THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS West Coast Region

FALL 2015

Seattle 2015

October 5-10

NEW! SEC301: Intro to Information Security

SEC401: Security Essentials Bootcamp Style

SEC501: Advanced Security Essentials – Enterprise Defender

SEC503: Intrusion Detection In-Depth

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling

Cyber Defense San Diego 2015

October 19-24

Register to compete in the SANS Cyber Defense Challenge at sans.org/cyber-defense-challenge

SEC505: Securing Windows with PowerShell and the Critical Security Controls

NEW! SEC511: Continuous Monitoring and Security Operations

NEW! SEC550: Active Defense, Offensive Countermeasures and Cyber Deception

SEC575: Mobile Device Security and Ethical Hacking

SEC760: Advanced Exploit Development for Penetration Testers

San Francisco 2015

November 30 - December 5

FOR508: Advanced Digital Forensics and Incident Response

NEW! FOR518: Mac Forensic Analysis

MGT414: SANS Training Program for CISSP® Certification

MGT514: IT Security Strategic Planning, Policy, and Leadership

AUD507: Auditing & Monitoring Networks, Perimeters, and Systems

Save $400

Register & pay early! See page 21 for more details.

SANS West Coast Region FALL 2015

Seattle
Seattle, WA
October 5-10
sans.org/seattle
#SANSSeattle

Cyber Defense San Diego
San Diego, CA | Oct 19-24
sans.org/cyberdefense
#CyberDefSD

San Francisco
San Francisco, CA
Nov 30 - Dec 5
sans.org/sanfrancisco
#SANS-SanFran

	Seattle	Cyber Defense San Diego	San Francisco
NEW! SEC301: Intro to Information Security			**SEC301** My-Ngoc Nguyen
SEC401: Security Essentials Bootcamp Style	**SEC401** Bryce Galbraith	**SEC401** Dr. Eric Cole	**SEC401** Bryce Galbraith
SEC501: Advanced Security Essentials – Enterprise Defender	**SEC501** Bryan Simon	**SEC501** Paul A. Henry	
SEC503: Intrusion Detection In-Depth		**SEC503** Mike Poor	
SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	**SEC504** Dave Shackleford	**SEC504** John Strand	**SEC504** Michael Murr
SEC505: Securing Windows with PowerShell and the Critical Security Controls	**SEC505** Jason Fossen		
NEW! SEC511: Continuous Monitoring and Security Operations		**SEC511** Seth Misenar	
NEW! SEC550: Active Defense, Offensive Countermeasures and Cyber Deception		**SEC550** Mick Douglas	
SEC575: Mobile Device Security and Ethical Hacking	**SEC575** Christopher Crowley		
SEC760: Advanced Exploit Development for Penetration Testers			**SEC760** Stephen Sims
FOR508: Advanced Digital Forensics and Incident Response	**FOR508** Jake Williams		
NEW! FOR518: Mac Forensic Analysis			**FOR518** Sarah Edwards
MGT414: SANS Training Program for CISSP® Certification		**MGT414** Eric Conrad	**MGT414** David R. Miller
MGT514: IT Security Strategic Planning, Policy, and Leadership			**MGT514** Frank Kim
AUD507: Auditing & Monitoring Networks, Perimeters, and System			**AUD507** David Hoelzer

TRAINING EVENTS:

San Francisco
Nov 30 - Dec 5
My-Ngoc Nguyen

SANS
SEC301

Five-Day Program
30 CPEs
Laptop Required

YOU WILL BE ABLE TO:

- Communicate with confidence regarding information security topics, terms, and concepts
- Understand and apply the Principles of Least Privilege
- Understand and apply the Confidentiality, Integrity, and Availability (CIA) Triad
- Build better passwords that are more secure while also being easier to remember and type
- Grasp basic cryptographic principles, processes, procedures, and applications
- Gain an understanding of computer network basics
- Have a fundamental grasp of any number of critical technical networking acronyms: TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS
- Utilize built-in Windows tools to see your network settings
- Recognize and be able to discuss various security technologies including anti-malware, firewalls, and intrusion detection systems.
- Determine your "SPAM IQ" to more easily identify SPAM email messages
- Understand physical security issues and how they support cybersecurity
- Have an introductory level of knowledge regarding incident response, business continuity, and disaster recovery planning
- Install and use the following tools: Password Safe, Secunia PSI, Malwarebytes, and Syncback

NEW

SEC301
Intro to Information Security

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.

