THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS Austin 2014

Austin, TX | April 28 - May 3

Choose from these popular courses:

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Intrusion Detection In-Depth *NEW!*

Implementing and Auditing the Twenty Critical Security Controls – In-Depth

Mobile Device Security and Ethical Hacking

"Beam me up SANS—
your training is out of this world!"
-T Munoz, FBI

GIAC Approved Training

Register at
www.sans.org/event/sans-austin-2014

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

SANS is excited to return to Austin for our security training in 2014. Again, we will be at the **Omni Hotel Downtown Austin** campus on **April 28 – May 3**. Do you want to enhance your computer security skills? Take advantage of SANS hands-on training, presented by security industry leaders who include: Dr. Eric Cole, Mike Poor, Bryce Galbraith, Kevin Fiscus, and Christopher Crowley. They will ensure that you not only learn the material, but that you will be able to apply our information security training the day you get back to the office! You'll see why SANS is the most trusted source in computer security training, certification, and research.

This brochure will walk you through course descriptions, instructor bios, and the bonus sessions which include a keynote speaker for the evening talk. You will find information about the *GIAC Certifications* that you can earn in addition to your training. Four of our courses offered at *SANS Austin 2014* are associated with a *GIAC Certification*. SEC401, SEC503, and SEC504 courses are aligned with *DoD Directive 8570*.

If you are considering a graduate program in cybersecurity, our recent accreditation of the *SANS Technology Institute* may interest you. To learn more about how the SANS master's degree programs have already graduated impressive cybersecurity leaders, see our website at **www.sans.edu** for more information and apply today!

Our campus, *Omni Austin Hotel Downtown*, is in the city that is known as the "Live Music Capital of the World." With more than 100 locations that feature music, you are sure to find entertainment that you enjoy. Choose from jazz and rock, or blues, country, reggae, or tejano.

A special discounted rate of $209 Single/Double will be honored at the Omni Austin Hotel Downtown based on space availability, and this rate includes high-speed Internet in your room. Government per diem rooms are available with proper ID; you must call the hotel and specifically ask for this rate. Make your reservations now, as this special rate is only available through April 4, 2014.

Receive a discount of up to $400 for any full course paid for by Wednesday, March 5, 2014! Start making your training and travel plans now; let your colleagues and friends know about *SANS Austin 2014*.

Here's what SANS alumni have said about the value of SANS training:

"SANS instructors are the best in the IT world. Their field knowledge plus delivery makes SANS the premier certification organization."
-Dave Dalton, Sentara Healthcare

"As an incident handler, SANS puts me on a more even footing and adds insight into this aspect of incident handling."
-David Quigley, NATO

"Highly impressed with the quality of instruction."
-Josh Howard, City Bank

"Looking forward to additional SANS training. Thoroughly enjoyed it!"
-Mark Smith, FBI

Courses-at-a-Glance

		MON 4/28	TUE 4/29	WED 4/30	THU 5/1	FRI 5/2	SAT 5/3
SEC401	Security Essentials Bootcamp Style	Page 1					
SEC503	Intrusion Detection In-Depth ***NEW!***	Page 2					
SEC504	Hacker Techniques, Exploits, and Incident Handling	Page 3					
SEC566	Implementing and Auditing the Twenty Critical Security Controls – In-Depth	Page 4					
SEC575	Mobile Device Security and Ethical Hacking	Page 5					

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Apr 28 - Sat, May 3
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPE/CMU Credits
Instructor: Dr. Eric Cole

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

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

It seems wherever you turn organizations are being broken into, and the fundamental question that everyone wants answered is: Why? Why is it that some organizations get broken into and others do not? Organizations are spending millions of dollars on security and are still compromised. The problem is they are doing good things but not the right things. Good things will lay a solid foundation, but the right things will stop your organization from being headline news in the *Wall Street Journal*. 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.

www.giac.org

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?

www.sans.edu

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.

www.sans.org/
cyber-guardian

"SEC401 is the best class I have ever taken. Dr. Cole is also the most knowledgeable and best instructor. I have over 2,800 hours of training. I would highly recommend SANS and especially Dr. Cole."
-Nicholas Christian, Tennessee Bureau of Investigation


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 503

Intrusion Detection In-Depth

SANS

Six-Day Program
Mon, Apr 28 - Sat, May 3
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Mike Poor

