



Philadelphia 2016

February 29 - March 5

Choose from these popular courses:

Security Essentials Bootcamp Style

**Hacker Tools, Techniques, Exploits,
and Incident Handling**

Windows Forensic Analysis

**Continuous Monitoring and
Security Operations**

ICS/SCADA Security Essentials

*“SANS teaches amazing
techniques that can be used
instantly in the real world!”*

-JONATHAN REITNAUER, VANGUARD



GIAC Approved Training

REGISTER AT sans.org/philadelphia-2016

**Save
\$400**

by registering & paying early!

See page 13 for more details.

SANS Instructors

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



Jonathan Ham
Certified Instructor



Heather Mahalik
Senior Instructor



Michael Murr
Principal Instructor



Billy Rios
SANS Instructor



Bryan Simon
Certified Instructor

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 7.

- **KEYNOTE: *Convergence Forensics: Leveraging Multiple Skills to Analyze Evidence*** – Heather Mahalik
- ***Assessing Deception*** – Michael Murr
- ***And more to come!***



The training campus for SANS Philadelphia 2016, Sonesta Philadelphia, is both a business hub, with many Fortune 500 Companies lining its bustling streets, as well as a family destination with an abundance of historical landmarks, museums, art, theaters, and other family-friendly attractions.

PAGE 13

Be sure to register and pay by January 6th for a \$400 tuition discount!

Courses-at-a-Glance

	MON 2-29	TUE 3-1	WED 3-2	THU 3-3	FRI 3-4	SAT 3-5
SEC401 Security Essentials Bootcamp Style	Page 2					
SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	Page 3					
SEC511 Continuous Monitoring and Security Operations	Page 4					
FOR408 Windows Forensic Analysis	Page 5					
ICS410 ICS/SCADA Security Essentials	Page 6					

Register today for SANS Philadelphia 2016!
sans.org/philadelphia-2016



@SANSInstitute
Join the conversation:
#SANSPhiladelphia

The Value of SANS Training & YOU



EXPLORE

- Read this brochure and note the courses that will enhance your role in your organization
- Use the Career Roadmap (sans.org/media/security-training/roadmap.pdf) to plan your growth in your chosen career path

RELATE

- Consider how security needs in your workplace will be met with the knowledge you'll gain in a SANS course
- Know the education you receive will make you an expert resource for your team

VALIDATE

- Pursue a GIAC certification after your training to validate your new expertise
- Add a NetWars challenge to your SANS experience to prove your hands-on skills

SAVE

- Register early to pay less using early-bird specials
- Consider group discounts or bundled course packages to make the most of your training budget

ADD VALUE

- Network with fellow security experts in your industry
- Prepare thoughts and questions before arriving to share with the group
- Attend SANS@Night talks and activities to gain even more knowledge and experience from instructors and peers alike

ALTERNATIVES

- If you cannot attend a live training event in person, attend the courses virtually via SANS Simulcast
- Use SANS OnDemand or vLive to complete the same training online from anywhere in the world, at any time

ACT

- Bring the value of SANS training to your career and organization by registering for a course today, or contact us at 301-654-SANS with further questions

Return on Investment

SANS live training is recognized as the best resource in the world for information security education. With SANS, you gain significant returns on your InfoSec investment. Through our intensive immersion classes, our training is designed to help your staff master the practical steps necessary for defending systems and networks against the most dangerous threats – the ones being actively exploited.

REMEMBER

*the SANS promise:
You will be able to apply
our information security
training the day you get
back to the office!*

SEC401:

Security Essentials Bootcamp Style

Six-Day Program

Mon, Feb 29 - Sat, Mar 5

9:00am - 7:00pm (Days 1-5)

9:00am - 5:00pm (Day 6)

Laptop Required

46 CPEs

Instructor: Jonathan Ham

▶ GIAC Cert: GSEC

▶ STI Master's Program

▶ Cyber Guardian

▶ DoDD 8570

▶ OnDemand Bundle

Who Should Attend

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

"The understanding I have after taking this course is light years ahead of where I was six days ago! Fantastic and informative!"

