

# SANS

# Virginia Beach 2016

August 22 – September 2

SANS OFFERS HANDS-ON, IMMERSION-STYLE  
**INFORMATION SECURITY TRAINING**  
TAUGHT BY REAL-WORLD PRACTITIONERS

Protect Your Company  
and Advance Your Career with  
Information **SECURITY TRAINING** from SANS!

16 courses on  
CYBER DEFENSE  
PEN TESTING  
DIGITAL FORENSICS  
SECURITY MANAGEMENT  
ICS SECURITY

*“SANS training is  
exceptional in  
every respect.”*

-HOWARD KEESE,

INSTITUTE FOR DEFENSE ANALYSES

REGISTER AT

[www.sans.org/virginia-beach](http://www.sans.org/virginia-beach)

**SAVE  
\$400**

by registering  
and paying early!

See page 25 for  
more details.



GIAC-Approved  
Training



## Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 20.

**KEYNOTE: *Quality Not Quantity: Continuous Monitoring's Deadliest Events*** – Eric Conrad

***Hactivism: Online Protest, Real-World Consequences*** – Cindy Murphy

***Jailbreak/Root Workshop for Mobile Devices*** – Chris Crowley

***HTTPDeux*** – Adrien de Beaupre

***How to Commit Card Fraud*** – G. Mark Hardy

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

**KEYNOTE: *The Current Reality: Defending a Compromised Network*** – Dr. Eric Cole

***ICS/SCADA Cyber Attacks: Fact vs. Fiction*** – Robert M. Lee

***Welcome Threat Hunters, Phishermen, and Other Liars*** – Rob Lee

***The Tap House*** – Philip Hagen

**Be sure to register and pay by June 29th for a \$400 tuition discount!**

## Courses-at-a-Glance

	MON 8-22	TUE 8-23	WED 8-24	THU 8-25	FRI 8-26	SAT 8-27	SUN 8-28	MON 8-29	TUE 8-30	WED 8-31	THU 9-1	FRI 9-2
SEC401 Security Essentials Bootcamp Style												Page 3
SEC501 Advanced Security Essentials – Enterprise Defender						Page 4						
SEC503 Intrusion Detection In-Depth												Page 5
SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling												Page 6
SEC511 Continuous Monitoring and Security Operations						Page 7						
SEC560 Network Penetration Testing and Ethical Hacking						Page 8						
SEC561 Immersive Hands-On Hacking Techniques						Page 9						
SEC575 Mobile Device Security and Ethical Hacking						Page 10	NEW!					
FOR408 Windows Forensic Analysis						Page 11						
FOR508 Advanced Digital Forensics and Incident Response												Page 12
FOR518 Mac Forensic Analysis												Page 13
FOR572 Advanced Network Forensics and Analysis												Page 14
FOR585 Advanced Smartphone Forensics						Page 15						
MGT414 SANS Training Program for CISSP® Certification												Page 16
MGT512 SANS Security Leadership Essentials for Managers with Knowledge Compression™						Page 17						
ICS515 ICS Active Defense and Incident Response												Page 18
CORE NetWars Tournament												P 19

Register today for SANS Virginia Beach 2016!

[www.sans.org/virginia-beach](http://www.sans.org/virginia-beach)



@SANSInstitute  
Join the conversation:  
#SANSVaBeach



## 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 teach SANS courses. This guarantees that what you learn in class will be up-to-date and relevant to your job. The lineup of instructors for Virginia Beach 2016 includes:**



**Carlos Cajigas**  
*SANS Instructor*



**Dr. Eric Cole**  
*Faculty Fellow*  
@derricole



**Eric Conrad**  
*Senior Instructor*  
@eric\_conrad



**Christopher Crowley**  
*Certified Instructor*  
@CCrowMontance



**Adrien de Beaupre**  
*Certified Instructor*  
@adriendb



**Jason Dely**  
*SANS Instructor*



**Sarah Edwards**  
*Certified Instructor*  
@iamevltwin



**Kevin Fiscus**  
*Certified Instructor*  
@kevinbfiscus



**Philip Hagen**  
*Certified Instructor*  
@PhilHagen



**G. Mark Hardy**  
*Certified Instructor*  
@g\_mark



**Rob Lee**  
*Faculty Fellow*  
@robtle  
@sansforensics



**Robert M. Lee**  
*Certified Instructor*  
@RobertMLee



**Seth Misenaar**  
*Senior Instructor*  
@sethmisenaar



**Cindy Murphy**  
*Certified Instructor*  
@cindymurph



**Michael Murr**  
*Principal Instructor*  
@mikemurr



**Bryan Simon**  
*Certified Instructor*  
@BryanOnSecurity



**Chad Tilbury**  
*Senior Instructor*  
@chadtilbury

# The Value of SANS Training & YOU



## EXPLORE

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

## RELATE

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

## VALIDATE

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

## SAVE

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

## ADD VALUE

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

## ALTERNATIVES

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

## ACT

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

## Return on Investment

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

## REMEMBER

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

## SEC401:

## Security Essentials Bootcamp Style

Six-Day Program

Sun, Aug 28 - Fri, Sep 2

9:00am - 7:00pm (Days 1-5)

9:00am - 5:00pm (Day 6)

46 CPEs

Laptop Required

Instructor: Dr. Eric Cole


[www.giac.org/gsec](http://www.giac.org/gsec)

[www.sans.edu](http://www.sans.edu)

[www.sans.org/cyber-guardian](http://www.sans.org/cyber-guardian)

[www.sans.org/8140](http://www.sans.org/8140)

**BUNDLE  
ONDEMAND**  
WITH THIS COURSE

[www.sans.org/ondemand](http://www.sans.org/ondemand)

"I received the best  
explanation of crypto ever.

Great job Dr. Cole!"

-AARON A.,

(NAVSEA) CDSA DAM NECK

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

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

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

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

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

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

**PREVENTION IS IDEAL BUT DETECTION IS A MUST.**

### Who Should Attend

- ▶ Security professionals who want to fill the gaps in their understanding of technical information security
- ▶ Managers who want to understand information security beyond simple terminology and concepts
- ▶ Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- ▶ IT engineers and supervisors who need to know how to build a defensible network against attacks
- ▶ Forensic analysts, penetration testers, and auditors who need a solid foundation of security principles so they can be as effective as possible at their jobs
- ▶ Anyone new to information security with some background in information systems and networking



### Dr. Eric Cole SANS Faculty Fellow

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. He currently performs leading-edge security consulting and works in research and development to advance the state of the art in information systems security. Dr. Cole has experience in information technology with a focus on perimeter defense, secure network design, vulnerability discovery, penetration testing, and intrusion detection systems. He has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. Dr. Cole is the author of several books, including *Hackers Beware*, *Hiding in Plain Site*, *Network Security Bible*, and *Insider Threat*. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cybersecurity for the 44th President and several executive advisory boards. Dr. Cole is founder of Secure Anchor Consulting, where he provides state-of-the-art security services and expert witness work. He also served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is actively involved with the SANS Technology Institute (STI) and SANS, working with students, teaching, and maintaining and developing courseware. @drrericcole

SEC501:

## Advanced Security Essentials – Enterprise Defender

Six-Day Program

Mon, Aug 22 - Sat, Aug 27

9:00am - 5:00pm

Laptop Required

36 CPEs

Instructor: Bryan Simon


[www.giac.org/gced](http://www.giac.org/gced)

[www.sans.edu](http://www.sans.edu)

[www.sans.org/8140](http://www.sans.org/8140)

**BUNDLE  
ONDEMAND**

WITH THIS COURSE

[www.sans.org/ondemand](http://www.sans.org/ondemand)

“One of the most knowledgeable and engaging teachers I’ve ever had – using real-world experiences to enforce teaching points was awesome!!”

