SANS Winter Training 2016

LAS VEGAS NEW ORLEANS SCOTTSDALE ANAHEIM

Las Vegas

Las Vegas, NV Jan 9-14

Security East

New Orleans, LA Jan 25-30

THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

Scottsdale

Scottsdale, AZ Feb 8-13

Anaheim

Anaheim, CA Feb 22-27

Choose from over 20 courses on cyber defense, pen testing, incident response, digital forensics, security management, and more!

sans.org/warmdestinations

SANS Las Vegas 2016

Jan 9-14

COURSES:	INSTRUCTORS:
SEC401	*Bryce Galbraith*
SEC504	*John Strand*
FOR578	*Mike Cloppert*
MGT414	*Eric Conrad*
MGT512	*David Hoelzer*
ICS410	*Paul A. Henry*

sans.org/las-vegas-2016

SANS Security East 2016

New Orleans, LA | Jan 25-30

COURSES:	INSTRUCTORS:
SEC401	*Bryan Simon*
SEC503	*Mike Poor*
SEC504	*Michael Murr*
SEC511	*Eric Conrad*
SEC542	*Seth Misenar*
SEC560	*Kevin Fiscus*
SEC566	*James Tarala*
SEC575	*Christopher Crowley*
FOR408	*David Cowen*
FOR526	*Alissa Torres*
MGT512	*G. Mark Hardy*
ICS515	*Robert M. Lee*

sans.org/security-east-2016

SANS Scottsdale 2016

Feb 8-13

COURSES:	INSTRUCTORS:
SEC401	*Bryan Simon*
SEC501	*Paul A. Henry*
SEC504	*John Strand*
SEC511	*Seth Misenar*
SEC560	*Ed Skoudis*
MGT414	*David R. Miller*
MGT514	*G. Mark Hardy*

sans.org/scottsdale-2016

SANS Anaheim 2016

Feb 22-27

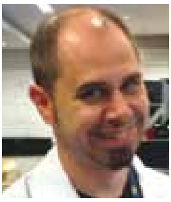
COURSES:	INSTRUCTORS:
SEC301	*David R. Miller*
SEC401	*Paul A. Henry*
SEC503	*Adrien de Beaupre*
SEC504	*Christopher Crowley*
SEC550	*Mick Douglas*
FOR508	*Chad Tilbury*
FOR518	*Sarah Edwards*
MGT512	*G. Mark Hardy*

sans.org/anaheim-2016

COURSES and TRAINING EVENTS	Las Vegas Jan 9-14	Sec East Jan 25-30	Scottsdale Feb 8-13	Anaheim Feb 22-27
SEC301 Intro to Information Security				SEC301 SIMULCAST AVAILABLE
SEC401 Security Essentials Bootcamp Style	SEC401	SEC401	SEC401	SEC401 SIMULCAST AVAILABLE
SEC501 Advanced Security Essentials — Enterprise Defender			SEC501	
SEC503 Intrusion Detection In-Depth		SEC503		SEC503 SIMULCAST AVAILABLE
SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	SEC504	SEC504	SEC504	SEC504 SIMULCAST AVAILABLE
SEC511 Continuous Monitoring and Security Operations		SEC511	SEC511	
SEC542 Web App Penetration Testing and Ethical Hacking NEW		SEC542		
SEC550 Active Defense, Offensive Countermeasures and Cyber Deception NEW				SEC550
SEC560 Network Penetration Testing and Ethical Hacking NEW		SEC560	SEC560	
SEC566 Implementing and Auditing the Critical Security Controls — In-Depth		SEC566		
SEC575 Mobile Device Security and Ethical Hacking		SEC575		
FOR408 Windows Forensic Analysis		FOR408		
FOR508 Advanced Digital Forensics and Incident Response				FOR508 SIMULCAST AVAILABLE
FOR518 Mac Forensic Analysis				FOR518
FOR526 Memory Forensics In-Depth		FOR526		
FOR578 Cyber Threat Intelligence NEW	FOR578			
MGT414 SANS Training Program for CISSP® Certification	MGT414		MGT414	
MGT512 SANS Security Leadership Essentials For Managers with Knowledge Compression™	MGT512	MGT512		MGT512
MGT514 IT Security Strategic Planning, Policy and Leadership NEW			MGT514	
ICS410 ICS/SCADA Security Essentials	ICS410			
ICS515 ICS Active Defense and Incident Response NEW		ICS515		

SANS WORLD-CLASS 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 line-up of instructors for these warm-destination events includes:



Mike Cloppert
SANS Instructor
@mikecloppert
FOR578 – Las Vegas

Eric Conrad
Senior Instructor
@eric_conrad
MGT414 – Las Vegas
SEC511 – Security East

