SANS CyberCon 2014

Online Training Event

Intense courses. Top instructors. No travel.

> *"I was surprised how much I liked this format (live virtual delivery). Because I have attended other SANS classes in person, I was skeptical, but I loved it."*
>
> -Jon Truan,
> Oak Ridge National Laboratory

Choose from seven popular courses:

Security Essentials Bootcamp Style

Network Penetration Testing and Ethical Hacking

Web App Penetration Testing and Ethical Hacking

SANS® +S™ Training Program for the CISSP® Certification Exam

Law of Data Security and Investigations

Auditing Security & Controls of Active Directory & Windows

Auditing Security and Controls of Oracle Databases

Register at www.sans.org/cybercon

SANS

Symantec.

Platinum Sponsor

Save $400 by registering early! See page 13 for more details.

What Is SANS CyberCon?

SANS CyberCon is a live online training event that meets in virtual classrooms, allowing students to interact directly with their classmates and instructors. SANS CyberCon students attend popular courses that are taught online by SANS' top instructors. Students also have the opportunity to attend daily bonus sessions that discuss current topics in information security.

In short, SANS CyberCon is perfect for professionals who wish to keep their skills current but cannot travel due to personal or professional commitments!

Why Choose SANS CyberCon?

Zero travel costs

Easier to get approved and ideal for individuals with no travel budget

Flexible

Get the training you need without neglecting your family and work obligations

Archive access

All class sessions are recorded and can be replayed for four months

Vouchers

CyberCon is a great way to spend voucher dollars

Courses-at-a-Glance

<table>
<tr><th>Courses-at-a-Glance</th><th>MON
2/10</th><th>TUE
2/11</th><th>WED
2/12</th><th>THU
2/13</th><th>FRI
2/14</th><th>SAT
2/15</th></tr>
<tr><td>SEC401 Security Essentials Bootcamp Style</td><td colspan="6">PAGE 2</td></tr>
<tr><td>SEC542 Web App Penetration Testing and Ethical Hacking</td><td colspan="6">PAGE 3</td></tr>
<tr><td>SEC560 Network Penetration Testing and Ethical Hacking</td><td colspan="6">PAGE 4</td></tr>
<tr><td>LEG523 Law of Data Security and Investigations</td><td colspan="5">PAGE 5</td><td></td></tr>
<tr><td>MGT414 SANS® +S™ Training Program for the CISSP® Cert Exam</td><td colspan="6">PAGE 6</td></tr>
<tr><td>AUD444 Auditing Security and Controls of Active Directory and Windows</td><td colspan="3">PAGE 7</td><td></td><td></td><td></td></tr>
<tr><td>AUD445 Auditing Security and Controls of Oracle Databases</td><td></td><td></td><td></td><td colspan="3">PAGE 7</td></tr>
</table>

Testimonials from SANS CyberCon Alumni

"CyberCon was the perfect solution for me. Because it was virtual, I was able to attend class on the first day without having to cancel a weekend getaway. Also, since I was paying for this myself not having to cover travel was huge."

-Mark Dirks, Steptoe & Johnson LLP

"The training event was a success and will be a great example that we at CoVantage Credit Union can use to show the feasibility of online learning."

-Aaron Hurt, CoVantage Credit Union

"Cybercon is the most learning you will do while you are still in your Pajamas... or "night job" clothes. It was a great class."

-Paul Tate, Raytheon

SECURITY 401

Security Essentials Bootcamp Style

Six-Day Program
Mon, Feb 10 - Sat, Feb 15
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPE/CMU Credits
Instructor: Dr. Eric Cole

- GIAC Cert: GSEC
- Masters Program
- Cyber Guardian
- DoDD 8570

SEC401's focus is to teach individuals the essential skills, methods, tricks, tools and techniques needed to protect and secure an organization's critical information assets and business systems. This course teaches you the right things that need to be done to keep an organization secure. The focus is not on theory but practical hands-on tools and methods that can be directly applied when a student goes back to work in order to prevent all levels of attacks, including the APT (advanced persistent threat). In addition to hands-on skills, we will teach you how to put all of the pieces together to build a security roadmap that can scale today and into the future. When you leave our training we promise that you will have the techniques that you can implement today and tomorrow to keep your organization at the cutting edge of cyber security. Most importantly, your organization will be secure because students will have the skill sets to use the tools to implement effective security.