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

Who Should Attend

- Intrusion detection analysts (all levels)
- Network engineers
- System, security, and network administrators
- Hands-on security managers

If you have an inkling of awareness of security (even my elderly aunt whose idea of a mobile device is a wheelchair, knows about the perils of the Interweb), you often hear the disconcerting news about another compromise at a high-profile company. The security landscape is continually changing from what was once only perimeter protection to a current exposure of always-connected and often-vulnerable. Along with this is a great demand for security savvy employees who can help creating an environment to detect and prevent intrusions. That is our goal in the Intrusion Detection In-Depth track – to acquaint you with the core knowledge, tools, and techniques to prepare you to defend your networks.

This course spans a wide variety of topics from foundational material such as TCP/IP to detecting an intrusion, building in breadth and depth along the way. It's kind of like the "soup to nuts" or bits to bytes to packets to flow of traffic analysis.

Industry expert Mike Poor has created a VMware distribution, Packetrix, specifically for this course. As the Packetrix name implies, the distribution contains many of the tricks of the trade to perform packet and traffic analysis. Packetrix is supplemented with demonstration "pcaps" – files that contain network traffic. This allows the student to follow along on her/his laptop with the class material and demonstrations. Additionally, these pcaps provide a good library of network traffic to use when reviewing the material, especially for certification.

There are several hands-on exercises each day to reinforce the course book material, allowing you to transfer the knowledge in your head to execution at your keyboard.

Exercises have two different approaches – a more basic one that assists you by giving hints for answering the questions. Students who feel that they would like more guidance can use this approach. The second approach provides no hints, permitting a student who may already know the material or who has quickly mastered new material a more challenging experience. Additionally, there is an "extra credit" stumper question for exercises intended to challenge the most advanced student.

By week's end, your head should be overflowing with newly gained knowledge and skills; and your luggage should be overflowing with course book material that didn't quite get absorbed into your brain during this intense week of learning. This will enable you to "hit the ground running" once returning to a live environment.

"I can get the content anywhere. Mike's ability to deliver the material is why I would recommend the class. He kept things interesting."
-Chris Kachigan, Lockheed Martin

"Day one of Intrusion Detection In-Depth is a strong, deep, and wide introduction into packet capture analysis. Can't wait for more! Love Mike's teaching style."
-Paul Claxton, AFN-BC

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570

Mike Poor *SANS Senior Instructor*

Mike is a founder and senior security analyst for the DC firm InGuardians, Inc. In the past he has worked for Sourcefire as a research engineer and for SANS leading its intrusion analysis team. As a consultant Mike conducts incident response, breach analysis, penetration tests, vulnerability assessments, security audits, and architecture reviews. His primary job focus, however, is in intrusion detection, response, and mitigation. Mike currently holds the GCIA certification and is an expert in network engineering and systems and network and web administration. Mike is an author of the international best-selling "Snort" series of books from Syngress, a member of the Honeynet Project, and a handler for the SANS Internet Storm Center.

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

Six-Day Program
Mon, Apr 28 - Sat, May 3
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Bryce Galbraith

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

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

If your organization has an Internet connection or one or two disgruntled employees (and whose doesn't!), 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.

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, the in-depth information in this course helps you turn the tables on computer attackers. This course addresses the latest cutting-edge insidious attack vectors and the "oldie-but-goodie" attacks that are still so prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course includes a time-tested, step-by-step process for responding to computer incidents; a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them; and a hands-on workshop for discovering holes before the bad guys do. Additionally, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.

This challenging course is particularly well suited to individuals who lead or are a part of an incident handling team. Furthermore, 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.

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570

"SEC504 is very challenging - but not in a bad way! Regardless of your experience level, you will learn something that will better you, whether it's in the workplace or at home office/network."
-Ives Bowman, DND, CFNOC

"Bryce is right on point. His delivery is concise, clear, and entertaining."
-Chris Shipp,
DM Petroleum Operations Co.

Bryce Galbraith *SANS Certified 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, he 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, he holds several security certifications and speaks at conferences around the world.

SECURITY 566

Implementing and Auditing the Twenty Critical Security Controls - In-Depth

Five-Day Program
Mon, Apr 28 - Fri, May 2
9:00am - 5:00pm
Laptop Required
30 CPE/CMU Credits
Instructor: Kevin Fiscus

Cybersecurity attacks are increasing and evolving so rapidly that is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches?

