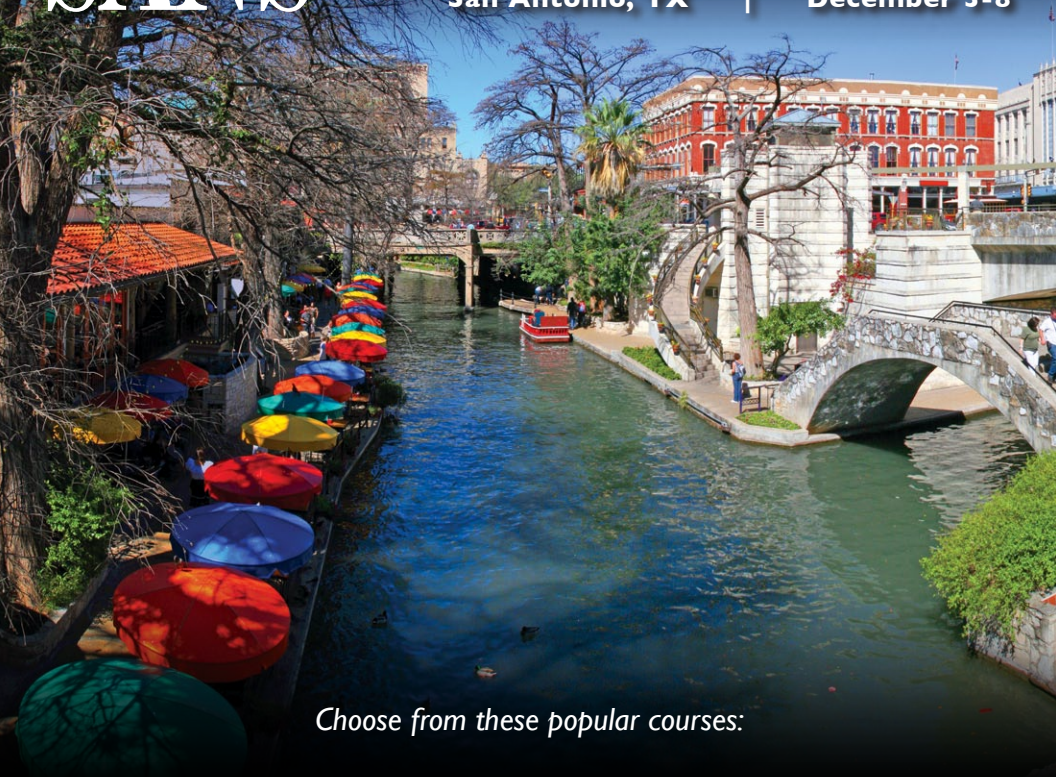
THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS San Antonio 2013

San Antonio, TX | December 3-8



Choose from these popular courses:

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Intrusion Detection In-Depth

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

Intro to Information Security

"Excellent training!
Instructors are passionate and enthusiastic!
I look forward to the classes."

-Bernardine Krupka, US Bank

GIAC Approved Training

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

Save $500
by registering early!
See page 13 for more details.

Dear Colleague,

We are excited to invite you to attend **SANS San Antonio 2013** from **December 3-8** at the **Hyatt Regency River Walk**. We are featuring four of our most popular courses in the Cyber Defense curriculum (SEC301, SEC401, SEC503, and MGT414). Mastery of the skills and techniques taught in the aforementioned courses will launch your career in cybersecurity (SEC301), advance your security career (SEC401), provide what you need to specialize as an intrusion detection analyst (SEC503), and prepare you for the CISSP certification (MGT414). Additionally, we are offering our popular **Hacker Techniques, Exploits & Incident Handling** course (SEC504).

The hallmark of our success is the comprehensive, intensive hands-on training that we provide, delivered by the most advanced and experienced instructors in the industry. Five of our top-rated instructors will be teaching at SANS San Antonio 2013: Johannes Ullrich, Ph.D., Fred Kerby, Steve Armstrong, Eric Conrad, and Bryce Galbraith. In the classroom, the knowledge, skills, and techniques you will learn will be enhanced by the instructors' real-world experiences and lab exercises. Our instructors will ensure that you not only learn the material but that you can apply it immediately upon returning to your office.