With the APT, organizations are going to be targeted. Whether the attacker is successful penetrating an organization's network depends on the organization's defense. While 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 works in cyber security. 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 cyber security, three questions must be answered:

1. What is the risk?
2. Is it the highest priority risk?
3. Is it the most cost-effective way of reducing the risk?

Security is all about making sure you are focusing on the right areas of defense. By attending SEC401, you will learn the language and underlying theory of computer security. In addition, you will gain the essential, up-to-the-minute knowledge and skills required for effective security if you are given the responsibility for securing systems and/or organizations.

"Fantastic overview class for anyone new to security, or as a powerful refresher. The class covers a broad range of security-focused topics, and the instructor (Dr. Eric Cole) did a fantastic job of inserting real-life experiences to enhance the learning experience."
-Peter Rath,
Compass Federal Consulting

"SEC401 doesn't assume a starting level of knowledge but delivers all the essentials to understand how networks work before showing how to secure them."
-Martyn Smith,
Logically Secure Ltd

Who Should Attend

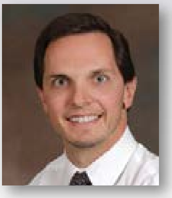
- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570



Dr. Eric Cole *SANS Faculty Fellow*

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole currently performs leading-edge security consulting and works in research and development to advance the state of the art in information systems security. Dr. Cole has experience in information technology with a focus on perimeter defense, secure network design, vulnerability discovery, penetration testing, and intrusion detection systems. He has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. Dr. Cole is the author of several books, including "Hackers Beware," "Hiding in Plain Site," "Network Security Bible," and "Insider Threat." He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Dr. Cole is founder of Secure Anchor Consulting, where he provides state-of-the-art security services and expert witness work. He also served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is actively involved with the SANS Technology Institute (STI) and SANS, working with students, teaching, and maintaining and developing courseware. He is a SANS faculty Fellow and course author.

SECURITY 542

Web App Penetration Testing and Ethical Hacking

Six-Day Program
Mon, Feb 10 - Sat, Feb 15
9:00am - 5:00pm
36 CPE/CMU Credits
Instructor: Timothy Tomes

- GIAC Cert: GWAPT
- Masters Program
- Cyber Guardian

Assess Your Web Apps in Depth

Web applications are a major point of vulnerability in organizations today. Web app holes have resulted in the theft of millions of credit cards, major financial and reputational damage for hundreds of enterprises, and even the compromise of thousands of browsing machines that visited websites altered by attackers. In this intermediate to advanced level class, you'll learn the art of exploiting web applications so you can find flaws in your enterprise's web apps before the bad guys do. Through detailed, hands-on exercises and training from a seasoned professional, you will be taught the four-step process for Web application penetration testing. You will inject SQL into back-end databases, learning how attackers exfiltrate sensitive data. You will utilize cross-site scripting attacks to dominate a target infrastructure in our unique hands-on laboratory environment. And you will explore various other web app vulnerabilities in depth with tried-and-true techniques for finding them using a structured testing regimen. You will learn the tools and methods of the attacker, so that you can be a powerful defender.

Throughout the class, you will learn the context behind the attacks so that you intuitively understand the real-life applications of our exploitation. In the end, you will be able to assess your own organization's web applications to find some of the most common and damaging Web application vulnerabilities today.

By knowing your enemy, you can defeat your enemy. General security practitioners, as well as website designers, architects, and developers, will benefit from learning the practical art of web application penetration testing in this class.

"Fun while you learn! Just don't tell your manager. Every class gives you invaluable information from real-world testing you cannot find in a book."
-David Fava, The Boeing Company

Who Should Attend

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

"SEC542 is an essential course for application Security professionals."
-John Yamich, Exact Target

"Web apps assessment is currently what I do. SEC542 really fills in the gaps in on-the-job training."
-James Kelly, Blue Canopy LLP

"With the infinite tools used for web application penetration, SEC542 helps you understand and use the best tools for your environment."
-Linh Sithihao, UT South Western Medical Center

Timothy Tomes *SANS Instructor*

Tim Tomes is a Senior Security Consultant and Researcher for Black Hills Information Security with experience in information technology and application development. A veteran, Tim spent nine years as an Officer in the United States Army conducting various information security related activities. Tim manages multiple open source projects such as the Recon-ng Framework, the HoneyBadger Geolocation Framework, and PushPin, is a SANS Instructor for SEC542 Web Application Penetration Testing, writes technical articles for PaulDotCom, and frequently presents at information security conferences such as ShmooCon and DerbyCon.

