THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS Las Vegas 2016

Las Vegas, NV January 9-14

Choose from these popular courses:

Cyber Threat Intelligence ***NEW!***

Security Essentials Bootcamp Style

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS Training Program for CISSP® Certification

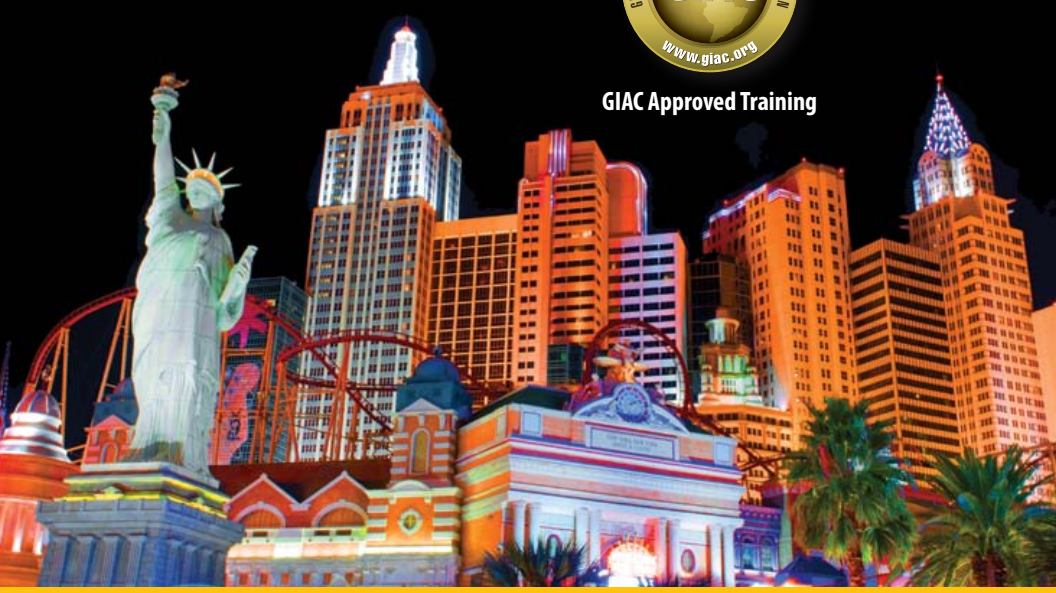
SANS Security Leadership Essentials For Managers with Knowledge Compression™

ICS/SCADA Security Essentials

"SANS continues to deliver instructors with high caliber, and content that is in line with current security trends, which is a need for security practitioners."

-Daniel Garcia, Baker Hughes

GIAC Approved Training



SAVE $400 on SANS Las Vegas courses!

Register and pay by Nov 18th – sans.org/las-vegas-2016

SANS Instructors

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

Mike Cloppert
SANS Instructor

Eric Conrad
Senior Instructor

Bryce Galbraith
Principal Instructor

Paul A. Henry
Senior Instructor

David Hoelzer
Faculty Fellow

John Strand
Senior Instructor

Evening Bonus Sessions

Don't miss these extra evening presentations that make SANS a great value for your security training:

Evolving Threats and Defenses – Paul A. Henry

Assessing, Testing, and Breaking Security Products – John Strand

Continuous Ownage: Why you Need Continuous Monitoring – Eric Conrad

How to Bring Some Advanced Persistent Trickery to Your Fight Against Advanced Persistent Threats – Bryce Galbraith

GnuRadio Bootstrap: Getting Started in Software-Defined Radio!

PAGE 8

Be sure to register and pay by Nov 18th for a $400 tuition discount!

The training campus for SANS Las Vegas 2016, Tuscany Suites & Casino, features spacious hotel accommodations, award-winning dining, casino gaming, and a variety of live entertainment. Experience all the excitement Las Vegas has to offer in a prime location, just two blocks away from the famous Las Vegas Strip.

PAGE 13

Courses-at-a-Glance

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!

