SANS

The Most Trusted Source for Information Security Training, Certification, and Research

GIAC CERTIFICATIONS

Security East 2020

New Orleans | February 1-8

NETWARS

Advance your career and protect your organization with cybersecurity training and GIAC certifications. Choose from **25+** hands-on, immersion style courses.

SAVE $300 Register and pay by **Dec 11th** Use code **EarlyBird20**

sans.org/security-east

"**SANS training is beyond valuable. You will learn skills and techniques that will help advance your personal career and protect your company. And you learn from the best instructors in the world who practice what they preach each day.**"

-Justin Bradshaw, **Wegmans**

Look inside for these new courses!

SEC450: **Blue Team Fundamentals: Security Operations and Analysis** | NEW!

MGT516: **Managing Security Vulnerabilities: Enterprise and Cloud** | NEW!

Courses at a Glance

For an up-to-date course list, please check the website at
www.sans.org/security-east/schedule

			GIAC CERTIFICATIONS	Page	Available via Simulcast	Bundle OnDemand with this course	Meets DoDD 8140 (8570) Requirements	Instructor	Security East 2020 Training Schedule: Sat 2-1 · Sun 2-2 · Mon 2-3 · Tue 2-4 · Wed 2-5 · Thu 2-6 · Fri 2-7 · Sat 2-8
CYBER DEFENSE	SEC301	Introduction to Cyber Security	GISF Information Security Fundamentals	10		●		Keith Palmgren	Mon–Fri
	SEC401	Security Essentials Bootcamp Style	GSEC Security Essentials	12	●	●	●	Bryan Simon	Mon–Sat
	SEC440	Critical Security Controls: Planning, Implementing, and Auditing		58		●		Randy Marchany	Sun–Mon
	SEC450	Blue Team Fundamentals: Security Operations and Analysis | **NEW!**		14		●		John Hubbard	Mon–Sat
	SEC455	SIEM Design & Implementation		58		●		John Hubbard	Sun–Mon
	SEC503	Intrusion Detection In-Depth	GCIA Intrusion Analyst	16	●	●	●	David Hoelzer	Mon–Sat
	SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling	GCIH Incident Handler	18	●	●	●	Joshua Wright	Mon–Sat
	SEC530	Defensible Security Architecture and Engineering	GDSA Defensible Security Architecture	20	●	●		Ismael Valenzuela	Mon–Sat
	SEC545	Cloud Security Architecture and Operations		22		●		Dave Shackleford	Mon–Fri
	SEC555	SIEM with Tactical Analytics	GCDA Detection Analyst	24	●	●		Mick Douglas	Mon–Sat
	SEC599	Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses	GDAT Defending Advanced Threats	26	●	●		Bryce Galbraith	Mon–Sat
PEN TESTING	SEC542	Web App Penetration Testing and Ethical Hacking	GWAPT Web Application Penetration Tester	30		●		Eric Conrad	Mon–Sat
	SEC560	Network Penetration Testing and Ethical Hacking	GPEN Penetration Tester	32		●		Jeff McJunkin	Mon–Sat
	SEC564	Red Team Exercises and Adversary Emulation		59				Jorge Orchilles	Sun–Mon
	SEC573	Automating Information Security with Python	GPYC Python Coder	34	●	●		Mark Baggett	Mon–Sat
	SEC580	Metasploit Kung Fu for Enterprise Pen Testing		59		●		Jeff McJunkin	Sun–Mon
	SEC642	Advanced Web App Pen Testing, Ethical Hacking, and Exploitation Techniques		36		●		Adrien de Beaupre	Mon–Sat
DFIR	FOR500	Windows Forensic Analysis	GCFE Forensic Examiner	38		●		Rob Lee	Mon–Sat
	FOR508	Advanced Incident Response, Threat Hunting, and Digital Forensics	GCFA Forensic Analyst	40	●	●	●	Hal Pomeranz	Mon–Sat
	FOR572	Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response	GNFA Network Forensic Analyst	42		●		Philip Hagen	Mon–Sat
	FOR578	Cyber Threat Intelligence	GCTI Cyber Threat Intelligence	44		●		Peter Szczepankiewicz	Mon–Fri
	FOR585	Smartphone Forensic Analysis In-Depth	GASF Advanced Smartphone Forensics	46	●	●		Heather Mahalik	Mon–Sat
MANAGEMENT	MGT414	SANS Training Program for CISSP® Certification	GISP Information Security Professional	48		●	●	Seth Misenar	Mon–Sat
	MGT415	A Practical Introduction to Cyber Security Risk Management		60				Russell Eubanks	Sun–Mon
	MGT514	Security Strategic Planning, Policy, and Leadership	GSTRT Strategic Planning, Policy, and Leadership	50		●		Mark Williams	Mon–Fri
	MGT516	Managing Security Vulnerabilities: Enterprise and Cloud | **NEW!**		52				David Hazar	Mon–Fri
DEV	SEC534	Secure DevOps: A Practical Introduction		60		●		Ben Allen	Sun–Mon
	SEC540	Cloud Security and DevOps Automation		54	●	●		Eric Johnson	Mon–Fri
ICS	ICS410	ICS/SCADA Security Essentials	GICSP Global Industrial Cyber Security Professional	56		●	●	Monta Elkins	Mon–Fri
NETWARS		Core NetWars Tournament		9				Jeff McJunkin	Thu–Fri
		Cyber Defense NetWars Tournament		9				Eric Conrad	Thu–Fri
		DFIR NetWars Tournament		9				Heather Mahalik, Philip Hagen	Thu–Fri

Contents

SANS Institute

The most trusted source for information security training, certification, and research

At the SANS Institute, our mission is to deliver the cutting-edge information security knowledge and skills that companies, military organizations, and governments need to protect their people and assets.

TRAINING ON THE CUTTING EDGE

SANS offers more than 65 unique courses, all designed to align with dominant security team roles, duties, and disciplines. Our courses prepare students to face today's threats and tomorrow's challenges.

The SANS curriculum spans the full range of cybersecurity fields including Cyber Defense, Penetration Testing & Ethical Hacking, Digital Forensics & Incident Response, Threat Hunting, Audit, Management, Critical Infrastructure and Control Systems Security, Secure Software Development, and more.

In SANS courses, students are immersed in hands-on lab exercises designed to help them practice, hone, and perfect what they've learned. And we constantly update and rewrite our courses to be sure the tools and techniques we're teaching are always current, and on the cutting edge.

LEARN FROM THE BEST

The SANS faculty is simply unmatched. All of our instructors are active security practitioners who bring their extensive knowledge and real-world experiences directly to the classroom.

SANS instructors work for high-profile organizations as red team leaders, CISOs, technical directors, and research fellows. In addition to their respected technical credentials, they're also expert teachers. Their passion for the topics they teach shines through, making the SANS classroom—both live and online—dynamic and effective.

GIAC CERTIFICATION

GIAC certifications are designed to ensure that students can apply their knowledge and skills in a real-world setting. More than 30 certifications align with SANS training courses, validating student mastery for professional use in critical, specialized InfoSec domains and job-specific roles. See **www.giac.org** for more information.

A TRAINING FORMAT FOR EVERY STUDENT

SANS holds more than 300 live training events around the world each year, so you can find a convenient time and place to take your course. These events provide an engaging learning environment and multiple opportunities to network with other security professionals and with SANS instructors and staff.

SANS training is also offered online, with several convenient options to suit your learning style. All of our online courses include at least four months of access to the course material, so students can revisit and rewind content anytime, anywhere.

RECOGNIZED AS A SUPERIOR INVESTMENT

Information security professionals from every member of the Fortune 100, and from small and mid-sized firms alike, say they return to SANS training again and again because they trust their training will result in practical and high-quality capabilities. SANS training is also embedded in government and military programs in the United States and allies around the world for the same reason.

Customer feedback drives our continuous effort to maintain the quality and impact of SANS training, so that we continue to deserve your trust.

THE SANS PROMISE

At the heart of everything we do is the SANS Promise: Students will be able to use their new skills as soon as they return to work.

REGISTER FOR SANS TRAINING

Learn more about SANS courses, and register online, at **www.sans.org**

The SANS suite of education resources for information security professionals includes:

SANS Training Live & Online

GIAC CERTIFICATIONS

SANS Technology Institute

SANS SECURITY AWARENESS

NETWARS EXPERIENCE

INTERNET STORM CENTER

CyberTalent

SANS Faculty

"SANS instructors are the best in the game. Their technical knowledge combined with presentation skills and real-world examples make for an unparalleled training experience. SANS rocks!"

-Chris Gergen, **Bank of North Dakota**

At SANS, our course authors and instructors are renowned cybersecurity experts who share their knowledge by drawing on their own their own real-world experiences and top-shelf curriculum. Industry professionals choose SANS training again and again, year after year, for access to these highly regarded experts.

