THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS San Francisco 2015

San Francisco, CA Nov 30 - Dec 5

"SANS brings together the best group of technical experts and the best presenters in the industry."

-Mark Jeanmougin, Vantiv

GIAC Approved Training

Choose from these popular courses:

IT Security Strategic Planning, Policy and Leadership *NEW!*

Security Essentials Bootcamp Style

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS Training Program for CISSP® Certification

Auditing & Monitoring Networks, Perimeters, and Systems

Intro to Information Security

Advanced Exploit Development for Penetration Testers

Mac Forensic Analysis

Register at
sans.org/sanfrancisco

SAVE
$400
by registering & paying early!
See page 13 for more details.

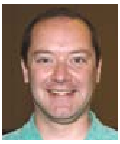
SAN FRANCISCO, CA **SANS San Francisco 2015** NOV 30 - DEC 5

SANS Instructors

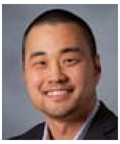
SANS Instructors are real-world practitioners who specialize in the subjects they teach. All instructors undergo rigorous training and testing in order to become SANS Certified Instructors. This guarantees that what you learn in class will be up-to-date and relevant to your job. The SANS San Francisco 2015 line-up of instructors includes:

Sarah Edwards
Certified Instructor

Bryce Galbraith
Principal Instructor



David Hoelzer
SANS Faculty Fellow



Frank Kim
Certified Instructor

David R. Miller
SANS Instructor

Michael Murr
Certified Instructor

My-Ngoc Nguyen
SANS Instructor

Stephen Sims
Senior Instructor

Evening Bonus Sessions

Don't miss these extra evening events that make SANS a great value for your security training:

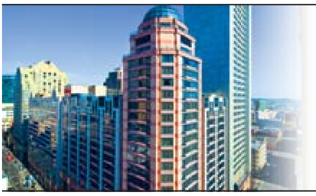
Ubiquity Forensics - Your iCloud and You
Sarah Edwards

Compli-promised: Balancing with Risk Management
My-Ngoc Nguyen

The NEW 2015 CISSP® exam was implemented on April 15, 2015
David Miller

PAGE 9

Be sure to register and pay by Oct 7th for a $400 tuition discount!



As convenient as it is historic, the Hilton San Francisco Union Square hotel is one of the largest hotels on the West Coast, offering exquisite views over the city.

PAGE 13

Courses-at-a-Glance

		MON 11/30	TUE 12/1	WED 12/2	THU 12/3	FRI 12/4	SAT 12/5
SEC301	**Intro to Information Security**	Page 1					
SEC401	**Security Essentials Bootcamp Style**	Page 2					
SEC504	**Hacker Tools, Techniques, Exploits, and Incident Handling**	Page 3					
SEC760	**Advanced Exploit Development for Penetration Testers**	Page 4					
FOR518	**Mac Forensic Analysis**	Page 5					
MGT414	**SANS Training Program for CISSP® Certification**	Page 6					
MGT514	**IT Security Strategic Planning, Policy, and Leadership** ***NEW!***	Page 7					
AUD507	**Auditing & Monitoring Networks, Perimeters, and Systems**	Page 8					

Register today for SANS San Francisco 2015!
sans.org/sanfrancisco

@SANSInstitute
Join the conversation:
#SANS-SanFran

SANS

SECURITY 301

Intro to Information Security

Five-Day Program
Mon, Nov 30 - Fri, Dec 4
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: My-Ngoc Nguyen
▸ GIAC Cert: GISF
▸ OnDemand Bundle

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.

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***

GIAC INFORMATION SECURITY FUNDAMENTALS GISF
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

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

My-Ngoc Nguyen *SANS Instructor*

My-Ngoc Nguyen (pronounced Mee-Nop Wynn) is the CEO/Principal Consultant for Secured IT Solutions. She brings 15 years of experience in information systems and technology, with the past 12 years being focused on cyber security and information assurance for both the government and commercial sectors. My-Ngoc is highly experienced in IT security and risk methodologies, and legal and compliance programs. She led a cyber security 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 to include; GPEN, GCIH, GSEC, CISSP and is a former QSA. My-Ngoc held a Top Security/Q clearance. 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 services to raise security awareness to Nevada residents called CyberSafeNV and is presently the chairman. @MenopN

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/sanfrancisco

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Nov 30 - Sat, Dec 5
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Bryce Galbraith

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

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

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

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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

