SANS

The Most Trusted Source for Information Security Training, Certification, and Research

PHOENIX-MESA 2017

Mesa, AZ | Oct 9-14

Protect Your Business and Advance Your Career

Seven hands-on, immersion-style information security courses taught by real-world practitioners

CYBER DEFENSE
ETHICAL HACKING
PENETRATION TESTING
MANAGEMENT

GIAC CERTIFICATIONS

"The instructors at SANS are the best in the world. They are experts in their field."

-Todd Howe, Sandia National Laboratories

SAVE $400

Register and pay by Aug 16th – Use code **EarlyBird17**

www.sans.org/phoenix-mesa

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 Phoenix-Mesa 2017 lineup of instructors includes:

Adrien de Beaupre
Certified Instructor
@adriendb

Russell Eubanks
Certified Instructor
@russelleubanks

G. Mark Hardy
Principal Instructor
@g_mark

Randy Marchany
Certified Instructor
@randymarchany

David R. Miller
Certified Instructor
@DRM_CyberDude

My-Ngoc Nguyen
Certified Instructor
@MenopN

John Strand
Senior Instructor
@strandjs

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 8.

KEYNOTE: ***If I Wake Evil!!!***
John Strand

HTTPdeux
Adrien de Beaupre

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

Anti-Ransomware: How to Turn the Tables
G. Mark Hardy

Save $400 when you register and pay by August 16th using code EarlyBird17

Courses at a Glance

	MON 10-9	TUE 10-10	WED 10-11	THU 10-12	FRI 10-13	SAT 10-14
SEC301 Intro to Information Security	Page 1					
SEC401 Security Essentials Bootcamp Style	Page 2					
SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	Page 3					
SEC560 Network Penetration Testing and Ethical Hacking	Page 4					
SEC566 Implementing and Auditing the Critical Security Controls – In-Depth	Page 5					
MGT414 SANS Training Program for CISSP® Certification	Page 6					
MGT514 IT Security Strategic Planning, Policy, and Leadership	Page 7					

SEC301

Intro to Information Security

GISF Certification

Information Security Fundamentals

www.giac.org/gisf

Five-Day Program
Mon, Oct 9 - Fri, Oct 13
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: My-Ngoc Nguyen

"Labs reinforced the security principles in a real-world scenario."
-Tyler Moore, Rockwell

"This is the perfect course for establishing a foundation for knowledge of aspects of information security, and the instructor is very knowledgeable and well-versed in the topics."
-Stephen Pridmore, Protective Life

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

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

- **Do you have basic computer knowledge, but are 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 (with some technical knowledge) 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: Intro 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 a basic knowledge of computers and technology but no prior knowledge of cybersecurity. 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.

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 Style**. 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 helping client organizations in both the public and private sectors 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 has top security certifications that include GPEN, GCIH, GSEC, and CISSP, and is a former QSA. She is a member of the FBI's InfraGard, the Information Systems Security Association (ISSA), the Information Systems Audit and Control Association (ISACA), and the International Information Systems Security Certification Consortium (ISC). My-Ngoc founded the non-profit organization CyberSafeNV to raise security awareness among Nevada residents and is currently the organization's chairperson. **@MenopN**

SEC401

Security Essentials Bootcamp Style

GSEC Certification
Security Essentials

www.giac.org/gsec

Six-Day Program
Mon, Oct 9 - Sat, Oct 14
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Russell Eubanks

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks
- Administrators responsible for building and maintaining systems that are being targeted by attackers
- Forensic specialists, penetration testers, and auditors who need a solid foundation of security principles to be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

"This course has opened my eyes to just how important security is, and has given me a deeper understanding of how to protect our systems."

-Travis Sorensen, Xpress Solutions

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

STOP and ask yourself the following questions:

- **Do you fully understand why some organizations get compromised and others do not?**
- **If there were compromised systems on your network, are you confident you would be able to find them?**
- **Do you know the effectiveness of each security device and are you certain they are all configured correctly?**
- **Are proper security metrics set up and communicated to your executives to drive security decisions?**

If you do not know the answers to these questions, SEC401 will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

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. Our 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 rise in 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 will 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.