There are only about 100 individuals in the world currently qualified as SANS Certified Instructors. Each is selected after proving his or her technical and teaching expertise through years of work and success. The instructors are the founders of international cybersecurity organizations, authors of best-selling books, and developers of the world's most advanced cyber ranges and Capture-the-Flag challenges. Many are regularly called upon to share their expertise with government and commercial organizations around the world.

In addition to their impressive résumés, every member of the SANS faculty is fully committed to providing the most comprehensive training possible. Our instructors do more than just stand in front of a classroom—they're present for their students every step of the way, with follow-ups, webcasts, mentoring, and more. Their goal is your success, and that dedication is what truly sets SANS training apart from all the rest.

Whether you train with SANS online or at one of our live events, we promise you'll be able to apply what you learn from these top-tier instructors as soon as you return to work.

Meet the SANS faculty:
www.sans.org/security-east/instructors

Securing **Approval** and **Budget** for Training

Packaging matters

Write a formal request

- All organizations are different, but because training requires a significant investment of both time and money, most successful training requests are made via a written document (short memo and/or a few Powerpoint slides) that justifies the need and benefit. Most managers will respect and value the effort.
- Provide all the necessary information in one place. In addition to your request, provide all the right context by including the summary pages on Why SANS?, the Training Roadmap, the instructor bio, and additional benefits available at our live events or online.

Clearly state the benefits

Be specific

- How does the course relate to the job you need to be doing? Are you establishing baseline skills? Transitioning to a more focused role? Decision-makers need to understand the plan and context for the decision.
- Highlight specifics of what you will be able to do afterwards. Each SANS course description includes a section titled "You Will Be Able To." Be sure to include this in your request so that you make the benefits clear. The clearer the match between the training and what you need to do at work, the better.

Set the context

Establish longer-term expectations

- Information security is a specialized career path within IT with practices that evolve as attacks change. Because of this, organizations should expect to spend 6%-10% of salaries to keep professionals current and improve their skills. Training for such a dynamic field is an annual, per-person expense—not a once-and-done item.
- Take a GIAC Certification exam to prove the training worked. Employers value the validation of skills and knowledge that a GIAC Certification provides. Exams are psychometrically designed to establish competency for related job tasks.
- Consider offering trade-offs for the investment. Many professionals build annual training expenses into their employment agreements even before joining a company. Some offer to stay for a year after they complete the training.

Build a **High-Performing** Security Organization

Based on our global research, SANS has identified effective strategies for building an information security group:

Use practical organizing principles to design your plan. Nearly all of the more complex frameworks may be reduced to a few simpler constructs, such as "Build and Maintain Defenses – Monitor and Detect Intrusion – Proactively Self-Assess – Respond to Incidents."

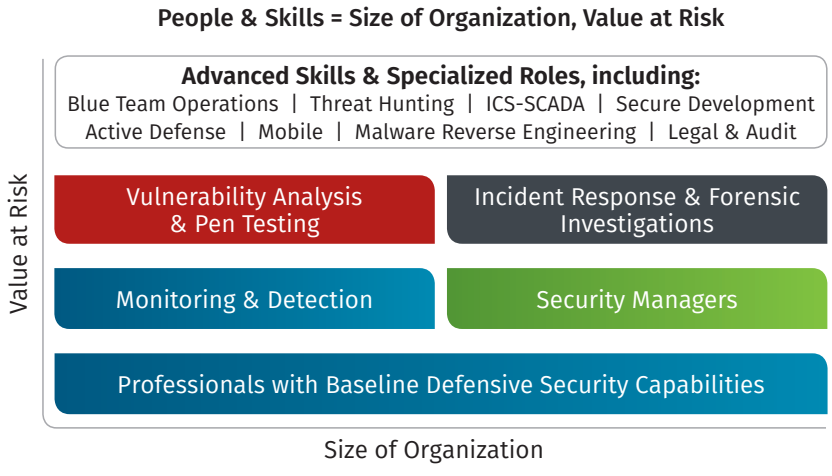
Prioritize your efforts within these areas, using the **Center for Internet Security Critical Controls**, as you mature your own organization.

Determine the number and types of professionals you need to perform the hands-on work, then **launch an ongoing campaign** to develop a team with the appropriate skills in mind. Cybersecurity is a specialized practice area within IT, and demands specialized training.

The job roles and skills required in information security grow and change as the organization scales. While every professional needs a baseline of knowledge and capabilities in cyber defense and incident response, over time you will develop specialized members of your team to work together in particular areas.

Four critical job roles typically emerge:

- **Security Monitoring & Detection Professionals –** Identifying security anomalies within your environment requires an increasingly sophisticated set of skills. All too often, vendor training teaches to the tool, without explaining how the tool works or how it can be best used. To deploy detection and monitoring tools and interpret their output, you need a more robust understanding of tools, techniques, and analysis.



- **Pen Testers & Vulnerability Analysts –** A professional who can find weaknesses is often a different breed than one focused exclusively on building defenses. A basic tenet of red team/blue team deployments is that finding vulnerabilities requires a different set of tools and a different way of thinking, but it's still essential in improving defenses.
- **Forensic Investigators & Incident Responders –** Larger organizations need specialized professionals who can move beyond first-level incident response. Whether you're maintaining a trail of evidence or hunting for threats, you need the skills to analyze attacks and develop appropriate remediation and recovery plans.
- **Security Managers –** As their staffs of talented technologists grow, organizations require effective leaders to manage them. These managers won't necessarily perform hands-on work, but they must understand enough about underlying technologies and frameworks to help set security strategy, develop appropriate policies, interact with their skilled practitioners, and measure outcomes.

Within (or beyond) these four areas, a high-performing security organization will purposefully develop its personnel to either be generalists who can engage in multiple tactics or specialists who deep dive into a critical niche. Along the entire spectrum from Active Defense to Cloud Defense, and from Python for InfoSec professionals to Malware Reengineering, SANS offers more than 30 courses to train for specialized roles or learn about more advanced topics, meeting the needs of security professionals at every level.

Training Roadmap | Development Paths

Key: Topic | Course Code | GIAC Certification | Essentials | ICS410 **ICS/SCADA Security Essentials** | GICSP | Course Title

Baseline Skills

New to Cyber Security — Concepts, Terms, and Skills

Security Fundamentals	SEC301 **Introduction to Cyber Security** | GISF

1 You are experienced in technology, but need to learn hands-on, essential security skills and techniques

Core Techniques — Prevent, Defend, Maintain

Every Security Professional Should Know

Security Essentials	SEC401 **Security Essentials Bootcamp Style** | GSEC
Hacker Techniques	SEC504 **Hacker Tools, Techniques, Exploits, and Incident Handling** | GCIH

All professionals entrusted with hands-on cybersecurity work should be trained to possess a common set of capabilities enabling them to secure systems, practice defense-in-depth, understand how attacks work, and manage incidents when they occur. To be secure, you should set a high bar for the baseline set of skills in your security organization.

Security Management — Managing Technical Security Operations

Every Security Manager Should Know

Leadership Essentials	MGT512 **Security Leadership Essentials for Managers** | GSLC
Critical Controls	SEC566 **Implementing and Auditing the Critical Security Controls – In-Depth** | GCCC

With an increasing number of talented technologists, organizations require effective leaders to manage their teams and processes. While managers will not necessarily perform hands-on work, they must know enough about the underlying technologies and frameworks to help set strategy, develop appropriate policies, interact with skilled practitioners, and measure outcomes.

Focus Job Roles

2 You are experienced in security, preparing for a specialized job role or focus

Monitoring & Detection — Intrusion Detection, Monitoring Over Time

Scan Packets & Networks

Intrusion Detection	SEC503 **Intrusion Detection In-Depth** | GCIA
Monitoring & Operations	SEC511 **Continuous Monitoring and Security Operations** | GMON

The detection of what is happening in your environment requires an increasingly sophisticated set of skills and capabilities. Identifying security anomalies requires increased depth of understanding to deploy detection and monitoring tools and to interpret their output.

Penetration Testing — Vulnerability Analysis, Ethical Hacking

Every Pen Tester Should Know

Networks	SEC560 **Network Penetration Testing and Ethical Hacking** | GPEN
Web Apps	SEC542 **Web App Penetration Testing and Ethical Hacking** | GWAPT

The professional who can find weakness is often a different breed than one focused exclusively on building defenses. A basic tenet of red team/blue team deployments is that finding vulnerabilities requires a different way of thinking, and different tools, but is essential for defense specialists to improve their defenses.

Incident Response & Threat Hunting — Host and Network Forensics

Every Forensics and IR Professional Should Know

Endpoint Forensics	FOR500 **Windows Forensic Analysis** | GCFE	FOR508 **Advanced Incident Response, Threat Hunting, and Digital Forensics** | GCFA
Network Forensics	FOR572 **Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response** | GNFA	

Whether you're seeking to maintain a trail of evidence on host or network systems, or hunting for threats using similar techniques, larger organizations need specialized professionals who can move beyond first-response incident handling in order to analyze an attack and develop an appropriate remediation and recovery plan.

