THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH

SANS San Antonio 2016

July 18-23

SANS OFFERS HANDS-ON, IMMERSION-STYLE

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

SAVE $400

by registering and paying early!

See page 17 for more details.

sans.org/san-antonio

Protect your company and advance your career with information security training this summer from SANS!

Eight courses on

CYBER DEFENSE | PEN TESTING

DIGITAL FORENSICS

SECURITY MANAGEMENT

"SANS courses are highly focused on content, plus excellent face-to-face networking opportunities are a win!"

-Paul Bobby, Lockheed Martin

Also featuring

CORE NETWARS TOURNAMENT

GIAC-Approved Training

SANS Instructors

SANS instructors are real-world practitioners who specialize in the subjects they teach. All instructors undergo rigorous training and testing in order to teach SANS courses. This guarantees that what you learn in class will be up to date and relevant to your job. The SANS San Antonio 2016 lineup of instructors includes:

Kevin Fiscus
Certified Instructor

Bryce Galbraith
Principal Instructor

G. Mark Hardy
Certified Instructor

Robert M. Lee
Certified Instructor

Michael Murr
Principal Instructor

My-Ngoc Nguyen
Certified Instructor

Keith Palmgren
Certified Instructor

Ismael Valenzuela
SANS Instructor

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 10.

KEYNOTE: ***Lessons Learned from the Attack on the Ukrainian Power Grid*** – Robert M. Lee

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

How to Commit Card Fraud – G. Mark Hardy

The 14 Absolute Truths of Security – Keith Palmgren

Debunking the Complex Password Myth – Keith Palmgren

The Red Pill. Become Aware: Squashing Security Misconceptions and More – My-Ngoc Nguyen

Be sure to register and pay by May 25th for a $400 tuition discount!

Courses-at-a-Glance

		MON 7-18	TUE 7-19	WED 7-20	THU 7-21	FRI 7-22	SAT 7-23
SEC301	Intro to Information Security	Page 2					
SEC401	Security Essentials Bootcamp Style	Page 3					
SEC503	Intrusion Detection In-Depth	Page 4					
SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling	Page 5					
SEC511	Continuous Monitoring and Security Operations	Page 6					
SEC550	Active Defense, Offensive Countermeasures, and Cyber Deception	Page 7					
FOR578	Cyber Threat Intelligence NEW!	Page 8					
MGT512	SANS Security Leadership Essentials for Managers with Knowledge Compression™	Page 9					

NETWARS

Are you one of the top Information Security Professionals?
Prove your knowledge and skills at

2 Nights of NetWars at SANS San Antonio 2016!

THU, JULY 21 – FRI, JULY 22 6:30-9:30 PM

Come and join us for this exciting event to test your skills in a challenging and fun learning environment. Registration for NetWars is **FREE OF CHARGE TO ALL STUDENTS AT SANS SAN ANTONIO 2016**. External participants are welcome to join for an entry fee of $1,450.

SANS NetWars is a dynamic cyber range that allows participants to build, practice, and measure their skills in a real-world environment using defensive, analytic, and offensive tactics. We designed NetWars to appeal to a wide range of participant skill sets by using a system with different levels.

All players start at Level 1, which measures foundational cybersecurity skills. More skilled players can rise rapidly through the ranks to a level suitable for their skill set – top players can make it to Level 4, and only the best of the best can reach level 5.

sans.org/san-antonio

SEC301:

Intro to Information Security

SANS

Five-Day Program
Mon, Jul 18 - Fri, Jul 22
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: My-Ngoc Nguyen

giac.org

Bundle OnDemand
with this course
sans.org/ondemand

"This course was very engaging. Although I have a security background, I found the information presented very informative and 100% correct on SCADA risks and vulnerabilities."
-Tyler Moore, Rockwell Automation

To determine if the SANS SEC301 course is right for you, ask yourself five simple questions:

- Are you new to information security and in need of an introduction to the fundamentals?
- Are you bombarded with complex technical security terms that you don't understand?
- Are you a non-IT security manager who lays awake at night worrying that your company will be the next mega-breach headline story on the 6 o'clock news?
- Do you need to be conversant in basic security concepts, principles, and terms, even if you don't need "deep in the weeds" detail?
- Have you decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification?

