THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS San Antonio 2015

San Antonio, TX August 17-22

Choose from these popular courses:

ICS Active Defense and Incident Response *NEW!*

Security Essentials Bootcamp Style

Hacker Tools, Techniques, Exploits, and Incident Handling

Network Penetration Testing and Ethical Hacking

Intrusion Detection In-Depth

SANS Security Leadership Essentials For Managers with Knowledge Compression™

SANS Training Program for CISSP Certification®

Advanced Network Forensics and Analysis

Save $400

Register & pay early!

See page 13 for more details.

"SANS training is the best in the world!"

-Nicolas Stevens, CISCO

Also featuring

CORE NETWARS TOURNAMENT

Register at sans.org/event/san-antonio-2015

GIAC Approved Training

The **SANS San Antonio 2015** cybersecurity training event from **August 17-22** features our most popular courses and top instructors ready to teach you cutting-edge skills and techniques to advance your security career.

SANS is the largest provider of security training and certification in the world, and the San Antonio 2015 event will offer some of our most requested courses. Mastery of the skills and techniques taught in these courses will provide what you need to specialize as an intrusion detection analyst, add to your understanding of attackers' tactics and strategies, mitigate your organization's vulnerabilities, show you methods to conduct network investigations, or prepare you for CISSP® certification.

SANS courses are enriched by internationally renowned instructors who are also industry practitioners and draw on real-world experiences to make the classroom come alive and ensure that students fully absorb the knowledge, skills, and techniques being taught.

All of the courses available at San Antonio 2015 offer **GIAC** certification and some align with **DoD Directive 8570**. To see a list of certifications and training courses, visit the GIAC webpage **giac.org** and register for your certification attempt.

Are you interested in earning a master's degree in cybersecurity? The **SANS Technology Institute** offers two different cybersecurity master's degrees as well as post-baccalaureate cybersecurity graduate certificates in specialized fields, such as penetration testing and ethical hacking, incident response, and cybersecurity engineering. For complete information go to **sans.edu** and apply today!

You can supplement your SANS training with an **OnDemand Bundle** option when purchasing a course and receive four months of online access to the course's custom e-learning program, accessible through your SANS portal account after your live training ends. To learn more about the specifics of the OnDemand Bundle visit **sans.org/ondemand/bundles**.

San Antonio 2015 also features our popular **CORE NetWars Tournament**, which is FREE to attendees taking a five- or six-day course. Core NetWars covers all aspects of IT security and includes challenges on vulnerability assessment, penetration testing, incident response, system hardening, malware analysis, and digital forensics. Learn more about NetWars at **sans.org/netwars/faq**.

SANS San Antonio 2015 will be held at the **Hilton Palacio del Rio** on the city's renowned River Walk, walking distance from an array of attractions ranging from the Alamo to the McNay Art museum and the La Cantera and Market Square shopping areas. 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 August 2, 2015.

Receive a **$400 discount** when registering for any 5-6 day course by entering the discount code "**EarlyBird15**" and paying by Wednesday, June 24, 2015.

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

"SANS instructors are great at making complex concepts more clear."
-David Rowell, NWS Training Center

"This is my 6th SANS training event and SANS continues to deliver. They offer relevant, practical, and highly informative courses that are taught by instructors who truly understand the content."
-Tyler Leet, Computer Services Inc.

"This course is providing much value to me on a professional level and will assist me in helping my company maintain high standards for their systems."
-Alan Baldridge, Meijer

Courses-at-a-Glance

The CORE NetWars Tournament will be held at SANS San Antonio 2015!

CORE NETWARS TOURNAMENT

SANS CORE NetWars Tournament is a computer and network security challenge designed to test your experience and skills in a safe, controlled environment while having a little fun with your fellow IT security professionals. Many enterprises, government agencies, and military bases are using NetWars to help identify skilled personnel and as part of extensive hands-on training. With CORE NetWars Tournament, you'll build a wide variety of skills while having a great time.