CISSP® Training	MGT414 **SANS Training Program for CISSP® Certification** | GISP

Crucial Skills, Specialized Roles

SANS's comprehensive course offerings enable professionals to deepen their technical skills in key practice areas. The courses also address other topics and audiences, such as security training for software developers, industrial control engineers, and non-technical personnel in management, legal, and audit roles.

3 You are a candidate for specialized or advanced training

Cyber Defense Operations — Harden Specific Defenses

Specialized Defensive Area

OSINT	SEC487 **Open-Source Intelligence (OSINT) Gathering and Analysis**
Advanced Generalist	SEC501 **Advanced Security Essentials – Enterprise Defender** | GCED
Cloud Security	SEC545 **Cloud Security Architecture and Operations**
Windows/Powershell	SEC505 **Securing Windows and PowerShell Automation** | GCWN
Linux/Unix Defense	SEC506 **Securing Linux/Unix** | GCUX
SIEM	SEC555 **SIEM with Tactical Analytics** | GCDA

Other Advanced Defense Courses

Security Architecture	SEC530 **Defensible Security Architecture and Engineering** | GDSA
Threat Defense	SEC599 **Defeating Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses** | GDAT

Specialized Penetration Testing — Focused Techniques and Areas

In-Depth Coverage

Vulnerability Assessment	SEC460 **Enterprise Threat and Vulnerability Assessment** | GEVA
Networks	SEC660 **Advanced Penetration Testing, Exploit Writing, and Ethical Hacking** | GXPN
	SEC760 **Advanced Exploit Development for Penetration Testers**
Web Apps	SEC642 **Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques**
Mobile	SEC575 **Mobile Device Security and Ethical Hacking** | GMOB
Wireless	SEC617 **Wireless Penetration Testing and Ethical Hacking** | GAWN
Python Coding	SEC573 **Automating Information Security with Python** | GPYC

Digital Forensics, Malware Analysis, & Threat Intel — Specialized Investigative Skills

Malware Analysis

Malware Analysis	FOR610 **Reverse-Engineering Malware: Malware Analysis Tools and Techniques** | GREM

Threat Intelligence

Cyber Threat Intelligence	FOR578 **Cyber Threat Intelligence** | GCTI

Digital Forensics & Media Exploitation

Smartphones	FOR585 **Smartphone Forensic Analysis In-Depth** | GASF
Memory Forensics	FOR526 **Advanced Memory Forensics & Threat Detection**
Mac Forensics	FOR518 **Mac and iOS Forensic Analysis and Incident Response**

Advanced Management — Advanced Leadership, Audit, Legal

Management Skills

Planning, Policy, Leadership	MGT514 **Security Strategic Planning, Policy, and Leadership** | GSTRT
Project Management	MGT525 **IT Project Management, Effective Communication, and PMP® Exam Prep** | GCPM

Audit & Legal

Audit & Monitoring	AUD507 **Auditing & Monitoring Networks, Perimeters, and Systems** | GSNA
Law & Investigations	LEG523 **Law of Data Security and Investigations** | GLEG

Industrial Control Systems

ICS Security Professionals Need

Essentials	ICS410 **ICS/SCADA Security Essentials** | GICSP
ICS Defense & Response	ICS515 **ICS Active Defense and Incident Response** | GRID

NERC Protection

NERC Security Essentials	ICS456 **Essentials for NERC Critical Infrastructure Protection** | GCIP

Development and Secure Coding

Every Developer Should Know

Secure Web Apps	DEV522 **Defending Web Applications Security Essentials** | GWEB
Secure DevOps	SEC540 **Cloud Security and DevOps Automation**

Language-Specific Courses

JAVA/JEE	DEV541 **Secure Coding in Java/JEE: Developing Defensible Applications**
.NET	DEV544 **Secure Coding in .NET: Developing Defensible Applications**

See in-depth course descriptions and the digital version of this roadmap at:
www.sans.org/roadmap

To learn more about additional SANS courses, go to:
www.sans.org/courses

Extend and Validate Your Training

Special Pricing

Add an OnDemand Bundle OR GIAC Certification Attempt

to your course within seven days of this event to get bundle pricing.*

Extend Your Training Experience with an 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

OnDemand Bundle price – $799

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

-Robert Jones, Team Jones, Inc.

Get Certified with GIAC Certifications

- Distinguish yourself as an information security leader
- 30+ GIAC cybersecurity certifications available
- Two practice exams included
- Four months of access to complete the attempt
- Save over $1,100 when added to your SANS training

GIAC bundle price – $799

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

-Christina Ford, Department of Commerce

More Information

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

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

NETWARS TOURNAMENT

SECURITY EAST 2020

THURSDAY, FEBRUARY 6 & FRIDAY, FEBRUARY 7

Choose from:

- Core NetWars *ALL NEW!*
- Cyber Defense NetWars
- DFIR NetWars

Develop skills in:

- Cyber Defense
- Digital Forensics & Incident Response
- Malware Analysis
- Packet Analysis
- Penetration Testing

NetWars takes place in the evening, after class, and gives you an immediate opportunity to apply what you've learned in a fun and collaborative environment.

- Play solo or on a team of up to 5 players.
- Experience NetWars for free when taking a 4-, 5-, or 6-day course.
- Add NetWars when you register for your course, as seating is limited.

What Our Students Think

> *"NetWars takes the concepts in the class and gives you an opportunity to put them into action. Highly recommend!"*
> - Kyle McDaniel, Lenovo

> *"SANS NetWars should be a course requirement. Nothing instills the knowledge and skills from the classroom like it!"*
> - Frank DePaola, EnPro Industries

> *"Great experience. Fantastic learning."*
> - Shenshen Zhao, Verizon

> *"Learned a lot and had a lot of fun."*
> - Gustavo Bobbio, Amazon

sans.org/netwars

SEC301: **Introduction to Cyber Security**

GISF
Information Security Fundamentals
www.giac.org/gisf

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Communicate with confidence regarding information security topics, terms, and concepts
- Understand and apply the Principles of Least Privilege
- Understand and apply the Confidentiality, Integrity, and Availability (CIA) Triad
- Build better passwords that are more secure while also being easier to remember and type
- Grasp basic cryptographic principles, processes, procedures, and applications
- Understand computer network basics
- Have a fundamental grasp of any number of critical technical networking acronyms, including TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS
- Utilize built-in Windows tools to see your network settings
- Recognize and be able to discuss various security technologies, including anti-malware, firewalls, and intrusion detection systems, content filters, sniffers, etc.
- Build a simple but fully functional firewall configuration
- Secure your browser using a variety of security plug-ins
- Secure a wireless access point (also known as a wireless router)
- Scan for malware, clean malware from a system, and whitelist legitimate software identified by an anti-malware scanner as "potentially unwanted"
- Access a number of websites to better understand password security, encryption, phishing, browser security, etc.

To determine if SANS SEC301: Introduction to Cyber Security is right for you, ask yourself five simple questions:

- Do you have basic computer knowledge, but are new to cybersecurity and in need of an introduction to the fundamentals?
- Are you bombarded with complex technical security terms that you don't understand?
- Are you a non-IT security manager who lays awake at night worrying that your company will be the next mega-breach headline story on the 6 o'clock news?
- Do you need to be conversant in basic security concepts, principles, and terms, even if you don't need "deep in the weeds" detail?
- Have you decided to make a career change to take advantage of the job opportunities in cybersecurity and need formal training and certification?

If you answer yes to any of these questions, then the SEC301: Introduction to Cyber Security training course is for you. Students with a basic knowledge of computers and technology but no prior cybersecurity experience can jump-start their security education with insight and instruction from real-world security experts in SEC301.

This completely revised and comprehensive five-day course covers a wide range of baseline topics, including terminology, the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles. The hands-on, step-by-step learning format will enable you to grasp all the information presented even if some of the topics are new to you. You'll learn fundamentals of cybersecurity that will serve as the foundation of your security skills and knowledge for years to come.

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

"SEC301 is an extremely valuable course, even for someone with 12 years of IT experience!"

-Brian Pfau, **Banfield Pet Hospital**

Keith Palmgren
SANS Senior Instructor

Keith Palmgren is an IT security professional with over 30 years of experience specializing in the field. He began his career with the U.S. Air Force working with cryptographic keys and codes management. He also worked in what was at the time the newly-formed Air Force computer security department. Following the Air Force, Keith worked as an MIS director for a small company before joining AT&T/Lucent as a Senior Security Architect working on engagements with the Department of Defense and the National Security Agency. Later, as Security Consulting Practice Manager for both Sprint and Netigy, Keith built and ran the security consulting practice. He was responsible for all security consulting worldwide and for leading dozens of security professionals on many consulting engagements across all business spectrums. For the last several years, Keith has run his own company, NetIP, Inc. He divides his time between consulting, training, and freelance writing projects. In his career, Keith has trained over 10,000 IT professionals and authored more than 20 IT security training courses including the SANS SEC301 course. Keith currently holds 10 computer security certifications (CISSP®, GSEC, GCIH, GCED, GISF, CEH, Security+, Network+, A+, CTT+).
@kpalmgren

Course Day Descriptions

Mon, Feb 3 – Fri, Feb 7
9:00am – 5:00pm
Hands-on labs

DAY 1: Security's Foundation

Every good security practitioner and every good security program begins with the same mantra: learn the fundamentals. SEC301 starts by instilling familiarity with core security terms and principles. By the time you leave the classroom after the first day, you will fully understand the Principle of Least Privilege and Confidentiality, Integrity, Availability (CIA), and you'll see why those principles drive all security discussions. You will be conversant in the fundamentals of risk management, security policy, and authentication/authorization/accountability.