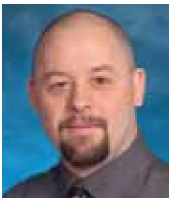
David Cowen
SANS Instructor
@hecfblog
FOR408 – Security East

Christopher Crowley
Certified Instructor
@CCrowMontance
SEC575 – Security East
SEC504 – Anaheim

Adrien de Beaupre
Certified Instructor
@adriendb
SEC503 – Anaheim

Mick Douglas
SANS Instructor
SEC550 – Anaheim

Sarah Edwards
Certified Instructor
@iamevltwin
FOR518 – Anaheim



Kevin Fiscus
Certified Instructor
@kevinbfiscus
SEC560 – Security East

Bryce Galbraith
Principal Instructor
@brycegalbraith
SEC401 – Las Vegas

G. Mark Hardy
Certified Instructor
@g_mark
MGT512 – Security East
MGT514 – Scottsdale
MGT512 – Anaheim

Paul A. Henry

Senior Instructor
@phenrycissp

ICS410 – Las Vegas
SEC501 – Scottsdale
SEC401 – Anaheim

David Hoelzer

Faculty Fellow
@it_audit

MGT512 – Las Vegas

Robert M. Lee

Certified Instructor
@RobertMLee

ICS515 – Security East

David R. Miller

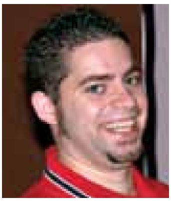
SANS Instructor

MGT414 – Scottsdale
SEC301 – Anaheim

Seth Misenar

Senior Instructor
@sethmisenar

SEC542 – Security East
SEC511 – Scottsdale



Michael Murr

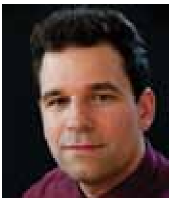
Principal Instructor
@mikemurr

SEC504 – Security East

Mike Poor

Senior Instructor
@Mike_Poor

SEC503 – Security East



Bryan Simon

Certified Instructor
@BryanOnSecurity

SEC401 – Security East
SEC401 – Scottsdale

Ed Skoudis

Faculty Fellow
@edskoudis

SEC560 –Scottsdale

John Strand

Senior Instructor
@strandjs

SEC504 – Las Vegas
SEC504 – Scottsdale

Bios on all instructors can be found at:
sans.org/event/**las-vegas-2016**/instructors
sans.org/event/**security-east-2016**/instructors
sans.org/event/**scottsdale-2016**/instructors
sans.org/event/**anaheim-2016**/instructors

James Tarala

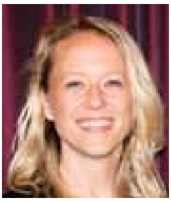
Senior Instructor
@isaudit

SEC566 – Security East

Chad Tilbury

Senior Instructor
@chadtilbury

FOR508 – Anaheim



Alissa Torres

Certified Instructor
@sibertor

FOR526 – Security East

"I am very convinced that all of SANS instructors are qualified and do an excellent job teaching very difficult subjects."
-Chris Tran, Applied Signal Technology, Inc.

TRAINING EVENTS:

Anaheim
February 22-26
David R. Miller

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

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 with 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.

"The training was very engaging. I have a security background and found the information presented informative, and 100% correct on SCADA risks and vulnerabilities."
-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 Corporation

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

GIAC INFORMATION SECURITY FUNDAMENTALS GISF
giac.org

▶II **Bundle OnDemand** with this course
sans.org/ondemand

SEC401
Security Essentials Bootcamp Style

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.

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 course 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. Our course will show you how to prevent your organization's security problems from being headline news in the Wall Street Journal!

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

With the 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 SECURITY ESSENTIALS GSEC
giac.org

SANS Technology Institute
sans.edu

supere aude
sans.org/cyber-guardian

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

MEETS DoDD 8570 REQUIREMENTS
sans.org/8570

Course updates, prerequisites, special notes, or laptop requirements: **sans.org/courses**

TRAINING EVENTS:

Las Vegas
January 9-14
Bryce Galbraith

Security East
January 25-30
Bryan Simon

Scottsdale
February 8-13
Bryan Simon

Anaheim
February 22-27
Paul A. Henry

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:

Scottsdale
February 8-13
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.

> *"SEC501 is the perfect course to immerse enterprise security staff into essential skills they need to do their jobs. Failing to attend this course is done at the peril of your organization."*
> -John N. Johnson, Houston PD

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.

> *"Instructor has real-world experience with the ability to tie real-world threats to theory and practice."*
> -Bruce Henkel, Harris Corporation

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.

> *"I was worried this course would overlap SEC401, but SEC501 takes everything I learned in SEC401 to the next level."*
> -Bryan Chou, Murphy USA

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 CERTIFIED ENTERPRISE DEFENDER
GCED
giac.org

SANS Technology Institute
sans.edu

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

MEETS DoDD 8570 REQUIREMENTS
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.