Who Should Attend:

- Security professionals
- System administrators
- Network administrators
- Ethical hackers
- Penetration testers
- Incident handlers
- Security auditors
- Vulnerability assessment personnel
- SOC staff members
- Forensic Analysts

In-Depth, Hands-On InfoSec Skills – Embrace the Challenge – CORE NetWars

NetWars competitions will be played over two evenings: August 20-21, 2015

Prizes will be awarded at the conclusion of the tournament.

REGISTRATION IS FREE BUT SPACE IS LIMITED
for students attending any long course at SANS San Antonio 2015
(NON-STUDENT ENTRANCE FEE IS $1,249).

Register at sans.org/event/san-antonio-2015

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Aug 17 - Sat, Aug 22
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Keith Palmgren

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

Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. Learn tips and tricks from the experts so that you can win the battle against the wide range of cyber adversaries that want to harm your environment.

Learn to build a security roadmap that can scale today and into the future.

SEC401: Security Essentials Bootcamp Style is focused on teaching you the essential information security skills and techniques you need to protect and secure your organization's critical information assets and business systems. This course will show you how to prevent your organization's security problems from being headline news in the *Wall Street Journal*!

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

With the advanced persistent threat, it is almost inevitable that organizations will be targeted. Whether the attacker is successful in penetrating an organization's network depends on the effectiveness of the organization's defense. Defending against attacks is an ongoing challenge, with new threats emerging all of the time, including the next generation of threats. Organizations need to understand what really works in cybersecurity. What has worked, and will always work, is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cybersecurity, three questions must be answered:

- What is the risk?
- Is it the highest priority risk?
- What is the most cost-effective way to reduce the risk?

Security is all about making sure you focus on the right areas of defense. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you'll need if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security instructors in the industry.

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

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

"This course (SEC401) provides an excellent refresher into the world of computer security, while providing some actionable information that can be used immediately."
-Christopher Deslandes, Dominion Resource Services

Keith Palmgren *SANS Certified Instructor*

Keith Palmgren is an IT security professional with 26 years of experience in the field. He began his career with the U.S. Air Force working with cryptographic keys & codes management. He also worked in, what was at the time, the newly-formed computer security department. Following the Air Force, Keith worked as an MIS director for a small company before joining AT&T/Lucent as a senior security architect working on engagements with the DoD and the National Security Agency. As security practice manager for both Sprint and Netigy, Keith built and ran the security consulting practice – responsible for all security consulting world-wide and for leading dozens of security professionals on many consulting engagements across all business spectrums. For the last several years, Keith has run his own company, NetIP, Inc. He divides his time between consulting, training, and freelance writing projects. As a trainer, Keith has satisfied the needs of nearly 5,000 IT professionals and authored a total of 17 training courses. Keith currently holds the CISSP, GSEC, CEH, Security+, Network+, A+, and CTT+ certifications. @kpalmgren

SECURITY 503

Intrusion Detection In-Depth

SANS

Six-Day Program
Mon, Aug 17 - Sat, Aug 22
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor:
Johannes Ullrich, Ph.D.

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

Reports of prominent organizations being hacked and suffering irreparable reputational damage have become all too common. How can you prevent your company from becoming the next victim of a major cyber attack?

Who Should Attend

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

SEC503: Intrusion Detection In-Depth delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence. You will learn about the underlying theory of TCP/IP and the most used application protocols, such as HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You'll get plenty of practice learning to configure and master different open-source tools like tcpdump, Wireshark, Snort, Bro, and many more. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that you can transfer knowledge to execution. Basic exercises include assistive hints while advanced options provide a more challenging experience for students who may already know the material or who have quickly mastered new material. In addition, most exercises include an "extra credit" stumper question intended to challenge even the most advanced student.

"Awesome course! Thanks for the in-depth analysis combined with real-life scenarios."
-Art Mason, Rackspace ISOC

"I loved this course. I had big expectations, because I have also taken SEC401 Security Essentials course and it was amazing too. All my expectations have been completed."
-Diana Moldovan, Betfair

Industry expert Mike Poor has created a VMware distribution, Packetrix, specifically for this course. As the name implies, Packetrix contains many of the tricks of the trade to perform packet and traffic analysis. It is supplemented with demonstration "pcaps," which are files that contain network traffic. This allows students to follow along on their laptops with the class material and demonstrations. The pcaps also provide a good library of network traffic to use when reviewing the material, especially for certification.