Four of our courses are aligned with the **DoD Directive 8570**. We encourage you to visit the **GIAC** page and register for your certification attempt today. Are you interested in a master's degree? You can also take courses that will lead to a master's degree at **SANS Technology Institute (STI)** – Information Security Management (MSISM) or Engineering (MSISE). See our STI page for more information and apply today!

SANS San Antonio 2013 is being held at the Hyatt Regency San Antonio River Walk, and a **special discounted rate of $189.00 S/D** will be honored based on space availability. The hotel is on the Paseo del Rio, better known as the River Walk, which means it is within walking distance of many attractions such as the Alamo mission, La Villita historic arts village, world-class shopping, and dining – from casual to upscale. Experience the holiday serenity of the River Walk as you stroll along the river guided by more than 6,000 luminarias that line the walkways to symbolically mark the "lighting of the way." Enjoy this centuries-old tradition that begins at dusk on Friday, Saturday, and Sunday!

Register and pay by October 9 to save $500 on tuition fees. Start making your training and travel plans now; let your colleagues and friends know about SANS San Antonio 2013. We look forward to seeing you there.

Kind regards,

Eric Bassel

Eric Bassel
SANS Director

Eric Bassel

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

"Security is a big focus for our IT organization. This face-to-face training, with other companies' experiences is a very effective way to learn."
-Michael Stothers,
The Boeing Company

"In the 5-6 days I have had at SANS, one thing has consistently impressed me: the caliber of presenters and instructors. They are excellent. This to me is one of the greatest strengths of SANS. Yes, the course content is good, but the instructors make a good course or class into an outstanding one."
-Jean Currie, Navy

"I never thought I could learn so much in such short time without feeling burned out. Great job making it engaging and interesting."
-Jeff Eubanks,
Mainstream Engineering Corp.

Courses-at-a-Glance

	MON 12/3	TUE 12/4	WED 12/5	THU 12/6	FRI 12/7	SAT 12/8
SEC301 Intro to Information Security	Page 3					
SEC401 Security Essentials Bootcamp Style	Page 4					
SEC503 Intrusion Detection In-Depth	Page 5					
SEC504 Hacker Techniques, Exploits, and Incident Handling	Page 6					
MGT414 SANS® +S™ Training Program for the CISSP® Certification Exam	Page 7					

Cyber Defense Career Roadmap

System Administrator/Security Administrator

The core courses in the career roadmap focus on teaching system and security administrators how to blend fundamental information security defense into their job role based on their unique knowledge of the systems they maintain. As the system or security administrators advance in their careers, a deeper knowledge of all security functions, including technical security policy foundations, are critical both for individual growth and advancement and to maintain defense against evolving security threats to any organization. These essential core foundational security courses will show you how to successfully apply and integrate critical security concepts into your job role.

Applicable Job Titles/Roles
- System Administrators
- Database Administrators
- Network Administrators
- Network Operations
- Help Desk/Technicians
- Security Analysts

Security Analyst

The core courses in the career roadmap focus on teaching security professionals how to analyze security solutions and develop cost-effective solutions. Security analysts need to be able to assess risk across a range of complex environments. An understanding of creative countermeasures is required to design various security solutions that can be deployed across an organization. This critical role requires understanding the importance of cybersecurity and a risk-based approach to help protect the organization. An analyst must be able to perform continuous monitoring and implement automated solutions that can audit and validate overall security across all aspects of an organization.

Applicable Job Titles/Roles
- System Administrators
- Database Administrators
- Network Administrators
- Network Operations
- Help Desk/Technicians
- Security Analysts

Intrusion Analyst/ Security Operations Center Monitoring

The core courses in the career roadmap focus on teaching how to effectively detect and deal with an incident to minimize its impact on an organization. Intrusion detection is a critical part of an organization's defensive posture because attacks are constantly occurring. Timely detection is critical, and the impact of a compromise can be minimized with proper skills. Professionals working in a security operations center must have a solid understanding of cyber security. The focus is on advanced methods of detection to catch both traditional and advanced threats within an organization's network.