-SHAWN S.,  
(NAVSEA) CDSA DAM NECK



### Bryan Simon SANS Certified Instructor

Bryan Simon is an internationally recognized expert in cybersecurity and has been working in the information technology and security field since 1991. Over the course of his career, Bryan has held various technical and managerial positions in the education, environmental, accounting, and financial services sectors. Bryan speaks on a regular basis at international conferences and with the press on matters of cybersecurity. He has instructed individuals from the FBI, NATO, and the UN in matters of cybersecurity, on two continents. Bryan has specialized expertise in defensive and offensive capabilities. He has received recognition for his work in IT security, and was most recently profiled by McAfee (part of Intel Security) as an IT Hero. Bryan holds 11 GIAC certifications including GSEC, GCWN, GCIH, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, and GCUX. Bryan’s scholastic achievements have resulted in the honor of sitting as a current member of the SANS Institute Advisory Board, and in his acceptance into the prestigious SANS Cyber Guardian program. Bryan is a SANS instructor for SEC401, SEC501, SEC505, and SEC511. @BryanOnSecurity

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.

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.

“I can’t stress enough how important the SEC501 course is for today’s network defenders. It’s a hostile world, so why settle for anything less than the best? SANS is simply the best!” -JOHN J., HOUSTON PD

Of course, 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.

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 prevention and detection measures, completing the security lifecycle.

### 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

SEC503:

# Intrusion Detection In-Depth

Six-Day Program  
Sun, Aug 28 - Fri, Sep 2  
9:00am - 5:00pm  
36 CPEs  
Laptop Required  
Instructor: Kevin Fiscus

# SANS



[www.giac.org/gcia](http://www.giac.org/gcia)



[www.sans.edu](http://www.sans.edu)



[www.sans.org/cyber-guardian](http://www.sans.org/cyber-guardian)



[www.sans.org/8140](http://www.sans.org/8140)

**▶ ||**  
**BUNDLE**  
**ONDEMAND**  
WITH THIS COURSE

[www.sans.org/ondemand](http://www.sans.org/ondemand)

*"This training allowed me to gain the knowledge to better defend systems and understand the underlying concepts, communications, and means of analysis."*  
-RYAN HUNT, ALERT LOGIC

*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?*

### Who Should Attend

- ▶ Intrusion detection analysts (all levels)
- ▶ Network engineers
- ▶ System, security, and network administrators
- ▶ Hands-on security managers

**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.

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.

*"SEC503 directly covers the necessary knowledge and skill set I use every day at my job. The added insight is worth the price."*

-MICHAEL GARRETT, FEDERAL RESERVE BANK OF SAN FRANCISCO

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.



### Kevin Fiscus SANS Certified Instructor

Kevin Fiscus is the founder of and lead consultant for Cyber Defense Advisors, where he performs security and risk assessments, vulnerability and penetration testing, security program design, policy development and security awareness with a focus on serving the needs of small and mid-sized organizations. Kevin has over 20 years of IT experience and has focused exclusively for the past 12 years on information security. Kevin currently holds the CISA, GPEN, GREM, GMOB, GCED, GCEFA-Gold, GCIA-Gold, GCIH, GAWN, GPPA, GCWN, GCSC-Gold, GSEC, SCSA, RCSE, and SnortCP certifications and is proud to have earned the top information security certification in the industry, the GIAC Security Expert. Kevin has also achieved the distinctive title of SANS Cyber Guardian for both red team and blue team. @kevinfiscus

SEC504:

## Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program

Sun, Aug 28 - Fri, Sep 2

9:00am - 7:15pm (Day 1)

9:00am - 5:00pm (Days 2-6)

37 CPEs

Laptop Required

Instructor: Michael Murr


[www.giac.org/gcih](http://www.giac.org/gcih)

[www.sans.edu](http://www.sans.edu)

[www.sans.org/cyber-guardian](http://www.sans.org/cyber-guardian)

[www.sans.org/8140](http://www.sans.org/8140)

**BUNDLE  
ONDEMAND**

WITH THIS COURSE

[www.sans.org/ondemand](http://www.sans.org/ondemand)

“This was an extremely engaging course that highlights new ways of looking into incident response.”

-RYAN GUEST,  
SOUTHERN COMPANY



### Michael Murr SANS Principal Instructor

Michael has been a forensic analyst with Code-X Technologies for over five years. He has conducted numerous investigations and computer forensic examinations, and performed specialized research and development. Michael has taught SANS SEC504 (Hacker Techniques, Exploits, and Incident Handling), SANS FOR508 (Computer Forensics, Investigation, and Response), and SANS FOR610 (Reverse-Engineering Malware). He has also led SANS@Home courses, and is a member of the GIAC Advisory Board. Currently, Michael is working on an open-source framework for developing digital forensics applications. He holds the GCIH, GCFA, and GREM certifications and has a degree in computer science from California State University at Channel Islands. Michael also blogs about digital forensics on his forensic computing blog ([www.forensicblog.org](http://www.forensicblog.org)). @mikemurr

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.**

“I love Mike Murr’s analogies they are spot on and help break down complex information. The intensity of the course is matched by the knowledge and enthusiasm of the instructor.” -ELIZABETH MURRELL, BOSTON MEDICAL CENTER

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

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

“This course provides an eye-opening overview of methods and tools used by bad actors as well as a good explanation of incident handling processes!”

-STEVEN J. SPARKS, HONEYWELL

### 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



SEC511:

# Continuous Monitoring and Security Operations

Six-Day Program

Mon, Aug 22 - Sat, Aug 27

9:00am - 7:00pm (Days 1-5)

9:00am - 5:00pm (Day 6)

Laptop Required

46 CPEs

Laptop Required

Instructor: Eric Conrad



# SANS



[www.giac.org/gmon](http://www.giac.org/gmon)



[www.sans.edu](http://www.sans.edu)



**BUNDLE ONDEMAND**

WITH THIS COURSE

[www.sans.org/ondemand](http://www.sans.org/ondemand)

“SEC511 is a good technical overview of why we fail today and offers practical solutions to fix security issues we all face.”

-BRAD MILHORN, COMPUCOM

We continue to underestimate the tenacity of our adversaries! Organizations are investing a significant amount of time and financial and human resources trying to prevent and combat 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.

### Who Should Attend

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

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.

“This training is valuable because it helped me understand network security from various types of prevention and provided good insight into endpoint security.”

-STEPHEN L. PERRY, ARDENT HEALTH SERVICES

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 is 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.



### Eric Conrad SANS Senior Instructor

Eric Conrad is lead author of the book *The CISSP Study Guide*. Eric's career began in 1991 as a UNIX systems administrator for a small oceanographic communications company. He gained information security experience in a variety of industries, including research, education, power, Internet, and healthcare. He is now president of Backshore Communications, a company focusing on intrusion detection, incident handling, information warfare, and penetration testing. He is a graduate of the SANS Technology Institute with a master of science degree in information security engineering. In addition to the CISSP, he holds the prestigious GIAC Security Expert (GSE) certification as well as the GIAC GPEN, GCIH, GCIA, GCFA, GAWN, and GSEC certifications. Eric also blogs about information security at [ericconrad.com](http://ericconrad.com). @eric\_conrad

SEC560:

## Network Penetration Testing and Ethical Hacking

Six-Day Program

Mon, Aug 22 - Sat, Aug 27

9:00am - 7:15pm (Day 1)

9:00am - 5:00pm (Days 2-6)

37 CPEs

Laptop Required

Instructor:

Adrien de Beupre


[www.giac.org/gpen](http://www.giac.org/gpen)

[www.sans.edu](http://www.sans.edu)

[www.sans.org/cyber-guardian](http://www.sans.org/cyber-guardian)

**BUNDLE  
ONDEMAND**

WITH THIS COURSE

[www.sans.org/ondemand](http://www.sans.org/ondemand)

“This course provides validation and confirmation of your skills and concepts, and then blows your mind with super powers.”