Preserving the security of your site in today's threat environment is more challenging than ever before. The security landscape is continually changing from what was once only perimeter protection to protecting exposed and mobile systems that are almost always connected and often vulnerable. Security-savvy employees who can help detect and prevent intrusions are therefore in great demand. Our goal in **SEC503: Intrusion Detection In-Depth** is to acquaint you with the core knowledge, tools, and techniques to defend your networks. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

giac.org

sans.edu

sans.org/
cyber-guardian


sans.org/8570


BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Johannes Ullrich, Ph.D. *SANS Senior Instructor*

As Dean of Research for the SANS Technology Institute, Johannes is currently responsible for the SANS Internet Storm Center (ISC) and the GIAC Gold program. He founded DShield.org in 2000, which is now the data collection engine behind the ISC. His work with the ISC has been widely recognized, and in 2004, Network World named him one of the 50 most powerful people in the networking industry. 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. His daily podcast summarizes current security news in a concise format. @johullrich

SECURITY 504

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, Aug 17 - Sat, Aug 22
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Donald Williams

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

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or one or two disgruntled employees (and whose does not!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth. As defenders, it is essential we understand these hacking tools and techniques.

Who Should Attend

- Incident handlers
- Penetration testers
- Ethical hackers
- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack

By helping you understand attackers' tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan, this course helps you turn the tables on computer attackers. It addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course provides a time-tested, step-by-step process for responding to computer incidents, and a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a hands-on workshop that focuses on scanning for, exploiting, and defending systems. It will enable you to discover the holes in your system before the bad guys do!

The course is particularly well-suited to individuals who lead or are a part of an incident handling team. General security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

"I have a better appreciation for the hacking threat; and the difficulties that a security team has in protecting us from that threat."
-Jim Dougherty, UCSC

"This course opened my eyes to the dangers out there. It provided me the skills necessary to protect my systems."
-Rob McBee, SMUD

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

Bundle OnDemand
with this course
sans.org/ondemand

Donald Williams *SANS Instructor*

Donald retired from active duty in 2014, with over 20 years of service in the U.S. Army. He possesses extensive experience in incident handling, intrusion analysis, and network auditing. During his career in the Army, he served as the Defensive Cyber Operations Chief for the Army's Regional Computer Emergency Response Team in South West Asia (RCERT-SWA), directly overseeing the intrusion analysis and incident response teams for one of the Army's largest networks spanning over 10 countries. Donald holds several GIAC certifications, including the GIAC Security Expert (GSE), GCIH, GCIA, and GSNA certifications, as well as numerous other industry certifications. @donaldjwilliam5

SECURITY 560

Network Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, Aug 17 - Sat, Aug 22
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Kevin Fiscus

- GIAC Cert: GPEN
- STI Master's Program
- Cyber Guardian
- OnDemand Bundle

As a cybersecurity professional, you have a unique responsibility to find and understand your organization's vulnerabilities, and to work diligently to mitigate them before the bad guys pounce. Are you ready? SANS SEC560, our flagship course for penetration testing, fully arms you to address this duty head-on.

SEC560 is the must-have course for every well-rounded security professional.

This course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks and wireless and web apps, with over 30 detailed hands-on labs throughout.

Who Should Attend

- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Red team members
- Blue team members

Learn the best ways to test your own systems before the bad guys attack.

Chock full of practical, real-world tips from some of the world's best penetration testers, SEC560 prepares you to perform detailed reconnaissance by examining a target's infrastructure and mining blogs, search engines, social networking sites and other Internet and intranet infrastructure. You will be equipped to scan target networks using best-of-breed tools. We will not just cover run-of-the-mill options and configurations, we will also go over the less-known but highly useful capabilities of the best pen test toolsets available today. After scanning, you will learn dozens of methods for exploiting target systems to gain access and measure real business risk, then examine post-exploitation, password attacks, wireless and web apps, pivoting through the target environment to model the attacks of real-world bad guys.

