location. This allows for:

- Focused, immersive learning without the distractions of your office environment
- Direct access to SANS Certified Instructors
- Interacting with and learning from other professionals
- Attending SANS@Night events, NetWars tournaments, vendor presentations, industry receptions, and many other activities

Our premier live training events in North America, serving thousands of students, are held in Orlando, Washington DC, Las Vegas, New Orleans, and San Diego. Regional events with hundreds of students are held in most major metropolitan areas during the year. See page 16 for upcoming training events in North America.

Summits

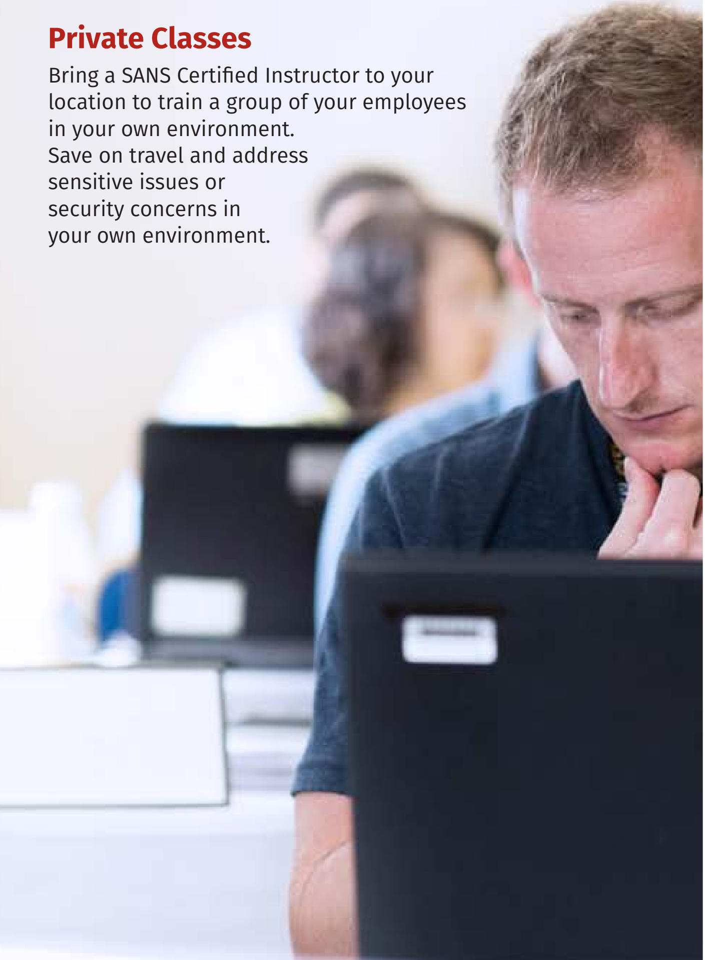
SANS Summits focus one or two days on a single topic of particular interest to the community. Speakers and talks are curated to ensure the greatest applicability to participants.

Community SANS Courses

Same SANS courses, courseware, and labs, are taught by up-and-coming instructors in a regional area. Smaller classes allow for more extensive instructor interaction. No need to travel; commute each day to a nearby location.

Private Classes

Bring a SANS Certified Instructor to your location to train a group of your employees in your own environment. Save on travel and address sensitive issues or security concerns in your own environment.



Online Training

SANS Online successfully delivers the same measured learning outcomes to students at a distance that we deliver live in classrooms. More than 30 courses are available for you to take whenever or wherever you want. Thousands of students take our courses online and achieve certifications each year.

Top reasons to take SANS courses online:

- Learn at your own pace, over four months
- Spend extra time on complex topics
- Repeat labs to ensure proficiency with skills
- Save on travel costs
- Study at home or in your office

Our SANS OnDemand, vLive, Simulcast, and SelfStudy formats are backed by nearly 100 professionals who ensure we deliver the same quality instruction online (including support) as we do at live training events.