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Sat, Jan 9 - Thu, Jan 14
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Bryce Galbraith

- 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

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

Bryce Galbraith *SANS Principal Instructor*

As a contributing author of the internationally bestselling book *Hacking Exposed: Network Security Secrets & Solutions*, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. Bryce has held security positions at global ISPs and Fortune 500 companies, was a member of Foundstone's renowned penetration testing team, and served as a senior instructor and co-author of Foundstone's Ultimate Hacking: Hands-On course series. Bryce is currently the owner of Layered Security, where he provides specialized vulnerability assessment and penetration testing services for clients. He teaches several of the SANS Institute's most popular courses and develops curriculum around current topics. He has taught the art of ethical hacking and countermeasures to thousands of IT professionals from a who's who of top companies, financial institutions, and government agencies around the globe. Bryce is an active member of several security-related organizations, holds several security certifications, and speaks at conferences around the world. @brycegalbraith

SECURITY 504

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Sat, Jan 9 - Thu, Jan 14
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: John Strand

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

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
- 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

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, 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.

"This course gave me a better understanding of what a hacker can do and how he does it – which will help me with incident handling."
-Jill Gallagher, HSBC

"This course helped me fill in the finer details and gaps in my knowledge. I understood the higher level concepts. I have worked with a few of the tools but this helped put it all together."
-Jenna Esparza, Los Alamos National Laboratory

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

Bundle OnDemand with this course
sans.org/ondemand

John Strand *SANS Senior Instructor*

Along with SEC504, John Strand also teaches SEC560: Network Penetration Testing and Ethical Hacking; SEC580: Metasploit Kung Fu for Enterprise Pen Testing; and SEC464: Hacker Detection for System Administrators. John is the course author for SEC464 and the co-author for SEC580. When not teaching for SANS, John co-hosts PaulDotCom Security Weekly, the world's largest computer security podcast. He also is the owner of Black Hills Information Security, specializing in penetration testing and security architecture services. He has presented for the FBI, NASA, the NSA, and at DefCon. In his spare time he writes loud rock music and makes various futile attempts at fly fishing. @strandjs

FORENSICS 578

Cyber Threat Intelligence

NEW

SANS

Five-Day Program
Sat, Jan 9 - Wed, Jan 13
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Mike Cloppert
▸ OnDemand Bundle

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

FOR578: Cyber Threat Intelligence will help network defenders and incident responders:

- Construct and exploit threat intelligence to detect, respond, and defeat advanced persistent threats (APTs)
- Fully analyze successful and unsuccessful intrusions by advanced attackers
- Piece together intrusion campaigns, threat actors, and nation-state organizations
- Manage, share, and receive intelligence on APT adversary groups
- Generate intelligence from their own data sources and share it accordingly
- Identify, extract, and leverage intelligence from APT intrusions
- Expand upon existing intelligence to build profiles of adversary groups
- Leverage intelligence to better defend against and respond to future intrusions

Who Should Attend

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

"Mike Cloppert rocks. Obviously, he's very smart and passionate about what he does."
-Nate DeWitt, eBay

Conventional network defenses such as intrusion detection systems and anti-virus tools focus on the vulnerability component of risk, and traditional incident response methodology pre-supposes a successful intrusion. However, the evolving sophistication of computer network intrusions has rendered these approaches insufficient to address the threats faced by modern networked organizations. Today's adversaries accomplish their goals using advanced tools and techniques designed to circumvent most conventional computer network defense mechanisms, go undetected during the intrusion, and then remain undetected on networks over long periods of time.

The collection, classification, and exploitation of knowledge about adversaries – collectively known as cyber threat intelligence – gives network defenders information superiority that can be used to reduce the adversary's likelihood of success with each subsequent intrusion attempt. Responders need accurate, timely, and detailed information to monitor new and evolving attacks, as well as methods to exploit this information to put in place an improved defensive posture. Threat intelligence thus represents a force multiplier for organizations looking to update their response and detection programs to deal with increasingly sophisticated advanced persistent threats.