"This course does a great job of condensing an overwhelming amount of information down to what an IT professional needs for a solid foundation."
-JD Holcomb

"The course material in SEC560 is presented very well and is excellent. All the labs worked for me and the instructor is very engaging."
-Marilyn Moux, Knowledge Consulting Group

You will bring comprehensive penetration testing and ethical hacking know-how back to your organization.

After building your skills in challenging labs over five days, the course culminates with a full-day, real-world network penetration test scenario. You will conduct an end-to-end penetration test, applying the knowledge, tools and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization.

GPEN
giac.org

SANS Technology Institute
sans.edu

sans.org/cyber-guardian

Bundle OnDemand
with this course
sans.org/ondemand

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. @kevinbfiscus

FORENSICS 572

Advanced Network Forensics and Analysis

SANS

Six-Day Program
Mon, Aug 17 - Sat, Aug 22
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Philip Hagen

- GIAC Cert: GNFA
- STI Master's Program
- OnDemand Bundle

digital-forensics.sans.org

"The instructor was very knowledgeable with relevant and interesting examples to illustrate key points."
-Everett Sherlock, Kapstone Paper

"This course was everything I've been looking for over the last few years. It covers all of the core attribute topics in today's corporate network environment."
-Troy Wojenroda, Huntington Ingalls Industries

Take your system-based forensic knowledge onto the wire. Incorporate network evidence into your investigations, provide better findings, and get the job done faster.

Forensic casework that does not include a network component is a rarity in today's environment. Performing disk forensics will always be a critical and foundational skill, but overlooking the network component of today's computing architecture is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, a data theft case, or an employee misuse scenario, the network often has an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent or even definitively prove that a crime actually occurred.

FOR572: Advanced Network Forensics and Analysis was built from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. We focus on the knowledge necessary to expand the forensic mindset from residual data on the storage media from a system or device to the transient communications that occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero.

Put another way: Bad guys are talking – we'll teach you to listen.

Who Should Attend

- Incident response team members and forensicators
- Security Operations Center (SOC) personnel and information security practitioners
- Network defenders
- Law enforcement officers, federal agents, and detectives
- Information security managers
- Network engineers
- IT professionals
- Anyone interested in computer network intrusions and investigations

giac.org

sans.edu

Bundle OnDemand
with this course
sans.org/ondemand

Philip Hagen *SANS Certified Instructor*

Philip Hagen has been working in the information security field since 1998, running the full spectrum including deep technical tasks, management of an entire computer forensic services portfolio, and executive responsibilities. Currently, Phil is an Evangelist at Red Canary, where he engages with current and future customers of Red Canary's managed threat detection service to ensure their use of the service is best aligned for success in the face of existing and future threats. Phil started his security career while attending the U.S. Air Force Academy, with research covering both the academic and practical sides of security. He served in the Air Force as a communications officer at Beale AFB and the Pentagon. In 2003, Phil became a government contractor, providing technical services for various IT and information security projects. These included systems that demanded 24x7x365 functionality. He later managed a team of 85 computer forensic professionals in the national security sector. He has provided forensic consulting services for law enforcement, government, and commercial clients prior to joining the Red Canary team. Phil is the course lead and co-author of FOR572: Advanced Network Forensics and Analysis. @PhilHagen

MANAGEMENT 414

SANS Training Program for CISSP Certification®

Content Updated for New Exam! Effective April 15th

SANS

Six-Day Program
Mon, Aug 17 - Sat, Aug 22
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPEs
Laptop NOT Needed
Instructor: Ted Demopoulos

- GIAC Cert: GISP
- DoDD 8570
- OnDemand Bundle

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

"It was extremely valuable to have an experienced information security professional teaching the course as he was able to use his practical knowledge in examples and explanations."
-Sean Hoar,
Davis Wright Tremaine

Need training for the CISSP® exam?