-TRIP HILLMAN, WEAVER LLP



### Adrien de Beupre SANS Certified Instructor

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

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

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

“As someone new to offense, this course was an amazing intro to the tactics and capabilities of an attacker.” -JOHN HUBBARD, GLAXOSMITHKLINE

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

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

### 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

## SEC561:

# Immersive Hands-On Hacking Techniques

Six-Day Program  
 Mon, Aug 22 - Sat, Aug 27  
 9:00am - 5:00pm  
 Laptop Required  
 36 CPEs  
 Laptop Required  
 Instructor: Kevin Fiscus

### Who Should Attend

- ▶ Security professionals
- ▶ Systems and network administrators
- ▶ Incident response analysts
- ▶ Forensic analysts
- ▶ Penetration testers
- ▶ Red and blue team members

“Hands-down, one of the best SANS courses I have taken. I learned cutting-edge pentesting techniques in a hands-on environment that challenged my abilities and increased my overall knowledge.”

-DAVE ODOM, BECHTEL

“Kevin is very engaging and keeps the class interesting.”

-BRETT BATES,  
 STATE OF WYOMING



### Kevin Fiscus SANS Certified Instructor

Kevin Fiscus is the founder and lead consultant for Cyber Defense Advisors, where he performs security and risk assessments, vulnerability and penetration testing, security program design, policy development and security awareness with a focus on serving the needs of small and mid-sized organizations. Kevin has over 20 years of IT experience and has focused exclusively for the past 12 years on information security. Kevin currently holds the CISA, GPEN, GREM, GMOB, GCED, GCFA-Gold, GCIA-Gold, GCIH, GAWN, GPPA, GCWN, GCSC-Gold, GSEC, SCSA, RCSE, and SnortCP certifications and is proud to have earned the top information security certification in the industry, the GIAC Security Expert. Kevin has also achieved the distinctive title of SANS Cyber Guardian for both red team and blue team. @kevinfiscus

To be a top penetration testing professional, you need fantastic hands-on skills for finding, exploiting and resolving vulnerabilities. Top instructors at SANS engineered **SEC561: Immersive Hands-On Hacking Techniques** from the ground up to help you get good fast. The course teaches in-depth security capabilities through 80%+ hands-on exercises, maximizing keyboard time during in-class labs and making this SANS' most hands-on course ever. With over 30 hours of intense labs, students experience a leap in their capabilities, as they come out equipped with the practical skills needed to handle today's pen test and vulnerability assessment projects in enterprise environments. Throughout the course, an expert instructor coaches students as they work their way through solving increasingly demanding real-world information security scenarios using skills that they will be able to apply the day they get back to their jobs.

“This course really forces you to think and the format rewards your hard work and dedication to finding the solutions.” -MICHAEL NUTBROWN, SOLERS, INC

People often talk about these concepts, but this course teaches you how to actually do them hands-on and in-depth. SEC561 shows penetration testers, vulnerability assessment personnel, auditors, and operations personnel how to leverage in-depth techniques to get powerful results in every one of their projects. The course is overflowing with practical lessons and innovative tips, all with direct hands-on application. Throughout the course, students interact with brand new and custom-developed scenarios built just for this course on the innovative NetWars challenge infrastructure, which guides students through the numerous hands-on labs providing questions, hints, and lessons learned as they build their skills.

### Topics addressed in the course include:

- ▶ Applying network scanning and vulnerability assessment tools to effectively map out networks and prioritize discovered vulnerabilities for effective remediation.
- ▶ Manipulating common network protocols to reconfigure internal network traffic patterns, as well as defenses against such attacks.
- ▶ Analyzing Windows and Linux systems for weaknesses using the latest enterprise management capabilities of the operating systems, including the super-powerful Windows Remote Management (WinRM) tools.
- ▶ Applying cutting-edge password analysis tools to identify weak authentication controls leading to unauthorized server access.
- ▶ Scouring through web applications and mobile systems to identify and exploit devastating developer flaws.
- ▶ Evading anti-virus tools and bypassing Windows User Account Control to understand and defend against these advanced techniques.
- ▶ Honing phishing skills to evaluate the effectiveness of employee awareness initiatives and your organization's exposure to one of the most damaging attack vectors widely used today.

SEC575:

## Mobile Device Security and Ethical Hacking

NEW

Six-Day Program  
 Mon, Aug 22 - Sat, Aug 27  
 9:00am - 5:00pm  
 36 CPEs  
 Laptop Required  
 Instructor:  
 Christopher Crowley



[www.giac.org/gmob](http://www.giac.org/gmob)



[www.sans.edu](http://www.sans.edu)



**BUNDLE  
 ONDEMAND**  
 WITH THIS COURSE

[www.sans.org/ondemand](http://www.sans.org/ondemand)

"I wish I had taken this course several years ago when first entering the mobile landscape. It would have saved me months of painful self-teaching, and is vastly more complete in many areas."

-JEREMY ERICKSON,

SANDIA NATIONAL LABS

Imagine an attack surface spread throughout your organization and in the hands of every user. It moves from place to place regularly, stores highly sensitive and critical data, and sports a wide range of wireless technologies all ripe for attack. There's no need to imagine any further because you actually already have this today: mobile devices. These devices are the biggest attack surface in most organizations, yet these same organizations often don't have the skills needed to assess them.

### NOW COVERING ANDROID MARSHMALLOW, iOS 9, APPLE WATCH AND ANDROID WEAR

Mobile devices are no longer a convenience technology; they are an essential tool carried or worn by users worldwide, often displacing conventional computers for everyday enterprise data needs. You can see this trend in corporations, hospitals, banks, schools, and retail stores throughout the world. Users rely on mobile devices more today than ever before – we know it, and the bad guys do too.

### LEARN HOW TO PEN TEST THE BIGGEST ATTACK SURFACE IN YOUR ENTIRE ORGANIZATION

This course is designed to give you the skills you need to understand the security strengths and weaknesses in **Apple iOS**, **Android**, and wearable devices including **Apple Watch** and **Android Wear**. With these skills, you will evaluate the security weaknesses of built-in and third-party applications. You'll learn how to bypass platform encryption, and how to manipulate Android apps to circumvent obfuscation techniques. You'll leverage automated and manual mobile application analysis tools to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels. You'll safely work with mobile malware samples to understand the data exposure and access threats affecting Android and iOS devices, and you'll exploit lost or stolen devices to harvest sensitive mobile application data.

