THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS Golden Gate 2013

San Francisco, CA | December 16-21

Choose from these popular courses:

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Network Penetration Testing and Ethical Hacking

Implementing and Auditing the Twenty Critical Security Controls

Defending Web Applications Security Essentials

"In one week, I am learning practical information that normally would take months to learn. Best of all, I can apply the knowledge immediately."

-Barry Lyons, Northrop Grumman

"The tools and methods in the course exercises will be immediately useful on the job."

-David Torrey, ThermoAnalytics, Inc

GIAC Approved Training

Register at www.sans.org/event/sans-golden-gate-2013

Save $500 by registering early!

See page 13 for more details.

SANS is bringing a new event to San Francisco in December with courses in IT security, network pen testing, defending web apps for developers, computer and network hacker exploits, and one on implementing and auditing the 20 Critical Controls. This brochure will provide a complete course schedule, course descriptions, instructor bios, and information about earning your master's degree through the **SANS Technology Institute (STI)**. Plus, don't miss our relevant evening talks including a keynote presentation and important topics regarding today's security concerns.

Four of our courses offered at **SANS Golden Gate 2013** are associated with a **GIAC Certification**. Put the skills you'll learn to practical use and join more than 51,000 GIAC certified professionals who make the InfoSec industry safe! Visit the **GIAC** page (7) for more information and register for your certification attempt today!

All of our instructors for SANS Golden Gate 2013 are industry leaders who have proven they understand the challenges you face on a daily basis. Their real-world experience increases the practical value of the course material, and they will ensure that you not only learn the material but that you can use it the day you return to the office.

San Francisco is a wonderful and diverse city offering excellent restaurants, great weather, and plenty of evening activities to give your brain a rest! Make your travel plans to attend SANS Golden Gate, now!

Our host hotel, **Hilton San Francisco Union Square**, has a special discounted SANS rate of $169.00 S/D, see the **Hotel Information** page (13) for details on how to get the best savings. The Hilton San Francisco Union Square is located in the heart of downtown and has easy access to shopping and dining and to Nob Hill and Chinatown. You will be there right before Christmas, and the city will be decorated and celebrating in many ways. People go to San Francisco around the holidays as the shopping, dining, and celebrations are tough to beat.

From the **weatherspark.com** website:

Temperature in San Francisco: *The month of December is characterized by gradually falling daily high temperatures, with daily highs ranging from 58°F to 54°F over the course of the month, exceeding 63°F or dropping below 49°F only one day in ten.*

Get the training you need to advance your career while enjoying this great city! Come see for yourself - register today for **SANS Golden Gate 2013**.

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

"This is my first SANS experience and it has been a positive one. I'm looking forward to more."
-Stephen Ellis, CB&I

"Easily the most beneficial training I've ever attended."
-Josh Howard, City Bank

"These controls should be in every security professional's playbook, SEC566 provides the necessary insight to make implementation manageable."
-Randy Pauli, Chelan County PUD

"I'm always blown away by the knowledge of the SANS instructors!"
-Caleb Queern, Cyveillance

"Course material was done very well and accommodated all skill levels."
-Ryan Lougheed, Covidien

Courses-at-a-Glance

		MON 12/16	TUE 12/17	WED 12/18	THU 12/19	FRI 12/20	SAT 12/21
SEC401	Security Essentials Bootcamp Style	Page 1					
SEC504	Hacker Techniques, Exploits, and Incident Handling	Page 2					
SEC560	Network Penetration Testing and Ethical Hacking	Page 3					
SEC566	Implementing and Auditing the Twenty Critical Security Controls – In-Depth	Page 4					
DEV522	Defending Web Applications Security Essentials	Page 5					

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Dec 16 - Sat, Dec 21
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPE/CMU Credits
Instructor: Chris Christianson

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

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.

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. Since all jobs today require an understanding of security, this course will help you understand why security is important and how it applies to your job. In addition, you will gain the essential, up-to-the-minute knowledge and skills required for effective security so that you will be prepared 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 gain cutting-edge knowledge you can put into practice immediately upon returning to work; and, (2) You will be taught by the best security instructors in the industry.