GIAC CERTIFIED INTRUSION ANALYST GCIA
giac.org

SANS Technology Institute
sans.edu

sapere aude
sans.org /cyber-guardian

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

MEETS DoDD 8570 REQUIREMENTS
sans.org/8570

TRAINING EVENTS:

Security East
January 25-30
Mike Poor

Anaheim
February 22-27
Adrien de Beaupre

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

TRAINING EVENTS:

Las Vegas
January 9-14
John Strand

Security East
January 25-30
Michael Murr

Scottsdale
February 8-13
John Strand

Anaheim
February 22-27
Christopher Crowley

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 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!

> *"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.

GIAC CERTIFIED INCIDENT HANDLER GCIH
giac.org

SANS Technology Institute
sans.edu

sapere aude
sans.org
/cyber-guardian

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

MEETS DoDD 8570 REQUIREMENTS
sans.org/8570

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.

"I work in net security with a lot of tools. The instructor provided a great perspective on the state of cyber defense and how we should be approaching it."

-Kevin South, Navient

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.

"The SEC511 material is excellent. I appreciated the background and pen test material to build up defense. Good defense understands offense."

-Kenneth Hall, BCBSMS

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 day five of this course will greatly increase your understanding and enhance your skills in implementing CM utilizing NIST framework.

GIAC CONTINUOUS MONITORING CERTIFICATION GMON
giac.org

SANS Technology Institute
sans.edu

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

TRAINING EVENTS:

Security East
January 25-30
Eric Conrad

Scottsdale
February 8-13
Seth Misenar

SANS
SEC511

Six-Day Program
36 CPEs
Laptop Required

WHO SHOULD ATTEND:

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

TRAINING EVENTS:

Security East
January 25-30
Seth Misenar

SANS
SEC542

Six-Day Program
36 CPEs
Laptop Required

WHO SHOULD ATTEND:

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

NEW

SEC542
Web App Penetration Testing and Ethical Hacking

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

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

> *"The content in SEC542 is very relevant as it features recently discovered vulnerabilities. It also effectively, from my view, caters to various experience levels."*
> -Malcolm King, Morgan Stanley

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

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

> *"This training was hands-on, not just focused on slides, and very helpful for the real world."* -Zach Moreno, Chico Security

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

GIAC WEB APPLICATION PENETRATION TESTER GWAPT
giac.org

SANS Technology Institute
sans.edu

sapere aude
sans.org/cyber-guardian

▶❚❚ **Bundle OnDemand** WITH THIS COURSE
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 may be able to immediately implement some of the measures we discuss in this course, while others may take a while. Either way, consider what we discuss as a collection of tools at your disposal when you need them to annoy attackers, determine who is attacking you, and, finally, attack the attackers.

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:

Anaheim
February 22-26
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:

Security East
January 25-30
Kevin Fiscus

Scottsdale
February 8-13
Ed Skoudis

SANS

SEC560

Six-Day Program
37 CPEs
Laptop Required

WHO SHOULD ATTEND:

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

NEW

SEC560
Network Penetration Testing and Ethical Hacking

As a cybersecurity professional, you have a unique responsibility to find and understand your organization's vulnerabilities, and to work diligently to mitigate them before the bad guys pounce. Are you ready? SANS SEC560, our flagship course for penetration testing, fully arms you to take on this task head-on.

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

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

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

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

> *"This course contained real-world material and scenarios applicable to security professionals."* -Wes Wright, Harland Clarke

You will learn how to perform detailed reconnaissance, learning about a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. You'll be equipped to scan target networks using best-of-breed tools from experience in our hands-on labs. We won't just cover run-of-the-mill options and configurations, but instead, we'll also go over less-well-known-but-super-useful capabilities of the best pen test toolsets available today. After scanning, you'll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You'll dive deep into post exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth. The final portion of the class includes a comprehensive hands-on lab, conducting a full-day penetration test against a target organization.

GIAC PENETRATION TESTER GPEN
giac.org

SANS Technology Institute
sans.edu

sapere aude
sans.org/cyber-guardian

Bundle OnDemand
WITH THIS COURSE
sans.org/ondemand

SEC566
Implementing and Auditing the Critical Security Controls – In-Depth

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches?

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

> *"The 20 controls presented in the course are requirements found in most regulated industries. I found the format and layout of each control well explained and easy to follow."* -Josh Ellis, Iberdrola USA

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

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle.

The British government's Center for the Protection of National Infrastructure describes the Controls as the "baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence."

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

- Create a strategy to successfully defend their data
- Implement controls to prevent data from being compromised
- Audit systems to ensure compliance with Critical Control standards.