Mobile device deployments introduce new threats to organizations, including advanced malware, data leakage, and the disclosure of enterprise secrets, intellectual property, and personally identifiable information assets to attackers. Further complicating matters, there simply are not enough people with the security skills needed to identify and manage secure mobile phone and tablet deployments. By completing this course, you'll be able to differentiate yourself as having prepared to evaluate the security of mobile devices, effectively assess and identify flaws in mobile applications, and conduct a mobile device penetration test – **all critical skills to protect and defend mobile device deployments.**

### 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



### Christopher Crowley SANS Certified Instructor

Christopher has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. His work experience includes penetration testing, computer network defense, incident response, and forensic analysis. He is the course author for SANS MGT535: Incident Response Team Management and holds the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GREM, GMOB, and CISSP certifications. His teaching experience includes SEC401, SEC503, SEC504, SEC560, SEC575, SEC580, FOR585, and MGT535; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor of the Year Award, which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities. @CCrowMontance

FOR408:

## Windows Forensic Analysis

Six-Day Program

Mon, Aug 22 - Sat, Aug 27

9:00am - 5:00pm

36 CPEs

Laptop Required

Instructors: Carlos Cajigas

Chad Tilbury



[www.giac.org/gcfe](http://www.giac.org/gcfe)



[www.sans.edu](http://www.sans.edu)



**BUNDLE  
ONDEMAND**

WITH THIS COURSE

[www.sans.org/ondemand](http://www.sans.org/ondemand)



[digital-forensics.sans.org](http://digital-forensics.sans.org)

"This is the best Windows forensic class in the world!"

-Bob A. Akin, SALC

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

Every organization must prepare for cyber crime occurring on its computer systems and within its networks. Demand has never been greater for analysts who can investigate crimes like fraud, insider threats, industrial espionage, employee misuse, and computer intrusions.

Government agencies increasingly require trained media exploitation specialists to recover key intelligence from Windows systems. To help solve these cases, SANS is training a new cadre of the world's best digital forensic professionals, incident responders, and media exploitation masters capable of piecing together what happened on computer systems second by second.

**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 to validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR408 teaches you how to mine this mountain of data.

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

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



#### Chad Tilbury SANS Senior Instructor

Chad Tilbury has been responding to computer intrusions and conducting forensic investigations since 1998. His extensive law enforcement and international experience stems from working with a broad cross-section of Fortune 500 corporations and government agencies around the world.

During his service as a Special Agent with the Air Force Office of Special Investigations, he investigated and conducted computer forensics for a variety of crimes, including hacking, abduction, espionage, identity theft, and multi-million dollar fraud cases. Chad is a graduate of the U.S. Air Force Academy and holds a B.S. and M.S. in computer science as well as GCFA, GCIH, GREM, and ENCE certifications. See Chad's complete bio at [sans.org/event/virginia-beach-2016/instructors@chadtilbury](http://sans.org/event/virginia-beach-2016/instructors@chadtilbury)



#### Carlos Cajigas SANS Instructor

As an incident responder, retired detective, cybercrimes investigator, and digital forensics trainer, Carlos has amassed a wealth of experience in high-technology crime investigations. He was a detective with the West Palm Beach Police Department, where he specialized in computer crime investigations. Carlos has a bachelor's and master's degree from Palm Beach Atlantic University (FL). In addition, he holds various certifications in the digital forensics field, including ENCE, CFCE, GCFA, and GCFA. See Carlos' complete bio at [sans.org/event/virginia-beach-2016/instructors](http://sans.org/event/virginia-beach-2016/instructors)

FOR508:

## Advanced Digital Forensics and Incident Response

Six-Day Program  
 Sun, Aug 28 - Fri, Sep 2  
 9:00am - 5:00pm  
 36 CPEs  
 Laptop Required  
 Instructor: Rob Lee



[www.giac.org/gcfa](http://www.giac.org/gcfa)



[www.sans.edu](http://www.sans.edu)



[www.sans.org/cyber-guardian](http://www.sans.org/cyber-guardian)



[www.sans.org/8140](http://www.sans.org/8140)



**BUNDLE  
 ONDEMAND**

WITH THIS COURSE

[www.sans.org/ondemand](http://www.sans.org/ondemand)



[digital-forensics.sans.org](http://digital-forensics.sans.org)

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

- > How the breach occurred
- > 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.

**“Traditional knowledge is useful, but this course provided the practical side of a growing trend.” -ERIK M., ARKANSAS STATE POLICE**

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.

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!**



**Rob Lee** SANS Faculty Fellow

Rob Lee is an entrepreneur and consultant in the Washington, DC area and currently the Curriculum Lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 15 years' experience in computer forensics, vulnerability and exploit development, intrusion detection/prevention, and incident response. Rob graduated from the U.S. Air Force Academy and earned his MBA from Georgetown University. He served in the U.S. Air Force as a member of the 609th Information Warfare Squadron (IWS), the first U.S. military operational unit focused on information warfare. Later, he was a member of the Air Force Office of Special Investigations (AFOSI) where he led crime investigations and an incident response team. Over the next seven years, he worked directly with a variety of government agencies in the law enforcement, U.S. Department of Defense, and intelligence communities as the technical lead for vulnerability discovery and exploit development teams, lead for a cyber-forensics branch, and lead for a computer forensic and security software development team. Most recently, Rob was a Director for MANDIANT, a commercial firm focusing on responding to advanced adversaries such as the APT. Rob co-authored the book *Know Your Enemy, 2nd Edition*. Rob is also co-author of the MANDIANT threat intelligence report “M-Trends: The Advanced Persistent Threat.”

@robtee & @sansforensics

## FOR518:

# Mac Forensic Analysis

Six-Day Program

Sun, Aug 28 - Fri, Sep 2

9:00am - 5:00pm

36 CPEs

Laptop Required

Instructor: Sarah Edwards



**BUNDLE  
ONDEMAND**  
WITH THIS COURSE  
[sans.org/ondemand](http://sans.org/ondemand)



[digital-forensics.sans.org](http://digital-forensics.sans.org)

“Sarah is an incredible instructor — her knowledge far surpasses anything I’ve ever experienced plus the reference material is invaluable.”

-BEN KECK, CIENA

“Very comprehensive in-depth coverage of the course topic. Excellent reference materials as a take-away.”

-JENNIFER B.,

INDIANA STATE POLICE



### Sarah Edwards *SANS Certified Instructor*

Sarah is a senior digital forensic analyst who has worked with various federal law enforcement agencies. She has performed a variety of investigations including computer intrusions, criminal cases, and counter-intelligence, counter-narcotics, and counter-terrorism investigations. Sarah’s research and analytical interests include Mac forensics, mobile device forensics, digital profiling, and malware reverse engineering. Sarah has presented at the following industry conferences; Shmoocon, CEIC, BsidessNOLA, TechnoSecurity, HTCIA, and the SANS DFIR Summit. She has a bachelor of science in information technology from Rochester Institute of Technology and a master’s in information assurance from Capitol College. [@iamevltwin](https://twitter.com/iamevltwin)

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

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

## FORENSICATE DIFFERENTLY!

*FOR518 will teach you:*

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

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

### Who Should Attend

- Experienced digital forensic analysts who want to solidify and expand their understanding of file system forensics and advanced Mac analysis
- Law enforcement officers, federal agents, or detectives who want to master advanced computer forensics and expand their investigative skill set
- Media exploitation analysts who need to know where to find the critical data they need from a Mac system
- Incident response team members who are responding to complex security incidents/intrusions from sophisticated adversaries and need to know what to do when examining a compromised system
- Information security professionals who want to become knowledgeable with Mac OS X and iOS system internals
- SANS FOR408, FOR508, FOR526, FOR610, FOR585 alumni looking to round out their forensic skills

FOR572:

## Advanced Network Forensics and Analysis

Six-Day Program

Sun, Aug 28 - Fri, Sep 2

9:00am - 5:00pm

36 CPEs

Laptop Required

Instructor: Philip Hagen


[www.giac.org/gnfa](http://www.giac.org/gnfa)

[www.sans.edu](http://www.sans.edu)

▶ II  
BUNDLE  
ONDEMAND

WITH THIS COURSE

[www.sans.org/ondemand](http://www.sans.org/ondemand)

[digital-forensics.sans.org](http://digital-forensics.sans.org)

“This course adds more techniques and processes along with a whole bunch of new fundamentals and tools to my arsenal.”