-DON CERVONE,

BRIDGEWATER ASSOCIATES



Jonathan Ham SANS Certified Instructor

Jonathan is an independent consultant who specializes in large-scale enterprise security issues, from policy and procedure to staffing and training, scalable prevention, detection, and response technology and techniques. With a keen understanding of "return on investment" and "total cost of ownership" (and an emphasis on process over products), he has helped his clients achieve greater success for over 12 years, advising everyone from small start-ups to Fortune 500 companies and public agencies. He's been commissioned to teach NCIS investigators how to use Snort, performed packet analysis from a facility more than 2000 feet underground, and chartered and trained the CIRT for one of the largest U.S. federal agencies. He has variously held the CISSP, GSEC, GCIA, and GCIH certifications, and is a member of the GIAC Advisory Board. A former combat medic, Jonathan still spends some of his time practicing a different kind of emergency response, volunteering and teaching for both the National Ski Patrol and the American Red Cross. @jhamcorp

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

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

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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

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

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

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



giac.org



sans.edu



sans.org/cyber-guardian



sans.org/8570

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

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program
 Mon, Feb 29 - Sat, Mar 5
 9:00am - 7:15pm (Day 1)
 9:00am - 5:00pm (Days 2-6)
 37 CPEs
 Laptop Required
 Instructor: Michael Murr
 ▶ GIAC Cert: GCIH
 ▶ STI Master's Program
 ▶ Cyber Guardian
 ▶ DoDD 8570
 ▶ OnDemand Bundle

"SEC504 walks through the entire incident handling process in full-depth with practical scenarios and labs."

-CHRISTOPHER HOLDEN, PROTIVITY

"This is the real deal. This is real-world stuff that we can implement in our environments tomorrow."

-GARRETT BENIS,

PACIFIC NORTHWEST NATIONAL LABORATORY



Michael Murr SANS Principal Instructor

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

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

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

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

Who Should Attend

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



giac.org



sans.edu



sans.org/cyber-guardian



sans.org/8570

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

SEC511:

Continuous Monitoring and Security Operations

Six-Day Program
 Mon, Feb 29 - Sat, Mar 5
 9:00am - 5:00pm
 36 CPEs
 Laptop Required
 Instructor: Bryan Simon
 ▶ GIAC Cert: GMON
 ▶ Master's Program
 ▶ OnDemand Bundle

"It is only day one and I already know SEC511 will arm me with the knowledge I need to lead my security program to effectively defend my organization."

-STACEY BOIVIN, ALBERTA ELECTRIC SYSTEM OPERATOR

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

-BRAD MILHORN, COMPUCOM



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 11 GIAC certifications including GSEC, GCWN, GCIH, GCEA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, and GCUX. Bryan's scholastic achievements have resulted in the honor of sitting as a current member of the Advisory Board for the SANS Institute, and his acceptance into the prestigious SANS Cyber Guardian program. Bryan is a SANS instructor for SEC401, SEC501, SEC505, and SEC511. @BryanOnSecurity

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

The underlying challenge for organizations victimized by an attack is timely incident detection. Industry data suggest that most security breaches typically go undiscovered for an average of seven months. Attackers simply have to find one way into most organizations, because they know that the lack of visibility and internal security controls will then allow them to methodically carry out their mission and achieve their goals.

The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM) taught in this course will best position your organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach is early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and this course will greatly increase your understanding and enhance your skills in implementing CM utilizing the NIST framework.

Who Should Attend

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



giac.org



sans.edu

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

FOR408:

Windows Forensic Analysis

Six-Day Program

Mon, Feb 29 - Sat, Mar 5

9:00am - 5:00pm

36 CPEs

Laptop Required

Instructor: Heather Mahalik

▶ GIAC Cert: GCFE

▶ STI Master's Program

▶ OnDemand Bundle



“After the course, I am able to have a good picture of the whole process from the basic hands-on to the organization of findings. Excellent!”

-JENNY BLAINE,
UNIVERSITY OF MINNESOTA

“FOR408 provides in-depth knowledge of the best forensic practices that can be applied directly to investigations.”

-NATHAN LEWIS, KPMG



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.

