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

SANS

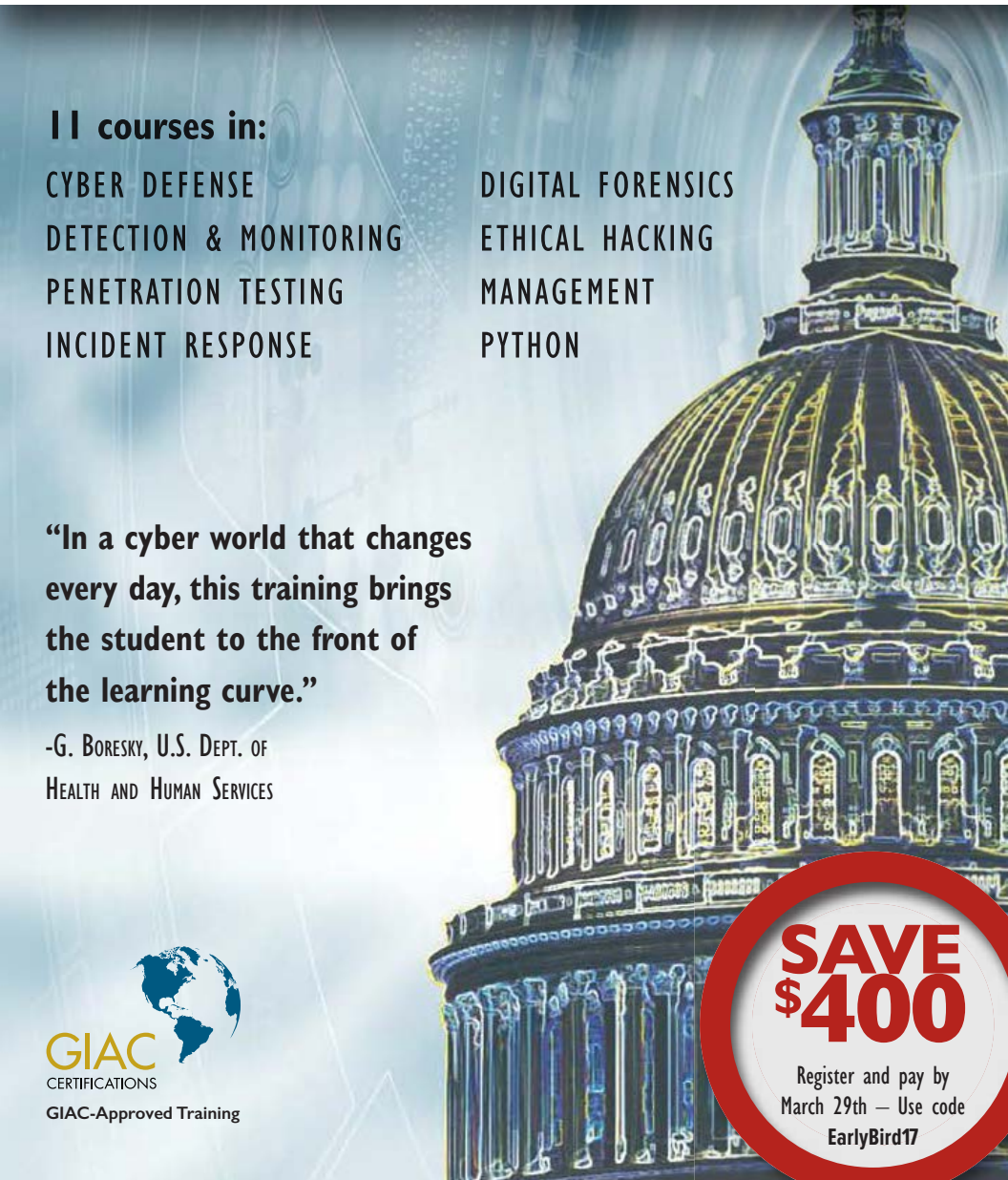
NORTHERN VIRGINIA Reston 2017

May 21-26

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

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS



11 courses in:

CYBER DEFENSE
DETECTION & MONITORING
PENETRATION TESTING
INCIDENT RESPONSE
DIGITAL FORENSICS
ETHICAL HACKING
MANAGEMENT
PYTHON

"In a cyber world that changes every day, this training brings the student to the front of the learning curve."