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

GIAC Critical Controls Certification GCCC
giac.org

SANS Technology Institute
sans.edu

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

Training Events:

Security East
January 25-29
James Tarala

SANS
SEC566

Five-Day Program
30 CPEs
Laptop Required

Who Should Attend:

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

TRAINING EVENTS:

Security East
January 25-30
Christopher Crowley

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

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 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 (ERP) to project management.

For all of its convenience, however, the ubiquitous use of mobile devices in the work place 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.

"Once again, SANS has exceeded my expectations and successfully re-focused my view of threats and risks. I recommend this course because it is very enlightening." -Charles Allen, EM Solutions, Inc.

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.

You will gain hands-on experience in designing a secure mobile phone network for local and remote users and learn how to make critical decisions to support devices effectively and securely. You will also be able to analyze and evaluate mobile software threats, and learn how attackers exploit mobile phone weaknesses so you can test the security of your own deployment. With these skills, you will be a valued mobile device security analyst, fully able to guide your organization through the challenges of securely deploying mobile devices.

GIAC MOBILE DEVICE SECURITY ANALYST
GMOB
giac.org

SANS Technology Institute
sans.edu

Bundle OnDemand
WITH THIS COURSE
sans.org/ondemand

FOR408
Windows Forensic Analysis

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

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

> *"I have been doing forensic investigations for several years, but would highly recommend this course (FOR408) for both new and old forensic investigations."* -Robert Galarza, JP Morgan Chase

Proper analysis requires real data for students to examine. The completely updated FOR408 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7, Windows 8/8.1, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows XP systems to just-discovered Windows 8.1 artifacts.

FOR408 is continually updated: This course utilizes a brand-new intellectual property theft and corporate espionage case that took over six months to create. You work in the real world and your training should include real practice data. Our development team used incidents from their own experiences and investigations and created an incredibly rich and detailed scenario designed to immerse students in a true investigation. The case demonstrates the latest artifacts and technologies an investigator might encounter while analyzing Windows systems. The incredibly detailed workbook details the tools and techniques step-by-step that each investigator should follow to solve a forensic case.

MASTER WINDOWS FORENSICS – YOU CAN'T PROTECT WHAT YOU DON'T KNOW ABOUT

GIAC CERTIFIED FORENSIC EXAMINER GCFE
giac.org

SANS Technology Institute
sans.edu

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

TRAINING EVENTS:

Security East
January 25-30
David Cowen

SANS
FOR408

Six-Day Program
36 CPEs
Laptop Required

WHO SHOULD ATTEND:

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

DFIR
digital-forensics.sans.org

TRAINING EVENTS:

Anaheim
February 22-27
Chad Tilbury

SANS
FOR508

Six-Day Program
36 CPEs
Laptop Required

WHO SHOULD ATTEND:

- Information security professionals
- Incident response team leaders and members
- Security Operations Center 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 or compromised
- What attackers took or changed
- How to handle incident containment and remediation

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.

"FOR508 is an extremely valuable course overall. It brings essential topics into one class and covers an extensive amount of topics along with excellent reference material."
-Edgar Zayas, U.S. Securities and Exchange Commission

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.

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 –
TIME TO GO HUNTING!

DFIR
digital-forensics.sans.org

GIAC CERTIFIED FORENSIC ANALYST GCFA
giac.org

SANS Technology Institute
sans.edu

sapere aude
sans.org/cyber-guardian

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

MEETS DoDD 8570 REQUIREMENTS
sans.org/8570

FOR518
Mac Forensic Analysis

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 was very comprehensive with in-depth coverage of the topic, plus excellent reference materials as a take away."*
> -Jennifer B., Indiana State Police

Times and trends change and forensic investigators and analysts need to change with them. **FOR518: Mac Forensic Analysis** 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.

> *"Sarah gave another great day of presentations and her knowledge is impressive. All of the material this week has been great and will come in handy for reference in the future!"*
> -Ben Keck, Ciena

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.

> *"Pound for pound, dollar for dollar, there is no other forensic training I have seen, from FTK to EnCase to anything private, that holds a candle to what was presented in this course."*
> -Kevin J. Ripa, Computer Evidence Recovery, Inc.

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:

Anaheim
February 22-27
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

TRAINING EVENTS:

Security East
January 25-30
Alissa Torres

SANS
FOR526

Six-Day Program
36 CPEs
Laptop Required

WHO SHOULD ATTEND:

- Incident response team members
- Experienced digital forensic analysts
- Red team members
- Penetration testers
- Exploit developers
- Law enforcement officers
- Federal agents or detectives
- SANS FOR508 and SEC504 graduates
- Forensics investigators

DFIR
digital-forensics.sans.org

FOR526
Memory Forensics In-Depth

Digital Forensics and Incident Response (DFIR) professionals need Windows memory forensics training to be at the top of their game. Investigators who do not look at volatile memory are leaving evidence at the crime scene. RAM content holds evidence of user actions, as well as evil processes and furtive behaviors implemented by malicious code. It is this evidence that often proves to be the smoking gun that unravels the story of what happened on a system.

