

SANS

Portland 2016

August 8-13

SANS OFFERS HANDS-ON, IMMERSION-STYLE
INFORMATION SECURITY TRAINING
TAUGHT BY REAL-WORLD PRACTITIONERS

**SAVE
\$400**

by registering
and paying early!

See page 13 for
more details.

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

Five courses on
CYBER DEFENSE
PEN TESTING
DIGITAL FORENSICS
ICS SECURITY

*"SANS training is superior
to other training programs
and far exceeded my
expectations!"*

-PAUL PETRASKO,
BEMIS COMPANY, INC.

REGISTER AT
sans.org/portland



GIAC-Approved
Training

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 Portland 2016 lineup of instructors includes:



Tim Conway
SANS Instructor



Adrien de Beaupre
Certified Instructor



My-Ngoc Nguyen
Certified Instructor



Bryan Simon
Certified Instructor



Chad Tilbury
Senior Instructor

Evening Bonus Sessions

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

KEYNOTE: Lessons in Incident Response – Chad Tilbury

HTTPDeux – Adrien de Beaupre

Continuous Ownage: Why You Need Continuous Monitoring – Bryan Simon



The training campus for SANS Portland 2016 is DoubleTree by Hilton Portland, a stylish and contemporary destination which proves that comfort and green living can work perfectly together; all while delivering the relaxing and inviting lodging experience for which DoubleTree is renowned.

SEE PAGE 13

Be sure to register and pay by June 15th for a \$400 tuition discount!

Courses-at-a-Glance

		MON 8-8	TUE 8-9	WED 8-10	THU 8-11	FRI 8-12	SAT 8-13
SEC401	Security Essentials Bootcamp Style	Page 2					
SEC560	Network Penetration Testing and Ethical Hacking	Page 3					
FORS08	Advanced Digital Forensics and Incident Response	Page 4					
MGT512	SANS Security Leadership Essentials for Managers with Knowledge Compression™	Page 5					
ICS456	Essentials for NERC Critical Infrastructure Protection	Page 6 NEW!					

Register today for SANS Portland 2016!
sans.org/portland



@SANSInstitute
Join the conversation:
#SANSPortland

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 the SANS Voucher Program 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!*

Security Essentials Bootcamp Style

Six-Day Program

Mon, Aug 8 - Sat, Aug 13

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

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

46 CPEs

Laptop Required

Instructor: Bryan Simon



giac.org



sans.edu



sans.org/cyber-guardian



sans.org/8140

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

"This course will give me
valuable insight to
support my job as a
cybersecurity engineer."

-ERIK MILLER, EXELON GENERATION



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

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 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.

Who Should Attend

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

SEC560:

Network Penetration Testing and Ethical Hacking

Six-Day Program

Mon, Aug 8 - Sat, Aug 13

9:00am - 7:15pm (Day 1)

9:00am - 5:00pm (Days 2-6)

37 CPEs

Laptop Required

Instructor:

Adrien de Beaupre



giac.org



sans.edu



sans.org/cyber-guardian



**BUNDLE
ONDEMAND**
WITH THIS COURSE

sans.org/ondemand

"This course provides

validation and

confirmation of your skills

and concepts, and then

blows your mind with

super powers."

-TRIP HILLMAN, WEAVER LLP



Adrien de Beaupre SANS Certified Instructor

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

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

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.

"The course content is excellent and coherently organized.

It will provide high value to my job." -MARGARITA JAUREGUI, INTEL CORPORATION

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.

FOR508:

Advanced Digital Forensics and Incident Response

Six-Day Program

Mon, Aug 8 - Sat, Aug 13

9:00am - 5:00pm

36 CPEs

Laptop Required

Instructor: Chad Tilbury



giac.org



sans.edu



sans.org/cyber-guardian



sans.org/8140

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



Chad Tilbury SANS Senior Instructor

Chad Tilbury has been responding to computer intrusions and conducting forensic investigations since 1998. His extensive law enforcement and international experience stems from working with a broad cross-section of Fortune 500 corporations and government agencies around the world. During his service as a Special Agent with the U.S. Air Force Office of Special Investigations, he investigated and conducted computer forensics for a variety of crimes, including hacking, abduction, espionage, identity theft, and multi-million dollar fraud cases. He has led international forensic teams and was selected to provide computer forensic support to the United Nations Weapons Inspection Team. Chad has worked as a computer security engineer and forensic lead for a major defense contractor and as the Vice President of Worldwide Internet Enforcement for the Motion Picture Association of America. In that role, he managed Internet anti-piracy operations for the seven major Hollywood studios in over 60 countries. Chad is a graduate of the U.S. Air Force Academy and holds a B.S. and M.S. in Computer Science as well as GCFA, GCIH, GREM, and ENCE certifications. He is currently a consultant specializing in incident response, corporate espionage, and computer forensics. @chadtilbury

SANS

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

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

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

Over 80% of all breach victims learn of a compromise from third-party notifications, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years.

“The instructor was beyond qualified and excellent! He took the time to answer questions and help the students, and the exercises flowed very well with the instruction.” -WILFREDO HERNANDEZ, FL DEPT. OF LAW ENFORCEMENT

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

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

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

Who Should Attend

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

SANS Security Leadership Essentials for Managers with Knowledge Compression™

Five-Day Program

Mon, Aug 8 - Fri, Aug 12

9:00am - 6:00pm (Days 1-4)

9:00am - 4:00pm (Day 5)

33 CPEs

Laptop NOT Needed

Instructor: My-Ngoc Nguyen



giac.org



sans.edu



sans.org/8140


**BUNDLE
ONDEMAND**

WITH THIS COURSE

sans.org/ondemand

"The course content is great because it is consistently updated to reflect current IT trends."

-TERENCE B.,

OFFICER TRAINING COMMAND



My-Ngoc Nguyen SANS Certified Instructor

My-Ngoc Nguyen (pronounced Mee-Nop Wynn) is the CEO/Principal Consultant for Secured IT Solutions. She brings 15 years of experience in information systems and technology, with the past 12 years focused on cybersecurity and information assurance for both the government and commercial sectors. My-Ngoc is highly experienced in IT security and risk methodologies, and legal and compliance programs. She led a cybersecurity program under a federal agency for a highly-regulated, first-of-a-kind project of national importance. With that experience, she has been assisting client organizations in both the public and private sectors to implement secure and compliant business processes and IT solutions using defense-in-depth and risk-based approaches. Along with a Master's degree in Management Information Systems, she carries top security certifications that include GPEN, GCIH, GSEC, and CISSP, and she is a former QSA. My-Ngoc has held a Top Security/Q clearance. She is an active member of the FBI's InfraGard, the Information Systems Security Association (ISSA), the Information Systems Audit and Control Association (ISACA), and the International Information Systems Security Certification Consortium (ISC). My-Ngoc co-founded the non-profit organization CyberSafeNV to raise security awareness in Nevada and is presently the chairman. @MenopN

This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to manage security. Lecture sections are intense; the most common student comment is that it's like drinking from a fire hose. The diligent manager will learn vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. In addition, the course has been engineered to incorporate the NIST Special Publication 800 series guidance so that it can be particularly useful to U.S. government managers and supporting contractors.

Essential security topics covered in this management track include network fundamentals and applications, power, cooling and safety, architectural approaches to defense in depth, cyber attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, web application security, and offensive and defensive information warfare, culminating with our management practicum. The material uses Knowledge Compression™, special charts, and other proprietary SANS techniques to help convey the key points of critical slides and keep the information flow rate at a pace senior executives demand every teaching hour of the course. The course has been evaluated and approved by CompTIA's CAQC Program for Security+ 2008 to ensure that managers and their direct reports have a common baseline for security terminology and concepts. You will be able to put what you learn into practice the day you get back into the office.

Knowledge Compression™

Maximize your learning potential!

Knowledge Compression™ is an optional add-on feature to a SANS class that aims to maximize the absorption and long-term retention of large amounts of data over a relatively short period of time. Through the use of specialized training materials, in-class reviews, examinations and test-taking instruction, Knowledge Compression™ ensures students have a solid understanding of the information presented to them. By attending classes that feature this advanced training product, you will experience some of the most intense and rewarding training programs SANS has to offer, in ways that you never thought possible!