"If you are just starting out in information security, this course has all the basics needed to get you started."
-Sherrie Audrict, Deltha Corporation

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.

"This class is great for IT professionals looking for their first step towards security awareness. I have been in IT for 17 years and I learned a lot on this first day of class."
-Paul Beninati, EMC

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.org

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

SEC401
Security Essentials Bootcamp Style

This course will teach you the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. You'll 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.

STOP and ask yourself the following questions:

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

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

"SEC401 is the best InfoSec training bar none. The value for the money is unbeatable!" -Ron Foupht, Sirius Computer Solutions

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. The 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 will need if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security instructors in the industry.

giac.org

sans.edu

sans.org/cyber-guardian

BUNDLE ONDEMAND WITH THIS COURSE
sans.org/ondemand

MEETS DoDD 8570 REQUIREMENTS
sans.org/8570

TRAINING EVENTS:

Seattle
October 5-10
Bryce Galbraith

Cyber Defense San Diego
October 19-24
Dr. Eric Cole

San Francisco
Nov 30 - Dec 5
Bryce Galbraith

SANS
SEC401

Six-Day Program
46 CPEs
Laptop Required

WHO SHOULD ATTEND:

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

TRAINING EVENTS:

Seattle
October 5-10
Bryan Simon

Cyber Defense San Diego
October 19-24
Paul A. Henry

SANS
SEC501

Six-Day Program
36 CPEs
Laptop Required

WHO SHOULD ATTEND:

- Incident response and penetration testers
- Security Operations Center engineers and analysts
- Network security professionals
- Anyone who seeks technical in-depth knowledge about implementing comprehensive security solutions

SEC501
Advanced Security Essentials – Enterprise Defender

Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad reputational damage. **SEC501: Advanced Security Essentials Enterprise Defender** builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

"I love the content, course, and instructor. This course will greatly enhance my effectiveness upon returning to the office."
-Andrew D'Albor, Chicago Bridge & Iron Company

It has been said of security that "prevention is ideal, but detection is a must." However, detection without response has little value. Network security needs to be constantly improved to prevent as many attacks as possible and to swiftly detect and respond appropriately to any breach that does occur. This PREVENT - DETECT - RESPONSE strategy must be in place both externally and internally. As data become more portable and networks continue to be porous, there needs to be an increased focus on data protection. Critical information must be secured regardless of whether it resides on a server, in a robust network architecture, or on a portable device.

"Very knowledgeable. Top-tier training and industry leading."
-Herbert Monford, Regions Bank

Despite an organization's best efforts to prevent network attacks and protect its critical data, some attacks will still be successful. Therefore, organizations need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks, looking for indications of an attack, and performing penetration testing and vulnerability analysis against your organization to identify problems and issues before a compromise occurs.

"After taking SEC401 and GSEC, this course is the perfect follow up, going deep into attacking techniques while understanding the most-used vulnerabilities and how to defend your network against those attacks."
-Fawaz AlHomoud, Saudi Aramco

Finally, once an attack is detected we must react quickly and effectively and perform the forensics required. Knowledge gained by understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

giac.org

sans.edu

sans.org/ondemand

sans.org/8570

SEC503
Intrusion Detection In-Depth

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

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

"Today has been brilliant, bringing all of our skills together to achieve the challenge. I wish we could do this every day!"
-Hayley Roberts, MOD

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

"This course provides a good basis of knowledge and presents important tools which will be at the core of any intrusion analysis."
-Thomas Kelly, DIA

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

TRAINING EVENTS:

Cyber Defense San Diego
October 19-24
Mike Poor

SANS
SEC503

Six-Day Program
36 CPEs
Laptop Required

WHO SHOULD ATTEND:

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

giac.org

sans.edu

sans.org/cyber-guardian

BUNDLE ONDEMAND WITH THIS COURSE
sans.org/ondemand

MEETS DoDD 8570 REQUIREMENTS
sans.org/8570

TRAINING EVENTS:

Seattle
October 5-10
Dave Shackleford

Cyber Defense San Diego
October 19-24
John Strand

San Francisco
Nov 30 - Dec 5
Michael Murr

SANS
SEC504

Six-Day Program
37 CPEs
Laptop Required

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
Hacker Tools, Techniques, Exploits and Incident Handling

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.

"The instructor opened my eyes and helped me understand how to approach the concepts of offensive security and incident handling. He is one of the very best."
-Stephen Ellis, CB&I

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 prevent, 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, exploiting, and defending systems. It will enable you to discover the holes in your system before the bad guys do!