SECURITY 560

Network Penetration Testing and Ethical Hacking

Six-Day Program
Mon, Feb 10 - Sat, Feb 15
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Instructor: Kevin Fiscus

- GIAC Cert: GPEN
- Masters Program
- Cyber Guardian

As cyber attacks increase, so does the demand for information security professionals who possess true network penetration testing and ethical hacking skills. There are several ethical hacking courses that claim to teach these skills, but few actually do. **SANS SEC560: Network Penetration Testing and Ethical Hacking** truly prepares you to conduct successful penetration testing and ethical hacking projects. The course starts with proper planning, scoping and recon, and then dives deep into scanning, target exploitation, password attacks, and wireless and web apps with detailed hands-on exercises and practical tips for doing the job safely and effectively. You will finish up with an intensive, hands-on Capture the Flag exercise in which you'll conduct a penetration test against a sample target organization, demonstrating the knowledge you mastered in this course.

Security vulnerabilities, such as weak configurations, unpatched systems, and botched architectures, continue to plague organizations. Enterprises need people who can find these flaws in a professional manner to help eradicate them from our infrastructures. Lots of people claim to have penetration testing, ethical hacking, and security assessment skills, but precious few can apply these skills in a methodical regimen of professional testing to help make an organization more secure. This class covers the ingredients for successful network penetration testing to help attendees improve their enterprise's security stance.

We address detailed pre-test planning, including setting up an effective penetration testing infrastructure and establishing ground rules with the target organization to avoid surprises and misunderstanding. Then, we discuss a time-tested methodology for penetration and ethical hacking across the network, evaluating the security of network services and the operating systems behind them.

Attendees will learn how to perform detailed reconnaissance, learning about a target's infrastructure by mining blogs, search engines, and social networking sites. We'll then turn our attention to scanning, experimenting with numerous tools in hands-on exercises. The class also discusses how to prepare a final report, tailored to maximize the value of the test from both a management and technical perspective.

Who Should Attend

- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing target networks and systems to find security vulnerabilities

www.giac.org

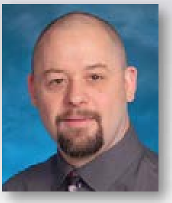
www.sans.edu

www.sans.org/cyber-guardian

"The Network Penetration and Ethical Hacking course provided me with good practice and tools for me to provide to my customers."
-Florent Batard, SCRT

"SEC560 helped me to take the stew of ideas and techniques in my head and organize them in a professional and usable way."
-Richard Tafoya,
Redflex Traffic Systems

"SEC560 presents great content, real-world expertise and application."
-Brice Toth, PSU



Kevin Fiscus *SANS Certified Instructor*

Kevin Fiscus is the founder of and lead consultant for Cyber Defense Advisors where he performs security and risk assessments, vulnerability and penetration testing, security program design, policy development and security awareness with a focus on serving the needs of small and mid-sized organizations. Kevin has over 20 years of IT experience and has focused exclusively on information security for the past 12. Kevin currently holds the CISA, GPEN, GREM, GCFA-Gold, GCIA-Gold, GCIH, GAWN, GCWN, GCSC-Gold, GSEC, SCSA, RCSE, and SnortCP certifications and is proud to have earned the top information security certification in the industry, the GIAC Security Expert. Kevin has also achieved the distinctive title of SANS Cyber Guardian for both red team and blue team. Kevin has taught many of SANS most popular classes including SEC401, SEC464, SEC504, SEC542, SEC560, SEC575, FOR508, and MGT414. In addition to his security work, he is a proud husband and father of two children.

LEGAL 523

Law of Data Security and Investigations

Five-Day Program
Mon, Feb 10 - Fri, Feb 14
9:00am - 5:00pm
30 CPE/CMU Credits
Instructor: Benjamin Wright

- GIAC Cert: GLEG
- Masters Program

New as of Summer 2013: Legal tips on confiscating and interrogating mobile devices.

New law on privacy, e-discovery, and data security is creating an urgent need for professionals who can bridge the gap between the legal department and the IT department. The needed professional training is uniquely available in SANS' LEG523 series of courses, including skills in the analysis and use of contracts, policies, and records management procedures.