SANS Technology Institute
www.sans.edu


www.sans.org/8140

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

Russell Eubanks *SANS Certified Instructor*

Russell Eubanks is Vice President and Chief Information Security Officer for the Federal Reserve Bank of Atlanta. He is responsible for developing and executing the information security strategy for both the Retail Payments Office and the Atlanta Reserve Bank. Russell has developed information security programs from the ground up and actively seeks opportunities to measurably increase their overall security posture. Russell is a Handler for the SANS Internet Storm Center, serves on the Editorial Panel for the Critical Security Controls, and maintains securityeverafter.com. He holds a bachelor's degree in computer science from the University of Tennessee at Chattanooga. **@russelleubanks**

SEC504

Hacker Tools, Techniques, Exploits, and Incident Handling

GCIH Certification
Incident Handler

www.giac.org/gcih

Six-Day Program
Mon, Oct 9 - Sat, Oct 14
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
(If your laptop supports only wireless, please bring a USB Ethernet adapter.)
Instructor: John Strand

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

"SEC504 fills in the gap of 'here's what adversaries do' and the evidence they leave."
-Kevin Heithaus, JPMorgan Chase

"The tools provided in SEC504 are ready-to-use in the 'real-world,' and I can already see how I'll be using and applying this course to my job."
-Jennifer Chavarria, Freeport LNG

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection and 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.**

"As someone who works in information security but has never had to do a full incident report, SEC504 taught me all the proper processes and steps."
-Todd Choryan, Motorola Solutions

This course enables you to turn the tables on computer attackers by helping you understand their 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. 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 for, detect, and respond to those attacks. 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, exploiting, and defending systems. **This course 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.

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

John Strand *SANS Senior Instructor*

Along with SEC504, John Strand also teaches SEC560: Network Penetration Testing and Ethical Hacking and SEC464: Hacker Detection for System Administrators. John is the course author for SEC464. When not teaching for SANS, John co-hosts PaulDotCom Security Weekly, the world's largest computer security podcast. He also is the owner of Black Hills Information Security, specializing in penetration testing and security architecture services. He has presented for the FBI, NASA, the NSA, and at DefCon. In his spare time he writes loud rock music and makes various futile attempts at fly fishing. **@strandjs**

SEC560

Network Penetration Testing and Ethical Hacking

GPEN Certification
Penetration Tester

www.giac.org/gpen

Six-Day Program
Mon, Oct 9 - Sat, Oct 14
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Adrien de Beaupre

Who Should Attend

- Security personnel whose jobs involve assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Defenders who want to better understand offensive methodologies, tools, and techniques
- Auditors who need to build deeper technical skills
- Red and blue team members
- Forensics specialists who want to better understand offensive tactics

"SEC560 introduces the whole process of penetration testing from the start of engagement to the end."

-Barry Tsang, Deloitte

"I like that the labs in SEC560 provided clear, step-by-step guidance. The instructor's level of knowledge and ability to relay information is fantastic."

- Bryan Barnhart, Infiltration Labs

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 task head-on.

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

With comprehensive coverage of tools, techniques, and methodologies for network penetration testing, SEC560 truly prepares you to conduct high-value penetration testing projects step-by-step and end-to-end. Every organization needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specially designed to get you ready for that role. The course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks, and web app manipulation, with more than 30 detailed hands-on labs throughout. The course is chock-full of practical, real-world tips from some of the world's best penetration testers to help you do your job safely, efficiently...and masterfully.

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

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test – and on the last day of the course you'll do just that. After building your skills in comprehensive and challenging labs over five days, the course culminates with a final full-day, real-world penetration test scenario. You'll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization, demonstrating the knowledge you've mastered in this course.

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

You will learn how to perform detailed reconnaissance, studying a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won't just cover run-of-the-mill options and configurations, we'll also go over the lesser known but super-useful capabilities of the best pen test toolsets available today. After scanning, you'll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You'll dive deep into post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth.