"Our organization has incident response pieces all over. This course is valuable in putting the pieces together and improving the plan and, more importantly, the mindset."
-Tyler Burwitz, TEEX

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.

SEC505
Securing Windows with PowerShell and the Critical Security Controls

How can we defend against pass-the-hash attacks, administrator account compromise, and the lateral movement of hackers inside our networks? How do we actually implement the Critical Security Controls on Windows in a large environment? How can we significantly reduce the client-side exploits that lead to advanced persistent threat malware infections? We tackle these tough problems in **SEC505: Securing Windows with PowerShell and the Critical Security Controls**.

"SEC505 is very well structured and organized and provided me with an in-depth understanding of Windows security." -Rochana Lahiri, BCBSLA

Understanding how penetration testers and hackers break into networks is not the same as knowing how to design defenses against them, especially when you work in a large and complex Active Directory environment. Knowing about tools like Metasploit, Cain, Netcat, and Poison Ivy is useful, but there is no simple patch against their abuse. The goal of this course is to show you ways to defend against both current Windows attack techniques and the likely types of attacks we can expect in the future. This requires more than just reactive patch management – we need to proactively design security into our systems and networks. That is what SEC505 is about.

Your adversaries want to elevate their privileges to win control over your servers and domain controllers, so a major theme of this course is controlling administrative powers through Group Policy and PowerShell scripting.

Learning PowerShell is probably the single best new skill for Windows administrators, especially with the trend toward cloud computing. Most of your competition in the job market lacks scripting skills, so knowing PowerShell is a great way to make your résumé stand out. This course devotes the entire first day to PowerShell, then we do more PowerShell exercises throughout the rest of the week. Don't worry, you don't need any prior scripting experience to attend.

"SEC505 has a direct impact on Windows is security and is a must for any system admin in this day and age." -Chris Linville, Raytheon

SEC505 will also prepare you for the GIAC Certified Windows Security Administrator (GCWN) exam to certify your Windows security expertise. The GCWN certification counts toward getting a Master's Degree in information security from the SANS Technology Institute (sans.edu) and also satisfies the Department of Defense 8570 computing environment requirement.

This is a fun course and a real eye-opener, even for Windows administrators with years of experience. Come have fun learning PowerShell and Windows security!

TRAINING EVENTS:

Seattle
October 5-10
Jason Fossen

SANS
SEC505

Six-Day Program
36 CPEs
Laptop Required

WHO SHOULD ATTEND:

- Windows security engineers and system administrators
- Anyone who wants to learn PowerShell
- Anyone who wants to implement the SANS Critical Security Controls
- Those who must enforce security policies on Windows hosts
- Anyone who needs a whole drive encryption solution
- Those deploying or managing a PKI or smart cards

giac.org

sans.edu

sans.org/cyber-guardian

BUNDLE ONDEMAND WITH THIS COURSE
sans.org/ondemand

MEETS DoDD 8570 REQUIREMENTS
sans.org/8570

TRAINING EVENTS:

Cyber Defense San Diego
October 19-24
Seth Misenar

Covers NIST SP800-137: Continuous Monitoring

SANS
SEC511

Six-Day Program
36 CPEs
Laptop Required

WHO SHOULD ATTEND:

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

NEW

SEC511
Continuous Monitoring and Security Operations

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

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

"SEC511 provides excellent info for self assessment of current SEC practices. Picked up a lot of tricks and new perspectives."
-Kyle Montgomery, NRECA

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

SANS is uniquely qualified to offer this course. Course authors Eric Conrad (GSE #13) and Seth Misenar (GSE #28) hold the distinguished GIAC Security Expert Certification (GSE). Both are experienced, real-world practitioners who apply the concepts and techniques they teach in this course on a daily basis.

giac.org

sans.edu

sans.org/ondemand

NEW

SEC550
Active Defense, Offensive Countermeasures, and Cyber Deception

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

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

You Will Be Able To

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

Author Statement

"I wrote this course to finally make defense fun, to finally add some confusion to the attackers, and to change the way we all look at defense. One of the most frequent questions I get is why offensive countermeasures are so important. Many people tell me that we cannot ignore patching, firewalls, policies, and other security management techniques. I cannot agree more. The techniques presented in this course are intended for organizations that have gone through the process of doing things correctly and want to go further. Get your house in order, and then play. Of course, there will be challenges for anyone trying to implement offensive countermeasures in their organization. However, they can all be faced and overcome."
- John Strand