If you answer yes to any of these questions, the **SEC301: Introduction to Information Security** training course is for you. Jump-start your security knowledge by receiving insight and instruction from real-world security experts on critical introductory topics that are fundamental to information security. This completely revised five-day comprehensive course covers everything from core terminology to the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles.

This course is designed for students who have no prior knowledge of security and limited knowledge of technology. The hands-on, step-by-step teaching approach will enable you to grasp all of the information presented even if some of the topics are new to you. You'll learn the fundamentals of information security that will serve as the foundation of your InfoSec skills and knowledge for years to come.

"SEC301 gave me a much broader understanding of security threats, terminology, processes and help resources." -John Wyatt, Kohler Co.

Written by a security professional with over 30 years of experience in both the public and private sectors, SEC301 provides uncompromising real-world insight from start to finish. The course prepares you for the Global Information Security Fundamentals (GISF) certification test, as well as for the next course up the line, **SEC401: Security Essentials Bootcamp**. It also delivers on the SANS promise: ***You will be able to use the knowledge and skills you learn in SEC301 as soon as you return to work.***

My-Ngoc Nguyen *SANS Certified Instructor*

My-Ngoc Nguyen (pronounced Mee-Nop Wynn) is the CEO/Principal Consultant for Secured IT Solutions. She has 15 years of experience in information systems and technology, with the past 12 years focused on cybersecurity and information assurance for both the government and commercial sectors. My-Ngoc is highly experienced in IT security and risk methodologies, and in legal and compliance programs. She led a cybersecurity program under a federal agency for a highly-regulated, first-of-a-kind project of national importance. With that experience, she has been assisting client organizations in both public and private sectors to implement secure and compliant business processes and IT solutions using defense-in-depth and risk-based approaches. Along with a Master's degree in Management Information Systems, she carries top security certifications, including GPEN, GCIH, GSEC, and CISSP and is a former QSA. She is an active member of the FBI's InfraGard, the Information Systems Security Association (ISSA), the Information Systems Audit and Control Association (ISACA), and International Information Systems Security Certification Consortium, (ISC). My-Ngoc co-founded the non-profit public service organization CyberSafeNV to raise security awareness among Nevada residents and is presently the organization's chairperson. @MenopN

SEC401:
Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Jul 18 - Sat, Jul 23
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Keith Palmgren

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8140

Bundle OnDemand
with this course
sans.org/ondemand

"SEC401 impressed upon me that it should be intertwined in every aspect and not be an afterthought in a project task."
-Glenn Dean, Elo Touch Solutions

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*!

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
- Forensic analysts, penetration testers, and auditors who need a solid foundation of security principles so they can be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

With the rise of advanced persistent threats, 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.

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 and 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 17 training courses. Keith currently holds the CISSP, GSEC, CEH, Security+, Network+, A+, and CTT+ certifications. @kpalmgren

SEC503:
Intrusion Detection In-Depth

SANS

Six-Day Program
Mon, Jul 18 - Sat, Jul 23
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Kevin Fiscus

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 analysts (all levels)
- Network engineers
- System, security, and network 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 will 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.

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.

"SEC503 directly covers the necessary knowledge and skill set I use day to day for my job. The added insight is worth the price."
-Michael Garrett, Federal Reserve Bank of San Francisco

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/8140

Bundle OnDemand
with this course
sans.org/ondemand

"This training allowed me to gain the knowledge to better defend systems and understand the underlying concept, communication, and means of analysis."
-Ryan Hunt, Alert Logic

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 for the past 12 years on information security. Kevin currently holds the CISA, GPEN, GREM, GMOB, GCED, GCFA-Gold, GCIA-Gold, GCIH, GAWN, GPPA, 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. @kevinbfiscus

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, Jul 18 - Sat, Jul 23
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Michael Murr

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"SEC504 is practical and can be utilized immediately."
-Abraham Rivera, Morgan Stanley

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
- 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. This 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.