GIAC certification under LEG523 demonstrates to employers that a professional has not only attended classes, but studied and absorbed the sophisticated content of these courses. Certification distinguishes any professional, whether an IT expert, an auditor, a paralegal, or a lawyer, and the value of certification will grow in the years to come as law and security issues become even more interlocked.

This course covers the law of business, contracts, fraud, crime, IT security, IT liability and IT policy &mdash; all with a focus on electronically stored and transmitted records.The course also teaches investigators how to prepare credible, defensible reports, whether for cyber, forensics, incident response, human resources or other investigations.

This course provides training and continuing education for many compliance programs under infosec and privacy mandates such as GLBA, HIPAA, FISMA and PCI-DSS.

Who Should Attend

- Investigators
- Security and IT professionals
- Lawyers
- Paralegals
- Auditors
- Accountants
- Technology managers
- Vendors
- Compliance officers
- Law enforcement
- Privacy officers
- Penetration testers

"This course was an eye-opener to the various legal issues in data security. Practices I will use when back in office."
-Albertus Wilson, Saudi Aramco

"Legal 523 is a great course to help the IT professional become aware of various laws, and the implications of the changing trends in cyber defense."
-Betty Lambuth,
Info Tech Solutions & Security

"Its applicability to real-life cases depicts the practicality of the course."
-Samson Okocha, National Identity Management Commission

Day 1: Fundamentals of IT Security Law and Policy

Day 2: E-Records, E-Discovery, and Business Law

Day 3: Contracting for Data Security and Other Technology

Day 4: The Law of IT Compliance: How to Conduct Investigations

- Lessons from day 4 will be invaluable to the effective and credible execution of any kind of investigation – internal, government, consultant, security incidents and the like. These lessons integrate with other tips on investigations introduced in other days of the LEGAL 523 course series.

Day 5: Applying Law to Emerging Dangers: Cyber Defense

- In-depth review of legal response to the major security breach at TJX.
- Learn how to incorporate effective public communications into your cyber security program.

The Legal 523 course is complementary to SANS' rigorous digital forensics program. Together, Legal 523 and the SANS' digital forensics program provide professional investigators an unparalleled suite of training resources.

www.giac.org

www.sans.edu

Benjamin Wright *SANS Senior Instructor*

Benjamin Wright is the author of several technology law books, including "Business Law and Computer Security," published by the SANS Institute. With 26 years in private law practice, he has advised many organizations, large and small, on privacy, e-commerce, computer security, and e-mail discovery and has been quoted in publications around the globe, from the Wall Street Journal to the Sydney Morning Herald. Mr. Wright is known for spotting and evaluating trends, such as the rise of whistleblowers wielding small video cameras. In 2010, Russian banking authorities tapped him for experience and advice on the law of cyber investigations and electronic payments. Wright maintains a popular blog at http://legal-beagle.typepad.com.

MANAGEMENT 414

SANS® +S™ Training Program for the CISSP® Certification Exam

Six-Day Program
Mon, Feb 10 - Sat, Feb 15
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPE/CMU Credits
Instructor: Paul A. Henry
- GIAC Cert: GISP
- DoDD 8570

MGT414 will cover the security concepts needed to pass the CISSP® exam. This is an accelerated review course that assumes the student has a basic understanding of networks and operating systems and focuses solely on the 10 domains of knowledge of the CISSP®:

Domain 1: Access Controls
Domain 2: Telecommunications and Network Security
Domain 3: Information Security Governance & Risk Management
Domain 4: Software Development Security
Domain 5: Cryptography
Domain 6: Security Architecture and Design
Domain 7: Security Operations
Domain 8: Business Continuity and Disaster Recovery Planning
Domain 9: Legal, Regulations, Investigations and Compliance
Domain 10:Physical (Environmental) Security

Each domain of knowledge is dissected into its critical components. Every component is discussed in terms of its relationship to other components and other areas of network security. After completion of the course, the student will have a good working knowledge of the 10 domains of knowledge and, with proper preparation, be ready to take and pass the CISSP® exam.

Who Should Attend

- Security professionals who are interested in understanding 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® 10 Domains
- Security professionals and managers looking for practical ways the 10 domains of knowledge can be applied to the current job
- In short, if you desire a CISSP® or your job requires it, MGT414 is the training for you to get GISP certified

"This course really helped me with all 10 domain areas, and focusing on the important details. Without MGT414, there is too much information to digest."
-Michael Nowatkowski, USMA

"MGT414 was worth the money. I'm self-employed so I made the decision to pay and attend, definitely worth it."
-Anna Cannington,
Cannon IT Services, LLC

Obtaining your CISSP® certification consists of:

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

www.giac.org

www.sans.org/8570

Note: CISSP® exams are not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam.