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

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

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

Who Should Attend

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

Students Will Learn:

- Detailed coverage of the eight domains of knowledge
- The analytical skills required to pass the CISSP® exam
- The technical skills required to understand each question
- The foundational information needed to become a Certified Information Systems Security Professional (CISSP®)

"As a developing security professional, this course sufficiently covers the core concepts needed to obtain CISSP."
-Kurt Zimmerman, Protivity Inc.

giac.org

sans.org/8570

▶II BUNDLE ONDEMAND WITH THIS COURSE
sans.org/ondemand

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

Ted Demopoulos *SANS Certified Instructor*

Ted Demopoulos' first significant exposure to computers was in 1977 when he had unlimited access to his high school's PDP-11 and hacked at it incessantly. He consequently almost flunked out but learned he liked playing with computers a lot. His business pursuits began in college and have been continuous ever since. His background includes over 25 years of experience in information security and business, including 20+ years as an independent consultant. Ted helped start a successful information security company, was the CTO at a "textbook failure" of a software startup, and has advised several other businesses. Ted is a frequent speaker at conferences and other events, quoted often by the press, and maintains Security Certs, a Web site on Security Certifications. He also has written two books on Social Media, has an ongoing software concern in Austin, Texas in the virtualization space, and is the recipient of a Department of Defense Award of Excellence. Ted lives in New Hampshire and more about him is available at Demopoulos Associates. In his spare time, he is also a food and wine geek, enjoys flyfishing, and playing with his children. @TedDemop

MANAGEMENT 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

SANS

Five-Day Program
Mon, Aug 17 - Fri, Aug 21
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop NOT Needed
Instructors: G. Mark Hardy

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

This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to manage security. Lecture sections are intense; the most common student comment is that it's like drinking from a fire hose. The diligent manager will learn vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to U.S. government managers and supporting contractors.

Who Should Attend

- All newly appointed information security officers
- Technically-skilled administrators who have recently been given leadership responsibilities
- Seasoned managers who want to understand what their technical people are telling them

Essential security topics covered in this management track include network fundamentals and applications, power, cooling and safety, architectural approaches to defense in depth, cyber attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, web application security, and offensive and defensive information warfare, culminating with our management practicum. The material uses Knowledge Compression™, special charts, and other proprietary SANS techniques to help convey the key points of critical slides and keep the information flow rate at a pace senior executives demand every teaching hour of the course. The course has been evaluated and approved by CompTIA's CAQC program for Security+ 2008 to ensure that managers and their direct reports have a common baseline for security terminology and concepts. You will be able to put what you learn into practice the day you get back into the office.

"Every IT security professional should attend – no matter what their position. This information is important to everyone."
-John Flood, NASA

"I've already learned much in this course, and it will greatly assist me in increasing my knowledge base and my interaction with my IT/CS departments."
-Jon Shadduck, Ameren Missouri

Knowledge Compression™

Maximize your learning potential!

Knowledge Compression™ is an optional add-on feature to a SANS class that aims to maximize the absorption and long-term retention of large amounts of data over a relatively short period of time. Through the use of specialized training materials, in-class reviews, examinations and test-taking instruction, Knowledge Compression™ ensures students have a solid understanding of the information presented to them. By attending classes that feature this advanced training product, you will experience some of the most intense and rewarding training programs SANS has to offer, in ways that you never thought possible!

giac.org

sans.edu

sans.org/8570

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

G. Mark Hardy *SANS Certified Instructor*

G. Mark Hardy is founder and President of National Security Corporation. He has been providing cyber security expertise to government, military, and commercial clients for over 30 years, and is an internationally recognized expert who has spoken at over 250 events worldwide. G. Mark serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. A retired U.S. Navy Captain, he was privileged to serve in command nine times, including responsibility for leadership training for 70,000 Sailors. He also served as wartime Director, Joint Operations Center for US Pacific Command, and Assistant Director of Technology and Information Management for Naval Logistics in the Pentagon, with responsibility for INFOSEC, Public Key Infrastructure, and Internet security. Captain Hardy was awarded the Defense Superior Service Medal, the Legion of Merit, five Meritorious Service Medals, and 24 other medals and decorations. A graduate of Northwestern University, he holds a BS in Computer Science, a BA in Mathematics, a Masters in Business Administration, a Masters in Strategic Studies, and holds the GSLC, CISSP, CISM and CISA certifications. @g_mark

INDUSTRIAL CONTROL SYSTEMS 515

ICS Active Defense and Incident Response

NEW

SANS

Five-Day Program
Mon, Aug 17 - Fri, Aug 21
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Robert M. Lee

This course is designed to empower students with the ability to understand and utilize active defense mechanisms in concert with incident response for industrial control system networks to respond to and deny cyber threats. This class uses a hands-on approach to give students a technical understanding of concepts such as generating and using threat intelligence, communicating control system needs to information technology personnel to deploy appropriate defenses, detecting malicious actors or threats on control system networks, and performing threat triage and incident response to ensure the safety and reliability of operations technology.