"This course is foundational and core strength building in the most critical areas of incident handling. It reinforces and develops understanding around roles and TTPs of both adversary and defender." -Araceli Ari Gomes, Dell Secureworks

Michael Murr *SANS Principal Instructor*

Michael has been a forensic analyst with Code-X Technologies for over five years, has conducted numerous investigations and computer forensic examinations, and has performed specialized research and development. Michael has taught SEC504: Hacker Tools, Techniques, Exploits and Incident Handling; FOR508: Advanced Digital Forensics and Incident Response; and FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques. He also has led SANS@Home courses and is a member of the GIAC Advisory Board. Currently, Michael is working on an open-source framework for developing digital forensics applications. Michael holds the GCIH, GCFA, and GREM certifications and has a degree in computer science from California State University at Channel Islands. Michael also blogs about digital forensics on his forensic computing blog (www.forensicblog.org). @mikemurr

SEC511:
Continuous Monitoring and Security Operations

New Extended Bootcamp Hours to Enhance Your Skills

SANS

Six-Day Program
Mon, Jul 18 - Sat, Jul 23
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Laptop Required
Instructor: Ismael Valenzuela

giac.org

sans.edu

We continue to underestimate the tenacity of our adversaries! Organizations are investing a significant amount of time and financial and human resources trying to prevent and combat cyber attacks, but despite this tremendous effort organizations are still getting compromised. The traditional perimeter-focused, prevention-dominant approach to security architecture has failed to prevent intrusions. No network is impenetrable, a reality that business executives and security professionals alike have to accept. Prevention is crucial, and we can't lose sight of it as the primary goal. However, a new proactive approach to security is needed to enhance the capabilities of organizations to detect threats that will inevitably slip through their defenses.

Who Should Attend

- Security architects
- Senior security engineers
- Technical security managers
- SOC analysts, engineers, and managers
- Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)
- Computer Network Defense analysts

The underlying challenge for organizations victimized by an attack is timely incident detection. Industry data suggest that most security breaches typically go undiscovered for an average of seven months. Attackers simply have to find one way into most organizations, because they know that the lack of visibility and internal security controls will then allow them to methodically carry out their mission and achieve their goals.

"This training is valuable because it helped me to understand network security from various types of prevention and provided good insight into endpoint security."
-Stephen L. Perry, Ardent Health Services

"[SEC511] develops very practical skills as opposed to theoretical. I can go back to work and actually use this."
-Charles Hill, SEC

The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM) taught in this course will best position your organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach is early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and this course will greatly increase your understanding and enhance your skills in implementing CM utilizing the NIST framework.

Ismael Valenzuela *SANS Instructor*

Since he founded one of the first IT Security consultancies in Spain, Ismael Valenzuela has participated as a security professional in numerous projects across the globe in the last 15 years. He currently works as IR/Forensics Technical Practice Manager at Intel Security in North America. Prior to joining Intel, Ismael worked as Global IT Security Manager for iSOFT Group Ltd, one of the world's largest providers of healthcare IT solutions. He holds a bachelor's degree in computer science from the University of Malaga (Spain), is certified in Business Administration, and holds many professional certifications including the highly regarded GIAC Security Expert (GSE #132) in addition to GREM, GCFA, GCIA, GCIH, GPEN, GCUX, GCWN, GWAPT, GSNA, CISSP, ITIL, CISM and IRCA 27001 Lead Auditor from Bureau Veritas UK. @aboutsecurity

SEC550:
Active Defense, Offensive Countermeasures & Cyber Deception

SANS

Five-Day Program
Mon, Jul 18 - Fri, Jul 22
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Bryce Galbraith

The current threat landscape is shifting. Traditional defenses are failing us. We need to develop new strategies to defend ourselves. Even more importantly, we need to better understand who is attacking us and why. You may be able to immediately implement some of the measures we discuss in this course, while others may take a while. Either way, consider what we discuss as a collection of tools at your disposal when you need them to annoy attackers, determine who is attacking you, and, finally, attack the attackers.

Who Should Attend

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

"SEC550 is the next step in the evolution of cyber defense in learning to make the hackers' job harder, track their movements, and get attribution."
-Mick Leach, Nationwide

SEC550: Active Defense, Offensive Countermeasures, and Cyber Deception is based on the Active Defense Harbinger Distribution live Linux environment funded by the Defense Advanced Research Projects Agency (DARPA). This virtual machine is built from the ground up for defenders to quickly implement Active Defenses in their environments. The course is very heavy with hands-on activities - we won't just talk about Active Defenses, we will work through labs that will enable you to quickly and easily implement what you learn in your own working environment.