"Excellent material for security professionals wanting a deeper level of knowledge on how to implement Security policies, procedures and defensive mechanisms."
-Brandon Smith, Dynetics

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/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, 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

Chris Christianson *SANS Instructor*

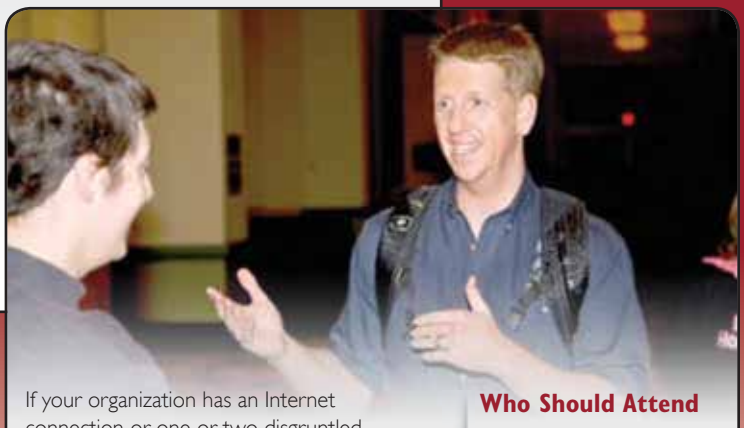
Chris Christianson is an Information Security Analyst and Network Engineer who lives and works in Northern California. He currently works in the financial industry and is the Assistant Vice President of Network Services for one of the nation's largest credit unions. With more than fifteen years of experience, Chris has spoken at conferences, contributed articles for magazines, and obtained many technical certifications including: CCSE, CCDP, CCNP, GSEC, CISSP, IAM, GCIH, CEH, IEM, GCIA, GREM, GPEN, and GWAPT. He has also earned a Bachelor of Science in Management Information Systems.

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

Six-Day Program
Mon, Dec 16 - Sat, Dec 21
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



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.

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

"SEC504 has opened my mind to potential threats against resources I consider 'secured'."
-Phillip Baca,
Drive Savers Data Recovery

"SEC504 should be taken by anyone in your company that has anything to do with security, and is especially valuable for system administrators and security personnel."
-Karl Findorff,
Xavier University of Louisiana

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570

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 and his team provide 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 speaks at numerous conferences, and holds several security certifications and blogs about security issues at http://blog.layeredsec.com.

SECURITY 560

Network Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, Dec 16 - Sat, Dec 21
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Tim Medin

- 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.

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

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. Our exploitation phase will include the use of exploitation frameworks, stand-alone exploits, and other valuable tactics, all with hands-on exercises in our lab environment. 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. The final portion of the class includes a comprehensive hands-on exercise, conducting a penetration test against a hypothetical target organization, following all of the steps.

www.giac.org

www.sans.edu

www.sans.org/
cyber-guardian

The course also describes the limitations of penetration testing techniques and other practices that can be used to augment penetration testing to find vulnerabilities in architecture, policies, and processes. We also address how penetration testing should be integrated as a piece of a comprehensive enterprise information security program.

"In the 5-6 days I have had at SANS, one thing that has consistently impressed me is the caliber of presenters and instructors. Yes, the course content is good, but the instructors make a good course into an outstanding one."
-Jean Currie, Navy

SEC560 is an excellent course! Extremely good hands-on exercises.
-Thomas Baillie, U.S. Navy

Tim Medin *SANS Instructor*

Tim Medin is a senior technical analyst at Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through the course of his career, Tim has performed penetration tests on a wide range of organizations and technologies. Prior to Counter Hack, Tim was a Senior Security Consultant for FishNet Security where the majority of his focus was on penetration testing. He gained information security experience in a variety of industries including previous positions in control systems, higher education, financial services, and manufacturing. Tim regularly contributes to the SANS Penetration Testing Blog (pen-testing.sans.org/blog) and the Command Line Kung Fu Blog (blog.commandlinekungfu.com). He is also project lead for the Laudanum Project, a collection of injectable scripts designed to be used in penetration testing.

SECURITY 566

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

Five-Day Program
Mon, Dec 16 - Fri, Dec 20
9:00am - 5:00pm
30 CPE/CMU Credits
Laptop Required
Instructor: Randy Marchany

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 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 SEC/AUD440, SEC401, SEC501, SANS Audit classes, and MGT512

"This class is extremely valuable for any organization wanting to know where they stand on security."
-David O'Brien, Costco

"SEC566 covers a lot of material in one stop. It would take months or years to collect information that this course provides in a week."
-Joseph Manning, Crate and Barrel

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 government's 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. Specifically, by the end of the course students will know how to:

- Create a strategy to successfully defend their data
- Implement controls to prevent data from being compromised
- Audit systems to ensure compliance with Critical Control standards.

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.