As threats evolve, an organization's security should too. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course on how to implement the Twenty Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense (DoD) personnel or contractors
- Federal agencies or clients
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC440, SEC401, SEC501, MGT512, and other SANS Audit courses

"SEC566 validates what I have been doing for years and provides an opportunity to hear other ideas and see other tools."
-Jay Aylsworth, FRBSR

"SEC566 continues to provide extremely valuable information. The security controls build on themselves seamlessly with excellent reach back."
-Michelle Cabral, Department of Defense

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle.

The British governments Center for the Protection of National Infrastructure describes the Controls as the baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence.

SANS in-depth, hands-on training will teach you how to master the specific techniques and tools needed to implement and audit the Critical Controls. It will help security practitioners understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats.

The course shows security professionals how to implement the controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.

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.

SECURITY 575

Mobile Device Security and Ethical Hacking

Six-Day Program
Mon, Apr 28 - Sat, May 3
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Christopher Crowley
- GIAC Cert: GMOB
- Masters Program

Mobile phones and tablets have become essential to enterprise and government networks, from small organizations to Fortune 500 companies and large-scale agencies. Often, mobile phone deployments grow organically, adopted by multitudes of end-users for convenient email access as well as managers and executives who need access to sensitive organizational resources from their favored personal mobile devices. In other cases, mobile phones and tablets have become critical systems for a wide variety of production applications from ERP to project management. With increased reliance on these devices, organizations are quickly recognizing that mobile phones and tablets need greater security implementations than a simple screen protector and clever password.

Who Should Attend

- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing, deploying or securing mobile phones and tablets
- Network and system administrators supporting mobile phones and tablets

Whether the device is an Apple iPhone or iPad, a Windows Phone, an Android or BlackBerry phone or tablet, the ubiquitous mobile device has become a hugely attractive and vulnerable target for nefarious attackers. The use of mobile devices introduces a vast array of new risks to organizations, including:

- **Distributed sensitive data storage and access mechanisms**
- **Lack of consistent patch management and firmware updates**
- **The high probability of device loss or theft, and more.**

Mobile code and apps are also introducing new avenues for malware and data leakage, exposing critical enterprise secrets, intellectual property, and personally identifiable information assets to attackers. To further complicate matters, today there simply are not enough people with the security skills needed to manage mobile phone and tablet deployments.

This course was designed to help organizations struggling with mobile device security by equipping personnel with the skills needed to design, deploy, operate, and assess a well-managed secure mobile environment. From practical policy development to network architecture design and deployment, and mobile code analysis to penetration testing and ethical hacking, this course will help you build the critical skills necessary to support the secure deployment and use of mobile phones and tablets in your organization.

You will gain hands-on experience in designing a secure mobile phone network for local and remote users and learn how to make critical decisions to support devices effectively and securely. You will also be able to analyze and evaluate mobile software threats, and learn how attackers exploit mobile phone weaknesses so you can test the security of your own deployment. With these skills, you will be a valued mobile device security analyst, fully able to guide your organization through the challenges of securely deploying mobile devices.

www.giac.org

www.sans.edu

"SEC575 provides a pretty comprehensive overview of different attack vectors and vulnerabilities in the mobile field. It covers many topics in enough depth to really get a foothold in the subject. I wish I had taken this course several years ago when first entering the mobile landscape. It would have saved me months of painful self-teaching, and is vastly more complete in many areas."
-Jeremy Erickson, Sandia National Labs

"In the fast-paced world of BYOD and mobile device management, SEC575 is a must course for Info Sec managers."
- Jude Meche, DSCC

Christopher Crowley *SANS Certified Instructor*

Christopher Crowley has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. His work experience includes penetration testing, computer network defense, incident response, and forensic analysis. Mr. Crowley is the course author for SANS Management 535 - Incident Response Team Management and holds the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GREM, GMOB, and CISSP certifications. His teaching experience includes SEC401, SEC503, SEC504, SEC560, SEC575, SEC580, and MGT535; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor of the year award, which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities.