-G. Boresky, U.S. Dept. of Health and Human Services

GIAC CERTIFICATIONS
GIAC-Approved Training

SAVE $400

Register and pay by March 29th – Use code **EarlyBird17**

www.sans.org/reston

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 Reston 2017 lineup of instructors includes:

Doc Blackburn
Instructor
@DocBlackburn

Carlos Cajigas
Instructor
@Carlos_Cajigas

Christopher Crowley
Principal Instructor
@CCrowMontance

Kevin Fiscus
Certified Instructor
@kevinbfiscus

Jason Fossen
Faculty Fellow
@JasonFossen

Tim Garcia
Certified Instructor
@tbg911

Paul A. Henry
Senior Instructor
@phenrycissp

Micah Hoffman
Certified Instructor
@WebBreacher

Jonathan Thyer
Instructor
@joff_thyer

Matthew Toussain
Instructor
@0sm0s1z

Mark Williams
Instructor
@securemdw

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 13.

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

Virtualizing Forensic Images Using Free Tools in Linux – Carlos Cajigas

Collecting and Exploiting Your "Private" Internet Data – Micah Hoffman

Shell Is Only The Beginning: Understanding Metasploit Post Exploitation Modules
Kevin Fiscus

Advancing the Security Agenda: Compelling Leadership to Support Security
Doc Blackburn

Save $400 when you register and pay by March 29th using code EarlyBird17

Courses at a Glance

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 justify 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? Place the particular course you wish to take into the context on the SANS Career Roadmap. 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 sections titled "You Will Be Able To." Be sure to include these 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 learning that passing a GIAC exam offers. 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.

SEC301:

Intro to Information Security

SANS

Five-Day Program
Mon, May 22- Fri, May 26
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Doc Blackburn

www.giac.org/gisf

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

"This course was the perfect blend of technical and practical information for someone new to the field, and I would recommend it!"
-Steve Mecco, Draper

"This training is very valuable as I start my position in IT security. There is so much to learn and many good concepts."
-Amy Swanson, Truven Health Analytics

To determine if the SANS SEC301 course is right for you, ask yourself five simple questions:

- Do you have basic computer knowledge but are new to information security and in need of an introduction to the fundamentals?
- Are you bombarded with complex technical security terms that you don't understand?
- Are you a non-IT security manager (with some technical knowledge) who lays awake at night worrying that your company will be the next mega-breach headline story on the 6 o'clock news?
- Do you need to be conversant in basic security concepts, principles, and terms, even if you don't need "deep in the weeds" detail?
- Have you decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification?

If you answer yes to any of these questions, the **SEC301: Introduction to Information Security** training course is for you. Jump-start your security knowledge by receiving insight and instruction from real-world security experts on critical introductory topics that are fundamental to information security. This completely revised five-day comprehensive course covers everything from core terminology to the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles.

This course is designed for students who have a basic knowledge of computers and technology but no prior knowledge of cybersecurity. The hands-on, step-by-step teaching approach will enable you to grasp all of the information presented even if some of the topics are new to you. You'll learn the fundamentals of information security that will serve as the foundation of your InfoSec skills and knowledge for years to come.

Authored by a security professional with over 30 years of experience in both the public and private sectors, SEC301 provides uncompromising real-world insight from start to finish. The course prepares you for the Global Information Security Fundamentals (GISF) certification test, as well as for the next course up the line, **SEC401: Security Essentials Bootcamp**. It also delivers on the SANS promise: ***You will be able to use the knowledge and skills you learn in SEC301 as soon as you return to work.***

Doc Blackburn *SANS Instructor*

Doc Blackburn has over 30 years of experience in system and software design, server and network administration and website programming. His interest in computers started in 1982 when he first started programming in DOS on a Texas Instruments TI-99 4a and continued as a dedicated computer hobbyist until he decided to make information technology a full-time career in 1998. Doc ran a successful IT consulting, hosting, and design firm for 12 years until he found his passion was in systems security and compliance. His well-rounded experience includes hardware, software, network design, project management, administration, programming, systems security, and compliance frameworks. He has vast experience at various levels of information technology from technical support to security leadership roles. He has been heavily involved in the technical design and implementation of NIH-approved FISMA-compliant information systems. His current work has focused on HIPAA, FERPA, PCI DSS, and FISMA compliant systems with an emphasis on IT risk management in enterprise environments. Doc holds ITIL, CISSP, HCISPP (healthcare, HIPAA), and PCI ISA (payment card industry) and GIAC GSEC, GISF, GPEN, GCPM, GCIA and GSLC certifications. He has a bachelor's degree from the University of Arizona. He is currently the IT Compliance Administrator for the University of Colorado Denver Anschutz Medical Campus. @DocBlackburn

SEC401:
Security Essentials Bootcamp Style

SANS

Six-Day Program
Sun, May 21 - Fri, May 26
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Tim Garcia

www.giac.org/gsec

www.sans.edu


www.sans.org/8140

Bundle OnDemand
with this course
www.sans.org/ondemand

"Everyone in cyber should attend this course because it covers many aspects of security and emerging trends."
-Pamela Livingston-Spruill, DOE/NNSA

This course will teach you the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. You'll 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*!