Randy Marchany *SANS Certified Instructor*

Randy is the Chief Information Security Officer of Virginia Tech and the Director of Virginia Tech's IT Security Laboratory. He is a co-author of the original "SANS Top 10 Internet Threats," the "SANS Top 20 Internet Threats," the "SANS Consensus Roadmap for Defeating DDoS Attacks," and the "SANS Incident Response: Step-by-Step" guides. He is a member of the Center for Internet Security development team that produced and tested the CIS Solaris, HPUX, AIX, Linux and Windows2000/XP security benchmarks and scoring tools. He was a member of the White House Partnership for Critical Infrastructure Security working group that developed a Consensus Roadmap for responding to the DDOS attacks of 2000.

DEVELOPER 522

Defending Web Applications Security Essentials

SANS

Six-Day Program
Mon, Dec 16 - Sat, Dec 21
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Dr. Johannes Ullrich
- GIAC Cert: GWEB
- Masters Program

This is the course to take if you have to defend web applications!

Traditional network defenses, such as firewalls, fail to secure web applications. The quantity and importance of data entrusted to web applications is growing, and defenders need to learn how to secure it. DEV522 covers the OWASP Top 10 and will help you to better understand web application vulnerabilities, thus enabling you to properly defend your organization's web assets.

Mitigation strategies from an infrastructure, architecture, and coding perspective will be discussed alongside real-world implementations that really work. The testing aspect of vulnerabilities will also be covered so you can ensure your application is tested for the vulnerabilities discussed in class.

Who Should Attend

- Application developers
- Application security analysts or managers
- Application architects
- Penetration testers who are interested in learning about defensive strategies
- Security professionals who are interested in learning about web application security
- Auditors who need to understand defensive mechanisms in web applications
- Employees of PCI compliant organizations who need to be trained to comply with PCI requirements

To maximize the benefit for a wider range of audiences, the discussions in this course will be programming language agnostic. Focus will be maintained on security strategies rather than coding level implementation.

DEV522: Defending Web Applications Security Essentials is intended for anyone tasked with implementing, managing, or protecting Web applications. It is particularly well suited to application security analysts, developers, application architects, pen testers, and auditors who are interested in recommending proper mitigations to web security issues and infrastructure security professionals who have an interest in better defending their web applications.

The course will cover the topics outlined by OWASP's Top 10 risks document as well as additional issues the authors found of importance in their day-to-day web application development practice. The topics that will be covered include:

- Infrastructure Security
- Server Configuration
- Authentication mechanisms
- Application language configuration
- Application coding errors like SQL Injection and Cross-Site Scripting
- Cross-Site Request Forging
- Authentication Bypass
- Web services and related flaws
- Web 2.0 and its use of web services
- XPATH and XQUERY languages and injection
- Business logic flaws
- Protective HTTP Headers

The course will make heavy use of hands-on exercises. It will conclude with a large defensive exercise, reinforcing the lessons learned throughout the week.

www.giac.org

www.sans.edu

"It is one of the best courses I have attended in defending and security web application. There are not many courses like this out there which cover the vulnerabilities and their mitigation so comprehensively."
-Vibha Fauver, JHU/APL

"This course really proved to me that ignorance is bliss. I learned a lot that I could immediately take back to the office."
-Shawn Shirley, Ferrum College

Dr. Johannes Ullrich *SANS Senior Instructor*

Dr. Johannes Ullrich is the Dean of Research and a faculty member of the SANS Technology Institute. In November of 2000, Johannes started the DShield.org project, which he later integrated into the Internet Storm Center. His work with the Internet Storm Center has been widely recognized. In 2004, Network World named him one of the 50 most powerful people in the networking industry. Secure Computing Magazine named him in 2005 one of the Top 5 influential IT security thinkers. His research interests include IPv6, Network Traffic Analysis and Secure Software Development. Johannes is regularly invited to speak at conferences and has been interviewed by major publications, radio as well as TV stations. He is a member of the SANS Technology Institute's Faculty and Administration as well as Curriculum and Long Range Planning Committee. As chief research officer for the SANS Institute, Johannes is currently responsible for the GIAC Gold program. Prior to working for SANS, Johannes worked as a lead support engineer for a web development company and as a research physicist. Johannes holds a PhD in Physics from SUNY Albany and is located in Jacksonville, Florida. He also maintains a daily security news summary podcast (http://isc.sans.edu/podcast.html) and enjoys blogging about application security.