-TOBY ANDREWS, WETROCK



### Philip Hagen SANS Certified Instructor

Philip Hagen has been working in the information security field since 1998, running the full spectrum including deep technical tasks, management of an entire computer forensic services portfolio, and executive responsibilities. Currently, Phil is an Evangelist at Red Canary, where he engages with current and future customers of Red Canary's managed threat detection service to ensure their use of the service is best aligned for success in the face of existing and future threats. Phil started his security career while attending the U.S. Air Force Academy, with research covering both the academic and practical sides of security. He served in the Air Force as a communications officer at Beale AFB and the Pentagon. In 2003, Phil became a government contractor, providing technical services for various IT and information security projects. These included systems that demanded 24x7x365 functionality. He later managed a team of 85 computer forensic professionals in the national security sector. He provided forensic consulting services for law enforcement, government, and commercial clients prior to joining the Red Canary team. Phil is the course lead and co-author of FOR572: Advanced Network Forensics and Analysis. @PhilHagen

Forensic casework that does not include a network component is a rarity in today's environment. Performing disk forensics will always be a critical and foundational skill for this career, but overlooking the network component of today's computing architecture is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, or employee misuse scenario, the network often has an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, or even definitively prove that a crime actually occurred.

### FOR572: Advanced Network Forensics and Analysis

was built from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. We focus on the knowledge necessary to expand the forensic mindset from residual data on the storage media from a system or device to the transient communications that occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero. Put another way: **Bad guys are talking – we'll teach you to listen.**

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will cover the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap exploration, ancillary network log examination, and more. We cover how to leverage existing infrastructure devices that may contain months or years of valuable evidence, as well as how to place new collection platforms while an incident is already under way.

Whether you are a consultant responding to a client's needs, a law enforcement professional assisting victims of cyber crime and seeking prosecution of those responsible, or an on-staff forensic practitioner, this course offers hands-on experience with real-world scenarios that will help take your work to the next level. Previous SANS security curriculum students and other network defenders will benefit from the FOR572 perspective on security operations as they take on more incident response and investigative responsibilities. SANS forensics alumni from FOR408 and FOR508 can take their existing knowledge and apply it directly to the network-based attacks that occur daily. In FOR572, we solve the same caliber of real-world problems without any convenient hard drive or memory images.

### Who Should Attend

- ▶ Incident response team members and forensicators
- ▶ Law enforcement officers, federal agents, and detectives
- ▶ Information security managers
- ▶ Network defenders
- ▶ IT professionals
- ▶ Network engineers
- ▶ Anyone interested in computer network intrusions and investigations
- ▶ Security Operations Center personnel and information security practitioners



FOR585:

## Advanced Smartphone Forensics

Six-Day Program

Mon, Aug 22 - Sat, Aug 27

9:00am - 5:00pm

36 CPEs

Laptop Required

Instructor: Cindy Murphy


[www.giac.org/gasf](http://www.giac.org/gasf)

[www.sans.edu](http://www.sans.edu)

**BUNDLE  
ONDEMAND**

WITH THIS COURSE

[www.sans.org/ondemand](http://www.sans.org/ondemand)

[digital-forensics.sans.org](http://digital-forensics.sans.org)

**“An incredibly valuable week of training and I would recommend it to anyone looking to expand their mobile forensic skills.” -MANNY ORTIZ, AT&T**



### Cindy Murphy SANS Certified Instructor

Cindy Murphy is a detective with the City of Madison, WI Police Department and has been a law enforcement officer since 1985. She is a certified forensic examiner and has been involved in computer forensics since 1999. Det. Murphy has directly participated in the examination of hundreds of hard drives, cell phones, and other items of digital evidence pursuant to criminal investigations, including financial crimes, homicides, missing persons, computer intrusions, sexual assaults, child pornography, and various other crimes. She has testified as a computer forensics expert in state and federal courts on numerous occasions, using her knowledge and skills to assist in the successful investigation and prosecution of criminal cases involving digital evidence. She also helped to develop the digital forensics certificate program at Madison Area Technical College. She has presented internationally on various digital forensics topics and frequently writes articles and whitepapers on various forensics-related topics. Det. Murphy earned her master's of science degree in forensic computing and cyber crime investigation at University College, Dublin, where she completed her dissertation on victim age estimation from child exploitation images. She is also involved with the Wisconsin Association of Computer Crimes Investigators (WACCI) and served as past president of the WACCI West Chapter. She has also been involved with the Chicago Electronic Crimes Task Force, High Tech Crime Consortium (HTCC), High Tech Crime Network (HTCN), and International Guild of Knot Tyers (IGKT). @cindymurph

Mobile devices are often a key factor in criminal cases, intrusions, IP theft, security threats, and more. Understanding how to leverage the data from the device in a correct manner can make or break your case and your future as an expert.

**FOR585: Advanced Smartphone Forensics** will teach you those skills.

Every time the smartphone “thinks” or makes a suggestion, the data are saved. It’s easy to get mixed up in what the forensic tools are reporting. Smartphone forensics is more than pressing the “find evidence” button and getting answers. Your team cannot afford to rely solely on the tools in your lab. You have to understand how to use them correctly to guide your investigation, instead of just letting the tool report what it believes happened on the device. It is impossible for commercial tools to parse everything from smartphones and understand how the data were put on the device. Examining and interpreting the data is your job, and this course will provide you and your organization with the capability to find and extract the correct evidence from smartphones with confidence.

This in-depth smartphone forensic course provides examiners and investigators with advanced skills to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. The course features 17 hands-on labs that allow students to analyze different datasets from smart devices and leverage the best forensic tools and custom scripts to learn how smartphone data hide and can be easily misinterpreted by forensic tools. Each lab is designed to teach you a lesson that can be applied to other smartphones. You will gain experience with the different data formats on multiple platforms and learn how the data are stored and encoded on each type of smart device. The labs will open your eyes to what you are missing by relying 100% on your forensic tools.

FOR585 is continuously updated to keep up with the latest malware, smartphone operating systems, third-party applications, and encryption. This intensive six-day course offers the most unique and current instruction available, and it will arm you with mobile device forensic knowledge you can apply immediately to cases you’re working on the day you leave the course.

Smartphone technologies are constantly changing, and most forensic professionals are unfamiliar with the data formats for each technology. Take your skills to the next level: it’s time for the good guys to get smarter and for the bad guys to know that their texts and apps can and will be used against them!