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 computer forensics, technical security topics, 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, where he is a consistent contributor. Paul serves as a featured and keynote speaker at seminars and conferences worldwide, delivering presentations on diverse topics including anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, firewall architectures, security architectures, and managed security services.

AUD444 Auditing Security and Controls of Active Directory and Windows

Three-Day Course
Mon, Feb 10 - Wed, Feb 12
9:00am - 5:00pm
18 CPE/CMU Credits
Instructor: Tanya Baccam

Who Should Attend

- Internal auditors
- IT specialist auditors
- IT auditors
- IT audit managers
- Information system auditors
- Information security officers

"AUD444 offers relevant theory backed by experience and great hands-on practice."
-Bryan Camereno,
Charles Schwab

Auditors need to be able to understand how Active Directory operates and the key business risks that are present. This course was written to teach auditors how to identify and assess those business risks. Active Directory and Windows systems are typically well known and utilized within organizational infrastructures. However, they can be difficult to audit since there are a large number of settings on the end system. This course provides the tools and techniques to effectively conduct an Active Directory and Windows audit, and while doing so identify key business process controls that may be missing. Students have the opportunity to look at the business process controls and then how those can be verified by looking at Active Directory and the Windows systems that exist. Plus, students are taught how to add additional value to their audits by being able to identify the technology risks that may have been overlooked. The hands-on exercises reinforce the topics discussed in order to give students the opportunity to conduct an audit on their own Windows systems, as well as understand the different security options that Windows provides.

Tanya Baccam *SANS Senior Instructor*

Tanya is a SANS senior instructor, as well as a SANS courseware author. With more than 10 years of information security experience, Tanya has consulted with a variety of clients about their security architecture in areas such as perimeter security, network infrastructure design, system audits, web server security, and database security. Currently, Tanya provides a variety of security consulting services for clients, including system audits, vulnerability and risk assessments, database assessments, web application assessments, and penetration testing. She has previously worked as the director of assurance services for a security services consulting firm and served as the manager of infrastructure security for a healthcare organization. She also served as a manager at Deloitte & Touche in the Security Services practice. Tanya has played an integral role in developing multiple business applications and currently holds the CPA, GIAC GCFW, GIAC GCIH, CISSP, CISM, CISA, CCNA, and OCP DBA certifications. Tanya completed a bachelor of arts degree with majors in accounting, business administration and management information systems.

AUD445 Auditing Security and Controls of Oracle Databases

Three-Day Course
Thu, Feb 13 - Sat, Feb 15
9:00am - 5:00pm
18 CPE/CMU Credits
Instructor: Tanya Baccam

Who Should Attend

- Internal auditors
- IT specialist auditors
- IT auditors
- IT audit managers
- Information system auditors
- Information security officers

"AUD445 covers the important knowledge needed to perform an effective Oracle database audit."
-Gary Johnson,
Colorado PERA

Over the past few years we have seen attackers target data since there is a financial incentive to being able to compromise valuable data. The media seems to be reporting new data compromises constantly. That means auditors need to be effectively auditing the controls that should exist to protect this valuable organizational asset.

Oracle Databases often store the data that's being targeted. Oracle Databases are very complex and challenging to audit! Auditors need to be able to effectively audit the processes and controls in place around the database to ensure the asset is being properly protected and the risks properly managed.

This course provides all of the details, including the IT process, procedural and technical controls, that you as an auditor should look for when conducting an Oracle database audit. Even better, you have the opportunity to get firsthand experience extracting and interpreting data from a live Oracle Database which allows you to be able to return and immediately conduct an Oracle Database audit. By getting hands-on experience, you get a better understanding of exactly how an Oracle Database operates and what data is available for audit purposes. The course is also put together in such a way that you can add additional value to the business and provide further security recommendations and benefits for the database being audited.

The information security field is growing and maturing rapidly. Are you positioned to grow with it? A Master's Degree in Information Security from the SANS Technology Institute will help you build knowledge and skills in management or technical engineering.