DAY 2: Computer Functions and Networking

This course day begins with an explanation of how computers handle numbers using decimal, binary, and hexadecimal numbering systems. It also provides an understanding of how computers encode letters using the American Standard Code for Information Interchange (ASCII). We then spend the remainder of the day on networking. All attacks or exploits have one thing in common: they take something that exists for perfectly valid reasons and misuse it in malicious ways. Always! So as security practitioners, to grasp what is invalid we must first understand what is valid – that is, how things like networks are supposed to work. Only once we have that understanding can we hope to understand the mechanics of malicious misuse of those networks – and only with that knowledge can we understand how security devices such as firewalls seek to thwart those attacks. The networking discussion begins with a non-technical explanation of how data move across a network. From there we move to fundamental terminology dealing with network types and standards. You'll learn about common network hardware such as switches and routers, and terms like "protocol" and "encapsulation." We'll give a very basic introduction to network addressing and port numbers and then work our way up the Open Systems Interconnection (OSI) protocol stack, introducing more detail only as we proceed to the next layer. In other words, we explain networking starting in non-technical terms and gradually progress to more technical detail as students are ready to take the next step. By the end of our discussions, you'll have a fundamental grasp of any number of critical technical networking acronyms that you've often heard but never quite understood, including TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS.

DAY 3: An Introduction to Cryptography

Cryptography is one of the most complex issues faced by security practitioners. It is not a topic you can explain in passing, so we will spend some time on it. Not to worry, we won't take you through the math behind cryptography. Instead, we learn basic crypto terminology and processes. What is steganography? What is substitution and transposition? What is a "work factor" in cryptography and why does it matter? What do we mean by symmetric and asymmetric key cryptography and "cryptographic hash," and why do you need to know? How are those concepts used together in the real world to create cryptographic systems?

DAY 4: Cyber Security Technologies – Part 1

Our fourth day in the classroom begins our exploration of cybersecurity technologies. We begin with wireless network security (WiFi and Bluetooth), and mobile device security (i.e., cell phones). We follow that with a brief look at some common attacks. We then move into a discussion of malware and anti-malware technologies. We end the day with an examination of several data protection protocols used for email encryption, secure remote access, secure web access, secure file transfer, and Virtual Private Network (VPN) technologies.

DAY 5: Cyber Security Technologies – Part 2

The final day of our SEC301 journey continues the discussion of cybersecurity technologies. The day begins by looking at several security technologies, including compartmentalization, firewalls, Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS), sniffers, content filters, etc. We then take a good look at browser and web security, and the difficulties of securing the web environment. For example, students will understand why and how their browser connects to anywhere from 5 to 100 different Internet locations each time they load a single web page. We end the day with a look at system security, including hardening operating systems, patching, virtual machines, cloud computing, and backup.

Who Should Attend

- Anyone new to cybersecurity and in need of an introduction to the fundamentals of security
- Those who feel bombarded with complex technical security terms they don't understand, but want to understand
- Non-IT security managers who deal with technical issues and understand them and who worry their company will be the next mega-breach headline story on the 6 o'clock news
- Professionals with basic computer and technical knowledge in all disciplines who need to be conversant in basic security concepts, principles, and terms, but who don't need "deep in the weeds" detail
- Those who have decided to make a career change to take advantage of the job opportunities in cybersecurity and need formal training and certification

"SEC301 is a great class for the individual who wants to learn an extensive amount of material in one week."

-Steven Chovanec,
Discover Financial Services

SEC401: **Security Essentials Bootcamp Style**

GSEC
Security Essentials
www.giac.org/gsec

6 Day Program	46 CPEs	Laptop Required

You Will Be Able To

- Apply what you learned directly to your job when you go back to work
- Design and build a network architecture using VLANs, NAC, and 802.1x based on advanced persistent threat indicators of compromise
- Run Windows command line tools to analyze the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat, etc.) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Install VMWare and create virtual machines to create a virtual lab to test and evaluate tools/security of systems
- Create an effective policy that can be enforced within an organization and design a checklist to validate security and create metrics to tie into training and awareness
- Identify visible weaknesses of a system using various tools and, once vulnerabilities are discovered, cover ways to configure the system to be more secure
- Build a network visibility map that can be used for hardening of a network – validating the attack surface and covering ways to reduce that surface by hardening and patching
- Sniff open protocols like telnet and ftp and determine the content, passwords, and vulnerabilities using WireShark

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.

Is SEC401: Security Essentials Bootcamp Style the right course for you?

STOP and ask yourself the following questions:

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

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

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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

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

Bryan Simon
SANS Principal Instructor

Bryan Simon is an internationally recognized expert in cybersecurity who 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 13 GIAC Certifications including the GSEC, GCWN, GCIH, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, GCUX, GISF, and GMON. 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. In addition to teaching SEC401, Bryan teaches SEC501: Advanced Security Essentials – Enterprise Defender; SEC505: Securing Windows and Powershell Automaton; and SEC511: Continuous Monitoring and Security Operations.
@BryanOnSecurity

Course Day Descriptions

Mon, Feb 3 – Sat, Feb 8
9:00am – 7:00pm (Days 1-5)
9:00am – 5:00pm (Day 6)
Evening bootcamp sessions; hands-on labs

This course is available via **Simulcast**. See page 64 for more information.

DAY 1: Network Security Essentials

A key way that attackers gain access to a company's resources is through a network connected to the Internet. A company wants to try to prevent as many attacks as possible, but in cases where it cannot prevent an attack, it must detect it in a timely manner. Therefore, an understanding and ability to create and identify the goals of building a defensible network architecture are critical. It is just as important to know and understand the architecture of the system, types of designs, communication flow and how to protect against attacks using devices such as routers and firewalls. These essentials, and more, will be covered during this first day in order to provide a firm foundation for the following days of training.

Topics: Defensible Network Architecture; Virtualization and Cloud Security; Network Device Security; Networking and Protocols; Securing Wireless Networks; Securing Web Communications

DAY 2: Defense-In-Depth and Attacks

To secure an enterprise network, you must understand the general principles of network security. On this second course day, we look at threats to our systems and take a "big picture" look at how to defend against them. You will learn that protections need to be layered – a principle called defense-in-depth. We explain some principles that will serve you well in protecting your systems. You will also learn about key areas of network security.

Topics: Defense-in-Depth; Access Control and Password Management; Security Policies; Critical Controls; Malicious Code and Exploit Mitigations; Advanced Persistent Threat (APT)

DAY 3: Threat Management

Whether targeting a specific system or just searching the Internet for an easy target, an attacker uses an arsenal of tools to automate finding new systems, mapping out networks, and probing for specific, exploitable vulnerabilities. This phase of an attack is called reconnaissance, and it can be launched by an attacker any amount of time before exploiting vulnerabilities and gaining access to systems and networks. In fact, evidence of reconnaissance activity can be a clue that a targeted attack is on the horizon.

Topics: Vulnerability Scanning and Penetration Testing; Network Security Devices; Endpoint Security; SIEM/Log Management; Active Defense

DAY 4: Cryptography, Risk Management, and Response

There is no silver bullet when it comes to security. However, there is one technology that would help solve a lot of security issues, though few companies deploy it correctly. This technology is cryptography. Concealing the meaning of a message can prevent unauthorized parties from reading sensitive information. This course section looks at various aspects of encryption and how it can be used to secure a company's assets. A related area called steganography, or information hiding, is also covered.

Topics: Cryptography; Cryptography Algorithms and Deployment; Applying Cryptography; Incident Handling and Response; Contingency Planning – BCP/DRP; IT Risk Management

DAY 5: Windows Security

Remember when Windows was simple? Windows XP desktops in a little workgroup...what could be easier? A lot has changed over time. Now, we have Windows tablets, Azure, Active Directory, PowerShell, Office 365, Hyper-V, Virtual Desktop Infrastructure (VDI), and so on. Microsoft is battling Google, Apple, Amazon.com, and other cloud giants for supremacy. The trick is to do it securely, of course. Windows is the most widely-used and targeted operating system on the planet. At the same time, the complexities of Active Directory, PKI, BitLocker, AppLocker, and User Account Control represent both challenges and opportunities. This section will help you quickly master the world of Windows security while showing you the tools that can simplify and automate your work. You will complete the day with a solid grounding in Windows security by looking at automation, auditing and forensics.