During a targeted attack, an organization needs a top-notch and cutting-edge incident response armed with the critical intelligence necessary to understand how adversaries operate and to combat the threat. FOR578 will train you and your team to detect, scope, and select resilient courses of action in response to such intrusions and data breaches.

THERE IS NO TEACHER BUT THE ENEMY!

Mike Cloppert *SANS Instructor*

Michael is the lead analyst for Lockheed Martin CIRT's Intel Fusion team, charged with collecting and managing intelligence on adversaries intent on stealing the organization's intellectual property, and with developing new detection and analysis techniques. Michael has worked as a security analyst in various sectors including the financial industry, federal government, and defense industry. He has an undergraduate degree in Computer Engineering from the University of Dayton and an MS in Computer Science from The George Washington University, has received a variety of industry certifications including SANS GCIA, GREM, and GCFA, and is a SANS Forensics and IR blog contributor. Michael's past speaking engagements include the DC3 Cybercrime Conference and the IEEE, along with various SANS events and many other engagements. @mikecloppert

MANAGEMENT 414

SANS Training Program for CISSP® Certification

SANS

Six-Day Program
Sat, Jan 9 - Thu, Jan 14
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPEs
Laptop NOT Needed
Instructor: Eric Conrad

- GIAC Cert: GISP
- DoDD 8570
- OnDemand Bundle

Note:
The CISSP® exam itself is not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam. Please note as well that the GISP exam offered by GIAC is NOT the same as the CISSP® exam offered by (ISC)².

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

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that has been specifically updated to prepare you to pass the 2015 version of the CISSP® exam.

Course authors Eric Conrad and Seth Misenar have revised MGT414 to take into account the 2015 updates to the CISSP® exam and prepare students to navigate all types of questions included in the new version.

MGT414 focuses solely on the 8 domains of knowledge as determined by (ISC)² that form a critical part of CISSP® exam. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

Who Should Attend

- Security professionals who want to understand the concepts covered in the CISSP® exam as determined by (ISC)²
- Managers who want to understand the critical areas of network security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® 8 domains
- Security professionals and managers looking for practical ways to apply the 8 domains of knowledge to their current activities

You Will Be Able To:

- Understand the 8 domains of knowledge that are covered on the CISSP® exam
- Analyze questions on the exam and be able to select the correct answer
- Apply the knowledge and testing skills learned in class to pass the CISSP® exam
- Understand and explain all of the concepts covered in the 8 domains of knowledge
- Apply the skills learned across the 8 domains to solve security problems when you return to work

GISP
giac.org

sans.org/8570

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Take advantage of the SANS CISSP® Get Certified Program currently being offered.
sans.org/special/cissp-get-certified-program

Eric Conrad *SANS Senior Instructor*

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

MANAGEMENT 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program
Sat, Jan 9 - Wed, Jan 13
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop NOT Needed
Instructor: David Hoelzer

- GIAC Cert: GSLC
- STI Master's Program
- DoDD 8570
- OnDemand Bundle

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. Additionally, 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.

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

"The blending of management and technologies in a course is challenging. SANS course writers and instructors provide timely information to their students."
-James Lamadrid, Federal Government

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!

giac.org

sans.edu

sans.org/8570

Bundle OnDemand with this course
sans.org/ondemand

David Hoelzer *SANS Faculty Fellow*

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

INDUSTRIAL CONTROL SYSTEMS 410

ICS/SCADA Security Essentials

SANS

Five-Day Program
Sat, Jan 9 - Wed, Jan 13
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Paul A. Henry
- GIAC Cert: GICSP
- OnDemand Bundle

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.

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

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.