"Bryce is one of the best tech instructors I have had to date, both articulate and engaging."
-Jacob Parks, Insperity

You Will Be Able To

- Track bad guys with callback Word documents
- Use Honeybadger to track web attackers
- Block attackers from successfully attacking servers with honeyports
- Block web attackers from automatically discovering pages and input fields
- Understand the legal limits and restrictions of Active Defense
- Obfuscate DNS entries
- Create non-attributable Active Defense Servers
- Combine geolocation with existing Java applications
- Create online social media profiles for cyber deception
- Easily create and deploy honeypots

What You Will Receive

- A fully functioning Active Defense Harbinger Distribution ready to deploy
- Class books and a DVD with the necessary tools and the OCM virtual machine, which is a fully functional Linux system with the OCM tools installed and ready to go for the class and for the students' work environments

Bryce Galbraith *SANS Principal Instructor*

As a contributing author of the international bestseller *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, was a member of Foundstone's renowned penetration testing team, and served as a senior instructor and co-author of Foundstone's Ultimate Hacking: Hands-On course series. Bryce is currently the owner of Layered Security, where he provides specialized vulnerability assessment and penetration testing services for clients. He teaches several of the SANS Institute's most popular courses and develops curriculum around current topics. He has taught the art of ethical hacking and countermeasures to thousands of IT professionals from a who's who of top companies, financial institutions, and government agencies around the globe. Bryce is an active member of several security-related organizations, holds several security certifications, and speaks at conferences around the world. @brycegalbraith

FOR578:
Cyber Threat Intelligence

NEW

SANS

Five-Day Program
Mon, Jul 18 - Fri, Jul 22
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Robert M. Lee

DFIR
digital-forensics.sans.org

Make no mistake: current computer network defense and incident response contain a strong element of intelligence and counterintelligence that analysts must understand and leverage in order to defend their computers, networks, and proprietary data.

FOR578: Cyber Threat Intelligence will help network defenders and incident responders:

- Construct and exploit threat intelligence to detect, respond, and defeat advanced persistent threats (APTs)
- Fully analyze successful and unsuccessful intrusions by advanced attackers
- Piece together intrusion campaigns, threat actors, and nation-state organizations
- Manage, share, and receive intelligence on APT adversary groups
- Generate intelligence from their own data sources and share it accordingly
- Identify, extract, and leverage intelligence from APT intrusions
- Expand upon existing intelligence to build profiles of adversary groups
- Leverage intelligence to better defend against and respond to future intrusions

Conventional network defenses such as intrusion detection systems and anti-virus tools focus on the vulnerability component of risk, and traditional incident response methodology pre-supposes a successful intrusion. However, the evolving sophistication of computer network intrusions has rendered these approaches insufficient to address the threats faced by modern networked organizations. Today's adversaries accomplish their goals using advanced tools and techniques designed to circumvent most conventional computer network defense mechanisms, go undetected during the intrusion, and then remain undetected on networks over long periods of time.

The collection, classification, and exploitation of knowledge about adversaries – collectively known as cyber threat intelligence – gives network defenders information superiority that can be used to reduce the adversary's likelihood of success with each subsequent intrusion attempt. Responders need accurate, timely, and detailed information to monitor new and evolving attacks, as well as methods to exploit this information to put in place an improved defensive posture. Threat intelligence thus represents a force multiplier for organizations looking to update their response and detection programs to deal with increasingly sophisticated advanced persistent threats.

During a targeted attack, an organization needs a top-notch and cutting-edge incident response armed with the critical intelligence necessary to understand how adversaries operate and to combat the threat. FOR578 will train you and your team to detect, scope, and select resilient courses of action in response to such intrusions and data breaches.

THERE IS NO TEACHER BUT THE ENEMY!

Who Should Attend

- Incident response team members
- Security Operations Center personnel and information security practitioners
- Experienced digital forensic analysts
- Federal agents and law enforcement officials
- SANS FOR408, FOR572, FOR508, or FOR610 graduates looking to take their skills to the next level

"This training was invaluable. It provided me with insight on how to set up my own intel-driven defense."
-Jason Miller, Warner Bros.