AUSTIN BONUS SESSIONS

SANS@Night Evening Talks

Enrich your SANS training experience! Evening talks given 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: APT: It is Time to Act *Dr. Eric Cole*

Albert Einstein said "We cannot solve our problems with the same thinking we used when we created them." With the new advanced and emerging threat vectors that are breaking into networks with relative ease, a new approach to security is required. The myth that these attacks are so stealthy they cannot be stopped is just not true. There is no such thing as an unstoppable adversary. It is time to act. In this engaging talk one of the experts on APT, Dr. Cole, will outline an action plan for building a defensible network that focuses on the key motto that "Prevention is Ideal but Detection is a Must". Better understand what the APT really is and what organizations can do to be better prepared. The threat is not going away, so the more organizations can realign their thinking with solutions that actually work, the safer the world will become.

Code Injection *Jake Williams*

The technological prowess of attackers has increased dramatically over the last several years. Gone are the days when you could hope to discover malware.exe running in the process list. Attackers are migrating to code injection as a method to remain hidden from prying eyes examining process list entries.

Sure, we've all heard the term code injection or DLL injection, but what does it really mean? How does it really work? Hint: it isn't magic. However, many explanations are bereft, with hand waving and pressing the "I believe" button. In this webcast, we'll talk about how code injection really works at a more technical level. We'll take a quick look at some malware that's performing code injection and discuss detection strategies for when your antivirus fails to detect it. Code injection is a huge topic and we can't cover every aspect in an hour, but the goal is for you to walk away understanding the basics of what's happening under the hood so you can speak intelligently to the topic.

Client Access is the Achilles' Heel of the Cloud *Bryce Galbraith*

Representations of cloud infrastructures often reassure us of their robust security mechanisms by prominently displaying the familiar gold lock in the center of the cloud. While many cloud providers genuinely do strive to deliver confidentiality, integrity, and availability the vital question remains: "Is our data actually secure or not?"

The elephant in the room is that client access *is* the Achilles' heel of the cloud. This talk has been rejected by more than one cloud conference because they would usually rather not talk about these risks. The truth remains, our data is vulnerable virtually everywhere *except* the cloud (assuming it is actually secure there to begin with).

This talk will clearly illustrate the realities of cloud infrastructure risks for those people who desire to look beyond the cost-savings and operational benefits clouds can provide and truly protect their zeros and ones, *wherever* they end up. Numerous demonstrations of hacker tools and techniques will show how attackers can access data even when the cloud infrastructure itself does not have any known vulnerabilities (e.g. sql-injection, XSS, session management flaws or other logic flaws) by simply bypassing most of the security controls we rely on when using cloud resources. If you are serious about protecting your data, you will want to be keenly aware of these risks.

DLP FAIL!!! Using Encoding, Steganography, and Covert Channels to Evade DLP and Other Critical Controls *Kevin Fiscus*

It's all about the information! Two decades after the movie Sneakers, the quote remains as relevant, if not more so. The fact that someone hacks into an environment is interesting but not that relevant. What is important is what happens after the compromise. If the data is destroyed or modified, organizations are negatively impacted but the benefits to an attacker for destruction or alteration are somewhat limited. Stealing information however, is highly profitable. Identity theft, espionage, and financial attacks involve the exfiltration of sensitive data. As a result, organizations deploy tools to detect and/or stop that data exfiltration. While these tools can be extremely valuable, many have serious weaknesses; attackers can encode, hide, or obfuscate the data, or can use secret communication channels. This session will talk about and demonstrate a range of these methods.

GIAC Program Overview

SANS Technology Institute Open House

What's Your Next Career Move?

SANS Technology Institute, an independent subsidiary of SANS, is now 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.

"It's great to learn from an organization at the forefront of both academics, and in the field."
-Joseph Faust, MSISE Program