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

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

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

giac.org

sans.edu

sans.org/
cyber-guardian

sans.org/8570

Bundle OnDemand
WITH THIS COURSE
sans.org/ondemand

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks

"Great explanations on crypto! Took a semester long course and this was much better. The instructor maintains the energy for the entire class and never hesitates to answer questions."
-David Lawrence,
Livermore National Laboratory

Bryce Galbraith *SANS Principal Instructor*

As a contributing author of the internationally bestselling book *Hacking Exposed: Network Security Secrets & Solutions*, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. Bryce has held security positions at global ISPs and Fortune 500 companies, he was a member of Foundstone's renowned penetration testing team and served as a senior instructor and co-author of Foundstone's Ultimate Hacking: Hands-On course series. Bryce is currently the owner of Layered Security where he 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, he holds several security certifications and speaks at conferences around the world. @brycegalbraith

SECURITY 504

Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program
Mon, Nov 30 - Sat, Dec 5
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Michael Murr

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

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

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

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

Who Should Attend

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

"This course gave me a better understanding of what a hacker can do and how he does it — which will help me with incident handling."
-Jill Gallagher, HSBC

"This course helped me fill in the finer details and gaps in my knowledge. I understood the higher level concepts. I have worked with a few of the tools but this helped put it all together."
-Jenna Esparza, Los Alamos National Laboratory

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

Bundle OnDemand
WITH THIS COURSE
sans.org/ondemand

Michael Murr *SANS Certified 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; 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 (http://www.forensicblog.org). @mikemurr

SECURITY 760

Advanced Exploit Development for Penetration Testers

Six-Day Program
Mon, Nov 30 - Sat, Dec 5
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Laptop Required
Instructor: Stephen Sims

Vulnerabilities in modern operating systems such as Microsoft Windows 7/8, Server 2012, and the latest Linux distributions are often very complex and subtle. Yet these vulnerabilities could expose organizations to significant attacks, undermining their defenses when attacked by very skilled adversaries. Few security professionals have the skillset to discover let alone even understand at a fundamental level why the vulnerability exists and how to write an exploit to compromise it. Conversely, attackers must maintain this skillset regardless of the increased complexity. **SEC760: Advanced Exploit Development for Penetration Testers** teaches the skills required to reverse-engineer 32- and 64-bit applications, perform remote user application and kernel debugging, analyze patches for one-day exploits, and write complex exploits, such as use-after-free attacks, against modern software and operating systems.

Who Should Attend

- Senior network and system penetration testers
- Secure application developers (C & C++)
- Reverse-engineering professionals
- Senior incident handlers
- Senior threat analysts
- Vulnerability researchers
- Security researchers

Some of the skills you will learn in SEC760 include:

- How to write modern exploits against the Windows 7 and 8 operating systems
- How to perform complex attacks such as use-after-free, Kernel exploit techniques, one-day exploitation through patch analysis, and other advanced topics
- The importance of utilizing a Security Development Lifecycle (SDL) or Secure SDLC, along with Threat Modeling
- How to effectively utilize various debuggers and plug-ins to improve vulnerability research and speed
- How to deal with modern exploit mitigation controls aimed at thwarting success and defeating determination

What You Will Receive

- Various preconfigured *NIX virtual machines; however, you are required to bring the Windows virtual machines discussed in the Laptop Requirements section
- Various tools on a course USB that are required for use in class
- Access to the in-class Virtual Training Lab with many in-depth labs
- Access to recorded course audio to help hammer home important network penetration testing lessons

> "As always, SANS training is extremely valuable for any security professional. This course sits on top of the mountain of great SANS material."
> -Doug Rodgers, Wells Fargo

> "This course is the challenge I was looking for. It will be overwhelming, but well worth it."
> -William Stott, Raytheon

Not sure if you are ready for SEC760?

Take this 10-question quiz.
sans.org/sec760/quiz

Stephen Sims *SANS Senior Instructor*

Stephen Sims is an industry expert with over 15 years of experience in information technology and security. Stephen currently works out of San Francisco as a consultant performing reverse engineering, exploit development, threat modeling, and penetration testing. Stephen has an MS in information assurance from Norwich University and is a course author and senior instructor for the SANS Institute. He is the author of SANS' only 700-level course, SEC760: Advanced Exploit Development for Penetration Testers, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author on SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking. He holds the GIAC Security Expert (GSE) certification as well as the CISSP, CISA, Immunity NOP, and many other certifications. In his spare time Stephen enjoys snowboarding and writing music. @Steph3nSims

FORENSICS 518

Mac Forensic Analysis

Six-Day Program
Mon, Nov 30 - Sat, Dec 5
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Sarah Edwards
▶ OnDemand Bundle

DFIR
digital-forensics.sans.org

Digital forensic investigators have traditionally dealt with Windows machines, but what if they find themselves in front of a new Apple Mac or iDevice? The increasing popularity of Apple devices can be seen everywhere, from coffee shops to corporate boardrooms, yet most investigators are familiar with Windows-only machines.