Topics: Windows Security Infrastructure; Service Packs, Hot Fixes, and Backups; Windows Access Controls; Enforcing Security Policy; Securing Windows Network Services; Automation, Auditing, and Forensics

DAY 6: Linux Security

While organizations do not have as many Unix/Linux systems, those that they do have are often some of the most critical systems that need to be protected. This final course day provides step-by-step guidance to improve the security of any Linux system. The course combines practical "how to" instructions with background information for Linux beginners, as well as security advice and best practices for administrators of all levels of expertise. This module discusses the foundational items that are needed to understand how to configure and secure a Linux system. It also provides an overview of the operating system and mobile markets. To lay a foundation, it provides an overview of the different operating systems that are based on Linux.

Topics: Linux Security: Structure, Permissions and Access; Hardening and Securing Linux Services; Monitoring and Attack Detection; Security Utilities

Who Should Attend

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

"SEC401 provided a vast library of information on developing a strong security posture, and in the course of the training, my brain shifted into a security-first gear thanks to the intense and deep exposure to the multitudinous recommendations for securing an organization's network and data."

-Laura Farvour, **University of Minnesota**

SEC450: **Blue Team Fundamentals: Security Operations and Analysis** | **NEW!**

6 Day Program | 35 CPEs | Laptop Required

You Will Be Able To

- Step into a Security Operations Center or cyber defense role with confidence
- Perform high-quality alert triage and investigation, free of bias and common mistakes
- Understand the most important protocols like DNS, HTTP(S), SMTP, ICMP, SMB, SSH, and more
- Use these protocols to identify malicious and anomalous traffic in your network, employing both heuristics and traffic content analysis
- Understand how logs are collected, parsed, enriched, and interpreted using a SIEM system
- Contain intrusions in both the short and long terms by picking the best tools for the job
- Use all the tools common to security operations – SIEMs, threat intelligence platforms, incident management systems, and automation
- Inspect and identify malicious files in a secure way
- Utilize network monitoring and tactical event logging to catch attacks before they become a problem
- Understand mental models for attack and defense to quickly evaluate any given situation
- Understand the technology, roles, and process required for efficient security operations
- Understand what it takes to defend a modern network
- Have a long and successful career as a cyber defender

Is your organization looking for a quick and effective way to onboard new security analysts, engineers, and architects? Do your Security Operations Center (SOC) managers need additional technical perspective on how to improve analysis quality, reduce turnover, and run an efficient SOC?

SEC450 is an accelerated on-ramp for new cyber defense team members and SOC managers. This course introduces students to the tools common to a defender's work environment, and packs in all the essential explanations of tools, processes, and data flow that every blue team member needs to know.

Students will learn the stages of security operations: how data are collected, where they are collected, and how threats are identified within those data. The class dives deep into tactics for triage and investigation of events that are identified as malicious, as well as how to avoid common mistakes and perform continual high-quality analysis. Students will learn the inner workings of the most popular protocols, and how to identify weaponized files as well as attacks within the hosts and data on their network.

The course employs practical, hands-on instruction using a simulated SOC environment with a real, fully-integrated toolset that includes:

- Security Information and Event Management (SIEM)
- An incident tracking and management system
- A threat intelligence platform
- Packet capture and analysis
- Automation tools

While cyber defense can be a challenging and engaging career, many SOCs are negatively affected by turnover. To preemptively tackle this problem, this course also presents research-backed information on preventing burnout and how to keep engagement high through continuous growth, automation, and false positive reduction. Students will finish the course with a full-scope view of how collection and detection work, how SOC tools are used and fit together, and how to keep their SOC up and running over the long term.

"I was able to use the information presented in the morning, during a work call at lunch, on day 1! The course paid for itself on the first day."

-Lawrence Nunn, **ARCYBER**

John Hubbard
SANS Certified Instructor

John Hubbard is a Security Operations Center (SOC) consultant and speaker, and the course author of SEC450 and SEC455. Additionally, John is an instructor for SANS blue team courses such as SEC511 and SEC555. Through his years of experience as a Lead Cyber Security Analyst and SOC Manager for GlaxoSmithKline, John developed real-world, first-hand knowledge of what it takes to defend an organization against advanced cyber-attacks. Today, John specializes in security operations, threat hunting, network security monitoring, SIEM design and optimization, and constructing defensible networks that allow organizations to protect their most sensitive data. John's mission to improve blue teams worldwide led him to partner with SANS to help develop the next generation of defensive talent around the world. John holds a bachelor's degree is in electrical engineering from Purdue University and a master's degree in computer engineering, focusing on information security, from SUNY Binghamton. In his free time, John enjoys FPV drone racing, coffee roasting, and slowing turning his home into a data center.
@SecHubb

Course Day Descriptions

Mon, Feb 3 – Sat, Feb 8
9:00am – 5:00pm
Hands-on labs

DAY 1: Blue Team Tools and Operations

This day starts with an introduction to the blue team, the mission of a SOC, and how to understand an organization's threat model and risk appetite. It is focused on top-down learning to explain the mindset of an analyst, the workflow, and monitoring tools used in the battle against attackers. Throughout this course day students will learn how SOC information management tools fit together, including incident management systems, threat intelligence platforms, SIEMs, and SOAR tools. We end the day describing the various groups of attackers, how their methods differ, and their motivations.

Topics: Introduction to the Blue Team Mission; SOC Overview; Defensible Network Concepts; Events, Alerts, Anomalies, and Incidents; Incident Management Systems; Threat Intelligence Platforms; SIEM; Automation and Orchestration; Who Are Your Enemies?

DAY 2: Understanding Your Network

Day 2 begins the technical journey of understanding the environment. To defend a network, you must thoroughly understand its architecture and the impact that it will have on analysis. This day introduces the concepts of a modern organization's network traffic flow by dissecting a basic home Internet connection and describing the features necessary for segmentation and monitoring. These modules ensure that students have a firm grasp on how network design affects their "view of the world" as an analyst. We then go in-depth on common network services. Day 2 provides thorough working explanations of the current and upcoming features of DNS, HTTP(S), SMTP, and more, with a focus on the most important points for analysts to understand. These sections explain what normal data look like, as well as the common fields and areas that are used to spot anomalous behavior. The focus will be on quickly recognizing the common tricks used by attackers to turn these everyday services against us.

Topics: Corporate Network Architecture; Traffic Capture and Visibility; Understanding DNS; DNS Analysis and Attacks; Understanding HTTP and HTTPS; Analyzing HTTP for Suspicious Activity; How SMTP and Email Attacks Work; Additional Important Protocols

Who Should Attend

- Security analysts
- Incident investigators
- Security engineers and architects
- Technical security managers
- SOC managers looking to gain additional technical perspective on how to improve analysis quality, reduce turnover, and run an efficient SOC
- Anyone looking to start their career on the blue team

DAY 3: Understaning Endpoints, Logs, and Files

It is extremely difficult to succeed at cyber defense without knowing where and how your data are produced, so day 3 takes us down to the host, logging, and file level. Starting with a survey of common endpoint-based attack tactics, we orient students to the array of techniques that are used against their hosts. These first sections, followed by a section on defense in-depth, will give students an idea of how each step of the attack lifecycle aligns with its defensive tools, and what students can use to prevent and detect adversary attack advancement on their endpoints. The course day then turns to the parsing and enrichment of logs, as well as how the SIEM normalization and categorization processes work. These topics give a complete view of what happens from the moment a log is generated to when it shows up in our security tools. The final part of day 3 provides students with the concepts needed to reason through the answer, diving into files at the byte level. Students will finish this day understanding how different common file formats work, how they are typically weaponized, and how to quickly decide whether or not a given sample is likely to be malicious.

Topics: Endpoint Attack Tactics; Endpoint Defense In-Depth; How Windows Logging Works; How Linux Logging Works; Interpreting Important Events; Kerberos and Active Directory Events; Log Collection, Parsing, and Normalization; Files Contents and Identification; Identifying and Handling Suspicious Files

DAY 4: Triage and Analysis

Now that the course has covered the ground required to understand the tools and data most frequently encountered by analysts, it's time to focus on analysis itself. This day will focus on how the analysis process works and explain how to avoid the common mistakes new analysts can slip into. We can combat the tendency to overlook the obvious by examining how our memory perception affects analysis and how cognitive biases cause us to fail to see what is right in front of us. The goal is to teach students not only how to think clearly, but also how to explain and leave a trail of how they reached their conclusions that can support future analysis and act as an audit trail. In addition, we will cover many of the mental models and concepts used in information security from both the offensive and defensive perspectives. Students will then use these models to look at an alert queue and get a quick and intuitive understanding of which alerts may pose the biggest threat, and thus must be attended to first. Safe analysis techniques and operational security concerns are covered to ensure that we do not give up our tactical advantage during the investigation process. We'll discuss specifics on alert triage methods and prioritization, as well as investigation techniques, so that students will leave this day better prepared to understand their alert queues and perform error-free investigation.