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

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

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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

Who Should Attend

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

Tim Garcia *SANS Certified Instructor*

Timothy Garcia is a seasoned security professional who loves the challenge and continuously changing landscape of defense. Tim currently works as an information security engineer for a Fortune 100 financial company, where he helps project teams ensure the security of IT operations and compliance with policies and regulations. He also leads the team that is tasked with firewall review, SIEM management and privileged access monitoring and policy compliance. Tim has worked as a systems engineer and database administrator and has expertise in systems engineering, project management and information security principles and procedures/compliance. Tim previously worked for Intel and served in the U.S. Navy. At SANS, Tim also works with the OnDemand team as a subject-matter expert, serves as a mentor for the Vet Success program, and provides consulting and content review for the Securing The Human project. Tim is a contributor to the Arizona Cyber Warfare Range and works with the local security community giving monthly talks on information security tools and techniques. Tim holds the CISSP, GSEC, GSLC, GISF, GMON, GAWN, GCCC, and GCED as well as the NSA-IAM certifications. He has extensive knowledge of security procedures and legislation such as Sarbanes-Oxley, GLBA, CobiT, COSO, and ISO 1779. @tbg911

SEC501:

Advanced Security Essentials – Enterprise Defender

SANS

Six-Day Program
Sun, May 21 - Fri, May 26
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: Paul A. Henry

www.giac.org/gced

SANS Technology Institute
www.sans.edu

www.sans.org/8140

Bundle OnDemand
with this course
www.sans.org/ondemand

"Paul Henry is an excellent instructor who presents large volumes of information effectively."
-Rowley Molina, Altria

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

Who Should Attend

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

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

"We aren't just learning how to use the tools, we also have real-world examples to avoid possible pitfalls. There is cloud-based analysis that is so useful, but I would never have thought of using it had Paul not covered it."
-Stuart Long, Bank of England

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

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

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

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Sun, May 21 - Fri, May 26
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Kevin Fiscus

www.giac.org/gcih

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

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

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

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

"If you love cybersecurity and learning how exploits work, you NEED this course!" -Jaid, U.S. Navy

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 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 will enable you to discover the holes in your system before the bad guys do!

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

"This was a valuable course and will benefit me in explaining the pieces attackers follow to gain access to system networks and the practices to mitigate these attacks." -Derek S., U.S. Air Force

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

SEC505:
Securing Windows and PowerShell Automation

SANS

Six-Day Program
Sun, May 21 - Fri, May 26
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jason Fossen

www.giac.org/gcwn

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

Bundle OnDemand
with this course
www.sans.org/ondemand

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

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

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

Who Should Attend

- Security Operations (SecOps) engineers
- Windows endpoint and server administrators
- Anyone who wants to learn PowerShell automation
- Anyone implementing the NSA Top 10 Mitigations
- Anyone implementing the CIS Critical Security Controls
- Those deploying or managing a Public Key Infrastructure (PKI) or smart cards
- Anyone who needs to reduce malware infections

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

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

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

If you are an IT manager or CIO, the aim for this course is to have it pay for itself 10 times over within two years, because automation isn't just good for SecOps/DevOps, it can save money, too.

This course is designed for systems engineers, security architects, and the SecOps team. The focus of the course is on how to automate the NSA Top 10 Mitigations and the CIS Critical Security Controls related to Windows, especially the ones that are difficult to implement in large environments.

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

"This is a really great course for anyone involved in administration or securing of windows environments." -David Hazar, Oracle

Jason Fossen *SANS Faculty Fellow*

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

SEC511:
Continuous Monitoring and Security Operations

New Extended Bootcamp Hours to Enhance Your Skills

SANS

Six-Day Program
Sun, May 21 - Fri, May 26
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Laptop Required
Instructor:
Christopher Crowley

www.giac.org/gmon

www.sans.edu

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

"This training provides excellent information for self assessment of current SEC practices. I picked up a lot of tricks and new perspectives."
-Kyle Montgomery, National Rural Electric Cooperative Association

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 analysts, engineers, and managers
- Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)
- Computer Network Defense analysts

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.