The SANS Technology Institute offers two unique master's degree programs:

Master of Science in Information Security Engineering

Master of Science in Information Security Management

SANS TECHNOLOGY INSTITUTE
KNOWLEDGE FOR PEACE
SCIENTIA PRO PACE

www.sans.edu **info@sans.edu**

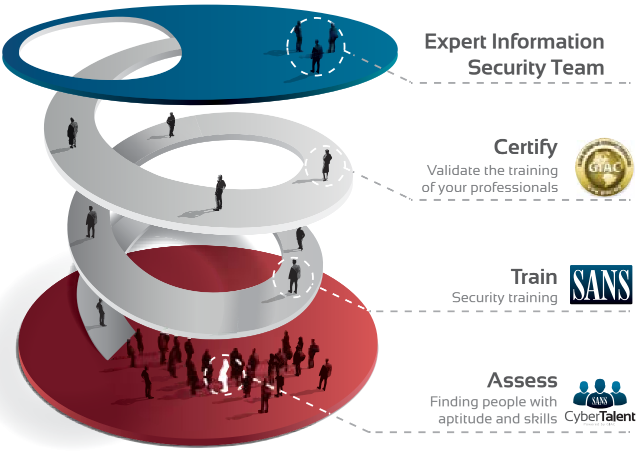
SANS CyberTalent
Powered by GIAC

Contact Us to Learn More

www.sans.org/cybertalent

A Web-Based Recruitment and Talent Management Tool

Introducing SANS CyberTalent Assessments, a new web-based recruitment and talent management tool that helps validate the skills of information security professionals. This unique tool can be used during the recruitment process of new information security employees and to assess the capabilities of your current staff to create a professional development plan. This tool will save you money and time, as well as provide you with the information required to ensure you have the right skills on your information security team.



Expert Information Security Team

Certify
Validate the training of your professionals

Train
Security training

Assess
Finding people with aptitude and skills

Benefits of SANS CyberTalent Assessments

For Recruiting

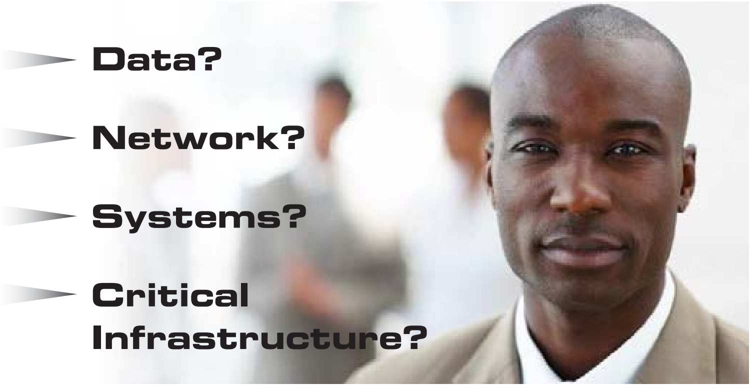
- Provides a candidate ranking table to compare the skills of each applicant
- Identifies knowledge gaps
- Saves time and money by identifying candidates with the proper skillset

For Talent Management

- Determines baseline knowledge levels
- Identifies knowledge gaps
- Helps design a professional development plan

U.S. and Canada 301.654.SANS (7267)
EMEA and APAC inquiries: + 44 (0) 20 3598 2363

How Are You Protecting Your



- Data?
- Network?
- Systems?
- Critical Infrastructure?

Risk management is a top priority. The security of these assets depends on the skills and knowledge of your security team. Don't take chances with a one-size-fits-all security certification.
Get GIAC certified!

GIAC offers over 27 specialized certifications in security, forensics, penetration testing, web application security, IT audit, management, and IT security law.

"GIAC is the only certification that proves you have hands-on technical skills."
-Christina Ford, Department of Commerce

"GIAC Certification demonstrates an applied knowledge versus studying a book."
-Alan C, USMC

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

Get Certified at
www.giac.org

Department of Defense Directive 8570
(DoDD 8570)

www.sans.org/8570

Department of Defense Directive 8570 (DoDD 8570) provides guidance and procedures for the training, certification, and management of all government employees who conduct information assurance functions in assigned duty positions. These individuals are required to carry an approved certification for their particular job classification. GIAC provides the most options in the industry for meeting 8570 requirements.