Topics: Alert Triage and Prioritization; Perception and Investigation; Memory and Investigation; Mental Models for Information Security; Structured Analysis Techniques; Analysis Tactics and OPSEC; Network, File, and Event Alerts; Intrusion Discovery; Incident Closing and Quality Review

DAY 5: Continuous Improvement, Analytics, and Automation

This day focuses squarely on improving the efficiency and enthusiasm of working in SOCs by tackling the most common problems head on. Through process optimization, careful analytic design and tuning, and workflow efficiency improvements, we can eliminate many of these common pain points. This frees us from the repetitive work we loathe and allows us to focus on what we do best – analysis! Having the time for challenging and novel work leads to a virtuous cycle of growth and engagement throughout the SOC – while improving everyone's life in the process. This day will focus on tuning your tools using clever analysis techniques and process automation to remove the monotonous and non-value-added activities from your day. We also cover containment activities, including the tools you can use and how to decide how to halt a developing incident or infection from the host or network angle. We'll wrap up the day with recommendations on skill growth, long-term career development, and how to get more involved in the cyber defense community.

Topics: Improving Life in the SOC; Analytic Features and Enrichment; New Analytic Design, Testing, and Sharing; Tuning and False Positive Reduction; Automation and Orchestration; Improving Operational Efficiency and Workflow; Containing Identified Intrusions; Skill and Career Development

DAY 6: Capstone: Defend the Flag

The course culminates in a team-based design, detect, and defend the flag competition. Powered by NetWars, day six provides a full day of hands-on work applying the principles taught throughout the week. Your team will be challenged to progress through multiple levels and missions designed to ensure mastery of the concepts and data covered during the course.

SEC503: **Intrusion Detection In-Depth**

GCIA
Intrusion Analyst
www.giac.org/gcia

6	46	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Configure and run open-source Snort and write Snort signatures
- Configure and run open-source Bro to provide a hybrid traffic analysis framework
- Understand TCP/IP component layers to identify normal and abnormal traffic
- Use open-source traffic analysis tools to identify signs of an intrusion
- Comprehend the need to employ network forensics to investigate traffic to identify and investigate a possible intrusion
- Use Wireshark to carve out suspicious file attachments
- Write tcpdump filters to selectively examine a particular traffic trait
- Craft packets with Scapy
- Use the open-source network flow tool SiLK to find network behavior anomalies
- Use your knowledge of network architecture and hardware to customize placement of IDS sensors and sniff traffic off the wire

SEC503 is one of the most important courses that you will take in your information security career. While past students describe it as the most difficult class they have ever taken, they also tell us it was the most rewarding. This course isn't for people who are simply looking to understand alerts generated by an out-of-the-box Intrusion Detection System (IDS). It's for people who want to deeply understand what is happening on their network today, and who suspect that there are very serious things happening right now that none of their tools are telling them about. If you want to be able to find zero-day activities on your network before disclosure, this is definitely the class for you.

What sets this course apart from any other training is that we take a bottom-up approach to teaching network intrusion detection and network forensics. Rather than starting with a tool and teaching you how to use that tool in different situations, this course teaches you how and why TCP/IP protocols work the way they do. After spending the first two days examining what we call "Packets as a Second Language," we add in common application protocols and a general approach to researching and understanding new protocols. With this deep understanding of how network protocols work, we turn our attention to the most widely used tools in the industry to apply this deep knowledge. The result is that you will leave this class with a clear understanding of how to instrument your network and the ability to perform detailed incident analysis and reconstruction.

These benefits alone make this training completely worthwhile. What makes the course as important as we believe it is (and students tell us it is), is that we force you to develop your critical thinking skills and apply them to these deep fundamentals. This results in a much deeper understanding of practically every security technology used today.

Mark Twain said, "It is easier to fool people than to convince them that they've been fooled." Too many IDS/IPS solutions provide a simplistic red/green, good/bad assessment of traffic, and too many untrained analysts accept that feedback as the absolute truth. This course emphasizes the theory that a properly trained analyst uses an IDS alert as a starting point for examination of traffic, not as a final assessment. SEC503 imparts the philosophy that the analyst must have access and the ability to examine the alerts to give them meaning and context. You will learn to investigate and reconstruct activity to deem if it is noteworthy or a false indication.

"SEC503 has changed my view on my network defense tools and the need to correlate data through multiple tools. The course is outstanding!"

-Ben Clark, **EY LLP**

David Hoelzer
SANS Faculty Fellow

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

Course Day Descriptions

Mon, Feb 3 – Sat, Feb 8
9:00am – 7:00pm (Days 1-5)
9:00am – 5:00pm (Day 6)
Evening bootcamp sessions; hands-on labs

This course is available via **Simulcast**. See page 64 for more information.

DAY 1: Fundamentals of Traffic Analysis – Part 1

Day 1 begins our bottom-up coverage of the TCP/IP protocol stack, providing a refresher or introduction, depending on your background, to TCP/IP. This is the first step in what we think of as a "Packets as a Second Language" course. Students begin to be introduced to the importance of collecting the actual packets involved in attacks and are immediately immersed in low-level packet analysis. We will cover the essential foundations such as the TCP/IP communication model, theory of bits, bytes, binary and hexadecimal, and the meaning and expected behavior of every field in the IP header. Students are introduced to the use of open-source Wireshark and tcpdump tools for traffic analysis.

Topics: Concepts of TCP/IP; Introduction to Wireshark; Network Access/Link Layer: Layer 2; IP Layer: Layer 3

DAY 2: Fundamentals of Traffic Analysis – Part 2

Day 2 continues where the first section ended. Students will gain a deep understanding of the primary transport layer protocols used in the TCP/IP model. Two essential tools, Wireshark and tcpdump, are further explored, using advanced features to give you the skills to analyze your own traffic. The focus of these tools is to filter large-scale data down to traffic of interest using Wireshark display filters and tcpdump Berkeley Packet Filters. These are used in the context of our exploration of the TCP/IP transport layers covering TCP, UDP, and ICMP. Once again, we discuss the meaning and expected function of every header field, covering a number of modern innovations that have very serious implications for modern network monitoring, and we analyze traffic not just in theory and function, but from the perspective of an attacker and defender.

Topics: Wireshark Display Filters; Writing tcpdump Filters; TCP; UDP; ICMP; Real-World Analysis – Command Line Tools

DAY 3: Application Protocols and Traffic Analysis

Day 3 builds on the foundation of the first two sections of the course, moving into the world of application layer protocols. Students are introduced to the versatile packet crafting tool Scapy. This is a very powerful Python-based tool that allows for the manipulation, creation, reading, and writing of packets. Scapy can be used to craft packets to test the detection capability of an IDS/IPS, especially important when a new user-created IDS rule is added, for instance for a recently announced vulnerability. Various practical scenarios and uses for Scapy are provided throughout this section.

Topics: Scapy; Advanced Wireshark; Detection Methods for Application Protocols; DNS; Microsoft Protocols; HTTP(2)/TLS; SMTP; IDS/IPS Evasion Theory; Identifying Traffic of Interest

DAY 4: Network Monitoring: Signatures vs. Behaviors

The fundamental knowledge gained from the first three sections provides the foundation for deep discussions of modern network intrusion detection systems during section 4. Everything that students have learned so far is now synthesized and applied to designing optimized detection rules for Snort/Firepower, and this is extended even further with behavioral detection using Zeek. The day begins with a discussion on network architecture, including the features of intrusion detection and prevention devices, along with a discussion about options and requirements for devices that can sniff and capture the traffic for inspection. This section provides an overview of deployment options and considerations, and allows students to explore specific deployment considerations that might apply to their respective organizations.

Topics: Network Architecture; Introduction to IDS/IPS Analysis; Snort; Zeek

DAY 5: Network Traffic Forensics

Day 5 continues the trend of less formal instruction and more practical application in hands-on exercises. It consists of three major topics, beginning with practical network forensics and an exploration of data-driven monitoring vs. alert-driven monitoring, followed by a hands-on scenario that requires students to use all of the skills developed so far. The second topic continues the theme of data-driven analysis by introducing large-scale analysis and collection using NetFlow and IPFIX data.

Topics: Introduction to Network Forensics Analysis; Using Network Flow Records; Examining Command and Control Traffic; Analysis of Large pcaps

DAY 6: Advanced IDS Capstone Event

The course culminates with a fun, hands-on, score-server-based IDS challenge. Students compete as solo players or on teams to answer many questions that require using tools and theory covered in the first five sections. The challenge presented is based on hours of live-fire, real-world data in the context of a time-sensitive incident investigation. The challenge is designed as a "ride-along" event, where students are answering questions based on the analysis that a team of professional analysts performed of these same data.

Who Should Attend

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

"I got a deeper understanding of key topics from SEC503. This training will help me get more data out of my investigations."

