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

SANS NORTHERN VIRGINIA Crystal City 2016

September 6-11

HANDS-ON, IMMERSION-STYLE

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

Defend your organization and advance your career!

Seven courses on

CYBER DEFENSE
PEN TESTING
DIGITAL FORENSICS
SECURITY MANAGEMENT

"SANS training is an excellent balance between theory and practical applications, and extremely relevant to current trends, concepts, and technologies."
-Chris S., Naval Surface Warfare Center

GIAC-Approved Training

SAVE $400

by registering and paying early!

See page 13 for more details.

www.sans.org/crystal-city

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 Crystal City 2016 lineup of instructors includes:

David Cowen
Certified Instructor
@hecfblog

Adrien de Beaupre
Certified Instructor
@adriendb

Tim Garcia
SANS Instructor
@tbg911

David Hoelzer
Faculty Fellow
@it_audit

My-Ngoc Nguyen
Certified Instructor
@MenopN

Alissa Torres
Certified Instructor
@sibertor

Mark Williams
SANS Instructor

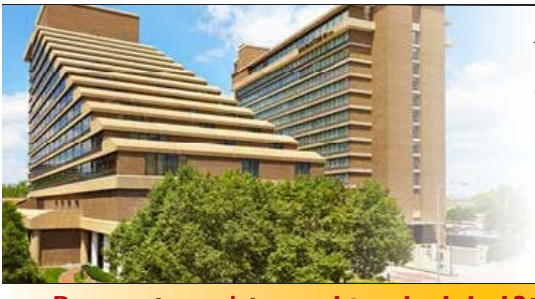
Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 9.

KEYNOTE: ***Exploitation 101: Stacks, NX/DEP, ASLR, and ROP!*** – David Hoelzer

HTTPDeux – Adrien de Beaupre

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



The training campus for SANS Crystal City 2016 is at the newly renovated DoubleTree by Hilton Hotel Washington DC-Crystal City.

PAGE 13

Be sure to register and pay by July 13th for a $400 tuition discount!

Courses-at-a-Glance

		MON 9-6	TUE 9-7	WED 9-8	THU 9-9	FRI 9-10	SAT 9-11
SEC301	Intro to Information Security	Page 2					
SEC401	Security Essentials Bootcamp Style	Page 3					
SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling	Page 4					
SEC542	Web App Penetration Testing and Ethical Hacking	Page 5					
FOR408	Windows Forensic Analysis	Page 6					
MGT512	SANS Security Leadership Essentials for Managers with Knowledge Compression™	Page 7					
MGT514	IT Security Strategic Planning, Policy and Leadership	Page 8					

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 (www.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 the SANS Voucher Program 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!

SEC301:

Intro to Information Security

SANS

Five-Day Program
Mon, Sep 6 - Fri, Sep 10
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: My-Ngoc Nguyen

www.giac.org/gisf

Bundle OnDemand
with this course
www.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, Sep 6 - Sat, Sep 11
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Tim Garcia

www.giac.org/gsec

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"I really appreciate this instructor and I am utilizing this course to improve my practices."
-Margaux Hoaglund, Union Pacific

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

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.

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

Tim Garcia *SANS Instructor*

Timothy Garcia is a seasoned security professional who loves the challenge and continuously changing landscape of defense. Tim started his career as an IT engineer and after working on a few security incidents related to Code Red and Nimda he realized he had found his calling. Tim currently works as an Information Security Consultant for Wells Fargo and has expertise in systems engineering, project management and information security principles and procedures/compliance. Before Wells Fargo, Tim worked for Intel and served in the military. Tim is as passionate about teaching security as he is performing it and receives the greatest joy when he sees the look in students' eyes when something they never quite understood finally makes sense. Tim holds the CISSP, GSEC, GCIH, and NSA-IAM certifications. He has extensive knowledge of security procedures and legislation such as Sarbanes-Oxley, GLBA, CobiT, COSO, and ISO 1779. When Tim is not defending systems, he enjoys playing sports, snowboarding and, most of all, spending time with his wife and four children. @tbg911

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, Sep 6 - Sat, Sep 11
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Alissa Torres

www.giac.org/gcih

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

Bundle OnDemand
with this course
www.sans.org/ondemand

"Alissa's upbeat style is effective and engaging."
-David Crafts, Cloudburst Security

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

"SEC504 is awesome! Everything included in this course is very useful in my job as a security professional!" -Vereleo Bateo, KCG Holdings, Inc.