Who Should Attend

- IT and OT support
- IT and OT cybersecurity
- ICS engineers

Hands-on Training

- CYBATI Kit Setup
- Pattern and Information Mapping
- ICS Honeypot
- Consuming Threat Intelligence
- Asset Discovery and Network Visualization
- Collecting the Right Data
- Detecting the Bad Data
- Analyzing and Responding
- Acquisition and Verification
- Indicators in Action
- Capturing the Malware
- Dynamic Malware Analysis
- Neutralizing Malware Callbacks
- IoC Development
- Targeted Attack Identification
- Day 5 is an entire day working through hands-on activities

Author Statement

In taking this course you will leave with the skills to identify and understand your networked infrastructure, monitor it for advanced threats, quickly respond to identified threats while keeping operations running, and extract lessons learned from interactions with the adversary to incorporate in your team's defense efforts or share with others in the form of threat intelligence.
-Robert M. Lee

Students Will Learn:

- Participants will gain hands-on experience with the following tools:
- CYBATIWorks Kit and Virtual Machine with PeakHMI
- Snort and Bro for tailoring and tuning Intrusion Detection System rules
- Wireshark and TCPDump for network traffic capturing and packet analysis
- FTK Imager and MD5Deep for forensic data acquisition and validation
- OpenIOC and YARA for developing Indicators of Compromise
- Xplico and NetworkMiner for network flow and data analysis

Robert M. Lee *SANS Instructor*

Robert M. Lee is a co-founder at the critical infrastructure cyber security company Dragos Security LLC where he has a passion for control system packet analysis, digital forensics, and threat intelligence research. Robert obtained his start in cyber security in the U.S. Air Force where he currently serves as an active-duty Cyberspace Operations Officer. He has been a member of multiple computer network operation teams including his establishing and leading of a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission in the intelligence community. He has published numerous articles and journals for various publications including SC Magazine, Air and Space Power Journal, Control Global, and Control Engineering and is a frequent speaker at conferences having previously presented at events such as SANS, IFRI, BSides, and TROOPERS. Robert received his B.S. from the United States Air Force Academy, his M.S. in Cybersecurity - Digital Forensics from Utica College, and is currently pursuing his PhD at Kings College London with research into cyber conflict and the cyber security of control systems. He is also the author of the book "SCADA and Me." @RobertMLee

SANS@NIGHT EVENING TALKS

Enrich your SANS training experience!

Evening talks by our instructors and selected subject-matter experts help you broaden your knowledge, hear from the voices that matter in computer security, and get the most for your training dollar.

KEYNOTE: The Internet of Evil Things *Johannes Ullrich, Ph.D*

Embedded systems are the new target. As our networks grow uncontrolled and unsupervised, forgotten machines will take over and rule us all soon. Analyzing the embedded malware that comes with this presents a number of challenges. Current debuggers and virtualization techniques that mimic these systems are incomplete and will not allow us to completely analyze malware the way we are used to in good old desktop malware environments. These malware blackboxes need different instrumentations and techniques. We will present some ideas on how to analyze these malware samples, and introduce you to embedded system analysis (unless your bot is removing this event from your smart watch's reminder list).

The 14 Absolute Truths of Security *Keith Palmgren*

Keith Palmgren has identified 14 absolute truths of security – things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these fourteen absolute truths and how they affect a security program can lead to the success of that program. Failing to recognize these truths will spell almost certain doom. Here we will take a non-technical look at each of the 14 absolute truths in turn, examine what they mean to the security manager, what they mean to the security posture, and how understanding them will lead to a successful security program.