"Outstanding content and instructor." -Al Foster, U.S. Department of the Interior

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.

"This course is full of practical and actionable advice for environments of any size."
-Jesse Lane, IAG

Christopher Crowley *SANS Principal Instructor*

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

SEC542:

Web App Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Sun, May 21 - Fri, May 26
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Micah Hoffman

www.giac.org/gwapt

www.sans.edu

www.sans.org/cyber-guardian

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

"Micah's knowledge gave me a better perspective on the development process, and helped peel back the onion on infrastructure and environments. This was a great course with a lot of good info!"
-EPHRAIM P., U.S. AIR FORCE

Web applications play a vital role in every modern organization. But if your organization does not 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.

Who Should Attend

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

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, so 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.

"This course has been well worth it!
I can't wait to take the advanced pen testing course." -BEN JOHNSON, TIME INC.

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.

Students will come to understand major web application flaws and their exploitation and, most importantly, learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organizations. 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. The course will help you demonstrate the true impact of web application flaws through exploitation.

In addition to 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 to hammer home lessons learned.**

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

SEC560:
Network Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Sun, May 21 - Fri, May 26
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Matthew Toussain

www.giac.org/gpen

www.sans.edu

www.sans.org/cyber-guardian

Bundle OnDemand
with this course
www.sans.org/ondemand

"Learning how attackers profile and exploit allows me to understand how to tailor our product offerings to provide real value."
-Travis Smith, Tripwire

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.

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.

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.

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.**

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

Matthew Toussain *SANS Instructor*

Matthew Toussain is an active-duty Air Force officer and the founder of Spectrum Information Security, a firm focused on maximizing the value proposition of information security programs. As an avid information security researcher, Matthew regularly hunts for vulnerabilities in computer systems and releases tools to demonstrate the effectiveness of attacks and countermeasures. He has been a guest speaker at many conference venues, including DEFCON, the largest security conference in the world. After graduating from the U.S. Air Force Academy, where he architected and instructed the summer cyber course that now trains over 400 cadets per year, Matthew served as the Senior Cyber Tactics Development Lead for the U.S. Air Force. He directed the teams responsible for developing innovative tactics, techniques, and procedures for offensive operations as well as for cyber protection teams (CPT). Later, as a member of the 688th Cyber Warfare Wing he managed the Air Force's transition of all 18 CPTs to fully operational capability. As a founding member of Spectrum, Matthew regularly performs a wide variety of information security services. He earned his master's degree in information security engineering as one of the first graduates of the SANS Technology Institute and supports many national and international cyber competitions including the CCDC, Netwars, and the National Security Agency's Cyber Defense Exercise as a red team member and instructor. @0sm0s1z

SEC573:

Automating Information Security for Python

NEW

SANS

Six-Day Program
Sun, May 21 - Fri, May 26
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jonathan Thyer

www.giac.org/gpyc

www.sans.edu

Who Should Attend

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

"SEC573 gave me exposure to tools and techniques I wouldn't have normally considered, but now are part of my arsenal."
-Allen C., DoD

All security professionals, including Penetration Testers, Forensics Analysts, Network Defenders, Security Administrators, and Incident Responders, have one thing in common: CHANGE. Change is constant. Technology, threats, and tools are constantly evolving. If we don't evolve with them, we'll become ineffective and irrelevant, unable to provide the vital defenses our organizations increasingly require.

Maybe your chosen Operating System has a new feature that creates interesting forensics artifacts that would be invaluable for your investigation, if only you had a tool to access it. Often for new features and forensics artifacts, no such tool has yet been released. You could try moving your case forward without that evidence or hope that someone creates a tool before the case goes cold… or you can write a tool yourself.

Or, perhaps an attacker bypassed your defenses and owned your network months ago. If existing tools were able to find the attack, you wouldn't be in this situation. You are bleeding sensitive data and the time-consuming manual process of finding and eradicating the attacker is costing you money and hurting your organization big time. The answer is simple if you have the skills: Write a tool to automate your defenses.

Or, as a penetration tester, you need to evolve as quickly as the threats you are paid to emulate. What do you do when "off-the-shelf" tools and exploits fall short? If you're good, you write your own tool.