TRAINING EVENTS:

Cyber Defense San Diego
October 19-24
Mick Douglas

SANS
SEC550

Five-Day Program
30 CPEs
Laptop Required

WHO SHOULD ATTEND:

- Security professionals and systems administrators who are tired of playing catch-up with attackers
- Anyone who is in IT and/or security and wants defense to be fun again

TRAINING EVENTS:

Seattle
October 5-10
Christopher Crowley

SEC575
Mobile Device Security and Ethical Hacking

Mobile phones and tablets have become essential to enterprise and government networks ranging from small organizations to Fortune 500 companies and large public agencies. Often, mobile phone deployments grow organically, adopted by multitudes of end-users for convenient email access, as well as by managers and executives who need access to sensitive organizational resources from their favored personal mobile devices. In other cases, mobile phones and tablets have become critical systems for a wide variety of production applications from enterprise resource planning to project management.

"Awesome course material. Day three really picked up the pace and demonstrated interesting techniques."
-Ted Moskalenko, University of Pennsylvania

For all of its convenience, however, the ubiquitous use of mobile devices in the workplace and beyond has brought new security risks. As reliance on these devices has grown exponentially, organizations have quickly recognized that mobile phones and tablets need greater security implementations than a simple screen protector and clever password. Whether an Apple iPhone or iPad, a Windows Phone, or an Android or BlackBerry phone or tablet, these devices have become hugely attractive and vulnerable targets for nefarious attackers. The use of such devices poses an array of new risks to organizations, including:

- Distributed sensitive data storage and access mechanisms
- Lack of consistent patch management and firmware updates
- The high probability of device loss or theft, and more

Mobile code and apps are also introducing new avenues for malware and data leakage, exposing critical enterprise secrets, intellectual property, and personally identifiable information assets to attackers. To further complicate matters, today there simply are not enough people with the security skills needed to manage mobile phone and tablet deployments.

"Very informative and good information on testing and securing the devices, and will help a lot when we get back to the office."
-Michael LaSalvia, Pfizer

SEC575: Mobile Device Security and Ethical Hacking is designed to help organizations secure their mobile devices by equipping personnel with the knowledge to design, deploy, operate, and assess a well-managed and safe mobile environment. The course will help you build the critical skills to support your organization's secure deployment and use of mobile phones and tablets. You will learn how to capture and evaluate mobile device network activity, disassemble and analyze mobile code, recognize weaknesses in common mobile applications, and conduct full-scale mobile penetration tests.

SANS SEC575

Six-Day Program
36 CPEs
Laptop Required

WHO SHOULD ATTEND:

- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing, deploying or securing mobile phones and tablets
- Network and system administrators supporting mobile phones and tablets

giac.org

sans.edu

sans.org/ondemand

SEC760
Advanced Exploit Development for Penetration Testers

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.

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

You Will Be Able To

- Discover zero-day vulnerabilities in programs running on fully-patched modern operating systems
- Create exploits to take advantage of vulnerabilities through a detailed penetration testing process
- Use the advanced features of IDA Pro and write your own IDC and IDA Python scripts
- Perform remote debugging of Linux and Windows applications
- Understand and exploit Linux heap overflows
- Write return-oriented shellcode
- Perform patch diffing against programs, libraries, and drivers to find patched vulnerabilities
- Perform Windows heap overflows and use-after-free attacks
- Use precision heap sprays to improve exploitability
- Perform Windows Kernel debugging up through Windows 8 64-bit
- Jump into Windows kernel exploitation

Not sure if you are ready for SEC760?

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

TRAINING EVENTS:

San Francisco
Nov 30 - Dec 5
Stephen Sims

SANS
SEC760

Six-Day Program
46 CPEs
Laptop Required

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

TRAINING EVENTS:

Seattle
October 5-10
Jake Williams

SANS
FOR508

Six-Day Program
36 CPEs
Laptop Required

WHO SHOULD ATTEND:

- Information security professionals
- Incident response team leaders and members
- Security Operations Center (SOC) personnel
- System administrators
- Experienced digital forensic analysts
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- SANS FOR408 and SEC504 graduates

FOR508
Advanced Digital Forensics and Incident Response

FOR508: Advanced Digital Forensics and Incident Response will help you determine:

- How the breach occured
- How systems were affected and compromised
- What attackers took or changed
- How to contain and mitigate the incident

DAY 0: A 3-letter government agency contacts you to say critical information was stolen through a targeted attack on your organization. They won't tell how they know, but they identify several breached systems within your enterprise. An Advanced Persistent Threat adversary, aka an APT, is likely involved – the most sophisticated threat you are likely to face in your efforts to defend your systems and data.