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

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

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

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



giac.org



sans.edu



sans.org/ondemand

Heather Mahalik SANS Senior Instructor

Heather Mahalik is a project manager for Ocean's Edge, where she uses her experience to manage projects focused on wireless cybersecurity and mobile application development. Heather has over 12 years of experience in digital forensics, vulnerability discovery of mobile devices, application reverse engineering and manual decoding. She is currently the course lead for FOR585: Advanced Smartphone Forensics. Previously, Heather headed the mobile device team for Basis Technology, where she led the mobile device exploitation efforts in support of the U.S. government. She also worked as a forensic examiner at Stroz Friedberg and the U.S. State Department Computer Investigations and Forensics Lab, where she focused on high-profile cases. Heather co-authored Practical Mobile Forensics and various white papers, and has presented at leading conferences and instructed classes focused on Mac forensics, mobile device forensics, and computer forensics to practitioners in the field. Heather blogs and hosts work from the digital forensics community at www.smarterforensics.com. @HeatherMahalik

ICS/SCADA Security Essentials

Five-Day Program

Mon, Feb 29 - Fri, Mar 4

9:00am - 5:00pm

30 CPEs

Laptop Required

Instructor: Billy Rios

▶ GIAC Cert: GICSP

▶ OnDemand Bundle

SANS

SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. **ICS410:**

ICS/SCADA Security Essentials provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

The course will provide you with:

- ▶ An understanding of industrial control system components, purposes, deployments, significant drivers, and constraints
- ▶ Hands-on lab learning experiences to control system attack surfaces, methods, and tools
- ▶ Control system approaches to system and network defense architectures and techniques
- ▶ Incident-response skills in a control system environment
- ▶ Governance models and resources for industrial cybersecurity professionals
- ▶ A license to Windows 10 and a hardware PLC for students to use in class and take home with them

When examining the greatest risks and needs in critical infrastructure sectors, the course authors looked carefully at the core security principles necessary for the range of tasks involved in supporting control systems on a daily basis. While other courses are available for higher-level security practitioners who need to develop specific skills such as industrial control system penetration testing, vulnerability analysis, malware analysis, forensics, secure coding, and red team training, most of these courses do not focus on the people who operate, manage, design, implement, monitor, and integrate critical infrastructure production control systems.

When students complete this course, they will have developed an appreciation, understanding, and common language that will enable them to work together to secure their industrial control system environments. The course will help develop cyber-secure-aware engineering practices and real-time control system IT/OT support carried out by professionals who understand the physical effects of actions in the cyber world.

Who Should Attend

The course is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:

- IT (includes operational technology support)
- IT security (includes operational technology security)
- Engineering
- Corporate, industry, and professional standards

"This training really opens you up to possibilities and issues that otherwise you wouldn't really think about."

-ALFONSO BARREIRO,

PANAMA CANAL

"Very satisfied with ICS410, and the instructor was very knowledgeable and great at balancing group backgrounds (IT vs. SCADA)."

-CHAD SLATER,

THE DOW CHEMICAL COMPANY

**Billy Rios** SANS Instructor

Billy is an accomplished author and speaker recognized as one of the world's most respected experts on emerging threats related to Industrial Control Systems (ICS), critical infrastructure, and medical devices. He has discovered thousands of security vulnerabilities in hardware and software supporting ICS and critical infrastructure. He has been publicly credited by the Department of Homeland Security (DHS) over 50 times for his support to the DHS ICS Cyber Emergency Response Team (ICS-CERT). Previously, Billy was a Lead at Google, where he directed the front-line response to externally reported security issues and incidents. Prior to Google, Billy was the Security Program Manager at Internet Explorer (Microsoft), where he led the company's response for several high-profile incidents, including the response for Operation Aurora. Before Microsoft, Billy worked as a penetration tester, an intrusion detection analyst, and served as an active duty Marine Corps Officer. Billy holds an MBA and a Master of Science in Information Systems. He was a contributing author for several publications including *Hacking, the Next Generation* (O'Reilly), *Inside Cyber Warfare* (O'Reilly), and *The Virtual Battle Field* (IOS Press). @XSSniper



giac.org



sans.org/ondemand

BONUS SESSIONS – 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.