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.

Instant Expert: Legitimately and Ethically *Ted Demopoulos*

Part of the Infosec Rock Star Series of talks: We naturally build expertise with experience, but we don't necessarily build "Expert Status". There are many reasons to develop expert status:

- Expert status gives you more influence
- People listen to experts readily
- Experts can make a bigger and more positive impact
- Experts are well paid
- Experts have a lot of flexibility to follow their passions in life

Even the mere concept of what constitutes an expert confuses most people. An expert is "a person with extensive knowledge or ability" which means they know significantly more than others. It is a relative term however. It doesn't mean #1 Expert in the world. It doesn't mean there is nothing else left to learn. Chances are that you are already an expert on several topics. In this talk we examine exactly what an expert is (again, you probably already are an expert), and the multiple ways to quickly, legitimately, and yes, sometimes even nearly instantly, develop expert status.

Debunking the Complex Password Myth *Keith Palmgren*

Perhaps the worst advice you can give a user is "choose a complex password." The result is the impossible-to-remember password requiring the infamous sticky note on the monitor. In addition, that password gets used at a dozen sites at home, AND the very same password gets used at work. The final result ends up being the devastating password compromise. In this one-hour talk, we will look at the technical and non-technical (human nature) issues behind passwords. Attendees will gain a more complete understanding of passwords and receive solid advice on creating more easily remembered AND significantly stronger passwords at work and at home, for their users, for themselves and even for their children.

FUTURE SANS TRAINING EVENTS

SANS Houston ICS Security Training
Houston, TX | June 1-5 | #SANSICS

SANSFIRE 2015
Baltimore, MD | June 13-20 | #SANSFIRE

SANS Rocky Mountain 2015
Denver, CO | June 22-27 | #SANSRockyMtn

SANS Capital City 2015
Washington, DC | July 6-11 | #SANSDC

SANS Digital Forensics & Incident Response SUMMIT & TRAINING
Austin, TX | July 7-14 | #DFIRSummit

SANS San Jose 2015
San Jose, CA | July 20-25 | #SANSSJ

SANS Minneapolis 2015
Minneapolis, MN | July 20-25 | #SANSmpls

SANS Boston 2015
Boston, MA | August 3-8 | #SANSBoston

SANS Cyber Defense SUMMIT & TRAINING
Nashville, TN | August 11-18 | #CyberDefenseSummit

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

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

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

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

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

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

ONLINE TRAINING

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

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

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

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

SANS SAN ANTONIO 2015

Hotel Information

Training Campus

Hilton Palacio del Rio

200 South Alamo Street
San Antonio, TX 78205
210-222-1400
sans.org/event/san-antonio-2015/location

Explore San Antonio from Hilton Palacio del Rio, and enjoy the hotel's contemporary hacienda-style setting. Spectacularly situated on the banks of the river, this hotel by the San Antonio River Walk offers private balconies and a range of thoughtful amenities. Unwind with a great night's sleep in a comfy bed and admire breathtaking panoramas of San Antonio.

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 August 2, 2015.

Top 5 reasons to stay at the Hilton Palacio del Rio

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 Palacio del Rio, 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 Palacio del Rio that you won't want to miss!
5. Everything is in one convenient location!

SANS SAN ANTONIO 2015

Registration Information

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

Register online at sans.org/event/san-antonio-2015/courses

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

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

Use code **EarlyBird15** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**6/24/15**	**$400.00**	**7/15/15**	**$200.00**

Some restrictions apply.

Group Savings (Applies to tuition only)

10% discount if 10 or more people from the same organization register at the same time

5% discount if 5-9 people from the same organization register at the same time

To obtain a group discount, complete the discount code request form at sans.org/security-training/discounts prior to registering.

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by July 29, 2015 – processing fees may apply.

SANS Voucher Credit Program

Expand your training budget! Extend your Fiscal Year. The SANS Voucher Discount Program pays you credits and delivers flexibility.
sans.org/vouchers


Open a
SANS
Account
Sign up for a
SANS Account
and receive free
webcasts, newsletters,
the latest news and
updates, and many other
free resources.
sans.org/account