Over 80% of all breach victims learn of a compromise from third-party notifications, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years.

"Knowledgeable and excellent examples that are relevant to the material, and provide information I can use in incident response investigating unauthorized activities."
-Rick Kozak, Cubic Transportation Systems

Incident response tactics and procedures have evolved rapidly over the past several years. Data breaches and intrusions are growing more complex. Adversaries are no longer compromising one or two systems in your enterprise; they are compromising hundreds. Your team can no longer afford antiquated incident response techniques that fail to properly identify compromised systems, provide ineffective containment of the breach, and ultimately fail to rapidly remediate the incident.

"FOR508 has been the best DFIR course I've taken so far. All the material is recent and it shows a lot of time went into the material."
-Louise Cheung, Stroz Friedberg

This in-depth incident response course provides responders with advanced skills to hunt down, counter, and recover from a wide range of threats within enterprise networks, including APT adversaries, organized crime syndicates, and hactivism. Constantly updated, FOR508 addresses today's incidents by providing hands-on incident response tactics and techniques that elite responders are successfully using in real-world breach cases.

GATHER YOUR INCIDENT RESPONSE TEAM – IT'S TIME TO GO HUNTING!

DFIR
digital-forensics.sans.org

GCFA
giac.org

SANS Technology Institute
sans.edu

sans.org
/cyber-guardian

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

MEETS DoDD 8570 REQUIREMENTS
sans.org/8570

FOR518
Mac Forensic Analysis

NEW

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.

"This course gives a top-to-bottom approach to forensic thinking that is quite needed in the profession."
-Naveel Koya, AC-DAC – Trivandrum

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.

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 has very comprehensive in-depth coverage of the course topic. Excellent reference materials as a takeaway."
-Jennifer B., Indiana State Police

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.

FORENSICATE DIFFERENTLY!

TRAINING EVENTS:

San Francisco
Nov 30 - Dec 5
Sarah Edwards

SANS
FOR518

Six-Day Program
36 CPEs
Laptop Required

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

digital-forensics.sans.org

TRAINING EVENTS:

Cyber Defense San Diego
October 19-24
Eric Conrad

San Francisco
Nov 30 - Dec 5
David R. Miller

SANS
MGT414

Six-Day Program
46 CPEs
Laptop NOT Needed

WHO SHOULD ATTEND:

- Security professionals who are interested in understanding 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 the 8 domains of knowledge can be applied to the current job

MGT414
SANS Training Program for CISSP® Certification

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.

"I think the course material and the instructor are very relevant for the task of getting a CISSP. The overall academic exercise is solid."
-Aaron Lewter, Availity

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.

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

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

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

You Will Receive With This Course:

- Course books for each of the 8 domains
- 320 questions to test knowledge and preparation for each domain

Note: CISSP® exams are not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam.

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

giac.org

Bundle OnDemand
WITH THIS COURSE
sans.org/ondemand

MEETS DoDD 8570 REQUIREMENTS
sans.org/8570

MGT514
IT Security Strategic Planning, Policy, and Leadership

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 navigate this new world of security by developing strategic plans, creating effective information security policy, and developing management and leadership skills.

This course teaches security professionals three critical skills:

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 strategic planning until we get promoted to a senior position, and then we are not equipped with the skills we need to run with the pack. Learn how to develop strategic plans that resonate with other IT and business leaders

Create Effective Information Security Policy
Policy is a manager's opportunity to express expectations for the workforce, set the boundaries of acceptable behavior, and empower people to do what they ought to be doing. It is easy to get wrong. Have you ever seen a policy and your response was, "No way, I am not going to do that?" Policy must be aligned with an organization's culture. We will break down the steps to policy development so that you have the ability to develop and assess policy to successfully guide your organization.

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

Effective leadership entails persuading team members to accomplish their objectives while removing obstacles and maintaining the well-being of the team in support of the organization's mission. Learn to utilize management tools and frameworks to better lead, inspire, and motivate your teams.

How the Course Works

Using case studies from Harvard Business School, case scenarios, team-based exercises, and discussions that put students in real-world scenarios, you will undertake activities that you will then be able to conduct with your own team members at work.