Times and trends change and forensic investigators and analysts need to change with them. The new **FOR518: Mac Forensic Analysis** course provides the tools and techniques necessary to take on any Mac case without hesitation. The intense hands-on forensic analysis skills taught in the course will enable Windows-based investigators to broaden their analysis capabilities and have the confidence and knowledge to comfortably analyze any Mac or iOS system.

Who Should Attend

- Experienced digital forensic analysts
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Incident response team members
- Information security professionals
- SANS FOR408, FOR508, FOR526, FOR610, and FOR585 alumni looking to round out their forensic skills

FORENSICATE DIFFERENTLY!

FOR518: Mac Forensic Analysis will teach you:

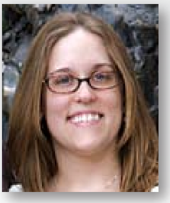
- **Mac Fundamentals:** How to analyze and parse the Hierarchical File System (HFS+) by hand and recognize the specific domains of the logical file system and Mac-specific file types.
- **User Activity:** How to understand and profile users through their data files and preference configurations.
- **Advanced Analysis and Correlation:** How to determine how a system has been used or compromised by using the system and user data files in correlation with system log files.
- **Mac Technologies:** How to understand and analyze many Mac-specific technologies, including Time Machine, Spotlight, iCloud, Versions, FileVault, AirDrop, and FaceTime.

FOR518: Mac Forensic Analysis aims to form a well-rounded investigator by introducing Mac forensics into a Windows-based forensics world. This course focuses on topics such as the HFS+ file system, Mac specific data files, tracking user activity, system configuration, analysis and correlation of Mac logs, Mac applications, and Mac exclusive technologies. A computer forensic analyst who successfully completes the course will have the skills needed to take on a Mac forensics case.

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

"Sarah is an incredible instructor — her knowledge far surpasses anything I've ever experienced plus the reference material is invaluable."
-Ben Keck, Ciena

"Very comprehensive in-depth coverage of the course topic. Excellent reference materials as a take-away."
-Jennifer B., Indiana State Police



Sarah Edwards *SANS Certified Instructor*

Sarah is a senior digital forensic analyst who has worked with various federal law enforcement agencies. She has performed a variety of investigations including computer intrusions, criminal, counter-intelligence, counter-narcotic, and counter-terrorism. Sarah's research and analytical interests include Mac forensics, mobile device forensics, digital profiling, and malware reverse engineering. Sarah has presented at the following industry conferences; Shmoocon, CEIC, BsidesNOLA, TechnoSecurity, HTCIA, and the SANS DFIR Summit. She has a Bachelor of Science in Information Technology from Rochester Institute of Technology and a Master's in Information Assurance from Capitol College. @iamevltwin

MANAGEMENT 414

SANS Training Program for CISSP® Certification

Content Updated for New Exam!
Effective April 15th

SANS

Six-Day Program
Mon, Nov 30 - Sat, Dec 5
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

- GIAC Cert: GISP
- DoDD 8570
- OnDemand Bundle

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

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

MGT414 focuses solely on the 8 domains of knowledge as determined by (ISC)² that form a critical part of CISSP® exam. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

Who Should Attend

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

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

"Best security training I have ever received and had just the right amount of detail for each domain."
-Tony Barnes,
United States Sugar Corp

You Will Be Able To:

- Understand the 8 domains of knowledge that are covered on the CISSP® exam.
- Analyze questions on the exam and be able to select the correct answer.
- Apply the knowledge and testing skills learned in class to pass the CISSP® exam.
- Understand and explain all of the concepts covered in the 8 domains of knowledge.
- Apply the skills learned across the 8 domains to solve security problems when you return to work