This course helps you 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 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 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 was my first SANS class.
I did not expect to learn as much as I did during the last 6 days."
-A. Zaman, Verizon

Alissa Torres *SANS Certified Instructor*

Alissa Torres specializes in advanced computer forensics and incident response. Her industry experience includes serving in the trenches as part of the Mandiant Computer Incident Response Team (MCIRT) as an incident handler and working on a internal security team as a digital forensic investigator. She has extensive experience in information security spanning government, academic, and corporate environments and holds a bachelor's degree from the University of Virginia and a master's from the University of Maryland in Information Technology. Alissa has taught at the Defense Cyber Investigations Training Academy (DCITA), delivering incident response and network basics to security professionals entering the forensics community. She has presented at various industry conferences and numerous B-Sides events. In addition to being a GIAC Certified Forensic Analyst (GCFA), she holds the GCFE, GPEN, CISSP, EnCE, CFCE, MCT and CTT+ certifications. @sibertor

SEC542:

Web App Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, Sep 6 - Sat, Sep 11
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Adrien de Beaupre

www.giac.org/gwapt

www.sans.edu

www.sans.org/cyber-guardian

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"(Day 6) Capture the Flag was an amazing eye opener to the real world of web pen testing."
-Derick Ansignia, Scarfold Consult

Web applications play a vital role in every modern organization. But if your organization does not properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

Who Should Attend

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

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organization. Unfortunately, there is no "patch Tuesday" for custom web applications, so major industry studies find that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

"As a web application developer, this course gives great insight into what I can do better and what to look for." -Joshua Barone, Geocent

Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but effective web application penetration testing requires something deeper.

Students will come to understand major web application flaws and their exploitation and, most importantly, learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organizations. Even technically gifted security geeks often struggle with helping organizations understand risk in terms relatable to business. Much of the art of penetration testing has less to do with learning how adversaries are breaking in than it does with convincing an organization to take the risk seriously and employ appropriate countermeasures. The goal of SEC542 is to better secure organizations through penetration testing, and not just show off hacking skills. The course will help you demonstrate the true impact of web application flaws through exploitation.

In addition to more than 30 formal hands-on labs, the course culminates in a web application pen test tournament, powered by the SANS NetWars Cyber Range. This Capture-the-Flag event on the final day brings students into teams to apply their newly acquired command of web application penetration testing techniques in a fun way to hammer home lessons learned.

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

FOR408:
Windows Forensic Analysis

SANS

Six-Day Program
Mon, Sep 6 - Sat, Sep 11
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: David Cowen

www.giac.org/gcfe

SANS Technology Institute
www.sans.edu

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

DFIR
digital-forensics.sans.org

"This course helped on both a professional and personal level. The information also helped me better communicate to non-InfoSec professionals the importance of having certain security controls.
-Maria Bello, Federal National Mortgage Association

Master Windows Forensics – You can't protect what you don't know about.

Every organization must prepare for cyber crime occurring on its computer systems and within its networks. Demand has never been greater for analysts who can investigate crimes like fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover key intelligence from Windows systems. To help solve these cases, SANS is training a new cadre of the world's best digital forensic professionals, incident responders, and media exploitation masters capable of piecing together what happened on computer systems second by second.

Who Should Attend

- Information security professionals
- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Anyone interested in a deep understanding of Windows forensics

"Current and up-to-date material. Cutting edge!"
-John Powell, SaskTel

FOR408: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can't protect what you don't know about, and understanding forensic capabilities and artifacts is a core component of information security. Learn to recover, analyze, and authenticate forensic data on Windows systems. Understand how to track detailed user activity on your network and how to organize findings for use in incident response, internal investigations, and civil/criminal litigation. Use your new skills for validating security tools, enhancing vulnerability assessments, identifying insider threats, tracking hackers, and improving security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR408 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR408 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7/8/10, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows XP systems to just-discovered Windows 10 artifacts.