> *"The training opened my eyes for the need to collect memory images as well as physical images for single computer analysis such as theft of IP or other employee investigations."*
> -Greg Caouette, Kroll Inc.

FOR526: Memory Forensics In-Depth provides the critical skills necessary for digital forensics examiners and incident responders to successfully perform live system memory triage and analyze captured memory images. The course uses the most effective freeware and open-source tools in the industry today and provides an in-depth understanding of how these tools work. FOR526 is a critical course for any serious DFIR investigator who wants to tackle advanced forensics, trusted insider, and incident response cases.

In today's forensics cases, it is just as critical to understand memory structures as it is to understand disk and registry structures. Having in-depth knowledge of Windows memory internals allows the examiner to access target data specific to the needs of the case at hand. For those investigating platforms other than Windows, this course also introduces OSX and Linux memory forensics acquisition and analysis using hands-on lab exercises.

There is an arms race between analysts and attackers. Modern malware and post-exploitation modules increasingly employ self-defense techniques that include more sophisticated rootkit and anti-memory analysis mechanisms that destroy or subvert volatile data. Examiners must have a deeper understanding of memory internals in order to discern the intentions of attackers or rogue trusted insiders. FOR526 draws on best practices and recommendations from experts in the field to guide DFIR professionals through acquisition, validation, and memory analysis with real-world and malware-laden memory images.

FOR526: Memory Forensics in-Depth will teach you:

- Proper Memory Acquisition: Demonstrate targeted memory capture to ensure data integrity and combat anti-acquisition techniques.
- How to Find Evil in Memory: Detect rogue, hidden, and injected processes, kernel-level rootkits, Dynamic Link Libraries (DLL) hijacking, process hollowing, and sophisticated persistence mechanisms.
- Effective Step-by-Step Memory Analysis Techniques: Use process timelining, high-low-level analysis, and walking the Virtual Address Descriptors (VAD) tree to spot anomalous behavior.
- Best Practice Techniques: Learn when to implement triage, live system analysis, and alternative acquisition techniques, as well as how to devise custom parsing scripts for targeted memory analysis.

MALWARE CAN HIDE, BUT IT MUST RUN.

FOR578
Cyber Threat Intelligence

NEW

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

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

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

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

"I absolutely loved this class! Mike provided a great framework for CTI that I will use to be more effective."

-Nate DeWitt, eBay, Inc.

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

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

THERE IS NO TEACHER BUT THE ENEMY!

TRAINING EVENTS:

Las Vegas
January 9-13
Mike Cloppert

SANS
FOR578

Five-Day Program
30 CPEs
Laptop Required

WHO SHOULD ATTEND:

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

DFIR
digital-forensics.sans.org

MGT414

SANS Training Program for CISSP® Certification

TRAINING EVENTS:

Las Vegas
January 9-14
Eric Conrad

Scottsdale
February 8-13
David R. Miller

Course Updated
for New CISSP® Exam

SANS
MGT414

Six-Day Program
46 CPEs
Laptop NOT Needed

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.

> *"SANS course materials are excellent and this course really hits the nail on the head. I have so much to take back to the office and share with my team and manager."*
> -Stacey Boivin, Alberta Electric System Operator

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

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® eight domains
- Security professionals and managers looking for practical ways to apply the eight domains of knowledge to their current job

You Will Be Able To

- Understand the eight 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 eight domains of knowledge
- Apply the skills learned across the eight domains to solve security problems when you return to work

You Will Receive With This Course:

- Course books for each of the eight domains
- 320 questions to test knowledge and preparation for each domain
- MP3 audio files of the complete course lecture

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

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

GIAC INFORMATION SECURITY PROFESSIONAL
GISP
giac.org

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

MEETS DoDD 8570 REQUIREMENTS
sans.org/8570

MGT512
SANS Security Leadership Essentials For Managers with Knowledge Compression™

This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to *manage* security. Lecture sections are intense; the most common student comment is that it's like drinking from a fire hose. The diligent manager will learn vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to U.S. government managers and supporting contractors.

> *"MGT512 is awesome! Lots of material covered, so I will need to go back and read the notes and study more. The course was very structured, relevant, and concise."* -Juan Canino, SWIFT

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

Knowledge Compression™

Maximize your learning potential!

Knowledge Compression™ is an optional add-on feature to a SANS class that aims to maximize the absorption and long-term retention of large amounts of data over a relatively short period of time. Through the use of specialized training materials, in-class reviews, examinations and test-taking instruction, Knowledge Compression™ ensures students have a solid understanding of the information presented to them. By attending classes that feature this advanced training product, you will experience some of the most intense and rewarding training programs SANS has to offer, in ways that you never thought possible!