**SMARTPHONE DATA CAN’T HIDE FOREVER – IT’S TIME TO OUTSMART THE MOBILE DEVICE!**

### Who Should Attend

- ▶ Experienced digital forensic analysts
- ▶ Media exploitation analysts
- ▶ Information security professionals
- ▶ Incident response teams
- ▶ Law enforcement officers, federal agents, and detectives
- ▶ IT auditors
- ▶ SANS SEC575, FOR408, FOR508, FOR518, and FOR572 graduates looking to take their skills to the next level

MGT414:

## SANS Training Program for CISSP® Certification

Six-Day Program

Sun, Aug 28 - Fri, Sep 2

9:00am - 7:00pm (Day 1)

8:00am - 7:00pm (Days 2-5)

8:00am - 5:00pm (Day 6)

46 CPEs

Laptop NOT Needed

Instructor: Seth Misener



[www.giac.org/gisp](http://www.giac.org/gisp)



[www.sans.org/8140](http://www.sans.org/8140)



**BUNDLE  
ONDEMAND**

WITH THIS COURSE

[www.sans.org/ondemand](http://www.sans.org/ondemand)

“I would recommend this class for anyone wanting to get a CISSP. I feel it gave me the tools to be confident to take the test.”

-MATTHEW TRUMMER,

LINCOLN ELECTRIC SYSTEMS

**SANS MGT414: SANS Training Program for CISSP® Certification** is an accelerated review course that has been specifically updated to prepare you to pass the 2016 version of the CISSP® exam.

Course authors Eric Conrad and Seth Misener have revised MGT414 to take into account the 2016 updates to the CISSP® exam and prepare students to navigate all types of questions included in the new version.

MGT414 focuses solely on the eight domains of knowledge as determined by (ISC)<sup>2</sup> 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 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

### Note:

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

### Who Should Attend

- ▶ Security professionals who want to understand the concepts covered in the CISSP® exam as determined by (ISC)<sup>2</sup>
- ▶ 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 activities

### Obtaining Your CISSP® Certification Consists of:

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

Take advantage of the SANS CISSP® Get Certified Program currently being offered.

[www.sans.org/cissp](http://www.sans.org/cissp)



### Seth Misener SANS Senior Instructor

Seth Misener serves as lead consultant and founder of Jackson, Mississippi-based Context Security, which provides information security thought leadership, independent research, and security training. Seth's background includes network and web application penetration testing, vulnerability assessment, regulatory compliance efforts, security architecture design, and general security consulting. He has previously served as both physical and network security consultant for Fortune 100 companies and the Health Insurance Portability and Accountability Act, and as information security officer for a state government agency. Prior to becoming a security geek, Seth received a bachelor's of science degree in philosophy from Millsaps College, where he was twice selected for a Ford Teaching Fellowship. Also, Seth is no stranger to certifications and thus far has achieved credentials that include CISSP, GPEN, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE. @sethmisener

MGT512:

## SANS Security Leadership Essentials for Managers with Knowledge Compression™

Five-Day Program

Mon, Aug 22 - Fri, Aug 26

9:00am - 6:00pm (Days 1-4)

9:00am - 4:00pm (Day 5)

33 CPEs

Laptop NOT Needed

Instructor: G. Mark Hardy



[www.giac.org/gslc](http://www.giac.org/gslc)



[www.sans.edu](http://www.sans.edu)



[www.sans.org/8140](http://www.sans.org/8140)



**BUNDLE  
ONDEMAND**

WITH THIS COURSE

[www.sans.org/ondemand](http://www.sans.org/ondemand)

"The course content is great because it is consistently updated to reflect current IT trends.

The instructor was knowledgeable and very down to earth."

-TERENCE B.,

OFFICER TRAINING COMMAND

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

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!



### G. Mark Hardy SANS Certified Instructor

G. Mark Hardy is founder and president of National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for over 30 years, and is an internationally recognized expert who has spoken at over 250 events world-wide. He serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. A retired U.S. Navy Captain, he was privileged to serve in command nine times, including responsibility for leadership training for 70,000 sailors. He also served as wartime Director, Joint Operations Center for U.S. Pacific Command, and Assistant Director of Technology and Information Management for Naval Logistics in the Pentagon, with responsibility for InfoSec, public key infrastructure, and Internet security. Captain Hardy was awarded the Defense Superior Service Medal, the Legion of Merit, five Meritorious Service Medals, and 24 other medals and decorations. A graduate of Northwestern University, he has bachelor's degrees in computer science and mathematics, and master's degrees in business administration and strategic studies, along with the GSLC, CISSP, CISM, and CISA certifications. @g\_mark

## ICS 515:

# ICS Active Defense and Incident Response

Five-Day Program  
 Mon, Aug 29 - Fri, Sep 2  
 9:00am - 5:00pm  
 30 CPEs  
 Laptop Required  
 Instructors: Robert M. Lee  
 Jason Dely

**▶ II**  
**BUNDLE**  
**ONDEMAND**  
 WITH THIS COURSE  
[www.sans.org/ondemand](http://www.sans.org/ondemand)

**“Awesome!! Rob explained the concepts clearly so that it was easy to grasp the ideas.”**

-SRINATH KANNAN, ACCENTURE

**“This course is the missing piece to get companies to take threats seriously, pursue the truth, and share their findings.”**

-ROB CANTU, DOE



### **Robert M. Lee** SANS Certified Instructor

Robert M. Lee is the CEO and founder of the critical infrastructure cybersecurity company Dragos Security LLC, where he has a passion for control system traffic analysis, incident response, and threat intelligence research. He is the course author of SANS ICS 515: Active Defense and Incident Response and the co-author of SANS FOR578: Cyber Threat Intelligence. Robert is also a non-resident National Cyber Security Fellow at New America focusing on policy issues relating to the cybersecurity of critical infrastructure and a PhD candidate at Kings College London. For his research and focus areas, he was named one of Passcode’s Influencers and awarded EnergySec’s 2015 Cyber Security Professional of the Year. Robert obtained his start in cybersecurity in the U.S. Air Force, where he served as a Cyber Warfare Operations Officer. He has performed defense, intelligence, and attack missions in various government organizations, including the establishment of a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Robert routinely writes articles in publications such as *Control Engineering* and the *Christian Science Monitor’s Passcode* and speaks at conferences around the world. He is also the author of *SCADA and Me* and the weekly web-comic ([www.LittleBobbyComic.com](http://www.LittleBobbyComic.com)) @RobertMLee



### **Jason Dely** SANS Instructor

Jason Dely is an Industrial Control Systems (ICS) security consultant for Cylance Inc. with over 15 years of professional experience in ICS and critical infrastructure security initiatives and solutions spanning multiple industry verticals. Jason is a leader and contributor in the management, consultation, assessment, planning, designing and implementation of a variety of ICS security and infrastructure projects across industries that include water utilities, oil and gas, steel, and chemical. Before joining Cylance, Jason worked for one of the world’s largest ICS vendors, where he contributed his security knowledge and integration experiences across ICS and IT technologies. Jason is frequently a speaker at various industry events and leverages his integration knowledge of securing ICS systems and their vulnerabilities to provide services and guidance to Cylance clients. Jason holds the CISSP, CISM, and GXPN certifications.

### ICS 515: ICS Active Defense and Incident Response

will help you deconstruct ICS cyber attacks, leverage an active defense to identify and counter threats in your ICS, and use incident response procedures to maintain the safety and reliability of operations.

This course will empower students to understand their networked industrial control system 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 internal to the network is known as active defense. An active defense is the approach needed to 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 with the ability to deconstruct targeted ICS attacks and fight these adversaries and others. The course uses a hands-on approach and real-world malware to break down cyber attacks on ICS from start to finish. Students will gain a practical and technical understanding of leveraging active defense concepts such as using threat intelligence, performing network security monitoring, and utilizing malware analysis and incident response to ensure the safety and reliability of operations. The strategy and technical skills presented in this course serve as a basis for ICS organizations looking to show that defense is do-able.