Robert M. Lee *SANS Certified Instructor*

Robert M. Lee is the CEO and founder of the critical infrastructure cybersecurity company Dragos Security LLC, where he has a passion for control system traffic analysis, incident response, and threat intelligence research. He is the course author of SANS ICS515: Active Defense and Incident Response and the co-author of SANS FOR578: Cyber Threat Intelligence. Robert is also a non-resident National Cyber Security Fellow at New America focusing on policy issues relating to the cybersecurity of critical infrastructure and a PhD candidate at Kings College London. For his research and focus areas, he was named one of Passcode's Influencers and awarded EnergySec's 2015 Cyber Security Professional of the Year. Robert obtained his start in cybersecurity in the U.S. Air Force, where he served as a Cyber Warfare Operations Officer. He has performed defense, intelligence, and attack missions in various government organizations, including the establishment of a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Robert routinely writes articles in publications such as *Control Engineering* and the *Christian Science Monitor's Passcode* and speaks at conferences around the world. He is also the author of *SCADA and Me* and the weekly web-comic (www.LittleBobbyComic.com) @RobertMLee

MGT512:

SANS Security Leadership Essentials for Managers with Knowledge Compression™

SANS

Five-Day Program
Mon, Jul 18 - Fri, Jul 22
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop NOT Needed
Instructor: G. Mark Hardy

giac.org

sans.edu

sans.org/8140

Bundle OnDemand
with this course
sans.org/ondemand

"The course content is great because it is consistently updated to reflect current IT trends. The instructor was knowledgeable, and very down to earth."
-Terence B., Officer Training Command

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 National Institute of Standards and Technology 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.

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!

G. Mark Hardy *SANS Certified Instructor*

G. Mark Hardy is founder and president of National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for over 30 years, and is an internationally recognized expert who has spoken at over 250 events world-wide. He 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 U.S. 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 the GSLC, CISSP, CISM, and CISA certifications. @g_mark

KEYNOTE: **Lessons Learned from the Attack on the Ukrainian Power Grid**
– Robert M. Lee

On December 23, 2015 there was a cyber attack on the Ukrainian power grid that left over 80,000 people in the dark. Robert Lee and the SANS ICS team were first to reveal the malware uncovered in the network and later confirmed the cyber attack. This presentation demonstrates lessons learned from the attack across threat intelligence, network security, incident response, and ICS/SCADA security.

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 are 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.

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 14 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 and the security posture, and see how understanding them will lead to a successful security program.

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.

The Red Pill. Become Aware: Squashing Security Misconceptions and More
– My-Ngoc Nguyen

"You take the blue pill, the story ends. You wake up in your bed and believe whatever you want to believe. You take the red pill, you stay in wonderland, and I show you how deep the rabbit hole goes." -Morpheus, to Neo in The Matrix

Take the red pill, come join us down this rabbit hole, and get your head out of the sand to better protect yourself, your company/organization, and the things that matter to you (e.g., your loved ones, your finances, your identity). In this presentation, you will get insights on common misconceptions and trends that led to many breaches, especially those that made headlines. We'll touch on some details from those headline breaches to show commonalities, address the main misconceptions, describe attackers' approaches, provide some statistics, and most importantly, provide helpful tips for all members of the audience.

How to Commit Card Fraud *– G. Mark Hardy*

Well, we're not going to show you how to commit fraud, but will show you how the bad guys do it and how you can protect yourself and your business. We'll take a look into the "dark web" and see how these big card heists are pulled off, why chip-and-pin won't solve the fraud problem, and why payment technologies like Apple Pay pose new risks. You'll learn the ecosystem of fraud, and how it's become a big business that costs banks and merchants over $16 billion annually. See if your bank even bothers to use the security protections it could – we'll have a mag stripe card reader so you can really see what's in your wallet.