GIAC SECURITY LEADERSHIP CERTIFICATION
GSLC
giac.org

SANS Technology Institute
sans.edu

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

MEETS DoDD 8570 REQUIREMENTS
sans.org/8570

TRAINING EVENTS:

Las Vegas
January 9-13
David Hoelzer

Security East
January 25-29
G. Mark Hardy

Anaheim
February 22-26
G. Mark Hardy

SANS
MGT512

Five-Day Program
33 CPEs
Laptop NOT Needed

WHO SHOULD ATTEND:

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

TRAINING EVENTS:

Scottsdale
February 8-13
G. Mark Hardy

SANS
MGT514

Five-Day Program
30 CPEs
Laptop NOT Needed

WHO SHOULD ATTEND:

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

NEW

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 budget and more opportunity. With this increased responsibility comes more scrutiny. Security business leaders must learn how to navigate in this new world of security.

This course teaches security professionals how to do three things:

- **Develop Strategic Plans**
  Strategic planning is hard for people in IT and IT Security because we spend so much time responding and reacting. We almost never get to practice until we get promoted to a senior position and then we are not equipped with the skills we need to run with the pack. Learn how to develop strategic plans that resonate with other IT and business leaders

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

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

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

How the Course Works

Using case studies from Harvard Business School, case scenarios, team-based exercises, and discussions that put students in real-world scenarios, you will undertake activities that you can 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, enable key innovations, and work effectively with your business partners.

"MGT514 is excellent training with encyclopedia coverage of the topic!"
-Alexander Kotkov, Ernst and Young

ICS410

ICS/SCADA Security Essentials

SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. **ICS410: ICS/SCADA Security Essentials** provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

The course will provide you with:

- An understanding of industrial control system components, purposes, deployments, significant drivers, and constraints
- Hands-on lab learning experiences to control system attack surfaces, methods, and tools
- Control system approaches to system and network defense architectures and techniques
- Incident-response skills in a control system environment
- Governance models and resources for industrial cybersecurity professionals

When examining the greatest risks and needs in critical infrastructure sectors, the course authors looked carefully at the core security principles necessary for the range of tasks involved in supporting control systems on a daily basis. While other courses are available for higher-level security practitioners who need to develop specific skills such as industrial control system penetration testing, vulnerability analysis, malware analysis, forensics, secure coding, and red team training, most of these courses do not focus on the people who operate, manage, design, implement, monitor, and integrate critical infrastructure production control systems.

"ICS410 really opens you up to possibilities and issues that otherwise you wouldn't really think about." -Alfonso Barreiro, Panama Canal Authority

With the dynamic nature of industrial control systems, many engineers do not fully understand the features and risks of many devices. In addition, IT support personnel who provide the communications paths and network defenses do not always grasp the systems' operational drivers and constraints. This course is designed to help traditional IT personnel fully understand the design principles underlying control systems and how to support those systems in a manner that ensures availability and integrity. In parallel, the course addresses the need for control system engineers and operators to better understand the important role they play in cybersecurity. This starts by ensuring that a control system is designed and engineered with cybersecurity built into it, and that cybersecurity has the same level of focus as system reliability throughout the system lifecycle.

When these different groups of professionals complete this course, they will have developed an appreciation, understanding, and common language that will enable them to work together to secure their industrial control system environments. The course will help develop cyber-secure-aware engineering practices and real-time control system IT/OT support carried out by professionals who understand the physical effects of actions in the cyber world.

GLOBAL INDUSTRIAL CYBER SECURITY PROFESSIONAL
GICSP
giac.org

TRAINING EVENTS:

Las Vegas
January 9-13
Paul A. Henry

SANS
ICS410

Five-Day Program
30 CPEs
Laptop Required

WHO SHOULD ATTEND:

The course is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:

- IT (includes operational technology support)
- IT security (includes operational technology security)
- Engineering
- Corporate, industry, and professional standards

TRAINING EVENTS:

Security East
January 25-29
Robert M. Lee

SANS

ICS515

Five-Day Program
30 CPEs
Laptop Required

WHO SHOULD ATTEND:

- Information technology and operational technology (IT and OT) cybersecurity personnel
- IT and OT support personnel
- ICS incident responders
- ICS engineers
- Security Operations Center personnel

NEW

ICS515
ICS Active Defense and Incident Response

ICS515: ICS Active Defense and Incident Response will empower students to understand their networked industrial control system (ICS) environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security. This process of monitoring, responding to, and learning from threats is known as "active defense." It is the approach needed to appropriately counter advanced adversaries targeting ICS, as has been seen with malware such as Stuxnet, HAVEX, and BlackEnergy2. Students can expect to come out of this course fully understanding how to to deconstruct targeted ICS attacks, with a focus on delivery methods and observable attributes. This knowledge demystifies adversary capabilities and gives actionable recommendations to defenders. The course uses a hands-on approach that shows real-world malware and breaks down cyber attacks on ICS from start to finish. Students will gain a practical and technical understanding of concepts such as generating and using threat intelligence, performing network security monitoring, and executing threat triage and incident response to ensure the safety and reliability of operations. The strategy presented in the course serves as a basis for ICS organizations looking to show that defense is doable.