Writing a tool is easier said than done, right? Not really. Python is a simple, user-friendly language that is designed to make automating tasks that security professionals perform quick and easy. Whether you are new to coding or have been coding for years, SEC573: Automating Information Security for Python will have you creating programs to make your job easier and make you more efficient. This self-paced class starts from the very beginning, assuming you have no prior experience or knowledge of programming. We cover all of the essentials of the language up front. If you already know the essentials, you will find that the pyWars lab environment allows advanced developers to quickly accelerate to more advanced material in the class. The self-paced style of the class will meet you where you are to let you get the most out of the class. Beyond the essentials we discuss file analysis, packet analysis, forensics artifact carving, networking, database access, website access, process execution, exception handling, object-oriented coding and more.

This course is designed to give you the skills you need for tweaking, customizing, or outright developing your own tools. We put you on the path of creating your own tools, empowering you in automating the daily routine of today's information security professional, and achieving more value in less time. Again and again, organizations serious about security emphasize their need for skilled tool builders. There is a huge demand for people who can understand a problem and then rapidly develop prototype code to attack or defend against it. Join us and learn Python in-depth and fully weaponized.

Jonathan Thyer *SANS Senior Instructor*

Jonathan (Joff) Thyer is a Senior Security Consultant, Researcher, and Penetration Tester with Black Hills Information Security. Joff has over 15 years of experience in the IT industry as an enterprise network architect, network security defender, and information security consultant. Joff has experience with intrusion detection and prevention systems, vulnerability analysis, penetration testing, engineering network infrastructure defense (including Cisco ISE deployment), and software development. Joff has taught Mastering Packet Analysis and mentored SEC503: Intrusion Detection In-Depth. Joff is also a co-host on the Security Weekly podcast, which features the latest information security news, research, interviews, and technical information. Joff holds a B.Sc. in mathematics, and a M.Sc. in computer science. He holds the GPEN Penetration Tester certification. @joff_thyer

FOR408:
Windows Forensic Analysis

SANS

Six-Day Program
Sun, May 21 - Fri, May 26
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Carlos Cajigas

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

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

Who Should Attend

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

www.giac.org/gcfe

www.sans.edu

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

"The methods taught and the tools introduced will be very beneficial to me as an analyst performing examinations."
-Joseph Selph, IBM

"The Windows registry forensic section blew my mind! I didn't think it stored that much information." -Tung Nguyen, Denver Water

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

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

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

Carlos Cajigas *SANS Instructor*

A native of San Juan, Puerto Rico, Carlos began his career with the West Palm Beach Police Department in Florida, first as a police officer and eventually as a digital forensics detective, examiner, and instructor specializing in computer crime investigations. During his law enforcement tenure, Carlos conducted examinations on hundreds of digital devices, from computers and mobile phones to GPS devices, and served as both a fact and expert witness in the Florida. Today, Carlos is a senior incident response analyst at IBM, where he is responsible for responding to computer and network security threats for clients located in North and South America. In addition, he holds various certifications in the digital forensics field including EnCase Certified Examiner (ENCE), Certified Forensic Computer Examiner (CFCE) from IACIS, and the GIAC Certifications GCFE and GCFA. @Carlos_Cajigas

MGT514:

IT Security Strategic Planning, Policy, and Leadership

SANS

Five-Day Program
Mon, May 22- Fri, May 26
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: Mark Williams

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

This course teaches security professionals how to do three things:

Who Should Attend

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

SANS Technology Institute
www.sans.edu

▶II **BUNDLE ONDEMAND** WITH THIS COURSE
www.sans.org/ondemand

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

"This is a great foundational course as we realize the importance of bringing a business perspective to security."
-Nairobi Kim, Wells Fargo

Develop Strategic Plans

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

Create Effective Information Security Policy

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

Develop Management and Leadership Skills

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

Mark Williams *SANS Instructor*

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

SANS@NIGHT EVENING TALKS

Enrich your SANS training experience!

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

KEYNOTE:

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

Jason Fossen

Windows 10 is not set in stone, Microsoft is continually releasing new major updates for the "Windows as a Service (WaaS)" deployment model. So, what's new for security in the latest version? Windows 10 includes significant changes for security and manageability in large organizations, but it can be hard to keep up! Windows Server 2016 also has several new security enhancements. What exactly are "Server Nano Hyper-V Containers" anyway? Is Server 2016 a compelling upgrade or should you wait? In this lively talk, Jason Fossen, author of the Securing Windows and PowerShell Automation (SEC505) course at SANS, will lay out what to love and fear in Windows 10 and Windows Server 2016. He will also talk about some of the epic changes going on at Microsoft, now that CEO Steve Ballmer is gone. Is it really a new era for Microsoft? Come join the presentation and see what Microsoft is betting its future on!