GISP
giac.org

sans.org/8570

▶❚❚ Bundle OnDemand
with this course
sans.org/ondemand

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

David R. Miller *SANS Instructor*

David has been a technical instructor since the early 1980s and has specialized in consulting, auditing, and lecturing on the topics of information systems 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 to include security zones, development of incident response teams and programs, design and implementation of public key infrastructures (PKI), security awareness training programs, specific security solution designs like secure remote access and strong authentication architectures, disaster recovery planning and business continuity planning, and pre-audit compliance gap analysis and remediation. He performs 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 include Microsoft Windows Active Directory enterprise designs, Security Information and Event Management (SIEM) systems, Intrusion Detection and Protection Systems (IDS / IPS), endpoint protection systems, patch management systems, configuration monitoring systems, enterprise data encryption for data at rest, in transit, in use, and within email systems, to describe a few. David is an author, a lecturer and technical editor of books, curriculum, certification exams, and computer-based training videos.

MANAGEMENT 514

IT Security Strategic Planning, Policy and Leadership

NEW

SANS

Five-Day Program
Mon, Nov 30 - Fri, Dec 4
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: Frank Kim
▸ STI Master's Program
▸ OnDemand Bundle

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

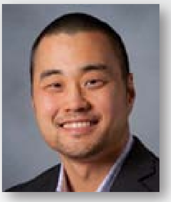
Leadership is a capability that must be learned, exercised and developed to better ensure organizational success. Strong leadership is brought about primarily through selfless devotion to the organization and staff, tireless effort in setting the example, and the vision to see and effectively use available 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.

"As I progress in my career within cybersecurity, I find that courses such as MGT514 will allow me to plan and lead organizations forward."
-Eric Burgan,
Idaho National Labs

"MGT514 contained good practical information, and both professional and personal value."
-Keith Turpin, Boeing

SANS Technology Institute
sans.edu

▶❚❚ Bundle OnDemand
WITH THIS COURSE
sans.org/ondemand



Frank Kim *SANS Certified Instructor*

As CISO at the SANS Institute Frank leads the security risk function for the most trusted source of computer security training, certification, and research in the world. He also helps shape, develop, and support the next generation of security leaders through teaching, developing courseware, and leading the management and software security curricula. Prior to the SANS Institute, Frank was Executive Director of Cyber Security at Kaiser Permanente with accountability for delivering innovative security solutions to meet the unique needs of the nation's largest not-for-profit health plan and integrated health care provider with annual revenue of $55 billion, 9.5 million members, and 175,000 employees. In recognition of his work, Frank was a two-time recipient of the CIO Achievement Award for business enabling thought leadership. Frank holds degrees from the University of California at Berkeley and is a SANS certified instructor as well as the author of popular courseware on strategic planning, leadership, and application security. @sansappsec

AUDIT 507

Auditing & Monitoring Networks, Perimeters, and Systems

Six-Day Program
Mon, Nov 30 - Sat, Dec 5
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: David Hoelzer
▸ GIAC Cert: GSNA
▸ STI Master's Program
▸ DoDD 8570
▸ OnDemand Bundle

Who Should Attend

- Auditors seeking to identify key controls in IT systems
- Audit professionals looking for technical details on auditing
- Managers responsible for overseeing the work of an audit or security team
- Security professionals newly tasked with audit responsibilities
- System and network administrators looking to better understand what an auditor is trying to achieve, how auditors think, and how to better prepare for an audit
- System and network administrators seeking to create strong change control management and detection systems for the enterprise

One of the most significant obstacles facing many auditors today is how exactly to go about auditing the security of an enterprise. What systems really matter? How should the firewall and routers be configured? What settings should be checked on the various systems under scrutiny? Is there a set of processes that can be put into place to allow an auditor to focus on the business processes rather than the security settings? All of these questions and more will be answered by the material covered in this course.

This course is specifically organized to provide a risk-driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practices, the students will have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation will be given from real-world examples.

One of the struggles that IT auditors face today is helping management understand the relationship between the technical controls and the risks to the business that these controls address. In this course these threats and vulnerabilities are explained based on validated information from real-world situations. The instructor will take the time to explain how this can be used to raise the awareness of management and others within the organization to build an understanding of why these controls specifically and auditing in general are important. From these threats and vulnerabilities, we will explain how to build the ongoing compliance monitoring systems and how to automatically validate defenses through instrumentation and automation of audit checklists.

You'll be able to use what you learn immediately. Five of the six days in the course will either produce or provide you directly with a general checklist that can be customized for your audit practice. Each of these days includes hands-on exercises with a variety of tools discussed during the lecture sections so that you will leave knowing how to verify each and every control described in the class. Each of the five hands-on days gives you the chance to perform a thorough technical audit of the technology being considered by applying the checklists provided in class to sample audit problems in a virtualized environment. Each student is invited to bring a Windows XP Professional or higher laptop for use during class. Macintosh computers running OS X may also be used with VMWare Fusion.