Convergence Forensics: Leveraging Multiple Skills to Analyze Evidence *Heather Mahalik*

One discipline is not enough to solve investigations relating to digital evidence. In this Keynote, Heather Mahalik will expand on scenarios where multiple skills are needed to hunt and uncover evidence. Network Forensics, Memory Forensics, Malware detection, Malware analysis and Data Synchronization between smartphones, Mac and Windows computers may change the way you need to look at your evidence. Simply having tunnel vision in your field will limit your success! A change in your approach may change your success rate when examining digital media.

Assessing Deception *Michael Murr*

This talk departs from the traditional aspects of information security and focuses on the human element of deception. Join us as we examine the process and the mechanics behind assessing deception, and dispel some of the common myths that pervade today's society. So if you are interested in learning the signs and clues that someone may be lying to you, make sure to attend this talk!

SANS

THE MOST TRUSTED NAME IN INFORMATION
AND SOFTWARE SECURITY TRAINING

*Our most
comprehensive
information security
training event of the
year...with something
for everyone!*

*SANS 2016
will be held at the*

**Walt Disney
World Swan and
Dolphin Resort**

**Register at
sans.org/sans-2016**

2016

Orlando, FL
March 12-21, 2016



Build Your Best Career

WITH!

SANS

Add an

OnDemand Bundle & GIAC Certification Attempt*

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

SPECIAL
PRICING



OnDemand Bundle

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

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

-ROBERT JONES, TEAM JONES, INC.



GIAC Certification

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

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

-CHRISTINA FORD, DEPARTMENT OF COMMERCE

MORE INFORMATION

sans.org/ondemand/bundles

giac.org



Security Awareness Training by the Most Trusted Source

Computer-based Training for your Employees

- End User**
 - Let employees train on their own schedule
- CIP v5**
 - Tailor modules to address specific audiences
- ICS Engineers**
 - Courses translated into many languages
- Developers**
 - Test learner comprehension through module quizzes
- Healthcare**
 - Track training completion for compliance reporting purposes



Visit SANS Securing The Human at securingthehuman.sans.org

Change Human Behavior | Manage Risk | Maintain Compliance | Protect Your Brand



The SANS Technology Institute transforms the world’s best cybersecurity training and certifications into a comprehensive and rigorous graduate education experience.

Master’s Degree Programs:

- ▶ M.S. in Information Security Engineering
- ▶ M.S. in Information Security Management

Specialized Graduate Certificates:

- ▶ Cybersecurity Engineering (Core)
 - ▶ Cyber Defense Operations
- ▶ Penetration Testing and Ethical Hacking
 - ▶ Incident Response

SANS Technology Institute, an independent subsidiary of SANS, is accredited by The Middle States Commission on Higher Education. 3624 Market Street | Philadelphia, PA 19104 | 267.285.5000 an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.



Eligible for veterans education benefits!

Earn industry-recognized GIAC certifications throughout the program

Learn more at www.sans.edu | info@sans.edu



GI Bill® is a registered trademark of the U.S. Department of Veterans Affairs (VA). More information about education benefits offered by VA is available at the official U.S. government website at www.benefits.va.gov/gibill.

Employers need good talent.
Veterans need good jobs.
SANS VetSuccess Immersion Academy
delivers both.

Introducing the SANS VetSuccess Immersion Academy, an intensive, accelerated program that provides the real-world training and certifications needed to fill critical jobs in cybersecurity.

For employers, the academy is a faster, more reliable, and less expensive way to find, train, certify, and employ highly qualified cybersecurity talent.

For transitioning veterans, the academy provides free accelerated training and certifications to quickly and effectively launch careers in cybersecurity.