The Value of SANS Training & YOU

EXPLORE

- Read this brochure and note the courses that will enhance your role in your organization
- Use the Career Roadmap (sans.org/media/security-training/roadmap.pdf) to plan your growth in your chosen career path

RELATE

- Consider how security needs in your workplace will be met with the knowledge you'll gain in a SANS course
- Know the education you receive will make you an expert resource for your team

VALIDATE

- Pursue a GIAC Certification after your training to validate your new expertise
- Add a NetWars challenge to your SANS experience to prove your hands-on skills

SAVE

- Register early to pay less using early-bird specials
- Consider group discounts or bundled course packages to make the most of your training budget

ADD VALUE

- Network with fellow security experts in your industry
- Prepare thoughts and questions before arriving to share with the group
- Attend SANS@Night talks and activities to gain even more knowledge and experience from instructors and peers alike

ALTERNATIVES

- If you cannot attend a live training event in person, attend the courses virtually via SANS Simulcast
- Use SANS OnDemand or vLive to complete the same training online from anywhere in the world, at any time

ACT

- Bring the value of SANS training to your career and organization by registering for a course today, or contact us at 301-654-SANS with further questions

Return on Investment

SANS live training is recognized as the best resource in the world for information security education. With SANS, you gain significant returns on your InfoSec investment. Through our intensive immersion classes, our training is designed to help your staff master the practical steps necessary for defending systems and networks against the most dangerous threats – the ones being actively exploited.

REMEMBER

the SANS promise:

You will be able to apply our information security training the day you get back to the office!

Build Your Best Career

WITH

SANS

Add an

OnDemand Bundle & GIAC Certification Attempt*

to your course within seven days of this event for just $659 each.

SPECIAL PRICING

OnDemand Bundle

- Four months of supplemental online review
- 24/7 online access to your course lectures, materials, quizzes, and labs
- Subject-matter expert support to help you increase your retention of course material

"The course content and OnDemand delivery method have both exceeded my expectations."

-Robert Jones, Team Jones, Inc.

GIAC Certification

- Distinguish yourself as an information security leader
- 30+ GIAC certifications to choose from
- Two practice exams included
- Four months of access to complete the attempt

"GIAC is the only certification that proves you have hands-on technical skills."

-Christina Ford, Department of Commerce

MORE INFORMATION

www.sans.org/ondemand/bundles www.giac.org

*GIAC and OnDemand Bundles are only available for certain courses.

Security Awareness Training by the Most Trusted Source

Computer-based Training for Your Employees

End User
CIP v5
ICS Engineers
Developers
Healthcare

- Let employees train on their own schedule
- Tailor modules to address specific audiences
- Courses translated into many languages
- Test learner comprehension through module quizzes
- Track training completion for compliance reporting purposes

Visit SANS Securing The Human at **securingthehuman.sans.org**

Change Human Behavior | Manage Risk | Maintain Compliance | Protect Your Brand

SANS Technology Institute

The SANS Technology Institute transforms the world's best cybersecurity training and certifications into a comprehensive and rigorous graduate education experience.

Master's Degree Programs:

- M.S. in Information Security Engineering
- M.S. in Information Security Management

Specialized Graduate Certificates:

- Cybersecurity Engineering (Core)
- Cyber Defense Operations
- Penetration Testing and Ethical Hacking
- Incident Response

SANS Technology Institute, an independent subsidiary of SANS, is accredited by The Middle States Commission on Higher Education.
3624 Market Street | Philadelphia, PA 19104 | 267.285.5000
an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

POST 9/11 GI BILL

Eligible for veterans education benefits!
Earn industry-recognized GIAC certifications throughout the program.
Learn more at www.sans.edu | info@sans.edu

GIAC

GI Bill® is a registered trademark of the U.S. Department of Veterans Affairs (VA).
More information about education benefits offered by VA is available at the official U.S. government website at www.benefits.va.gov/gibill.

Employers need good talent. Veterans need good jobs. SANS VetSuccess Immersion Academy delivers both.

Introducing the SANS VetSuccess Immersion Academy, an intensive, accelerated program that provides the real-world training and certifications needed to fill critical jobs in cybersecurity.

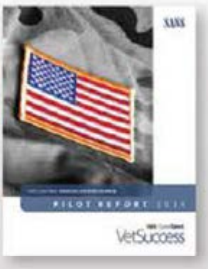
For employers, the academy is a faster, more reliable, and less expensive way to find, train, certify, and employ highly qualified cybersecurity talent.