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

Adrien de Beaupre *SANS Certified Instructor*

Adrien de Beaupre works as an independent consultant in beautiful Ottawa, Ontario. His work experience includes technical instruction, vulnerability assessment, penetration testing, intrusion detection, incident response and forensic analysis. He is a member of the SANS Internet Storm Center (isc.sans.edu). He is actively involved with the information security community, and has been working with SANS since 2000. Adrien holds a variety of certifications including the GXPN, GPEN, GWAPT, GCIH, GCIA, GSEC, CISSP, OPST, and OPSA. When not geeking out he can be found with his family, or at the dojo. @adriendb

SEC566

Implementing and Auditing the Critical Security Controls – In-Depth

GCCC Certification
Critical Controls

www.giac.org/gccc

Five-Day Program
Mon, Oct 9 - Fri, Oct 13
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Randy Marchany

Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel or contractors
- Staff and clients of federal agencies
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC/AUD440, SEC401, SEC501, SANS Audit classes, and MGT512

"This training gets right to the point quickly, and the labs are very clear and concise."

-Duane Harper, Community Health Systems

SANS Technology Institute
www.sans.edu

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches? This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS).

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

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

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle. The British government's Center for the Protection of National Infrastructure describes the Controls as the "baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence."

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

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

Randy Marchany *SANS Certified Instructor*

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

MGT414

SANS Training Program for CISSP® Certification

GISP Certification
Information Security Professional

www.giac.org/gisp

Six-Day Program
Mon, Oct 9 - Sat, Oct 14
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: David R. Miller

Who Should Attend

- Security professionals who are interested in understanding the concepts covered on the CISSP® exam as determined by $(ISC)^2$
- Managers who want to understand the critical areas of information security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® eight domains
- Security professionals and managers looking for practical ways the eight domains of knowledge can be applied to their current job

www.sans.org/8140

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that is specifically designed to prepare students to successfully pass the CISSP® exam.

MGT414 focuses solely on the eight domains of knowledge as determined by $(ISC)^2$ that form a critical part of the 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.

Obtaining Your CISSP® Certification Consists of:

- **Fulfilling minimum requirements for professional work experience**
- **Completing the Candidate Agreement**
- **Review of your résumé**
- **Passing the CISSP® 250 multiple-choice question exam with a scaled score of 700 points or greater**
- **Submitting a properly completed and executed Endorsement Form**
- **Periodic audit of CPEs to maintain the credential**

"I would recommend this course for anyone wanting to get a CISSP®. I feel it gave me the tools to be confident to take the test."
-Matthew Trummer, Lincoln Electric Systems

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

"I feel prepared for my exam after taking this course."
-Tom DiNunzio, Exelon

David R. Miller *SANS Certified Instructor*

David has been a technical instructor since the early 1980s and has specialized in consulting, auditing, and lecturing on information system security, legal and regulatory compliance, and network engineering. David has helped many enterprises develop their overall compliance and security program, including policy writing, network architecture design (including security zones), development of incident response teams and programs, design and implementation of public key infrastructures, security awareness training programs, specific security solution designs such as secure remote access and strong authentication architectures, disaster recovery planning and business continuity planning, and pre-audit compliance gap analysis and remediation. He serves as a security lead and forensic investigator on numerous enterprise-wide IT design and implementation projects for Fortune 500 companies, providing compliance, security, technology, and architectural recommendations and guidance. Projects he's currently working on include Microsoft Windows Active Directory enterprise designs, security information and event management systems, intrusion detection and protection systems, endpoint protection systems, patch management systems, configuration monitoring systems, and enterprise data encryption for data at rest, in transit, in use, and within email systems. David is an author, lecturer and technical editor of books, curriculum, certification exams, and computer-based training videos. **@DRM_CyberDude**

MGT514

GSTRT Certification

Strategic Planning, Policy, and Leadership

www.giac.org/gstrt

IT Security Strategic Planning, Policy, and Leadership

Five-Day Program
Mon, Oct 9 - Fri, Oct 13
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: G. Mark Hardy

Who Should Attend

- CISOs
- Information security officers
- Security directors
- Security managers
- Aspiring security leaders
- Other security personnel who have team lead or management responsibilities

"I moved into management a few years ago and am currently working on a new security strategy/ roadmap and this class just condensed the past two months of my life into a one-week course and I still learned a lot!"

-Travis Evans, SiriusXM

SANS Technology Institute
www.sans.edu

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

As security professionals we have seen the landscape change. Cybersecurity is now more vital and relevant to the growth of your organization than ever before. As a result, information security teams have more visibility, more budget, and more opportunity. However, with this increased responsibility comes more scrutiny.