GOLDEN GATE 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: The Security Impact of IPv6 *Dr. Johannes Ullrich*

IPv6 is more then just lots of addresses. IPv6 is protocol moving IP into the modern world of gigabit networks connecting billions of machines with gigabytes of RAM. In many ways, this transition is similar to the "DC" to "AC" conversion in the electric world. While we still use DC in many places, AC has shown to be more flexible and scalable. Its initial adoption was hindered by security concerns, and DC supporters like Edison went to great lengths to demonstrate the security problems by stealing pets and electrocuting them in public displays. The fear of IPv6 is in many ways a fear of the unknown. IPv6 has some inherent risks, in particular if the protocols opportunities are not well understood, and IPv4 thinking is applied to its deployment. We will discuss the impact of IPv6 on security architecture, intrusion detection, and network forensics, without harming anybody's pet.

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...

GIAC Program Overview

GIAC certification provides assurance that a certified individual meets a minimum level of ability and possesses the skills necessary to do the job. Find out why this is important to your career.

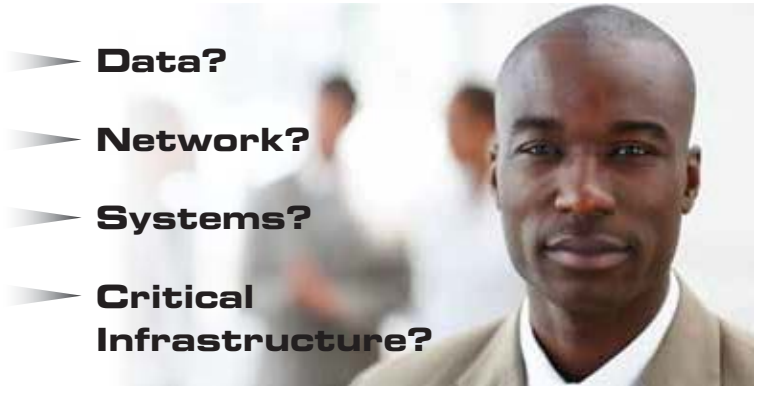
SANS Technology Institute Open House *Dr. Johannes Ullrich*

SANS Technology Institute Master of Science degree programs offer candidates an unparalleled opportunity to excel in the two aspects of security that are most important to the success of their employer and their own careers: management skills and technical mastery.

Over the next 20 years, information technology will become so central to all aspects of our lives, from recreation to warfare, that information security will rise in importance and scale. It will become a profession with more than 500,000, and perhaps as many as 1,000,000, people employed in positions in which they have significant roles in shaping the security of their employers' systems. Those people need managers, technical directors, and chief information security officers who are deeply skilled in the technology and who have excellent management skills.

If you aspire to help lead your organization's or your country's information security program and you have the qualifications, organizational backing, and personal drive to excel in these challenging degree programs, we will welcome you into the program.

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

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 DoD 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

SANS CYBER GUARDIAN PROGRAM

www.sans.org/
cyber-guardian

Stay ahead of cyber threats!

Join the SANS Cyber Guardian program today.

How the Program Works

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.

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

Program Prerequisites

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

Core Courses

SEC503 Intrusion Detection In-Depth (GCIA)

SEC504 Hacker Techniques, Exploits, and Incident Handling (GCIH)

SEC560 Network Penetration Testing and Ethical Hacking (GPEN)

FOR508 Advanced Computer Forensic Analysis & Incident Response (GCFA)

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

Blue Team Courses

SEC502 Perimeter Protection In-Depth (GCFW)

SEC505 Securing Windows & Resisting Malware (GCWN)

SEC506 Securing Linux/Unix (GCUX)

Red Team Courses

SEC542 Web App Penetration Testing & Ethical Hacking (GWAPT)

SEC617 Wireless Ethical Hacking, Penetration Testing, and Defenses (GAWN)

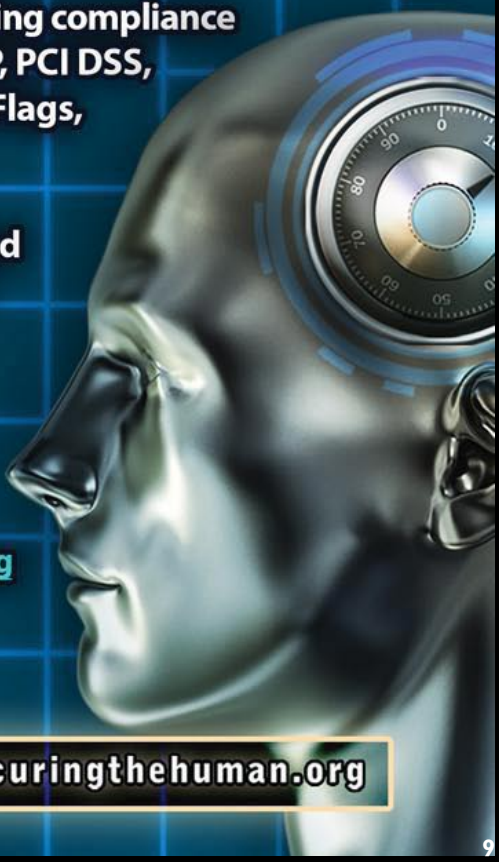
SEC660 Advanced Penetration Testing, Exploits, and Ethical Hacking (GXPN)

The SANS Cyber Guardian program is a unique opportunity for information security individuals or organizational teams to develop specialized skills in incident handling, perimeter protection, forensics, and penetration testing.