FIGHT CRIME. UNRAVEL INCIDENTS...ONE BYTE AT A TIME

David Cowen *SANS Certified Instructor*

David Cowen is a Partner at G-C Partners, LLC, where his team of expert digital forensics investigators pushes the boundaries of what is possible on a daily basis. He has been working in digital forensics and incident response since 1999 and has performed investigations covering thousands of systems in the public and private sectors. Those investigations have involved everything from revealing insider threats to serving as an expert witness in civil litigation and providing the evidence to put cyber criminals behind bars. David has authored three series' of books on digital forensics: *Hacking Exposed Computer Forensics* (1st-3rd editions); *Infosec Pro Guide to Computer Forensics*; and the *Anti Hacker Toolkit* (Third Edition). His research into file system journaling forensics has created a new area of analysis that is changing the industry. Combined with Triforce products, David's research enables examiners to go back in time to find previously unknown artifacts and system interactions. @hecfblog

MGT512:

SANS Security Leadership Essentials for Managers with Knowledge Compression™

SANS

Five-Day Program
Mon, Sep 6 - Fri, Sep 10
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop NOT Needed
Instructor: David Hoelzer

www.giac.org/gslc

SANS Technology Institute
www.sans.edu

www.sans.org/8140

Bundle OnDemand
with this course
www.sans.org/ondemand

"SANS MGT512 has been instrumental in bridging the gaps in my knowledge and has prepared me to take on bigger responsibilities."
-Mir Shajee, Accenture

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. In addition, the course has been engineered to incorporate the NIST Special Publication 800 series guidance so that it can be particularly useful to U.S. government managers and supporting contractors.

Who Should Attend

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

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

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!

David Hoelzer *SANS Faculty Fellow*

David Hoelzer is the author of more than 20 sections of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past 25 years. Recently, David was called upon to serve as an expert witness for the Federal Trade Commission for ground-breaking GLBA Privacy Rule litigation. David has been highly involved in governance at the SANS Technology Institute, serving as a member of the Curriculum Committee as well as Audit Curriculum Lead. As a SANS instructor, David has trained security professionals from agencies such as the NSA and DHHS, Fortune 500 companies, various Department of Defense sites, national laboratories, and many colleges and universities. David is a research fellow for the Center for Cybermedia Research and for the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC). He also is an adjunct research associate for the UNLV Cybermedia Research Lab and a research fellow with the Internet Forensics Lab. David has written and contributed to more than 15 peer-reviewed books, publications, and journal articles. Currently, he serves as the principal examiner and director of research for Enclave Forensics, a New York/Las Vegas-based incident response and forensics company. He also serves as the chief information security officer for Cyber-Defense, an open-source security software solution provider. In the past, David served as the director of the GIAC Certification program, bringing the GIAC Security Expert certification to life. He holds a BS in IT, Summa Cum Laude, having spent time either attending or consulting for Stony Brook University, Binghamton University, and American Intercontinental University. @it_audit

MGT514:

IT Security Strategic Planning, Policy, and Leadership

SANS

Five-Day Program
Mon, Sep 6 - Fri, Sep 10
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: Mark Williams

SANS Technology Institute
www.sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"This is a great foundational course as we realize the importance of bringing a business perspective to security."
-Nairobi Kim, Wells Fargo

"The balance is great and the full policy in the appendix helped to round out the analysis. The policy discussions and slides were quite helpful."
-Jason Popp, Nordstrom Inc.

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 do three things:

Who Should Attend

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

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.

"Mark did a great job engaging the students. This was a tough course, however, he pulled participation out of everyone." -Todd Wagner, Caterpillar

Mark Williams *SANS Instructor*

Mark Williams currently holds the position of Principal Systems Security Officer at BlueCross BlueShield of Tennessee. Mark holds multiple certifications in security and privacy including the CISSP, CISA, CRISC, and CIPP/IT. He has authored and taught courses at undergraduate and graduate levels, as well as public seminars around the world. He has worked in public and private sectors in the Americas, Canada, and Europe in the fields of security, compliance, and management. Mark has more than 20 years of international high-tech business experience working with major multinational organizations, governments, and private firms. During his career Mark has consulted on issues of privacy and security, led seminars, and developed information security, privacy, and compliance-related programs.

SANS@NIGHT EVENING TALKS

Enrich your SANS training experience!