SANS Training Courses for DoDD Approved Certifications

SANS TRAINING COURSE		DoDD APPROVED CERT
SEC401	Security Essentials Bootcamp Style	GSEC
SEC501	Advanced Security Essentials – Enterprise Defender	GCED
SEC503	Intrusion Detection In-Depth	GCIA
SEC504	Hacker Techniques, Exploits, and Incident Handling	GCIH
AUD507	Auditing Networks, Perimeters, and Systems	GSNA
FOR508	Advanced Computer Forensic Analysis and Incident Response	GCFA
MGT414	SANS® +S™ Training Program for the CISSP® Certification Exam	CISSP
MGT512	SANS Security Essentials for Managers with Knowledge Compression™	GSLC

Compliance/Recertification:

To stay compliant with DoDD 8570 requirements, you must maintain your certifications. GIAC certifications are renewable every four years. Go to www.giac.org to learn more about certification renewal.

DoDD 8570 certification requirements are subject to change, please visit http://iase.disa.mil/eta/iawip for the most updated version.

For more information, contact us at 8570@sans.org or visit www.sans.org/8570

Real Threats

Real Skills

Real Success

Join Today!

Contact us at
onsite@sans.org
to get started!

**www.sans.org/
cyber-guardian**

SANS
CYBER GUARDIAN
PROGRAM

This program begins with hands-on core courses that will build and increase your knowledge and skills. These skills will be reinforced by taking and passing the associated GIAC certification exam. After completing the core courses, you will choose a course and certification from either the Red or Blue Team. The program concludes with participants taking and passing the GIAC Security Expert (GSE) certification.

Prerequisites

- Five years of industry-related experience
- A GSEC certification (with a score of 80 or above) or CISSP certification

Core Courses

SEC503 (GCIA) | SEC504 (GCIH) | SEC560 (GPEN) | FOR508 (GCFA)

After completing the core courses, students must choose one course and certification from either the Blue or Red Team

Blue Team Courses

SEC502 (GPPA) | SEC505 (GCWN) | SEC506 (GCUX)

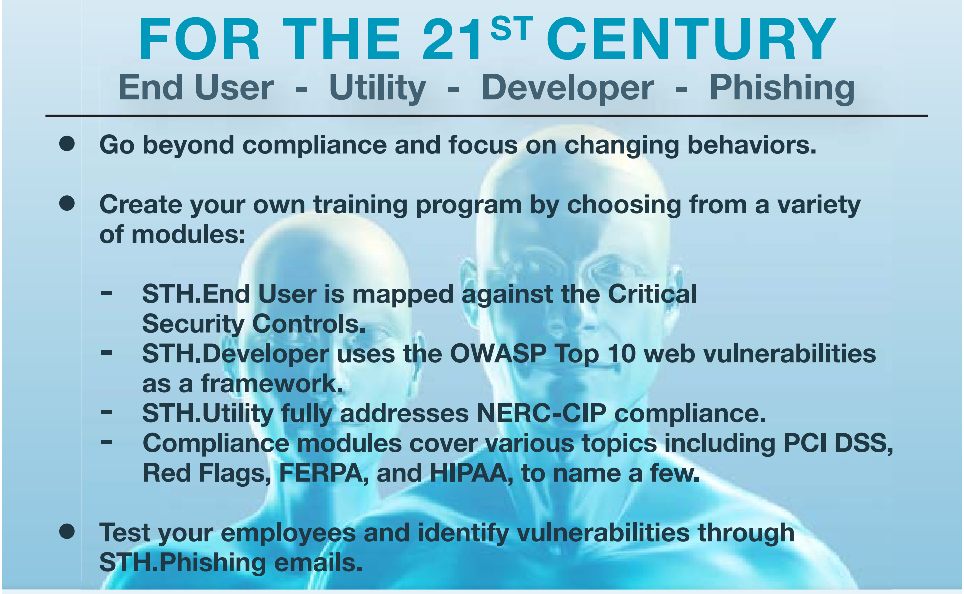
Red Team Courses

SEC542 (GWAPT) | SEC617 (GAWN) | SEC660 (GXPN)

SECURITY AWARENESS

FOR THE 21ST CENTURY

End User - Utility - Developer - Phishing



- Go beyond compliance and focus on changing behaviors.
- Create your own training program by choosing from a variety of modules:
  - STH.End User is mapped against the Critical Security Controls.
  - STH.Developer uses the OWASP Top 10 web vulnerabilities as a framework.
  - STH.Utility fully addresses NERC-CIP compliance.
  - Compliance modules cover various topics including PCI DSS, Red Flags, FERPA, and HIPAA, to name a few.
- Test your employees and identify vulnerabilities through STH.Phishing emails.