> **"I am thoroughly pleased with the OnDemand modality. From a learning standpoint, I lose nothing. In fact, the advantage of setting my own pace with respect to balancing work, family, and training is significant, not to mention the ability to review anything that I might have missed the first time."**
>
> -Kevin E., U.S. Army

> **"The decision to take five days away from the office is never easy, but so rarely have I come to the end of a course and had no regret whatsoever. This was one of the most useful weeks of my professional life."**
>
> -Dan Trueman, Novae PLC

Future Training Events

Northern Virginia – Reston	Reston, VA	May 21-26
Atlanta	Atlanta, GA	May 30 - June 4
Houston	Houston, TX	June 5-10
San Francisco Summer	San Francisco, CA	June 5-10
Rocky Mountain	Denver, CO	June 12-17
Charlotte	Charlotte, NC	June 12-17
Minneapolis	Minneapolis, MN	June 19-24
Columbia, MD	Columbia, MD	June 26 - July 1
ICS & Energy	Houston, TX	July 10-15
Los Angeles – Long Beach	Long Beach, CA	July 10-15

SANSFIRE Washington, DC July 22-29

San Antonio	San Antonio, TX	Aug 6-11
Boston	Boston, MA	Aug 7-12
New York City	New York, NY	Aug 14-19
Salt Lake City	Salt Lake City, UT	Aug 14-19
Chicago	Chicago, IL	Aug 21-26
Virginia Beach	Virginia Beach, VA	Aug 21 - Sep 1
Tampa – Clearwater	Clearwater, FL	Sep 5-10
San Francisco Fall	San Francisco, CA	Sep 5-10

Network Security Las Vegas, NV Sep 10-17

Baltimore	Baltimore, MD	Sep 25-30
Rocky Mountain Fall	Denver, CO	Sep 25-30
Phoenix-Mesa	Mesa, AZ	Oct 9-14
Tysons Corner Fall	Washington, DC	Oct 16-21
San Diego Fall	San Diego, CA	Oct 30 - Nov 4
Seattle	Seattle, WA	Oct 30 - Nov 4

Future Summit Events

Security Operations Center	Washington, DC	June 5-12
Digital Forensics	Austin, TX	June 22-29
Security Awareness	Nashville, TN	July 31 - Aug 9
Data Breach	Chicago, IL	Sep 25 - Oct 2
Secure DevOps	Denver, CO	Oct 10-17

Future Community SANS Events

Local, single-course events are also offered throughout the year via SANS Community. Visit **www.sans.org/community** for up-to-date Community course information.

Hotel Information

Omni Parker House

60 School Street
Boston, MA 02108
Phone: 617-227-8600
www.sans.org/event/boston-2017/location

This grand luxury hotel has been symbolic of Boston's rich history and culture since 1855. Old World charm and elegance are accompanied by all of the modern conveniences of a world-class establishment. Nestled in the heart of downtown Boston, Omni Parker House is located along the Freedom Trail and at the foot of Beacon Hill, Boston Common, Quincy Market and Faneuil Hall Marketplace. Omni Parker House is just 2.3 miles from Logan International Airport (10 minutes).

Special Hotel Rates Available

A special discounted rate of $215.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through **July 14, 2017**.

Top 5 reasons to stay at the Omni Parker House

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 Omni Parker House 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 Omni Parker House that you won't want to miss!

5 Everything is in one convenient location!

Registration Information

Register online at **www.sans.org/boston**

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

Select your course 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.

Pay Early and Save*

Use code **EarlyBird17** when registering early

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code by	**6-14-17**	**$400.00**	**7-5-17**	**$200.00**

*Some restrictions apply. Early bird discounts do not apply to Hosted courses.

SANS Voucher Program

Expand your training budget!

Extend your fiscal year. The SANS Voucher Program provides flexibility and may earn you bonus funds for training.

www.sans.org/vouchers

Cancellation & Access Policy

If an attendee must cancel, a substitute may attend instead. Substitution requests can be made at any time prior to the event start date. Processing fees will apply. All substitution requests must be submitted by email to registration@sans.org. If an attendee must cancel and no substitute is available, a refund can be issued for any received payments by **July 12, 2017**. A credit memo can be requested up to the event start date. All cancellation requests must be submitted in writing by mail or fax and received by the stated deadlines. Payments will be refunded by the method that they were submitted. Processing fees will apply.

Open a **SANS 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 FAQs
- Tip of the Day
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

www.sans.org/account