"ICS environments are unique and require specialized skills and processes to effectively manage the threats and vulnerabilities."

-John Ballentine, EthosEnergy

ICS515 will teach you:

- How threat intelligence is generated and how to use what is available in the community to support ICS environments. The analysis skills you learn will enable you to critically analyze and apply information from threat intelligence reports on a daily basis.
- How to identify ICS assets and their network topologies and how to monitor ICS hotspots for abnormalities and threats. Methodologies such as network security monitoring and approaches to reducing the control system threat landscape will be introduced and reinforced through hands-on labs.
- How to safely and properly respond to an incident internally. You will learn how to identify device malfunctions from cyber threats and prepare and use sources of forensic data that can benefit incident response. You will also break down ICS malware to understand various delivery techniques and observable behaviors.
- How to operate through an attack and gain the information necessary to instruct teams and decision-makers on when operations must shut down, or if it is safe to respond to the threat and continue operations. We will use threat and malware analysis techniques that are effective even for undermanned operational technology (OT) security teams.
- Through a full-day of hands-on labs, you will reinforce the concepts and skills of active defense: threat intelligence, asset identification and network security monitoring, incident response, and threat and environment manipulation. We will stress the ongoing and dynamic nature of the process and how teams can work together to ensure the safety and reliability of control system networks.

"Awesome!! In this course, being my 6th SANS course, Robert M. Lee demonstrated and reiterated the fact that SANS has the world's best instructors!! The course was like a catalyst. It boosted my knowledge about the threats facing ICS environments, and provided me with a framework to actively defend these threats."

-Srinath Kannan, Accenture

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.

Las Vegas

KEYNOTE: ***Evolving Threats and Defenses*** – Paul A. Henry

Assessing, Testing, and Breaking Security Products – John Strand

Continuous Ownage: Why you Need Continuous Monitoring – Eric Conrad

How to Bring Some Advanced Persistent Trickery to Your Fight Against Advanced Persistent Threats – Bryce Galbraith

Descriptions of Las Vegas Bonus Sessions can be found at **sans.org/event/las-vegas-2016/bonus-sessions**

Security East

KEYNOTE: ***Data Theft in the 21st Century*** – Mike Poor

Continuous Ownage: Why you Need Continuous Monitoring – Eric Conrad, Seth Misenar

Card Fraud 101 – G. Mark Hardy

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

Using an Open Source Threat Model for Prioritized Defense – James Tarala

Understanding Your ICS Topologies – Robert M. Lee

Descriptions of Security East Bonus Sessions can be found at **sans.org/event/security-east-2016/bonus-sessions**

Scottsdale

KEYNOTE: ***Evolving Threats and Defenses*** – Paul A. Henry

Card Fraud 101 – G. Mark Hardy

Offensive Countermeasures, Active Defenses, and Internet Tough Guys – John Strand

Overview of the New 2015 CISSP® Exam – David R. Miller

Descriptions of Scottsdale Bonus Sessions can be found at **sans.org/event/scottsdale-2016/bonus-sessions**

Anaheim

KEYNOTE: ***Tales from the Battlefield: Lessons in Incident Response*** – Chad Tilbury

Complete App Pwnage with multi-POST XSRF – Adrien de Beaupre

SANS 8 Mobile Device Security Steps – Christopher Crowley

Evolving Threats – Paul A. Henry

Overview of the New 2015 CISSP® Exam – David R. Miller

Card Fraud 101 – G. Mark Hardy

Powercat Has Power! – Mick Douglas

Descriptions of Anaheim Bonus Sessions can be found at **sans.org/event/anaheim-2016/bonus-sessions**

Build Your Best Career

WITH

SANS

Add an

OnDemand Bundle & GIAC Certification Attempt*

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

SPECIAL PRICING

OnDemand Bundle

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

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

-Robert Jones, Team Jones, Inc.

GIAC Certification

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

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

-Christina Ford, Department of Commerce

MORE INFORMATION

sans.org/ondemand/bundles giac.org

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

SANS
Technology
Institute

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

> “I was challenged by both the coursework and faculty. Earning a graduate degree from SANS had a direct and positive influence on my career.”
>
> -Russ McRee, MSISE Director, Security Response & Investigations, Microsoft

POST-9/11 GI BILL

The SANS Technology Institute is approved to accept and/or certify veterans for education benefits. Programs also typically qualify for corporate tuition reimbursement plans.