For transitioning veterans, the academy provides free accelerated training and certifications to quickly and effectively launch careers in cybersecurity.

Find out how your organization can benefit from hiring graduates or launching an academy to meet your specific talent needs.

Read the Pilot Program Results Report
Visit sans.org/vetsuccess

SANS | CyberTalent
IMMERSION ACADEMY



Read the Pilot Program Results Report
Visit sans.org/vetsuccess

Women's Academy Pilot
1st cohort graduation
Spring 2016

FUTURE SANS TRAINING EVENTS

Security West 2016
San Diego, CA | Apr 29 - May 6

Baltimore Spring 2016
Baltimore, MD | May 9-14

Houston 2016
Houston, TX | May 9-14

Security Operations Center
SUMMIT & TRAINING 2016
Crystal City, VA | May 19-26

SANSFIRE 2016
Washington, DC | Jun 11-18

Digital Forensics & Incident Response
SUMMIT & TRAINING 2016
Austin, TX | Jun 23-30

Salt Lake City 2016
Salt Lake City, UT | Jun 27 - Jul 2

Rocky Mountain 2016
Denver, CO | Jul 11-16

Minneapolis 2016
Minneapolis, MN | Jul 18-23

ICS Security & Training – Houston 2016
Houston, TX | Jul 25-30

San Jose 2016
San Jose, CA | Jul 25-30

Boston 2016
Boston, MA | Aug 1-6

Security Awareness
SUMMIT & TRAINING 2016
San Francisco, CA | Aug 5-10

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

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events

Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with Your Peers

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

Community SANS

Live Training in Your Local Region with Smaller Class Sizes

sans.org/community

Private Training

Your Location! Your Schedule!

sans.org/private-training

Mentor

Live Multi-Week Training with a Mentor

sans.org/mentor

Summit

Live IT Security Summits and Training

sans.org/summit

ONLINE TRAINING

OnDemand

E-learning Available Anytime, Anywhere, at Your Own Pace

sans.org/ondemand

vLive

Online Evening Courses with SANS' Top Instructors

sans.org/vlive

Simulcast

Attend a SANS Training Event without Leaving Home

sans.org/simulcast

OnDemand Bundles

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

SANS SAN ANTONIO 2016

Hotel Information

Training Campus
Hilton Palacio del Rio

200 South Alamo Street
San Antonio, TX 78205
210-222-1400
sans.org/event/san-antonio-2016/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 July 5, 2016. To make reservations, please call (800) HILTONS and ask for the SANS group rate.

Top 5 reasons to stay at 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 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 Hilton Palacio del Rio that you won't want to miss!
5. Everything is in one convenient location!

SANS SAN ANTONIO 2016

Registration Information

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

Register online at sans.org/san-antonio

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 **EarlyBird16** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**5-25-16**	**$400.00**	**6-15-16**	**$200.00**

Some restrictions apply.

SANS Voucher Program

Expand your training budget!

Extend your fiscal year. The SANS Voucher Program provides flexibility and may earn you bonus funds for training.

sans.org/vouchers

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 June 29, 2016 – processing fees may apply.

Open a **SANS Portal Account** today to enjoy these FREE resources:

WEBCASTS

Ask The Expert Webcasts – SANS experts bring current and timely information on relevant topics in IT Security.

Analyst Webcasts – A follow-on to the SANS Analyst Program, Analyst Webcasts provide key information from our whitepapers and surveys.

WhatWorks Webcasts – The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT Security issues.

Tool Talks – Tool Talks are designed to give you a solid understanding of a problem, and to show how a vendor's commercial tool can be used to solve or mitigate that problem.

NEWSLETTERS

NewsBites – Twice-weekly high-level executive summary of the most important news relevant to cybersecurity professionals

OUCH! – The world's leading monthly free security-awareness newsletter designed for the common computer user

@RISK: The Consensus Security Alert – A reliable weekly summary of (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) how recent attacks worked, and (4) other valuable data

OTHER FREE RESOURCES

- InfoSec Reading Room
- Top 25 Software Errors
- 20 Critical Controls
- Security Policies
- Intrusion Detection FAQ
- Tip of the Day
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

sans.org/security-resources