Applicable Job Titles/Roles
- System Administrators
- Security Analysts/Specialists
- Intrusion Detection Analysts
- IDS Specialists
- SOC Engineer

Cyber Defense Career Roadmap

Security Engineer

The core courses in the career roadmap focus on teaching the critical technical skills required to implement and maintain a range of risk-based security solutions. Security continues to be a high priority, and many organizations have dedicated personnel to focus solely on implementing effective defensive solutions across the enterprise. These professionals need more than a core foundation of expertise; they must have deeper technical knowledge to be able to solve a variety of complex problems involving cybersecurity. Defense specialists require a working knowledge of the critical technology and strategy not only to defend against a variety of attacks but also to perform timely detection. Both preventive and detective components are required to implement and integrate a cybersecurity strategy.

Applicable Job Titles/Roles

- Security Analyst
- Security Architect
- Security Auditor
- Security Engineer

Operations Management

The core courses in the career roadmap focus on teaching the skills required to understand and run security operations within an enterprise organization. Security is a critical part of organizational operations. Operational managers must understand the language of security, how it could impact a business, and strategies that can be used to properly secure an enterprise. As threats continue to increase in sophistication, it is critical that anyone overseeing technology or involved in the day-to-day operations understand the various approaches that can be used to reduce the risk to an organization. Operational managers must know what questions to ask to make sure staff are focused on the highest priority areas.

Applicable Job Titles/Roles

- Audit Compliance Management
- Consultant/Director
- IT Management
- Data Center Manager

Cybersecurity Manager/Officer

The core courses in the career roadmap focus on teaching executives the language and importance of cybersecurity. Cybersecurity has entered the boardroom. Leaders in every organization need to have a high level of understanding of security to ensure that decisions are aligned with the organization's risk posture. Managers, directors, vice-presidents, and executives need to be able to ask the right questions to address issues that could affect the reputation and success of the organization. This career track will equip managers and executives to be fluent in the language of security and what it means to make proper risk decisions.

Applicable Job Titles/Roles

- Chief Information Officer
- Chief Information Security Officer
- Director/Security Consultant
- Security Manager
- Business Unit Managers

SECURITY 301

Intro to Information Security

SANS

Five-Day Program
Tue, Dec 3 - Sat, Dec 7
9:00am - 5:00pm
30 CPE/CMU Credits
Laptop Required
Instructor: Fred Kerby
▸ GIAC Cert: GISF

This introductory certification course is the fastest way to get up to speed in information security. Written and taught by battle-scarred security veterans, this entry-level course covers a broad spectrum of security topics and is liberally sprinkled with real-life examples. A balanced mix of technical and managerial issues makes this course appealing to attendees who need to understand the salient facets of information security and the basics of risk management. Organizations often tap someone who has no information security training and say, "Congratulations, you are now a security officer." If you need to get up to speed fast, Security 301 is the course for you!

Who Should Attend

- Persons new to information technology who need to understand the basics of information assurance, computer networking, cryptography, and risk evaluation
- Managers and information security officers who need a basic understanding of risk management and the tradeoffs between confidentiality, integrity, and availability
- Managers, administrators, and auditors who need to draft, update, implement, or enforce policy

We begin by covering basic terminology and concepts, and then move to the basics of computers and networking as we discuss Internet Protocol, routing, Domain Name Service, and network devices. We cover the basics of cryptography, security management, and wireless networking, then we look at policy as a tool to effect change in your organization. On the final day of the course, we put it all together with an implementation of defense in-depth.

This course will help you develop the skills to bridge the gap that often exists between managers and system administrators, and learn to communicate effectively with personnel in all departments and at all levels within your organization.