GIAC SYSTEMS AND NETWORK AUDITOR GSNA
giac.org

SANS Technology Institute
sans.edu

sans.org/8570

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

David Hoelzer *SANS Faculty Fellow*

David Hoelzer is a high-scoring SANS Fellow instructor and author of more than twenty 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 twenty-five 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 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 organizations including NSA, DHHS, Fortune 500 security engineers and managers, various Department of Defense sites, national laboratories, and many colleges and universities. David is a research fellow in the Center for Cybermedia Research and also a research fellow for the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC). He also is an adjunct research associate of 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, David 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. David 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

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.

Ubiquity Forensics – Your iCloud and You

Sarah Edwards

Ubiquity or "Everything, Everywhere" – Apple uses this term to describe iCloud-related items and its availability across all devices. iCloud enables us to have our data synced with every Mac, iPhone, iPad, and PC, as well as accessible with your handy web browser. You can access your email, documents, contacts, browsing history, notes, keychains, photos, and more all with just a click of the mouse or a tap of the finger on any device, all synced within seconds. Much of this data get cached on your devices. This presentation will explore the forensic artifacts related to this cached data. Where is the data stored; how to look at it; how is it synced; and what other sensitive information can be found that you may not have known existed!

Compli-promised: Balancing with Risk Management

My-Ngoc Nguyen

Many of the organizations recently breached were said to be compliant to their respective regulatory requirements (e.g PCI, FISMA,SOX, HIPAA, etc). Because it has been mistakenly implied that compliance means secure, compliance bodies just increase the requirements and repercussions for noncompliance. In a knee-jerk reaction, organizations focus on compliance at the expense of real security. It then becomes a numbers game and organizations compromise (pun intended) quality of security controls for checking the box on the audit list. The numbers of controls (ranging from 105 to 612 depending on the mandate) are so daunting, however. So organizations become less secure, "If you have everything to do, you do nothing" as Alan Paller (SANS) quoted. The compromise to just comply leads to the compromise of the organization. Don't be like those firms and compromise. Become securer by addressing the controls of your highest risk and most prioritized risk and as a by-product, compliant. This talk will provide an overview of security trends and breaches, the threat landscape, commonalities in the vulnerabilities of the compromised organizations, and relate it all to a risk perspective.

The NEW 2015 CISSP® exam was implemented on April 15, 2015

David Miller

Are you interested in the CISSP® certification? How might it improve your career? On the resume? Getting a new job? On the business card? Maintaining your career and moving you up the ladder. With your skill set? As the professional you are. How about helping with that pay raise? We will look at how management views this well sought-after certification. Have you been studying for it? Do you plan to take the exam real soon? On January 15, 2015, (ISC)^2, the certifying body for the CISSP® certification exam, released a new set of exam objectives for the CISSP® certification exam. These changes were implemented on the CISSP certification exam beginning April 15, 2015. This new set of exam objectives is a major change from the previous version of the CISSP exam. (ISC)^2 has moved and merged content to form 8 Domains of the Common Body of Knowledge, down from 10 Domains in the previous exam. They have also added numerous new topics to the objectives. You will need to know about the new material you will be tested on. Learn the new shape and the new topics of the 2015 CISSP® certification exam.

Build Your Best Career WITH SANS

Add an

OnDemand Bundle & GIAC Certification Attempt

to your course within seven days of this event for just $629 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

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

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

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

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

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

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

ONLINE TRAINING

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

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

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

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

SANS 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

Now eligible for Veterans Education benefits!
Earn industry-recognized GIAC certifications throughout the program
Learn more at www.sans.edu | info@sans.edu

GLOBAL INFORMATION ASSURANCE CERTIFICATION GIAC www.giac.org

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.