SANS SECURING THE HUMAN

For a free trial visit us at:
www.securingthehuman.org

Unable to Join us at CyberCon?

Check out these other Online Training options:

OnDemand www.sans.org/ondemand

Comprehensive e-learning available anytime, anywhere, at your own pace

If you're a self-motivated learner, SANS OnDemand may be the right learning platform for you. Choose from more than 25 pre-recorded courses and take them whenever and wherever you want. Each course gives you four months of access to our OnDemand computer-based training system and includes a mix of presentation slides, audio of SANS' top instructors teaching the material, video demonstrations, and quizzes. If you have questions about the material, our online subject-matter experts are available to help.

vLive www.sans.org/vlive

Convenient online instruction from SANS' top instructors

If you prefer a structured and interactive learning environment, vLive may be right for you. vLive classes meet online two evenings a week. Every class is recorded in case someone misses a session or wishes to review the material again. Students may view the class archives for six months.

Simulcast www.sans.org/simulcast

Attend a SANS training event without leaving home

Event Simulcast allows students to attend a SANS training event without leaving home. Simply log into a virtual classroom to see, hear, and participate in the class as it is being taught LIVE at the event. The Event Simulcast option is available for many classes offered at our largest training events.

SelfStudy www.sans.org/selfstudy

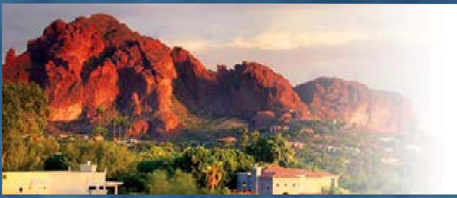
Self-paced training for the motivated and disciplined infosec student

For students who enjoy working independently, we offer the SANS SelfStudy program. SelfStudy students receive printed course materials and MP3 files of SANS' world-class instructors teaching the material. Work through the books and MP3s at your own pace!

FUTURE SANS TRAINING EVENTS

SANS Security East 2014
New Orleans, LA | January 20-25

SANS AppSec 2014
Austin, TX | February 3-8



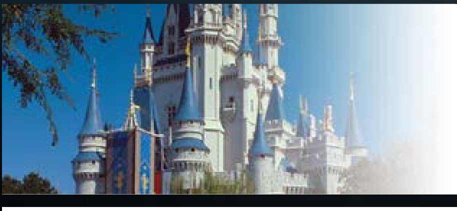
SANS Scottsdale 2014
Scottsdale, AZ | Feb 17-22

SANS Cyber Guardian 2014
Baltimore, MD | March 3-8

SANS DFIRCON 2014
Monterey, CA | March 5-10

ICS Security
Summit 2014 - Orlando
Lake Buena Vista, FL | March 12-18

SANS Northern Virginia 2014
Reston, VA | March 17-22



SANS 2014
Orlando, FL | April 5-14

SANS Digital Forensics & Incident Response SUMMIT
Austin, TX | June 3-10

See a complete list of all future SANS training events at sans.org/security-training/by-location/all

REGISTRATION INFORMATION

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

How to Register

To register, go to www.sans.org/event/cybercon-spring-2014/schedule/course.

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

How to tell if there is room available in a course:

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.

Register Early and Save

Register & Pay By

DATE	DISCOUNT
January 1, 2014	**$400.00**
January 15, 2014	**$250.00**

Cancellation date: January 27, 2014

Look for E-mail Confirmation – It Will Arrive Soon After You Register

We recommend you register and pay early to ensure you get your first choice of courses. An immediate e-mail confirmation is sent to you when the registration is submitted properly. If you have not received e-mail confirmation within two business days of registering, please call the SANS Registration office at **301-654-7267** – 9am - 8pm ET.

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 **January 27, 2014** – processing fees may apply.

SANS Voucher Credit Program

Expand your Training Budget! Extend your Fiscal Year.

The SANS Discount Program that pays you credits and delivers flexibility.
www.sans.org/vouchers

Certification

Take the GIAC exam associated with your course, get your certification, and save money! GIAC certification goes beyond theory by testing your practical security skills. You'll receive a discount on a certification exam if you purchase it in conjunction with its associated course.

OnDemand

Want anytime access to course materials, lectures, and assessment tests? Add an OnDemand bundle to your course registration for a fraction of the normal cost. After the course ends, you'll get four months of access to our online learning system allowing you to hone your skills at your own pace and be fully prepared for certification exams.