This course teaches security professionals how to handle three critical tasks:

- **Develop Strategic Plans**
  Strategic planning is hard for people in IT and IT security, because we spend so much time responding and reacting. We almost never get to practice until we get promoted to a senior position, and then we are not equipped with the skills we need to run with the pack. Learn how to develop strategic plans that resonate with other IT and business leaders.
- **Create Effective Information Security Policy**
  Policy is a manager's opportunity to express expectations for the workforce, set the boundaries of acceptable behavior, and empower people to do what they ought to be doing. It is easy to get wrong. Have you ever seen a policy and your response was, "No way, I am not going to do that!"? Policy must be aligned with an organization's culture. We will break down the steps to policy development so that you have the ability to develop and assess policy to successfully guide your organization.
- **Develop Management and Leadership Skills**
  Leadership is a capability that must be learned, exercised, and developed to better ensure organizational success. Strong leadership is brought about primarily through selfless devotion to the organization and staff, tireless effort in setting the example, and the vision to see and effectively use available resources toward the end goal. Effective leadership entails persuading team members to accomplish their objectives while removing obstacles and maintaining the well-being of the team in support of the organization's mission. Learn to utilize management tools and frameworks to better lead, inspire, and motivate your teams.

How the Course Works

Using case studies from Harvard Business School, team-based exercises, and discussions that put students in real-world scenarios, students will participate in activities they can carry out with their own team members when they return to work.

The next generation of security leadership must bridge the gap between security staff and senior leadership by strategically planning how to build and run effective security programs. After taking this course, you will have the fundamental skills to create strategic plans to protect your company, enable key innovations, and work effectively with your business partners.

G. Mark Hardy *SANS Principal Instructor*

G. Mark Hardy is the founder and president of National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for over 35 years, and is an internationally recognized expert and keynote speaker who has presented at over 250 events world-wide. He provides consulting services as a virtual CISO, expert witness testimony, and domain expertise in blockchain and cryptocurrency. G. Mark serves on the Advisory Board of CyberWATCH, an Information Assurance/ Information Security Advanced Technology Education Center of the National Science Foundation. He is a retired U.S. Navy captain and was entrusted with nine command assignments, including responsibility for leadership training for 70,000 sailors. A graduate of Northwestern University, he holds a BS in computer science, a BA in mathematics, a master's degree in business administration, and a master's degree in strategic studies, and holds the GSLC, CISSP, CISM and CISA certifications. @g_mark

Bonus Sessions

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: If I Wake Evil!!!

John Strand

Let's say I went to the dark side to get their sweet, sweet cookies...Let's say that all goodness had left me...How would I attack you? This talk will answer that question. It will also show you how to stop me.

HTTPdeux

Adrien de Beaupre

This presentation will discuss the relatively new HTTP2 protocol that has been recently and widely adopted as a standard. Most browsers and web servers can support it, but relatively little security research has been done on the new protocol. There are very few tools to perform security testing, and penetration testing is challenging. The presentation will include a demo of a HTTP2 vulnerability being exploited.

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 [src]

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 have led to many breaches, especially those that were headlined. We'll touch on some details from those headlined breaches to show commonalities, address the main misconceptions, describe attackers' approaches, provide some statistics, and most importantly, provide helpful tips applicable to all members of the audience.

Anti-Ransomware: How to Turn the Tables

G. Mark Hardy

OMG! We just got hit with Ransomware! What you don't usually hear next is LOL! You can build defenses that prevent Ransomware from paralyzing your organization – we'll show you how. Ransomware is a billion dollar industry, and it's getting even bigger. Lost productivity costs far more than the average ransom, so executives just say, "Pay the darn thing." But what if you could stop Ransomware in its tracks? We'll demonstrate tools and methodologies that are battle-proven and ACTUALLY WORK as evidenced by fully contained Ransomware "explosions" that went nowhere. We'll offer insights into the future of this attack vector, and we'll venture predictions on how this "industry" will evolve and what to expect next.

Enhance Your Training Experience

Add an
OnDemand Bundle & GIAC Certification Attempt*
to your course within seven days
of this event for just $689 each.

SPECIAL PRICING

Extend Your Training Experience with an 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.

Get Certified with GIAC Certifications

- Distinguish yourself as an information security leader
- 30+ GIAC cybersecurity certifications available
- 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.

SANS Training Formats

Whether you choose to attend a training class live or online, the entire SANS team is dedicated to ensuring your training experience exceeds expectations.