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.

giac.org

BUNDLE ONDEMAND WITH THIS COURSE
sans.org/ondemand

"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

Paul A. Henry *SANS Senior Instructor*

Paul Henry 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. Paul 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 Department of Defense's Satellite Data Project (USA), and both government as well as telecommunications projects throughout Southeast Asia. Paul is frequently cited by major and trade print publications as an expert in 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 serves as a featured speaker at seminars and conferences worldwide, delivering presentations on diverse topics including anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, perimeter security, and incident response. @phenrycissp

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: Evolving Threats and Defenses

Paul A. Henry

For nearly two decades, defenders have fallen into the "crowd mentality trap." They have simply settled on doing the same thing everyone else was doing, while at the same time attackers have clearly evolved both in terms of malware delivery vectors and attack methodology. Today our defenses focus primarily on the gateway and on attempting to outwit attacker's delivery methods. This leaves us woefully exposed, and according to a recent Data Breach Report has resulted in 3,765 incidents, 806 million records exposed, and $157 billion in data breach costs in only the past six years. This presentation will highlight recent/current developments in the evolution of both attacks and defenses.

Assessing, Testing and Breaking Security Products

John Strand

In this talk we will be covering how to properly test the various security tools like AV/IDS/IPS/DLP your organization depends on every day. We will also be sharing part of the framework BHIS uses to evaluate these controls for companies. Because sharing is caring.

Continuous Ownage: Why You Need Continuous Monitoring

John Strand

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 Seth Misenar and Eric Conrad's new course: SANS SEC511: Continuous Monitoring and Security Operations.

How to Bring Some Advanced Persistent Trickery to Your Fight Against Advanced Persistent Threats

Bryce Galbraith

You know you have intruders in your house...but this is your house and no one knows it better than you. Don't sit back and wait. It's game on... This presentation will explore ways that you can frustrate, annoy, and potentially reveal Advanced Persistent Threats (APTs) with active defense, offensive countermeasures and cyber deception (legally and ethically).

GnuRadio Bootstrap: Getting Started in Software-Defined Radio!

Build Your Best Career

WITH

SANS

Add an

OnDemand Bundle & **GIAC Certification Attempt**

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

SPECIAL PRICING

OnDemand Bundle

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

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

-Robert Jones, Team Jones, Inc.

GIAC Certification

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

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

-Christina Ford, Department of Commerce

MORE INFORMATION

www.sans.org/ondemand/bundles www.giac.org

*GIAC and OnDemand Bundles are only available for certain courses.

SANS SECURING THE HUMAN

Security Awareness Training by the Most Trusted Source

Computer-based Training for your Employees

End User
Phishing
CIP v5
ICS Engineers
Developers
Healthcare

- Let employees train on their own schedule
- Tailor modules to address specific audiences
- Courses translated into many languages
- Test learner comprehension through module quizzes
- Track training completion for compliance reporting purposes
- Test employee behavior through phishing emails

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.

POST 9/11 GI BILL

Now eligible for Veterans Education benefits!
Earn industry-recognized GIAC certifications throughout the program
Learn more at www.sans.edu | info@sans.edu

GIAC GLOBAL INFORMATION ASSURANCE CERTIFICATION www.giac.org

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.

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

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

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

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

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

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

ONLINE TRAINING

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

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

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

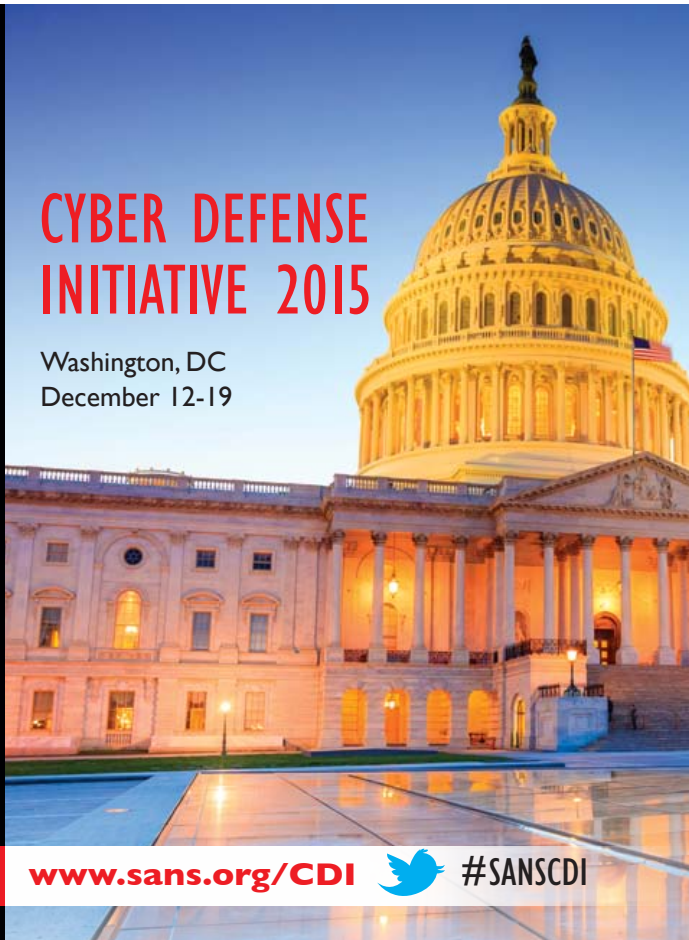
OnDemand Bundles sans.org/ondemand/bundles
Extend Your Training with an OnDemand Bundle Including Four Months of E-learning