Virtualizing Forensic Images Using Free Tools in Linux – *Carlos Cajigas*

Have you ever needed to boot a forensic image to preview the system in a live manner? Would you like to do it without changing a single bit? It is possible! In this session we will discuss the tools and steps required for converting the Donald Blake forensic image into a Virtual Machine (VM). This process is useful, because it gives you the ability to boot an image of an OS drive into a VM, all while preserving the integrity of the image. All changes made by the OS are saved and stored to a cache file. Come see how you accomplish this using free tools under Linux Ubuntu. The presentation will include a live demo.

Collecting and Exploiting Your "Private" Internet Data

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 you're looking for answers to these questions, come to this presentation. We will walk through how an attacker can leverage Burp Suite and Recon-ng to perform OSINT gathering on potential targets and use search engines to locate their homes. You'll learn about the psychology behind why people share what they do, and be entertained by the wit and humor of the speaker.

Shell Is Only The Beginning: Understanding Metasploit Post Exploitation Modules – *Kevin Fiscus*

Metasploit is a fantastic hacking tool. Having a huge range or exploits and a collection of different payloads that are easy to use makes compromising vulnerable systems almost trivial. Many a penetration tester have been given the opportunity to do their "happy dance" by compromising a system and getting shell on the target system. Getting shell, however, is only the beginning of the penetration test. When taking martial arts it is common to hear that becoming a blackbelt is only the beginning of the training. Penetration testing is similar. The test really begins when you get shell. Once you have access to the compromised system, what do you do? This talk will discuss the often overlooked post-exploitation modules in Metasploit. These are the components in Metasploit that allow you to capture keystrokes, identify new targets, grab credentials, identify users, determine what applications are installed and even identify if you have compromised a physical or virtual host. During this talk we will describe and demonstrate many of these modules adding to your arsenal of penetration testing techniques.

Advancing the Security Agenda: Compelling Leadership to Support Security – *Doc Blackburn*

Are you having trouble convincing the decision-makers in your business to support security initiatives? Are your concerns being ignored? You are not alone! One of the biggest challenges InfoSec professionals face today is getting leadership to support their activities. There have been many recent cases of security not getting enough resources until after a breach. Unfortunately, many times, the security team is shown the door after the breach because it was considered their fault. Don't let this happen to you. You know what to do, and how to do it. You know how important it is to your organization. The technology exists to fix your concerns. So, why won't leadership fund it? Find out how to gain support for your activities and receive the support your security initiatives need.

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

LIVE CLASSROOM TRAINING

Multi-Course Training Events www.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 www.sans.org/community
Live Training in Your Local Region with Smaller Class Sizes

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

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

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

ONLINE TRAINING

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

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

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

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

FUTURE SANS TRAINING EVENTS

San Jose 2017
San Jose, CA | March 6-11

Tysons Corner SPRING 2017
McLean, VA | March 20-25

ICS Security
SUMMIT & TRAINING 2017
Orlando, FL | March 20-27

Pen Test Austin 2017
Austin, TX | March 27 - April 1

SANS 2017
Orlando, FL | April 7-14

Threat Hunting and IR
SUMMIT & TRAINING 2017
New Orleans, LA | April 18-25

Automotive Cybersecurity
SUMMIT 2017
Detroit, MI | May 1-8

Security West 2017
San Diego, CA | May 9-18

Atlanta 2017
Atlanta, GA | May 30 - June 4

Houston 2017
Houston, TX | June 5-10

San Francisco SUMMER 2017
San Francisco, CA | June 5-10

Security Operations Center
SUMMIT & TRAINING 2017
Washington, DC | June 5-12

Rocky Mountain 2017
Denver, CO | June 12-17

Charlotte 2017
Charlotte, NC | June 12-17

Minneapolis 2017
Minneapolis, MN | June 19-24

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

SANS RESTON 2017

Hotel Information

Training Campus

Sheraton Reston Hotel

11810 Sunrise Valley Drive
Reston, VA 20191
703-620-9000
sans.org/event/reston-2017/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, and 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.

The negotiated group rate is less than the government per diem rate. This rate includes high-speed Internet in your room and is only available through May 5, 2017. To make reservations, please call 703-620-9000.

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 2017

Registration Information

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

Register online at www.sans.org/reston

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.

Use code **EarlyBird17** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**3-29-17**	**$400.00**	**4-19-17**	**$200.00**

Some restrictions apply.

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

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by April 26, 2017 – processing fees may apply.