Who Should Attend

- ▶ All newly appointed information security officers
- ▶ Technically-skilled administrators who have recently been given leadership responsibilities
- ▶ Seasoned managers who want to understand what their technical people are telling them

Essentials for NERC Critical Infrastructure Protection

NEW

SANS

Five-Day Program
 Mon, Aug 8 - Fri, Aug 12
 9:00am - 5:00pm
 30 CPEs
 Laptop Required
 Instructor: Tim Conway

Who Should Attend

- ▶ IT and OT (ICS) cybersecurity
- ▶ Field support personnel
- ▶ Security operations personnel
- ▶ Incident response personnel
- ▶ Compliance staff
- ▶ Team leaders
- ▶ Governance officials
- ▶ Vendors/Integrators
- ▶ Auditors

“SANS course work is the most thorough learning available anywhere. What you learn is not only conceptual, but it also is hands-on showing you what you do, why you do it, and how you can apply what you learn to real-world solutions to problems.”

-DUANE TUCKER,
 BAYMARK PARTNERS

ICS456: Essentials for NERC Critical Infrastructure Protection is a five-day course that empowers students with knowledge of the “what” and the “how” of the Version 5/6 standards. The course addresses the role of the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), and the regional entities. It provides multiple approaches to identifying and categorizing BES Cyber Systems and helps asset owners determine the specific implementations applicable to the requirements. Additionally, the course covers implementation strategies for the Version 5/6 standards with a balanced practitioner approach to both cybersecurity benefits and regulatory compliance. The course sections are as follows:

ICS456.1: Asset Identification and Governance A transition is under way from NERC Critical Infrastructure Protection (CIP) programs that are well defined and understood to a new CIP paradigm that expands its scope into additional environments and adds significantly more complexity. On day one, students will develop an understanding of the electric sector regulatory structure and history as well as an appreciation for how the CIP standards fit into the overall framework of the reliability standards.

ICS456.2: Access Control and Monitoring Strong physical and cyber access controls are at the heart of any good cybersecurity program. On day two we move beyond the “what” of CIP compliance to understanding the “why” and the “how.”

ICS456.3: System Management CIP-007 has consistently been one of the most violated standards going back to CIP version 1. With the CIP standards moving to a systematic approach with varying requirement applicability based on system impact rating, the industry now has new ways to design and architect system management approaches. Throughout day three, students will dive into CIP-007.

ICS456.4: Information Protection and Response Education is key to every organization's success with NERC CIP. After this session on information protection and response, ICS456 students will be knowledgeable advocates for CIP when they return to their place of work.

ICS456.5: CIP Process On the final day students will learn the key components for running an effective CIP compliance program. Topics will include CIP processes for maintaining compliance, preparing for an audit and following up on it, CIP industry activities, standards process, and the CIP of the future.



Tim Conway SANS Instructor

Tim is the Technical Director of ICS and SCADA programs at SANS. He is responsible for developing, reviewing, and implementing technical components of the SANS ICS and SCADA product offerings. He previously served as the Director of CIP Compliance and Operations Technology at Northern Indiana Public Service Company (NIPSCO), where he was responsible for Operations Technology, NERC CIP Compliance, and the NERC training environments for the operations departments within NIPSCO Electric. Tim was also an EMS Computer Systems Engineer at NIPSCO for eight years, with responsibility over the control system servers and the supporting network infrastructure. He was the chair of the RFC CIPC, and is the current chair of the NERC CIP Interpretation Drafting Team, member of the NESCO advisory board, chair of the NERC CIPC GridEx Working Group, and chair of the NBISE Smart Grid Cyber Security panel.

SANS@NIGHT EVENING TALKS

KEYNOTE: Lessons in Incident Response – *Chad Tilbury*

As more organizations face off against advanced adversaries, classic incident response processes are being adapted and updated to address new threats and speed the recovery process. This talk illustrates multiple real-world case studies demonstrating some exciting new approaches to incident response. Learn how incident response teams are detecting, responding to and attributing attacks from targeted attackers, and get a taste for the future of incident response.