"If you are just starting out in information security, this course has all the basics needed to get you started."
-Sherrie Aud, Deltha Corporation

GISF
www.giac.org

"The information is immediately usable in the organization. Moreover, Mr. Kerby makes the presentation interesting and real-world, as well as practical and beneficial."
-Robert Smith, CMS

"Great crash-course and immersion for security and technology! From the logistics to the IS and OS, the necessary pieces of the cybersecurity puzzle have come together."
-Ansley LaBarre, EWA/IIT

Fred Kerby *SANS Senior Instructor*

Fred is an engineer, manager, and security practitioner whose experience spans several generations of networking. He was the Information Assurance Manager at the Naval Surface Warfare Center, Dahlgren Division for more than sixteen years. His team is one of the recipients of the SANS Security Technology Leadership Award as well as the Government Technology Leadership Award. Fred received the Navy Meritorious Civilian Service Award in recognition of his technical and management leadership in computer and network security. A frequent speaker at SANS, Fred's presentations reflect his opinions and are not the opinions of the Department of the Navy.

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Tue, Dec 3 - Sun, Dec 8
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPE/CMU Credits
Instructor: Bryce Galbraith

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

"I'm a newbie to security. This course presented a ton of information on this subject in a fast-paced, easy-to-understand manner."
-Michael Horkan, Rockwell Automation

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

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 cybersecurity. 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 cybersecurity. What has worked and will always work is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cybersecurity, three questions must be answered:

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.

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 503

Intrusion Detection In-Depth

SANS

Six-Day Program
Tue, Dec 3 - Sun, Dec 8
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Dr. Johannes Ullrich

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

If you have an inkling of awareness of security (even my elderly aunt knows about the perils of the Interweb!), you often hear the disconcerting news about another high-profile company getting compromised. 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 to detect and prevent intrusions. That is our goal in the **Intrusion Detection In-Depth** course - to acquaint you with the core knowledge, tools, and techniques to prepare you to defend your networks.

Who Should Attend

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

This track 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.

www.giac.org

Hands-on exercises supplement the course book material, allowing you to transfer the knowledge in your head to your keyboard using the Packetrix VMware distribution created by industry practitioner and SANS instructor Mike Poor. As the Packetrix name implies, the distribution contains many of the tricks of the trade to perform packet and traffic analysis. All 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 each exercise intended to challenge the most advanced student.

www.sans.edu

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

www.sans.org/cyber-guardian

www.sans.org/8570

"Intrusion Detection is vital for Security administrations. This helps us to be proactive in identifying security threats."
-Sukhwinder, Accenture

"Intrusion detection skills are a must-have for technical security professionals and this course gives us the knowledge to be successful."
-Josh Johnson, Wegmans Food Markets

"There is information in SEC503 that I have never seen before in my 17 years in IT."
-Jesse Trucks, ORNL

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 (https://isc.sans.edu/podcast.html) and enjoys blogging about application security (http://software-security.sans.org/blog).

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Tue, Dec 3 - Sun, Dec 8
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Steve Armstrong

- 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

www.giac.org

www.sans.edu

www.sans.org/
cyber-guardian

www.sans.org/8570

"This class should be required for all security personnel because it really gives you a functional understanding of the security dangers we read about every day."
-Joe Rudich, Blue Cross Blue Shield of Minnesota

"This class teaches you all of the hacking techniques that you need as an incident handler."
-Demonique Lewis, TerpSys

"Perfect for security personnel who wish to have a formal incident handling process."
-Stephen Thrall, Delta Dental of Michigan

Steve Armstrong *SANS Certified Instructor*

Steve started working in the security arena in 1994 whilst serving in the UK Royal Air Force. He specialized in the technical aspects of IT security from 1997 onward, and before retiring from active duty, he lead the RAF's penetration and TEMPEST testing teams. He founded Logically Secure in 2006 to provide specialist security advice to government departments, defense contractors, the online video gaming industry, and both music and film labels worldwide. In addition to contributing to the OSSTMM and authoring the SME targeted Certified Digital Security (CDS) standard and the music and film industry's digital security standards (CDSA), Steve provides wireless penetration testing and incident response services for some of the biggest household names in media.

MANAGEMENT 414

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

Six-Day Program
Tue, Dec 3 - Sun, Dec 8
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPE/CMU Credits
Laptop NOT Needed
Instructor: Eric Conrad

- GIAC Cert: GISP
- DoDD 8570

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

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

www.giac.org

www.sans.org/8570

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.