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

KEYNOTE:

Exploitation 101: Stacks, NX/DEP, ASLR, and ROP!

David Hoelzer

In this two-hour talk we will begin with basic stack overflows and then introduce the various protections one at a time – and then demonstrate how they are defeated! The talk will cover stack overflows, bypassing DEP/NX (non-executable stacks), defeating ASLR, and defeating code signing with ROP. While the talk covers technical topics, even attendees with less of a technical background will walk away with an appreciation of just how easy exploit development actually is!

HTTPDeux

Adrien de Beaupre

This talk will discuss the HTTP/2 protocol, which has only recently been approved and published. The agenda will include reasons why the new protocol was developed, how it is implemented, tools that can use it, and challenges it presents to penetration testers.

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.

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.

SANS VOUCHER PROGRAM

The SANS Voucher Program allows an organization to manage their training budget from a single SANS Account, potentially receive bonus funds based on their investment level, and centrally administer their training.

Training Investment & Bonus Funds

To open a Voucher Account, an organization pays an agreed upon training investment. Based on the amount of the training investment, an organization could be eligible to receive bonus funds.

The investment and bonus funds:

- Can be applied to **any live or online SANS training course, SANS Summit, GIAC certification, or certification renewal***
- can be increased at any time by making additional investments
- need to be utilized within 12 months, however, the term can be extended by investing additional funds before the end of the 12 month term

*Current exceptions are the Partnership Program, Security Awareness Training,and SANS workshops hosted at events and conferences run by other companies.

Flexibility & Control

The online SANS Admin Tool allows the organization's Program Administrator to manage the account at anytime from anywhere.

With the SANS Admin Tool, the Administrator can:

- approve student enrollment and manage fund usage
- view fund usage in real time
- view students' certification status and test results
- obtain OnDemand course progress by student per course

By creating a Voucher Account, your organization can:

- Simplify the procurement process with a single invoice and payment
- Easily change course attendees if previous plans change
- Lock-in your hard fought training budget and utilize over time
- Control how, where, and for whom funds are spent
- Allow employees to register for training while managing approvals centrally

Getting Started

Complete and submit the form online at **www.sans.org/vouchers** and a SANS representative in your region will contact you within 24 business hours.

Get started today and within as little as one week, we can create your Account and your employees can begin their training.

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

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

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

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

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

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

ONLINE TRAINING

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

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

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

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

FUTURE SANS TRAINING EVENTS

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

San Antonio 2016
San Antonio, TX | 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 1-10

Portland 2016
Portland, OR | Aug 8-13

Dallas 2016
Dallas, TX | Aug 8-13

Data Breach Summit
Chicago, IL | Aug 18

Chicago 2016
Chicago, IL | Aug 22-27

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

SANS CRYSTAL CITY 2016

Hotel Information

Training Campus

DoubleTree by Hilton Washington DC-Crystal City

300 Army Navy Drive
Arlington, VA 22202 | 703-416-4100
www.sans.org/event/crystal-city-2016/location

Enjoy stunning views of the nation's capital from the newly renovated DoubleTree by Hilton Hotel Washington DC-Crystal City. With modern furnishings, carpet, bathrooms and upgraded WiFi in all of our guest rooms and suites, you are sure to enjoy your stay. Located in vibrant Crystal City, our hotel in Arlington, VA, provides easy access to restaurants, shops, the metro, Reagan National Airport, and Washington DC. Our hotel features DC monument views, balconies, and space for up to 1,000 guests. Windows Over Washington Collection, our reimagined event space on the 14th floor, opened in February 2016 with modern furnishings and unparalleled views of the DC skyline.

Special Hotel Rates Available

A special discounted rate of $169.00 S/D will be honored based on space availability.
Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through August 14, 2016.

Top 5 reasons to stay at DoubleTree by Hilton

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 DoubleTree by Hilton 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 DoubleTree by Hilton that you won't want to miss!
5. Everything is in one convenient location!

SANS CRYSTAL CITY 2016

Registration Information

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

Register online at www.sans.org/crystal-city

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	**7-13-16**	**$400.00**	**8-3-16**	**$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.

www.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 August 17, 2016 – processing fees may 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 FAQ
- Tip of the Day
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

www.sans.org/security-resources