HTTPDeux – *Adrien de Beaupre*

This talk will discuss the HTTP/2 protocol, which has only recently been approved and published. The agenda will include reasons why the new protocol was developed, how it is implemented, tools that can use it, and challenges it presents to penetration testers.

Continuous Ownage: Why You Need Continuous Monitoring

– *Bryan Simon*

Repeat after me: I will be breached. Most organizations realize this fact too late, usually after a third party informs them months after the initial compromise. Treating security monitoring as a quarterly auditing process means most compromises will go undetected for weeks or months. The attacks are continuous, and the monitoring must match. This talk will help you face this problem and describe how to move your organization to a more defensible security architecture that enables continuous security monitoring. The talk will also give you a hint at the value you and your organization will gain from attending SANS SEC511: Continuous Monitoring and Security Operations.

SANS

NETWORK SECURITY

Las Vegas

September 10-19, 2016

*Save
the
Date!*

SAVE \$400

Register and pay for any long course and
enter code **EarlyBird16** before 7/20/16.

sans.org/NetworkSecurity-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

www.sans.org/ondemand/bundles

www.giac.org

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 sponsoring an academy to meet your specific talent needs.

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

SANS | **CyberTalent**
IMMERSION ACADEMY



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

*Women's Academy Pilot
1st cohort graduation
Spring 2016*



VetSuccess



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

SANS
Technology
Institute

**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 the VA is available at the official U.S. government website at www.benefits.va.gov/gibill.

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

FUTURE SANS TRAINING EVENTS

SANSFIRE 2016

Washington, DC | Jun 11-18

Digital Forensics & Incident Response

SUMMIT & TRAINING 2016

Austin, TX | Jun 23-30

Salt Lake City 2016

Salt Lake City, UT | Jun 27 - Jul 2

Rocky Mountain 2016

Denver, CO | Jul 11-16

Minneapolis 2016

Minneapolis, MN | Jul 18-23

San Antonio 2016

San Antonio, TX | Jul 18-23

ICS Security & Training – Houston 2016

Houston, TX | Jul 25-30

San Jose 2016

San Jose, CA | Jul 25-30

Boston 2016

Boston, MA | Aug 1-6

Security Awareness

SUMMIT & TRAINING 2016

San Francisco, CA | Aug 1-10

Dallas 2016

Dallas, TX | Aug 8-13

Data Breach Summit

Chicago, IL | Aug 18

Chicago 2016

Chicago, IL | Aug 22-27

Virginia Beach 2016

Virginia Beach, VA | Aug 22 - Sep 2

Crystal City 2016

Crystal City, VA | Sep 6-11

Network Security 2016

Las Vegas, NV | Sep 10-19

Seattle 2016

Seattle, WA | Oct 3-8

The latest information on all events can be found at

sans.org/security-training/by-location/all



SANS PORTLAND 2016
Hotel Information
Training Campus
DoubleTree by Hilton Portland
1000 NE Multnomah Street
Portland, OR 97232
503-281-6111
sans.org/event/portland-2016/location

The newly renovated DoubleTree by Hilton Portland is a stylish and contemporary destination and proof that comfort and green living can work perfectly together; all while delivering the relaxing and inviting lodging experience for which DoubleTree is renowned. Conveniently located in the heart of Portland's thriving metro area, the DoubleTree by Hilton Portland is close to public transportation and within walking distance to top Portland attractions.

Special Hotel Rates Available

A special discounted rate of \$199.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through July 15, 2016. To make reservations, please call (503) 281-6111 and ask for the SANS group rate.

Top 5 reasons to stay at DoubleTree by Hilton Portland

- 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 DoubleTree by Hilton Portland 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 DoubleTree by Hilton Portland that you won't want to miss!
- 5 Everything is in one convenient location!

SANS PORTLAND 2016
Registration Information
We recommend you register early to ensure you get your first choice of courses.



Register online at sans.org/portland

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

Use code
EarlyBird16
 when registering early

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	6-15-16	\$400.00	7-13-16	\$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.

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 July 20, 2016 — processing fees may apply.

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