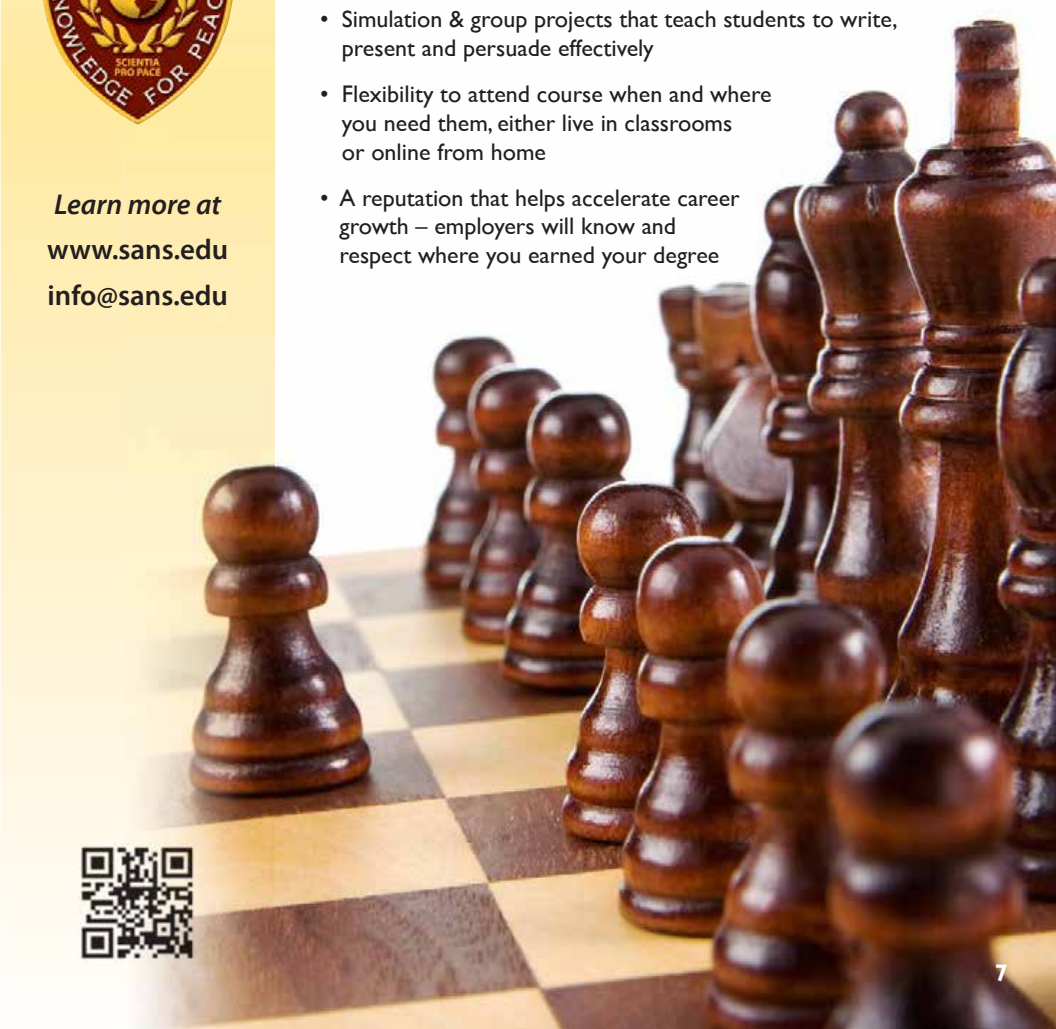
Two unique, respected master's degree programs:

Master of Science in Information Security Engineering

Master of Science in Information Security Management

SANS Technology Institute offers key qualities students seek in a cyber master's program:

- World-class, cutting-edge technical courses that establish and specialize your skills
- Teaching faculty with an unparalleled reputation for industry leadership, who bring the material to life
- Simulation & group projects that teach students to write, present and persuade effectively
- Flexibility to attend course when and where you need them, either live in classrooms or online from home
- A reputation that helps accelerate career growth – employers will know and respect where you earned your degree



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

How Are You Protecting Your

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 20 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

Learn more about GIAC and how to *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.

DoD Baseline IA Certifications

IAT Level I	IAT Level II	IAT Level III
A+CE Network+CE SSCP	**GSEC** Security+CE SSCP	**GCED** **GCIH** **CISSP** (or Associate) CISA

IAM Level I	IAM Level II	IAM Level III
GSLC CAP Security+CE	**GSLC** **CISSP** (or Associate) CAP, CASP CISM	**GSLC** **CISSP** (or Associate) CISM

Computer Network Defense (CND) Certifications

CND Analyst	CND Infrastructure Support	CND Incident Responder	CND Auditor	CND Service Provider Manager
GCIA **GCIH** CEH	SSCP CEH	**GCIH** **GCFA** CSIH, CEH	**GSNA** CISA CEH	CISSP - ISSMP CISM

Information Assurance System Architecture & Engineering (IASAE) Certifications

IASAE I	IASAE II	IASAE III
CISSP (or Associate)	**CISSP** (or Associate) CASP	CISSP - ISSEP CISSP - ISSAP

Computer Environment (CE) Certifications

GCWN **GCUX**

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.