FUTURE SANS TRAINING EVENTS

SANS Cyber Security Enforcement SUMMIT & TRAINING
Dallas, TX | September 21-26

SANS Baltimore 2015
Baltimore, MD | September 21-26 | #SANSBaltimore

SANS Seattle 2015
Seattle, WA | October 5-10 | #SANSSeattle

SANS Tysons Corner 2015
Tysons Corner, VA | October 12-17 | #SANSTysonsCorner

SANS Cyber Defense San Diego 2015
San Diego, CA | October 19-24 | #CyberDefSD

SANS South Florida 2015
Fort Lauderdale, FL | November 9-14 | #SANSFLA

SANS Pen Test Hackfest SUMMIT & TRAINING
Alexandria, VA | November 16-23

SANS Security Leadership SUMMIT & TRAINING
Dallas, TX | December 3-10

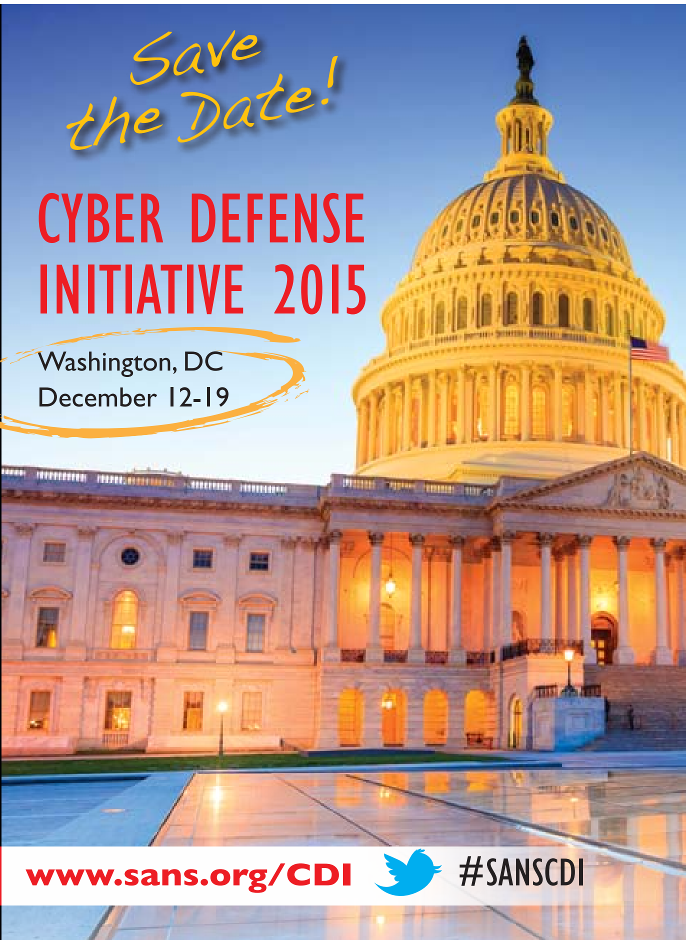
SANS Cyber Defense Initiative 2015
Washington, DC | December 12-19 | #SANSCDI

SANS

CDI

Cyber Defense and Security Training

Over 25 hands-on immersion courses along with NetWars Tournaments



Save the Date!

CYBER DEFENSE INITIATIVE 2015

Washington, DC
December 12-19

REGISTER AT **www.sans.org/CDI** #SANSCDI

SANS SAN FRANCISCO 2015

Hotel Information

Training Campus

Hilton San Francisco Union Square

333 O'Farrell Street
San Francisco, CA 94102
415-771-1400
sans.org/event/san-francisco-2015/location

As convenient as it is historic, the Hilton San Francisco Union Square hotel is one of the largest hotels on the West Coast, offering exquisite views over the city. Located in the heart of downtown San Francisco, this stylish and sophisticated hotel offers easy access to Nob Hill, Chinatown and fantastic shopping and entertainment venues in one of the USA's most diverse and dynamic cities.

Special Hotel Rates Available

A special discounted rate of $219.00 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 Nov. 9, 2015.

Top 5 reasons to stay at the Hilton San Francisco Union Square

1. All SANS attendees receive complimentary high-speed Internet when booking in the SANS block.
2. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
3. By staying at the Hilton San Francisco Union Square, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
4. SANS schedules morning and evening events at the Hilton San Francisco Union Square that you won't want to miss!
5. Everything is in one convenient location!

SANS SAN FRANCISCO 2015

Registration Information

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

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

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

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

Use code **EarlyBird15** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**10/7/15**	**$400.00**	**10/28/15**	**$200.00**

Some restrictions apply.

Group Savings (Applies to tuition only)

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

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

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

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by November 11, 2015 – processing fees may apply.

SANS Voucher Credit Program

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

Open a SANS Portal Account

Sign up for a SANS Portal Account and receive free webcasts, newsletters, the latest news and updates, and many other free resources.

sans.org/account