SECURITY AWARENESS

FOR THE 21st CENTURY

- Go beyond compliance and focus on changing behaviors.
- Training is mapped against the 20 Critical Controls framework.
- Create your own program by choosing a variety of End User awareness modules.
- Enhance training by adding compliance topics, such as NERC-CIP, PCI DSS, HIPAA, FERPA, and Red Flags, to name a few.
- Test your employees and identify vulnerabilities through phishing emails.
- For a free trial visit us at www.securingthehuman.org



SANS SECURING THE HUMAN

www.securingthehuman.org

What's Your Next Career Move?

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

STI offers two unique master's degree programs:

Master of Science in Information Security Engineering

Master of Science in Information Security Management

"The STI master's degree program combines the best of administrative and technical security into the curriculum. When you achieve your degree, you're well versed and can address any and all challenges placed before you."

-Kevin Fuller, MSISE Student

Apply today!
Cohorts are forming now.
www.sans.edu

SANS TECHNOLOGY INSTITUTE
KNOWLEDGE FOR PEACE
SCIENTIA PRO PACE

www.sans.edu
info@sans.edu
855-672-6733

FUTURE SANS TRAINING EVENTS

SANS Baltimore 2013

Baltimore, MD | October 14-19

www.sans.org/event/baltimore-2013

SANS Chicago 2013

Chicago, IL | Oct 28 - Nov 2

www.sans.org/event/chicago-2013

SANS South Florida 2013

Fort Lauderdale, FL | November 4-9

www.sans.org/event/south-florida-2013

SANS Pen Test Hackfest
TRAINING EVENT AND SUMMIT

Washington, DC | November 7-14

www.sans.org/event/pen-test-hack-fest-2013

SANS San Diego 2013

San Diego, CA | November 18-23

www.sans.org/event/san-diego-2013

SANS San Antonio 2013

San Antonio, TX | December 3-8

www.sans.org/event/san-antonio-2013

SANS Cyber Defense Initiative 2013

Washington, DC | December 12-19

www.sans.org/event/cyber-defense-initiative-2013

SANS Security East 2014

New Orleans, LA | January 20-25

www.sans.org/event/security-east-2014

SANS Scottsdale 2014

Scottsdale, AZ | February 17-22

www.sans.org/event/scottsdale-2014

SANS TRAINING FORMATS

LIVE CLASSROM 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 GOLDEN GATE 2013

Hotel Information

Training Campus
Hilton San Francisco Union Square

333 O'Farrell Street
San Francisco , CA 94102
www.sans.org/event/sans-golden-gate-2013/location

Special Hotel Rates Available

A special discounted rate of $169.00 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 November 25, 2013. To make reservations please call (800) HILTONS (800-445-8667) and ask for the SANS group rate.

As convenient as it is historic, the Hilton San Francisco Union Square hotel is one of the largest hotels on the West Coast, offering exquisite views over the city. Located in the heart of downtown San Francisco, this stylish and sophisticated hotel offers easy access to Nob Hill, Chinatown, and fantastic shopping and entertainment venues in one of the USA's most diverse and dynamic cities.

Top 5 reasons to stay at the Hilton San Francisco Union Square

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 Hilton San Francisco Union Square, 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 Hilton San Francisco Union Square that you won't want to miss!
5. Everything is in one convenient location!

SANS GOLDEN GATE 2013

Registration Information

We recommend you register early to ensure you get your first choice of courses.
Register online at www.sans.org/event/sans-golden-gate-2013

To register, go to www.sans.org/event/sans-golden-gate-2013

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.

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 **November 20, 2013** – processing fees may apply.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	10/30/13	$500.00	11/13/13	$250.00

Some restrictions apply.

Group Savings (Applies to tuition only)

15% discount if 12 or more people from the same organization register at the same time
10% discount if 8 - 11 people from the same organization register at the same time
5% discount if 4 - 7 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.

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**