SANS TRAINING COURSE	DoDD APPROVED CERT
SEC401	GSEC
SEC501	GCED
SEC503	GCIA
SEC504	GCIH
AUD507	GSNA
FOR508	GCFA
MGT414	CISSP
MGT512	GSLC

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

SECURING THE HUMAN

SECURITY AWARENESS FOR THE 21ST CENTURY

End User - Utility - Engineer - 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.
  - STH.Engineer focuses on security behaviors for individuals who interact with, operate, or support Industrial Control Systems.
  - 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

FUTURE SANS TRAINING EVENTS

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

CyberCon Online Training Event

SANS CyberCon Spring 2014

Online | Feb 10-15

SANS Scottsdale 2014

Scottsdale, AZ | Feb 17-22

SANS Cyber Guardian 2014

Baltimore, MD | March 3-8

dē-'fər-'kän

SANS DFIRCON 2014

Monterey, CA | March 5-10

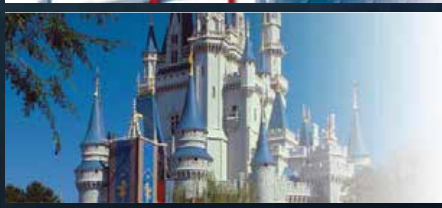
SANS ICS Industrial Control Systems

ICS Security SUMMIT 2014 - ORLANDO

Lake Buena Vista, FL | March 12-18

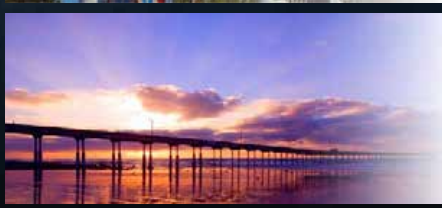
SANS Northern Virginia 2014

Reston, VA | March 17-22



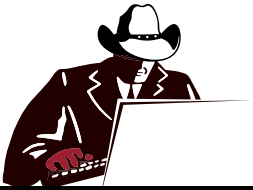
SANS 2014

Orlando, FL | April 5-14



SANS Security West 2014

San Diego, CA | May 8-17



Digital Forensics & Incident Response SUMMIT

Austin, TX | June 3-10

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

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

OnSite
Live Training at Your Office Location
www.sans.org/onsite

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

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

ONLINE TRAINING

OnDemand
E-learning available anytime, anywhere, at your own pace
www.sans.org/ondemand

vLive
Convenient online instruction from SANS' top instructors
www.sans.org/vlive

Simulcast
Attend a SANS training event without leaving home
www.sans.org/simulcast

CyberCon
Live online training event
www.sans.org/cybercon

SelfStudy
Self-paced online training for the motivated and disciplined infosec student www.sans.org/selfstudy

SANS AUSTIN 2014

Hotel Information

Training Campus
Omni Austin Hotel Downtown

700 San Jacinto @ 8th Street
Austin, TX 78701
www.sans.org/event/sans-austin-2014/location

Special Hotel Rates Available

A special discounted rate of $209.00 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 April 4, 2014. To make reservations please call 800-843-6664 and ask for the SANS group rate.

The Omni Austin Hotel Downtown is a magnificently appointed luxury hotel that surrounds you with comfort and style. Enjoy our well-appointed accommodations with spectacular views. With the heart of the thriving downtown business center at your doorstep, you'll be just steps away from the Austin Convention Center and the Texas State Capitol. The 6th Street Entertainment District is walking distance from the hotel.

Top 5 reasons to stay at the Omni Austin Hotel Downtown

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 Omni Austin Hotel Downtown, 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 Omni Austin Hotel Downtown that you won't want to miss!
5. Everything is in one convenient location!

SANS AUSTIN 2014

Registration Information

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

Register online at www.sans.org/event/sans-austin-2014/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.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**3/5/14**	**$400.00**	**3/19/14**	**$250.00**

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 www.sans.org/security-training/discounts prior to registering.

**Early-bird rates and/or other discounts cannot be combined with the group discount.*

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by April 9, 2014 – 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.
www.sans.org/vouchers