-Alphonse Wichrowski, **Allegiant Air**

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

GCIH
Incident Handler
www.giac.org/gcih

6 Day Program	37 CPEs	Laptop Required

You Will Be Able To

- Apply incident handling processes in-depth, including preparation, identification, containment, eradication, and recovery, to protect enterprise environments
- Analyze the structure of common attack techniques in order to evaluate an attacker's spread through a system and network, anticipating and thwarting further attacker activity
- Utilize tools and evidence to determine the kind of malware used in an attack, including rootkits, backdoors, and trojan horses, choosing appropriate defenses and response tactics for each
- Use built-in command-line tools such as Windows tasklist, wmic, and reg as well as Linux netstat, ps, and lsof to detect an attacker's presence on a machine
- Analyze router and system ARP tables along with switch CAM tables to track an attacker's activity through a network and identify a suspect
- Use memory dumps and the Volatility tool to determine an attacker's activities on a machine, the malware installed, and other machines the attacker used as pivot points across the network
- Gain access to a target machine using Metasploit, and then detect the artifacts and impacts of exploitation through process, file, memory, and log analysis
- Analyze a system to see how attackers use the Netcat tool to move files, create backdoors, and build relays through a target environment
- Run the Nmap port scanner and Nessus vulnerability scanner to find openings on target systems, and apply tools such as tcpdump and netstat to detect and analyze the impacts of the scanning activity

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection and 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.

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 them. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a hands-on workshop that focuses on scanning, exploiting, and defending systems. This course 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.

"The training offered at SANS is the best in the industry, and the SEC504 course is a must for any IT security professional – highly recommended."

-Michael Hoffman, **Shell Oil Products US**

"SEC504 is the essential cert course needed to trust if a candidate is valuable enough to do incident response."

-Troy Merritt, **Blueshield of CA**

Joshua Wright
SANS Senior Instructor

Joshua Wright is a senior technical analyst with Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through his experiences as a penetration tester, Josh has worked with hundreds of organizations on attacking and defending mobile devices and wireless systems, ethically disclosing significant product and protocol security weaknesses to well-known organizations. As an open-source software advocate, Josh has conducted cutting-edge research resulting in several software tools that are commonly used to evaluate the security of widely deployed technology targeting WiFi, Bluetooth, and ZigBee wireless systems, smart grid deployments, and the Android and Apple iOS mobile device platforms. As the technical lead of the innovative CyberCity, Josh also oversees and manages the development of critical training and educational missions for cyber warriors in the U.S. military, government agencies, and critical infrastructure providers. **@joswr1ght**

Course Day Descriptions

Mon, Feb 3 – Sat, Feb 8
9:00am – 7:15pm (Day 1)
9:00am – 5:00pm (Days 2-6)
Extended hours; hands-on labs

This course is available via **Simulcast**. See page 64 for more information.

DAY 1: Incident Handling Step-by-Step and Computer Crime Investigation

The first part of this section looks at the invaluable Incident Handling Step-by-Step Model, which was created through a consensus process involving experienced incident handlers from corporations, government agencies, and educational institutes, and has been proven effective in hundreds of organizations. This section is designed to provide students a complete introduction to the incident handling process, using the six steps (preparation, identification, containment, eradication, recovery, and lessons learned) necessary to prepare for and deal with a computer incident. The second part of this section examines from-the-trenches case studies to understand what does and does not work in identifying computer attackers. This section provides valuable information on the steps a systems administrator can take to improve the chances of catching and prosecuting attackers.

Topics: Preparation; Identification; Containment; Eradication; Recovery; Special Actions for Responding to Different Types of Incidents; Incident Record-Keeping; Incident Follow-Up

DAY 2: Computer and Network Hacker Exploits – Part 1

Seemingly innocuous data leaking from your network could provide the clue needed by an attacker to blow your systems wide open. This day-long course covers the details associated with reconnaissance and scanning, the first two phases of many computer attacks.

Topics: Reconnaissance; Scanning; Intrusion Detection System (IDS) Evasion; Enumerating Windows Active Directory Targets

DAY 3: Computer and Network Hacker Exploits – Part 2

Computer attackers are ripping our networks and systems apart in novel ways while constantly improving their techniques. This course day covers the third phase of many hacker attacks – gaining access. Attackers employ a variety of strategies to take over systems from the network level up to the application level. This section covers the attacks in depth, from the details of buffer overflow and format string attack techniques to the latest in session hijacking of supposedly secure protocols.

Topics: Physical-layer Attacks; Gathering and Parsing Packets; Operating System and Application-level Attacks; Netcat: The Attacker's Best Friend; Endpoint Security Bypass

DAY 4: Computer and Network Hacker Exploits – Part 3

This course day starts out by covering one of attackers' favorite techniques for compromising systems: worms. We will analyze worm developments over the last two years and project these trends into the future to get a feel for the coming Super Worms we will face. Then the course turns to another vital area often exploited by attackers: web applications. Because most organizations' homegrown web applications do not get the security scrutiny of commercial software, attackers exploit these targets using SQL injection, cross-site scripting, session cloning, and a variety of other mechanisms discussed in detail.

Topics: Password Cracking; Web Application Attacks; Denial of Service Attacks

DAY 5: Computer and Network Hacker Exploits – Part 4

This course day covers the fourth and fifth phases of many hacker attacks: maintaining access and covering their tracks. Computer attackers install backdoors, apply Rootkits, and sometimes even manipulate the underlying kernel itself to hide their nefarious deeds. Each of these categories of tools requires specialized defenses to protect the underlying system. In this course, we will analyze the most commonly used malicious code specimens and explore future trends in malware designed to obscure an attacker's presence and disguise attribution.

Topics: Maintaining Access; Covering the Tracks; Putting It All Together

DAY 6: Hacker Tools Workshop

Over the years, the security industry has become smarter and more effective in stopping hackers. Unfortunately, hacker tools are becoming smarter and more complex. One of the most effective methods to stop the enemy is to actually test the environment with the same tools and tactics an attacker might use against you. This workshop lets you put what you have learned over the past week into practice.

Topics: Hands-on Analysis

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
- General security practitioners and security architects who want to design, build, and operate their systems to prevent, detect, and respond to attacks

"I will almost always recommend SEC504 as a baseline so that everyone is speaking the same language. I want my sys-admins to take it, my network admins to take it, even my devs to take it, regardless of whether they're going to eventually move into an incident handling role. In my opinion it is the most critical, foundational class that SANS offers."

-Kevin Wilcox,
Information Security Specialist

SEC530: **Defensible Security Architecture and Engineering**

GDSA
Defensible Security Architecture
www.giac.org/gdsa

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Analyze a security architecture for deficiencies
- Apply the principles learned in the course to design a defensible security architecture
- Determine appropriate security monitoring needs for organizations of all sizes
- Maximize existing investment in security architecture by reconfiguring existing assets
- Determine capabilities required to support continuous monitoring of key Critical Security Controls
- Configure appropriate logging and monitoring to support a Security Operations Center and continuous monitoring program

Who Should Attend

- Security architects
- Network engineers
- Network architects
- Security analysts
- Senior security engineers
- System administrators
- Technical security managers
- CND analysts
- Security monitoring specialists
- Cyber threat investigators

SEC530: Defensible Security Architecture and Engineering is designed to help students build and maintain a truly defensible security architecture. "The perimeter is dead" is a favorite saying in this age of mobile, cloud, and the Internet of Things, and we are indeed living in new a world of "de-perimeterization" where the old boundaries of "inside" and "outside" or "trusted" and "untrusted" no longer apply.

This changing landscape requires a change in mindset, as well as a repurposing of many devices. Where does it leave our classic perimeter devices such as firewalls? What are the ramifications of the "encrypt everything" mindset for devices such as Network Intrusion Detection Systems?

In this course, students will learn the fundamentals of up-to-date defensible security architecture. There will be a heavy focus on leveraging current infrastructure (and investment), including switches, routers, and firewalls. Students will learn how to reconfigure these devices to better address the threat landscape they face today. The course will also suggest newer technologies that will aid in building a robust security infrastructure.

While this is not a monitoring course, it will dovetail nicely with continuous security monitoring, ensuring that security architecture not only supports prevention, but also provides the critical logs that can be fed into a Security Information and Event Management (SIEM) system in a Security Operations Center.

Hands-on labs will reinforce key points in the course and provide actionable skills that students will be able to leverage as soon as they return to work.

"As a systems programmer working on the development of security tools, the architectural content provided has been highly informative and extremely valuable."

-Merv Hammer, **Workday Inc.**

"SEC530 provided an excellent understanding of application attacks and how to protect against them."

-Shayne Douglass, **AMEWAS Inc.**

Ismael Valenzuela
SANS Certified Instructor

Ismael Valenzuela founded one of the first IT security consultancies in Spain and has participated as a security professional in numerous projects across the globe over the past 17 years. As a top cybersecurity expert with a strong technical background and deep knowledge of penetration testing, security architectures, intrusion detection and computer forensics, Ismael has provided security consultancy, advice and guidance to large government and private organizations, including major EU Institutions and U.S. government agencies. Prior to his current role as Principal Engineer at McAfee, where he leads research on threat hunting using machine-learning and expert-system-driven investigations, Ismael led the delivery of Security Operations Center, incident response and forensics services for the Foundstone Services team within Intel globally. Previously, Ismael worked as Global IT Security Manager for iSOFT Group Ltd, one of the world's largest providers of healthcare IT solutions, managing its security operations in more than 40 countries. He holds a bachelor's degree in computer science from the University of Malaga (Spain), has a certificate in business administration, and holds many professional certifications, including the highly regarded GIAC Security Expert (GSE #132) in addition to the GREM, GCFA, GCIA, GCIH, GPEN, GCUX, GCWN, GWAPT, GSNA, GMON, CISSP®, ITIL, CISM, and IRCA 27001 Lead Auditor from Bureau Veritas UK.
@aboutsecurity

Course Day Descriptions

Mon, Feb 3 – Sat, Feb 8
9:00am – 5:00pm
Hands-on labs

This course is available via **Simulcast**. See page 64 for more information.