Live Classroom Instruction

Premier Training Events

Our most recommended format, live SANS training events feature SANS's top instructors teaching multiple courses at a single time and location. This allows for:

- Focused, immersive learning without the distractions of your office environment
- Direct access to SANS Certified Instructors
- Interacting with and learning from other professionals
- Attending SANS@Night events, NetWars tournaments, vendor presentations, industry receptions, and many other activities

Our premier live training events in North America, serving thousands of students, are held in Orlando, Washington DC, Las Vegas, New Orleans, and San Diego. Regional events with hundreds of students are held in most major metropolitan areas during the year. See page 12 for upcoming training events in North America.

Summits

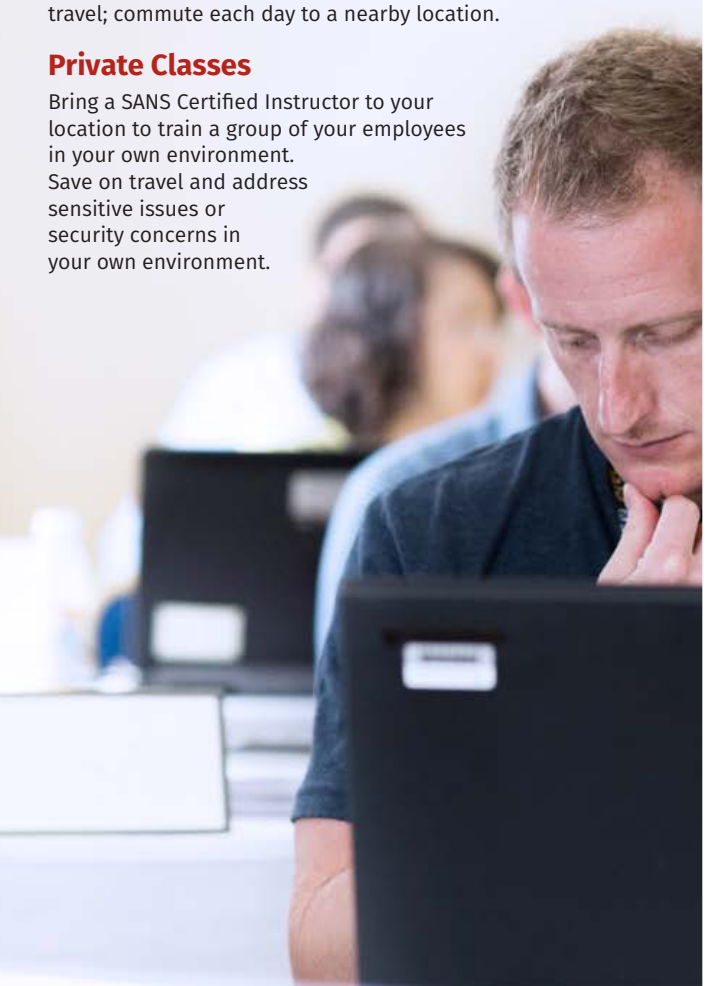
SANS Summits focus one or two days on a single topic of particular interest to the community. Speakers and talks are curated to ensure the greatest applicability to participants.

Community SANS Courses

Same SANS courses, courseware, and labs taught by up-and-coming instructors in a regional area. Smaller classes allow for more extensive instructor interaction. No need to travel; commute each day to a nearby location.

Private Classes

Bring a SANS Certified Instructor to your location to train a group of your employees in your own environment. Save on travel and address sensitive issues or security concerns in your own environment.



Online Training

SANS Online successfully delivers the same measured learning outcomes to students at a distance that we deliver live in classrooms. More than 30 courses are available for you to take whenever or wherever you want. Thousands of students take our courses online and achieve certifications each year.

Top reasons to take SANS courses online:

- **Learn at your own pace, over four months**
- **Spend extra time on complex topics**
- **Repeat labs to ensure proficiency with skills**
- **Save on travel costs**
- **Study at home or in your office**

Our SANS OnDemand, vLive, Simulcast, and SelfStudy formats are backed by nearly 100 professionals who ensure we deliver the same quality instruction online (including support) as we do at live training events.