### Who Should Attend

- ▶ ICS incident response team leads and members
- ▶ ICS and operations technology security personnel
- ▶ IT security professionals
- ▶ Security Operations Center (SOC) team leads and analysts
- ▶ ICS red team and penetration testers
- ▶ Active defenders

**“This course is on the right track filling in gaps of the intel gathering and the analysis reporting of incidents and event.”-SAM B., U.S. ARMY**

# NETWARS



Are you one of the top Information Security Professionals?

Prove your knowledge and skills at

## Four Nights of NetWars at SANS Virginia Beach 2016!

AUG 25-26 & AUG 31 – SEPT 1

6:30-9:30 PM

Come and join us for this exciting event to test your skills in a challenging and fun learning environment. Registration for NetWars is **FREE OF CHARGE TO ALL STUDENTS AT SANS VIRGINIA BEACH 2016.**

External participants are welcome to join for an entry fee of \$1,450.

SANS NetWars is a dynamic cyber range that allows participants to build, practice, and measure their skills in a real-world environment using defensive, analytic, and offensive tactics. We designed NetWars to appeal to a wide range of participant skill sets by using a system with different levels.

All players start at Level 1, which measures foundational cybersecurity skills. More skilled players can rise rapidly through the ranks to a level suitable for their skill set – top players can make it to Level 4, and only the best of the best can reach level 5.

[www.sans.org/virginia-beach](http://www.sans.org/virginia-beach)

## KEYNOTE: **Quality Not Quantity: Continuous Monitoring's Deadliest Events**

*Eric Conrad*

Most Security Operations Centers are built for compliance, not security. One well-known retail firm suffered the theft of over a million credit cards. Some 60,000 true positive events were reported to their SOC during that breach... and missed: lost in the noise of millions. If you are bragging about how many events your SOC “handles” each day, you are doing it wrong. This presentation will show you how to focus on quality instead of quantity, and we'll provide an actionable list of the deadliest events that occur during virtually every successful breach.

## **Hactivism: Online Protest, Real-World Consequences** – *Cindy Murphy*

In an Internet-connected world, national, state, and local political conflicts and social issues such as officer-involved shootings can quickly attract the attention of a worldwide audience. When hactivists become involved, concerns can quickly arise regarding critical infrastructure, network security, public safety, and individual officer safety. Detective Murphy will present information about various groups involved in hactivism, discuss the history, motivations, and methods used by hactivists, provide case study examples of incidents where hactivism has led to real-world consequences, and provide strategies for successful investigation of hactivist incidents to identify responsible parties.

## **Jailbreak/Root Workshop for Mobile Devices** – *Chris Crowley*

This is primarily a hands-on workshop with a brief discussion of tools for jailbreak of vulnerable iOS and Android platforms. Bring an older iOS device (an iPhone 3GS from ebay will work great) or a Nexus 7 tablet (or Nexus 4 phone) to root or jailbreak. This session is intended to allocate time to jailbreak and root devices to help attendees understand the methods available for unrestricting mobile devices. The unrestricted device is useful for application assessments and pen testing. Warning, the techniques discussed could render the devices completely inoperable. Bring a device that can become unusable without you becoming upset.

## **HTTPDeux** – *Adrien de Beupre*

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

## **How to Commit Card Fraud** – *G. Mark Hardy*

Well, we're not going to show you how to commit fraud, but will show you how the bad guys do it and how you can protect yourself and your business. We'll take a look into the “dark web” and see how these big card heists are pulled off, why chip-and-pin won't solve the fraud problem, and why payment technologies like Apple Pay pose new risks. You'll learn the ecosystem of fraud, and how it's become a big business that costs banks and merchants over \$16 billion annually. See if your bank even bothers to use the security protections it could – we'll have a mag stripe card reader so you can really see what's in your wallet. Certified SANS instructor G. Mark Hardy is the CEO and founder of CardKill Inc., a start-up that helps banks preemptively kill stolen cards BEFORE they are used in fraud.

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

It's all about the information! Two decades after the movie *Sneakers*, the quote remains as relevant as ever, if not more so. The fact that someone hacks into an environment is interesting but not that relevant. What is important is what happens after the compromise. If the data are destroyed or modified, organizations are negatively impacted but the benefits to an attacker for destruction or alteration are somewhat limited. Stealing information, however, is highly profitable. Identity theft, espionage, and financial attacks involve the exfiltration of sensitive data. As a result, organizations deploy tools to detect and/or stop that data exfiltration. While these tools can be extremely valuable, many have serious weaknesses; attackers can encode, hide, or obfuscate the data, or can use secret communication channels. This session will talk about and demonstrate a range of these methods.

## KEYNOTE: **The Current Reality: Defending a Compromised Network**

*Dr. Eric Cole*

Designing and securing a network is very complex. With detailed requirements to support all of the latest devices, mobile computing, cloud services, and the portability requirements of data, current networks are porous, difficult to secure, and very compromised. When people hear about networks being compromised, they should not be surprised. Networks directly connected to the Internet are compromised and should be the new baseline for designing and building out security. The question is how to implement security based on the assumption that security is more than just setting up and protecting perimeters. In this talk, Dr. Cole will share real-life examples of security solutions that work to protect current environments that might be already compromised. The focus of security is not on preventing a compromise, but on controlling the amount of damage caused by a compromise, which is done by focusing in on dwell time and lateral movement.

## **ICS/SCADA Cyber Attacks: Fact vs. Fiction** – *Robert M. Lee*

Industrial Control Systems (ICS) play a huge role in almost every aspect of modern day life. Supervisory control and data acquisition (SCADA), for example, plays a large role in monitoring and controlling the power grid, oil pipelines, and more. It's understandable then that they gain attention in national headlines when they come under attack. Due to this glare of public attention and the complexity behind getting the technical details right, there have been some cases where the stories have just been downright wrong. These inaccurate case studies push hype and confusion, which drives the investment of resources into trying to solve the wrong problem. The threat is real, but plenty of the stories are not. In this presentation, Robert M. Lee, ICS515 author and FOR578 co-author, will break down a number of high-profile stories that are fiction and then deconstruct real threats to show the actual issues in the community and what can be learned about defense.

## **Welcome Threat Hunters, Phishermen, and Other Liars** – *Rob Lee*

Over the past few years, a new term has continually popped up in the IT Security community called “threat hunting.” While the term seems like it is new, it really is the reason all of us joined IT Security in the first place: to find evil. While I was at Mandiant and in the U.S. Air Force, “finding evil” was in fact our tagline when we were on assignments.

This talk was put together to outline what exactly “threat hunting” means and step you through exactly what it is and how it works. When I first started in IT Security back in the late 1990s, my job was to find threats in the network. This led to automated defenses such as Intrusion Detection Systems, monitoring egress points, logging technology, and monitoring the defensive perimeter hoping nothing would get in. Today, while the community is trying to identify intrusions, threat hunting has evolved into something more than the loose definition of “find evil,” primarily due to the massive amount of incident response data currently collected about our attackers. This data has evolved into cyber threat intelligence. The hunt to “find evil” will be better targeted if you're armed with cyber threat intelligence about what you're looking for and what your adversaries are likely interested in. Such intelligence can be used to great effect when employed properly and proactively against a threat group. Threat hunting has improved the accuracy of threat detection because we can now focus our searching on the adversaries exploiting our networks — humans hunting humans. Even with knowing where to look, tools are now being introduced to help make hunting more practical across an enterprise.