"The course covers a great deal of government and industry-specific content that is necessary for passing the CISSP."
-Rob Oatman, U.S. Coast Guard Academy

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

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

"This course breaks the huge CISSP study books down into manageable chunks, and helped me focus and identify weaknesses. The instructor's knowledge and teaching skills are excellent."
-Jeff Jones,
Constellation Energy Group

"MGT414 provides a comprehensive overview on an astounding array of access control principles in a manner that is easy to digest and apply to real-world enterprise scenarios!"
-Ryan King, CalAmp Corp

Eric Conrad *SANS Certified Instructor*

Eric Conrad is lead author of the book "The CISSP Study Guide." Eric's career began in 1991 as a UNIX systems administrator for a small oceanographic communications company. He gained information security experience in a variety of industries, including research, education, power, Internet, and health care. He is now president of Backshore Communications, a company focusing on intrusion detection, incident handling, information warfare, and penetration testing. He is a graduate of the SANS Technology Institute with a master of science degree in information security engineering. In addition to the CISSP, he holds the prestigious GIAC Security Expert (GSE) certification as well as the GIAC GPEN, GCIH, GCIA, GCFA, GAWN, and GSEC certifications. Eric also blogs about information security at www.ericconrad.com.

SAN ANTONIO 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: Real-World Risk – What Incident Responders Can Leverage from IT Operations *Eric Conrad*

Incident Response teams can develop an early warning system to detect breaches and breach activity before an incident becomes persistent by working with system administrators. SANS Instructor Eric Conrad will show how to break the cycle of the left hand not knowing what the right hand is doing, using the framework of the 20 Critical Security Controls.

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.

Network Forensic and Visualization Techniques *Steve Armstrong*

Ahead of the launch of the new SANS course FOR572: Advanced Network Forensics and Analysis, one of the course authors will look at some of the techniques and tools that can be utilized to help identify what has been happening on your network. We will also look at how good visualization techniques can help identify attackers and communicate that evidence to other non-technical staff.

GIAC Program Overview

SANS Technology Institute Open House

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

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 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

FUTURE SANS TRAINING EVENTS

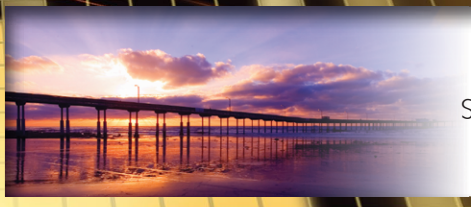
SANS Seattle 2013
Seattle, WA | October 7-14
www.sans.org/event/seattle-2013

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 Cyber Defense Initiative 2013
Washington, DC | December 12-19
www.sans.org/event/cyber-defense-initiative-2013

SANS Golden Gate 2013
San Francisco, CA | December 16-21
www.sans.org/event/sans-golden-gate-2013

SANS Security East 2014
New Orleans, LA | January 20-25
www.sans.org/event/security-east-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 SAN ANTONIO 2013

Hotel Information

Training Campus
Hyatt Regency San Antonio Riverwalk

123 Losoya Street
San Antonio, TX 78205
www.sans.org/event/san-antonio-2013/location

Special Hotel Rates Available

A special discounted rate of $189.00 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 18, 2013. Make reservations at https://resweb.passkey.com/go/SAN2013

With a spectacular location directly on the River Walk that overlooks the historic Alamo mission, Hyatt Regency San Antonio offers luxurious accommodations and a full range of modern services and amenities for your comfort and convenience. Step into the soaring 16-story atrium lobby and enjoy a warm welcome from Hyatt's exceptional staff, setting the stage for an exceptional San Antonio experience. Surrounded by a large variety of restaurants, bars, clubs, shops and tourist attractions, the hotel's excellent location raises them above all other San Antonio River Walk hotels.

Top 5 reasons to stay at the Hyatt Regency San Antonio

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 Hyatt Regency San Antonio, 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 Hyatt Regency San Antonio that you won't want to miss!
5. Everything is in one convenient location!

SANS SAN ANTONIO 2013

Registration Information

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

To register, go to
www.sans.org/event/san-antonio-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 **October 30, 2013** – processing fees may apply.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	10/9/13	$500.00	10/23/13	$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**