"I am thoroughly pleased with the OnDemand modality. From a learning standpoint, I lose nothing. In fact, the advantage of setting my own pace with respect to balancing work, family, and training is significant, not to mention the ability to review anything that I might have missed the first time."

-Kevin E., U.S. Army

"The decision to take five days away from the office is never easy, but so rarely have I come to the end of a course and had no regret whatsoever. This was one of the most useful weeks of my professional life."

-Dan Trueman, Novae PLC

Future Training Events

SANSFIRE — Washington, DC — July 22-29

San Antonio	San Antonio, TX	Aug 6-11
Boston	Boston, MA	Aug 7-12
New York City	New York, NY	Aug 14-19
Salt Lake City	Salt Lake City, UT	Aug 14-19
Chicago	Chicago, IL	Aug 21-26
Virginia Beach	Virginia Beach, VA	Aug 21 - Sep 1
Tampa – Clearwater	Clearwater, FL	Sep 5-10
San Francisco Fall	San Francisco, CA	Sep 5-10

Network Security — Las Vegas, NV — Sep 10-17

Baltimore Fall	Baltimore, MD	Sep 25-30
Rocky Mountain Fall	Denver, CO	Sep 25-30
Phoenix-Mesa	Mesa, AZ	Oct 9-14
Tysons Corner Fall	McLean, VA	Oct 16-21
San Diego	San Diego, CA	Oct 30 - Nov 4
Seattle	Seattle, WA	Oct 30 - Nov 4
Miami	Miami, FL	Nov 6-11
San Francisco Winter	San Francisco, CA	Nov 27 - Dec 2
Austin Winter	Austin, TX	Dec 4-9

Cyber Defense Initiative — Washington, DC — Dec 12-19

Future Summit Events

Security Awareness	Nashville, TN	July 31 - Aug 9
Data Breach	Chicago, IL	Sep 25 - Oct 2
Secure DevOps	Denver, CO	Oct 10-17
SIEM & Tactical Analytics	Scottsdale, AZ	Nov 28 - Dec 5
Cyber Threat Intelligence	Washington, DC	Jan 27 - Feb 6

Future Community SANS Events

Local, single-course events are also offered throughout the year via SANS Community. Visit **www.sans.org/community** for up-to-date Community course information.

Hotel Information

Sheraton Mesa Hotel at Wrigleyville West
860 North Riverview
Mesa, AZ 85201
Phone: 480-664-1221
www.sans.org/event/phoenix-mesa-2017/location

Located in a popular suburb of Phoenix, the Sheraton Mesa Hotel at Wrigleyville West is nestled between the Chicago Cubs' spring training park and Riverview Park, in the new area of Wrigleyville West. Many shopping and dining options are within walking distance, and Tempe Marketplace is also nearby. Phoenix Sky Harbor International Airport is only 8 miles away. The Sheraton Mesa Hotel at Wrigleyville West makes it easy to stay productive in an onsite business center or relax in its resort-style facilities. The one-acre resort-style pool area features three swimming pools, two heated wading pools, two hot tubs, cabanas, poolside services, and a sundeck area.

Special Hotel Rates Available

A special discounted rate of $165.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID. These rates include high-speed Internet in your room and are only available through **September 15, 2017**.

Top 5 reasons to stay at the Sheraton Mesa Hotel

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 Sheraton Mesa Hotel, 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 Sheraton Mesa Hotel that you won't want to miss!
5. Everything is in one convenient location!

Registration Information

Register online at **www.sans.org/phoenix-mesa**

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

Select your course 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.

Pay Early and Save*

Use code **EarlyBird17** when registering early

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code by	**8-16-17**	**$400.00**	**9-6-17**	**$200.00**

*Some restrictions apply. Early bird discounts do not apply to Hosted courses.

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.

www.sans.org/vouchers

Cancellation & Access Policy

If an attendee must cancel, a substitute may attend instead. Substitution requests can be made at any time prior to the event start date. Processing fees will apply. All substitution requests must be submitted by email to **registration@sans.org**. If an attendee must cancel and no substitute is available, a refund can be issued for any received payments by **September 20, 2017**. A credit memo can be requested up to the event start date. All cancellation requests must be submitted in writing by mail or fax and received by the stated deadlines. Payments will be refunded by the method that they were submitted. Processing fees will apply.

Open a **SANS 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 FAQs
- Tip of the Day
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

www.sans.org/account