## **The Tap House** – *Philip Hagen*

Packets move pretty fast. The field of network forensics needs to move fast, too. Whether you are investigating a known incident, hunting unidentified adversaries in your environment, or enriching forensic findings from disk- and memory-based examinations, it's critical to stay abreast of the latest developments in the discipline. In this SANS@Night talk, Phil Hagen will discuss some of the latest technologies, techniques, and tools that you'll want to know about in pursuit of forensication nirvana. Phil is also an avid craft beer fan, so there's a good chance you'll also learn something about a new national beer or an interesting local one. This presentation will be helpful for everyone who wants to keep up-to-date on the most cutting-edge facets of network forensics.

# Build Your Best Career

WITH!

# SANS

Add an

**OnDemand Bundle & GIAC Certification Attempt\***

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

SPECIAL  
PRICING



## OnDemand Bundle

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

*“The course content and OnDemand delivery method have both exceeded my expectations.”*

-ROBERT JONES, TEAM JONES, INC.



## GIAC Certification

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

*“GIAC is the only certification that proves you have hands-on technical skills.”*

-CHRISTINA FORD, DEPARTMENT OF COMMERCE

## MORE INFORMATION

[www.sans.org/ondemand/bundles](http://www.sans.org/ondemand/bundles)

[www.giac.org](http://www.giac.org)





Security Awareness Training by the Most Trusted Source

## Computer-based Training for Your Employees

- End User** • Let employees train on their own schedule
- CIP v5** • Tailor modules to address specific audiences
- ICS Engineers** • Courses translated into many languages
- Developers** • Test learner comprehension through module quizzes
- Healthcare** • Track training completion for compliance reporting purposes



Visit SANS Securing The Human at  
[securingthehuman.sans.org](http://securingthehuman.sans.org)

**Change Human Behavior | Manage Risk | Maintain Compliance | Protect Your Brand**

**SANS**  
Technology  
Institute

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

### **Master's Degree Programs:**

- ▶ M.S. in Information Security Engineering
- ▶ M.S. in Information Security Management

### **Specialized Graduate Certificates:**

- ▶ Cybersecurity Engineering (Core)
  - ▶ Cyber Defense Operations
- ▶ Penetration Testing and Ethical Hacking
  - ▶ Incident Response

SANS Technology Institute, an independent subsidiary of SANS, is accredited by The Middle States Commission on Higher Education.  
3624 Market Street | Philadelphia, PA 19104 | 267.285.5000  
an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.



*Eligible for veterans education benefits!*

*Earn industry-recognized GIAC certifications throughout the program.*

Learn more at [www.sans.edu](http://www.sans.edu) | [info@sans.edu](mailto:info@sans.edu)



GI Bill® is a registered trademark of the U.S. Department of Veterans Affairs (VA).  
More information about education benefits offered by VA is available at the official U.S. government website at [www.benefits.va.gov/gibill](http://www.benefits.va.gov/gibill).

# SANS TRAINING FORMATS

## LIVE CLASSROOM TRAINING



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



**Community SANS** [www.sans.org/community](http://www.sans.org/community)  
*Live Training in Your Local Region with Smaller Class Sizes*



**Private Training** [www.sans.org/private-training](http://www.sans.org/private-training)  
*Live Onsite Training at Your Office Location. Both In-person and Online Options Available*



**Mentor** [www.sans.org/mentor](http://www.sans.org/mentor)  
*Live Multi-Week Training with a Mentor*



**Summit** [www.sans.org/summit](http://www.sans.org/summit)  
*Live IT Security Summits and Training*

## ONLINE TRAINING



**OnDemand** [www.sans.org/ondemand](http://www.sans.org/ondemand)  
*E-learning Available Anytime, Anywhere, at Your Own Pace*



**vLive** [www.sans.org/vlive](http://www.sans.org/vlive)  
*Online Evening Courses with SANS' Top Instructors*



**Simulcast** [www.sans.org/simulcast](http://www.sans.org/simulcast)  
*Attend a SANS Training Event without Leaving Home*



**OnDemand Bundles** [www.sans.org/ondemand/bundles](http://www.sans.org/ondemand/bundles)  
*Extend Your Training with an OnDemand Bundle Including Four Months of E-learning*

# FUTURE SANS TRAINING EVENTS

## SANSFIRE 2016

Washington, DC | Jun 11-18

## Digital Forensics & Incident Response SUMMIT & TRAINING 2016

Austin, TX | Jun 23-30

## Salt Lake City 2016

Salt Lake City, UT | Jun 27 - Jul 2

## Rocky Mountain 2016

Denver, CO | Jul 11-16

## Minneapolis 2016

Minneapolis, MN | Jul 18-23

## San Antonio 2016

San Antonio, TX | Jul 18-23

## San Jose 2016

San Jose, CA | Jul 25-30

## ICS Security Training – Houston 2016

Houston, TX | Jul 25-30

## Boston 2016

Boston, MA | Aug 1-6

## Security Awareness SUMMIT & TRAINING 2016

San Francisco, CA | Aug 1-10

## Portland 2016

Portland, OR | Aug 8-13

## Dallas 2016

Dallas, TX | Aug 8-13

## Data Breach Summit

Chicago, IL | Aug 18

## Chicago 2016

Chicago, IL | Aug 22-27

Information on all events can be found at  
[www.sans.org/security-training/by-location/all](http://www.sans.org/security-training/by-location/all)

# HOTEL INFORMATION

Training Campus

## Hilton Virginia Beach Oceanfront

3001 Atlantic Avenue  
Virginia Beach, VA 23451  
757-213-3000

[www.sans.org/event/virginia-beach-2016/location](http://www.sans.org/event/virginia-beach-2016/location)



### Special Hotel Rates Available

A special discounted rate of \$199.00 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 July 22, 2016. To make reservations please call (800) HILTONS (800-445-8667) and ask for the SANS group rate.

Due to a high demand for security training at SANS Virginia Beach 2016, the following courses will take place at the Hilton Garden Inn Virginia Beach Oceanfront: FOR585, ICS515, MGT414, SEC501, SEC503, and SEC575. The hotel is less than a five-minute walk from the Hilton Virginia Beach Oceanfront, and is accessible from both the Boardwalk and Atlantic Avenue. We thank you for your understanding in advance.

Training Campus

## Hilton Garden Inn Virginia Beach Oceanfront

3315 Atlantic Avenue  
Virginia Beach, VA 23451  
757-305-9000

[www.sans.org/event/virginia-beach-2016/location](http://www.sans.org/event/virginia-beach-2016/location)

### Special Hotel Rates Available

A special discounted rate of \$189.00 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 July 22, 2016. To make reservations please call (877)-STAYHGI (877-782-9444) and ask for the SANS group rate.

## SANS VIRGINIA BEACH 2016

# Registration Information

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



Register online at [www.sans.org/virginia-beach](http://www.sans.org/virginia-beach)

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.

## Pay Early and Save

Use code  
**EarlyBird16**  
when registering early

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	6-29-16	\$400.00	7-20-16	\$200.00

Some restrictions apply.

## SANS Voucher Program

**Expand your training budget!**

Extend your fiscal year. The SANS Voucher Program provides flexibility and may earn you bonus funds for training.

[www.sans.org/vouchers](http://www.sans.org/vouchers)

## Cancellation




You may substitute another person in your place at any time, at no charge, by e-mail: [registration@sans.org](mailto:registration@sans.org) or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by August 3, 2016 — 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)**

[www.sans.org/security-resources](http://www.sans.org/security-resources)