GIAC
GLOBAL INFORMATION ASSURANCE CERTIFICATION
www.giac.org

Students earn industry-recognized GIAC certifications during their course of studies.

Master of Science Degrees

- Master of Science in Information Security Engineering (MSISE)
- Master of Science in Information Security Management (MSISM)

Graduate Certificates

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

To learn more,
visit **www.sans.edu**
or email **info@sans.edu**

The SANS Technology Institute,
an independent subsidiary of SANS, is accredited by
The Middle States Commission on Higher Education
(3624 Market Street, Philadelphia, PA 19104 – 267.284.5000),
an institutional accrediting agency recognized by the
U.S. Secretary of Education and the Council
for Higher Education Accreditation.

Group Discounts for SANS Security Training

sans.org/vouchers

SANS Universal Voucher Credit Program

The ***SANS Universal Voucher Credit Program*** provides organizations of all sizes with a 12-month online account that is convenient and easy to manage. SANS will maximize your training investment by providing you with bonus credits. SANS Universal Voucher Credits can be used for any SANS live or online training format as well as GIAC certification exams. This will give you maximum flexibility and an easy one-time procurement process.

SANS Universal Voucher Credit Benefits

- **Valid for classroom, online learning, and GIAC certification**
- **Cost savings help you expand your training budget**
- **Extends your fiscal year**
- **Free Learning Management Tool featuring online enrollment and usage reports**
- **Online access to credits, orders, and GIAC certification results**
- **Fully transferable**
- **Only one procurement is needed for 12 months, but you can add funds to renew the account at any time**
- **Great way to motivate and retain your valued employees**

If your organization prefers online training, find out how you can earn an additional 5% bonus with a ***SANS Online Voucher Credit Program*** for OnDemand and vLive courses. To learn more, please contact onlinevoucher@sans.org or visit the SANS Voucher Credit Program. SANS Universal Credit allows you to invest today, earn instant credits, and decide later how to spend your training credits over the next 12 months to maximize your investment and extend your fiscal year.

Create an Account

Creating your SANS Universal or Online Voucher Credit Account is easy.

- Visit sans.org/vouchers for details
- Email Vouchers@sans.org for a proposal or questions
- Designate a "Voucher Administrator" responsible for allocating credits.

Questions?

E-mail
vouchers@sans.org

or call
301-654-SANS (7267)
Mon-Fri, 9am-8pm EST

HOTEL INFORMATION

LAS VEGAS 2016

Tuscany Suites and Casino

255 E. Flamingo Road
Las Vegas, NV 89169
702-732-2564
sans.org/event/las-vegas-2016/location

Special Hotel Rates Available*

A special discounted rate of $96.00 S/D.

Government per diem rooms may be 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 Dec 8, 2015.

SECURITY EAST 2016

Hilton New Orleans Riverside

Two Poydras Street
New Orleans, LA 70130
504-561-0500
sans.org/event/security-east-2016/location

Special Hotel Rates Available*

A special discounted rate of $199.00 S/D.

Government per diem rooms may be 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 Jan 1, 2016.

SCOTTSDALE 2016

Hilton Scottsdale Resort & Villas

6333 North Scottsdale Road
Scottsdale, AZ 85250
480-948-7750
sans.org/event/scottsdale-2016/location

Special Hotel Rates Available*

A special discounted rate of $219.00 S/D.

Government per diem rooms may be 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 Feb 3, 2016.

ANAHEIM 2016

Anaheim Majestic Garden Hotel

900 South Disneyland Drive
Anaheim, CA 92870
714-234-2413
sans.org/event/anaheim-2016/location

Special Hotel Rates Available*

A special discounted rate of $148.00 S/D.

Government per diem rooms may be 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 Feb 4, 2016.

**Price will be honored based on space availability*

REGISTRATION INFORMATION

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

Register online at:

LAS VEGAS:	sans.org/event/las-vegas-2016/courses
SECURITY EAST:	sans.org/event/security-east-2016/courses
SCOTTSDALE:	sans.org/event/scottsdale-2016/courses
ANAHEIM:	sans.org/event/anaheim-2016/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 **EarlyBird16** when registering early

Pay Early and Save

Pay and enter code by the dates listed to the right for special discounts

EVENT	DATE	DISCOUNT	DATE	DISCOUNT
Las Vegas	11-18-15	$400.00	12-9-15	$200.00
Security East	12-2-15	$400.00	12-23-15	$200.00
Scottsdale	12-16-15	$400.00	1-6-16	$200.00
Anaheim	12-30-15	$400.00	1-20-16	$200.00

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** today to enjoy these FREE resources:

WEBCASTS

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

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

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

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

NEWSLETTERS

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

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

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

OTHER FREE RESOURCES

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

sans.org/security-resources