SANS

CDI

Cyber Defense and Security Training

Over 25 hands-on immersion courses along with NetWars Tournaments



REGISTER AT www.sans.org/CDI #SANSCDI

FUTURE SANS TRAINING EVENTS

SANS Cyber Defense San Diego 2015
San Diego, CA | Oct 19-24 | #CyberDefSD

SANS South Florida 2015
Fort Lauderdale, FL | Nov 9-14

SANS Pen Test Hackfest SUMMIT & TRAINING 2015
Alexandria, VA | Nov 16-23

SANS San Francisco 2015
San Francisco, CA | Nov 30 - Dec 5

SANS Security Leadership SUMMIT & TRAINING 2015
Dallas, TX | Dec 3-10

SANS Security East 2016
New Orleans, LA | Jan 25-30

SANS Scottsdale 2016
Scottsdale, AZ | Feb 8-13

SANS McLean 2016
McLean, VA | Feb 15-20

SANS Anaheim 2016
Anaheim, CA | Feb 22-27

SANS Philadelphia 2016
Philadelphia, PA | Feb 29 - Mar 5

SANS 2016
Orlando, FL | Mar 12-21

SANS Reston 2016
Reston, VA | Apr 4-9

SANS Atlanta 2016
Atlanta, GA | Apr 4-9

SANS Austin 2016
Austin, TX | Apr 18-23

SANS Security West 2016
San Diego, CA | May 1-6

SANS Houston 2016
Houston, TX | May 9-14

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

SANS LAS VEGAS 2016

Hotel Information

Training Campus
Tuscany Suites and Casino

255 E. Flamingo Road
Las Vegas, NV 89169 US
702-732-2564
sans.org/event/las-vegas-2016/location

Discover the pleasures of our all-suites Las Vegas Resort. Tuscany Suites & Casino features the best in spacious hotel accommodations, award-winning dining, exciting casino gaming, and a variety of live entertainment. Experience the excitement of all Las Vegas has to offer in a prime location, just two blocks away from the famous Las Vegas Strip and minutes away from McCarran International Airport.

Special Hotel Rates Available

A special discounted rate of $96.00 S/D will be honored based on space availability.

The SANS room rate is less than the current prevailing government per diem rate for Las Vegas. Should this change per diem rooms will be made available. These rates include high-speed Internet in your room and are only available through Dec. 8, 2015.

Top 5 reasons to stay at the Tuscany Suites and Casino

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 Tuscany Suites and Casino 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 Tuscany Suites and Casino that you won't want to miss!
5. Everything is in one convenient location!

SANS LAS VEGAS 2016

Registration Information

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

Register online at sans.org/las-vegas-2016/courses

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

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

Use code **EarlyBird16** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**11/18/15**	**$400.00**	**12/9/15**	**$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 December 16, 2015 – 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
sans.org/security-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 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) insightful explanations of how recent attacks worked, and other valuable data

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)