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

TRAINING EVENTS:

San Francisco
Nov 30 - Dec 5
Frank Kim

SANS
MGT514

Five-Day Program
30 CPEs
Laptop NOT Needed

WHO SHOULD ATTEND:

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

TRAINING EVENTS:

San Francisco
Nov 30 - Dec 5
David Hoelzer

SANS
AUD507

Six-Day Program
36 CPEs
Laptop Required

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

AUD507
Auditing & Monitoring Networks, Perimeters, and Systems

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 provided through 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 information 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 ongoing compliance monitoring systems and automatically validate defenses through instrumentation and automation of audit checklists.

"AUD507 provided me additional insight to the technical side of security auditing. Great course and a super instructor!" -Carlos E., U.S. Army

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.

A great audit is more than marks on a checklist; it is the understanding of what the underlying controls are, what the best practices are, and why they are optimal. Sign up for this course and experience the mix of theoretical, hands-on, and practical knowledge.

giac.org

sans.edu

sans.org/ondemand

sans.org/8570

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

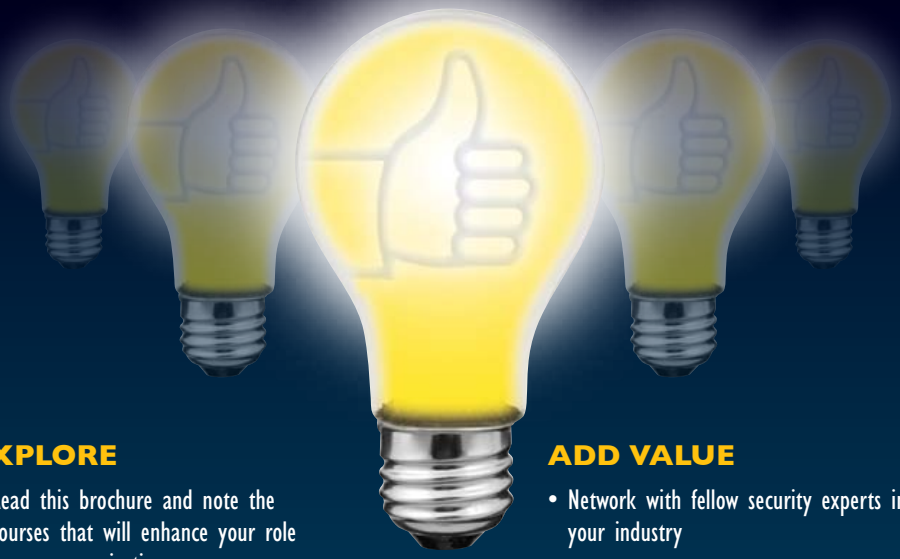
"GIAC is the only certification that proves you have hands-on technical skills."

-Christina Ford, Department of Commerce

MORE INFORMATION

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

The Value of SANS Training and *YOU*



EXPLORE

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

RELATE

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

VALIDATE

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

SAVE

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

ADD VALUE

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

ALTERNATIVES

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

ACT

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

Return on Investment

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

REMEMBER

the SANS promise:

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

FUTURE SANS TRAINING EVENTS

SANS Crystal City 2015
Crystal City, VA | September 8-13 | #SANSCrystalCity

SANS Network Security 2015
Las Vegas, NV | September 12-21 | #SANSNetworkSecurity

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

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

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

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 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

HOTEL INFORMATION

SEATTLE 2015

Training Campus
Renaissance Seattle Hotel

515 Madison Street
Seattle, WA 98104
206-583-0300

sans.org/event/seattle-2015/location

Special Hotel Rates Available

A special discounted rate of $179.00 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 September 4, 2015.

CYBER DEFENSE SAN DIEGO 2015

Training Campus
Hard Rock Hotel

207 Fifth Avenue
San Diego, CA 92101
619-702-3000

sans.org/event/cyber-defense-san-diego-2015/location

Special Hotel Rates Available

A special discounted rate of $210.00 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 September 25, 2015.

SAN FRANCISCO 2015

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

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 November 9, 2015.

REGISTRATION INFORMATION

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

Register online at:

SEATTLE: sans.org/event/seattle-2015/courses
CD SAN DIEGO: sans.org/event/cyber-defense-san-diego-2015/courses
SAN FRANCISCO: 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

	EVENT	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	Seattle	8/12/15	$400.00	9/2/15	$200.00
	CD San Diego	8/26/15	$400.00	9/23/15	$200.00
	San Francisco	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 respective dates (see website for dates) – processing fees may apply.


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