Find out how your organization can benefit from hiring graduates or launching an academy to meet your specific talent needs.

sans.org/cybertalent/immersion-academy
Email: immersionacademy@sans.org

SANS | CyberTalent
IMMERSION ACADEMY



Read the Pilot Program
Results Report
Visit sans.org/vetsuccess

Women's Academy Pilot
1st cohort graduation
Spring 2016



VetSuccess

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING



Multi-Course Training Events

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



Community SANS

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



Private Training

Your Location! Your Schedule!
sans.org/private-training



Mentor

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



Summit

Live IT Security Summits and Training
sans.org/summit

ONLINE TRAINING



OnDemand

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



vLive

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



Simulcast

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



OnDemand Bundles

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

OTHER SANS TRAINING EVENTS

SANS Cyber Defense Initiative 2015

Washington, DC | December 12-19

SANS Las Vegas 2016

Las Vegas, NV | January 9-14

SANS Security East 2016

New Orleans, LA | January 25-30

SANS Cyber Threat Intelligence SUMMIT & TRAINING

Alexandria, VA | February 3-10

SANS Scottsdale 2016

Scottsdale, AZ | February 8-13

SANS Northern Virginia – McLean 2016

McLean, VA | February 15-20

ICS Security SUMMIT & TRAINING

Orlando, FL | February 16-23

SANS Anaheim 2016

Anaheim, CA | February 22-27

SANS 2016

Orlando, FL | March 12-21

SANS Reston 2016

Reston, VA | April 4-9

SANS Atlanta 2016

Atlanta, GA | April 4-9

Threat Hunting & Incident Response SUMMIT & TRAINING 2016

New Orleans, LA | April 12-19

SANS Pen Test Austin 2016

Austin, TX | April 18-23

SANS Security West 2016

San Diego, CA | May 1-6

SANS Cyber Guardian 2016

Baltimore, MD | May 9-14

SANS Houston 2016

Houston, TX | May 9-14

SANSFIRE 2016

Washington, DC | June 11-20

SANS Salt Lake City 2016

Salt Lake City, UT | June 27 - July 1

SANS Rocky Mountain 2016

Denver, CO | July 11-16

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



SANS PHILADELPHIA 2016

Hotel Information

Training Campus
Sonesta Philadelphia

1800 Market Street
Philadelphia, PA 19103
215-561-7500

sans.org/event/philadelphia-2016/location

Sonesta Philadelphia is both a business hub, with many Fortune 500 Companies lining its bustling streets, and a family destination with an abundance of historical landmarks, museums, art, theaters, and other family-friendly attractions. Philadelphia is steeped in history, and no visit is complete without seeing the famous Liberty Bell, or a number of other well-known historic attractions.

Special Hotel Rates Available

A special discounted rate of \$149.00 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 Feb. 4, 2016.

Top 5 reasons to stay at the Sonesta Philadelphia

- 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 Sonesta Philadelphia, 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 Sonesta Philadelphia that you won't want to miss!
- 5 Everything is in one convenient location!

SANS PHILADELPHIA 2016

Registration Information

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



Register online at sans.org/event/philadelphia-2016/courses

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

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



Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	1-6-16	\$400.00	1-27-16	\$200.00

Some restrictions apply.

Group Savings (Applies to tuition only)

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

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

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

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by February 10, 2016 — processing fees may apply.


SANS Voucher Credit Program

Expand your training budget! Extend your fiscal year. The SANS Voucher Discount Program pays you credits and delivers flexibility.




sans.org/vouchers

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

WEBCASTS

-  **Ask The Expert Webcasts** — SANS experts bring current and timely information on relevant topics in IT Security.
-  **Analyst Webcasts** — A follow-on to the SANS Analyst Program, Analyst Webcasts provide key information from our whitepapers and surveys.
-  **WhatWorks Webcasts** — The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT Security issues.
-  **Tool Talks** — Tool Talks are designed to give you a solid understanding of a problem, and to show how a vendor's commercial tool can be used to solve or mitigate that problem.

NEWSLETTERS

-  **NewsBites** — Twice-weekly high-level executive summary of the most important news relevant to cybersecurity professionals
-  **OUCH!** — The world's leading monthly free security-awareness newsletter designed for the common computer user
-  **@RISK: The Consensus Security Alert** — A reliable weekly summary of (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) how recent attacks worked, and (4) other valuable data

OTHER FREE RESOURCES

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

sans.org/security-resources