DAY 1: Defensible Security Architecture and Engineering

Day 1 of the course describes hardening systems and networks at every layer, from layer one (physical) to layer seven (applications and data). To quote Richard Bejtlich's *The Tao of Network Security Monitoring*, defensible networks "encourage, rather than frustrate, digital self-defense." The section begins with an overview of traditional network and security architectures and their common weaknesses. The defensible security mindset is "build it once, build it right." All networks must perform their operational functions effectively, and security can be complementary to this goal. It is much more efficient to bake security in at the outset than to retrofit it later. The discussion will then turn to layer one (physical) and layer two (data link) best practices, including many "ripped from the headlines" tips the co-authors have successfully deployed in the trenches to harden the infrastructure in order to prevent and detect modern attacks. Examples include the use of private VLANs, which effectively kills the malicious client-to-client pivot, and 802.1X and NAC, which mitigate rogue devices. Specific Cisco IOS syntax examples are provided to harden switches.

Topics: Traditional Security Architecture Deficiencies; Defensible Security Architecture; Threat, Vulnerability, and Data Flow Analysis; Layer 1 Best Practices; Layer 2 Best Practices; Netflow

DAY 2: Network Security Architecture and Engineering

Day 2 continues hardening the infrastructure and moves on to layer three: routing. Actionable examples are provided for hardening routers, with specific Cisco IOS commands to perform each step. The section then continues with a deep dive on IPv6, which currently accounts for 23% of Internet backbone traffic, according to Google, while simultaneously being used and ignored by most organizations. This section will provide deep background on IPv6, discuss common mistakes (such as applying an IPv4 mindset to IPv6), and provide actionable solutions for securing the protocol. The section wraps up with a discussion of VPN and stateful layer three/four firewalls.

Topics: Layer 3: Router Best Practices; Layer 3 Attacks and Mitigation; Layer 2 and 3 Benchmarks and Auditing Tools; Securing SNMP; Securing NTP; Bogon Filtering, Blackholes, and Darknets; IPv6; Securing IPv6; VPN; Layer 3/4 Stateful Firewalls; Proxy

DAY 3: Network-Centric Security

Organizations own or have access to many network-based security technologies ranging from next-generation firewalls to web proxies and malware sandboxes. Yet the effectiveness of these technologies is directly affected by their implementation. Too much reliance on built-in capabilities like application control, antivirus, intrusion prevention, data loss prevention, or other automatic evil-finding deep packet inspection engines leads to a highly preventative-focused implementation, with huge gaps in both prevention and detection. Day 3 focuses on using application layer security solutions that an organization already owns with a modern mindset. By thinking outside the box, even old controls like a spam appliance can be used to catch modern attacks such as phishing via cousin domains and other spoofing techniques. And again, by engineering defenses for modern attacks, both prevention and detection capabilities gain significantly.

Topics: NGFW; NIDS/NIPS; Network Security Monitoring; Sandboxing; Encryption; Secure Remote Access; Distributed Denial-of-Service (DDOS)

DAY 4: Data-Centric Security

Organizations cannot protect something they do not know exists. The problem is that critical and sensitive data exist all over. Complicating this even more is that data are often controlled by a full application stack involving multiple services that may be hosted on-premise or in the cloud. Day 4 focuses on identifying core data where they reside and how to protect those data. Protection includes the use of data governance solutions and full application stack security measures such as web application firewalls and database activity monitoring, as well as keeping a sharp focus on securing the systems hosting core services such as on-premise hypervisors, cloud computing platforms, and container services such as Docker. The data-centric security approach focuses on what is core to an organization and prioritizes security controls around it. Why spend copious amounts of time and money securing everything when controls can be optimized and focused on securing what matters? Let's face it: Some systems are more critical than others.

Topics: Application (Reverse) Proxies; Full Stack Security Design; Web Application Firewalls; Database Firewalls/Database Activity Monitoring; File Classification; Data Loss Prevention (DLP); Data Governance; Mobile Device Management (MDM) and Mobile Application Management (MAM); Private Cloud Security; Public Cloud Security; Container Security

DAY 5: Zero-Trust Architecture: Addressing the Adversaries Already in Our Networks

Today, a common security mantra is "trust but verify." But this is a broken concept. Computers are capable of calculating trust on the fly, so rather than thinking in terms of "trust but verify" organizations should be implementing "verify then trust." By doing so, access can be constrained to appropriate levels at the same time that access can become more fluid. This section focuses on implementing a zero-trust architecture where trust is no longer implied but must be proven. By doing so, a model of variable trust can be used to change access levels dynamically. This, in turn, allows for implementing fewer or more security controls as necessary given a user's and a device's trust maintained over time. The focus is on implementing zero trust with existing security technologies to maximize their value and impact for an organization's security posture. During this section encryption and authentication will be used to create a hardened network, whether external or internal. Also, advanced defensive techniques will be implemented to stop modern attack tools in their tracks while leaving services fully functional for authorized assets.

Topics: Zero-Trust Architecture; Credential Rotation; Compromised Internal Assets; Securing the Network; Tripwire and Red Herring Defenses; Patching; Deputizing Endpoints as Hardened Security Sensors; Scaling Endpoint Log Collection/Storage/Analysis

DAY 6: Hands-On Secure-the-Flag Challenge

The course culminates in a team-based Design-and-Secure-the-Flag competition. Powered by NetWars, day six provides a full day of hands-on work applying the principles taught throughout the week. Your team will progress through multiple levels and missions designed to ensure mastery of the modern cyber defense techniques promoted throughout this course. Teams will assess, design, and secure a variety of computer systems and devices, leveraging all seven layers of the OSI model.

Topics: Capstone – Design/Detect/Defend

SEC545: **Cloud Security Architecture and Operations**

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Revise and build internal policies to ensure cloud security is properly addressed
- Understand all major facets of cloud risk, including threats, vulnerabilities, and impact
- Articulate the key security topics and risks associated with SaaS, PaaS, and IaaS cloud deployment models
- Evaluate Cloud Access Security Brokers (CASBs) to better protect and monitor SaaS deployments
- Build security for all layers of a hybrid cloud environment, starting with hypervisors and working to application layer controls
- Evaluate basic virtualization hypervisor security controls
- Design and implement network security access controls and monitoring capabilities in a public cloud environment
- Design a hybrid cloud network architecture that includes IPSec tunnels
- Integrate cloud identity and access management (IAM) into security architecture
- Evaluate and implement various cloud encryption types and formats
- Develop multi-tier cloud architectures in a Virtual Private Cloud (VPC), using subnets, availability zones, gateways, and NAT
- Integrate security into DevOps teams, effectively creating a DevSecOps team structure
- Build automated deployment workflows using Amazon Web Services and native tools
- Incorporate vulnerability management, scanning, and penetration testing into cloud environments

Dave Shackleford
SANS Senior Instructor

As more organizations move data and infrastructure to the cloud, security is becoming a major priority. Operations and development teams are finding new uses for cloud services, and executives are eager to save money and gain new capabilities and operational efficiency by using these services. But will information security prove to be an Achilles' heel? Many cloud providers do not provide detailed control information about their internal environments, and quite a few common security controls used internally may not translate directly to the public cloud.

SEC545: Cloud Security Architecture and Operations will tackle these issues one by one. We'll start with a brief introduction to cloud security fundamentals, then cover the critical concepts of cloud policy and governance for security professionals. For the rest of day one and all of day two, we'll move into technical security principles and controls for all major cloud types (SaaS, PaaS, and IaaS). We'll learn about the Cloud Security Alliance framework for cloud control areas, then delve into assessing risk for cloud services, looking specifically at technical areas that need to be addressed.

The course then moves into cloud architecture and security design, both for building new architectures and for adapting tried-and-true security tools and processes to the cloud. This will be a comprehensive discussion that encompasses network security (firewalls and network access controls, intrusion detection, and more), as well as all the other layers of the cloud security stack. We'll visit each layer and the components therein, including building secure instances, data security, identity and account security, and much more. We'll devote an entire day to adapting our offense and defense focal areas to the cloud. This will involve looking at vulnerability management and pen testing, as well as covering the latest and greatest cloud security research. On the defense side, we'll delve into incident handling, forensics, event management, and application security.

We wrap up the course by taking a deep dive into SecDevOps and automation, investigating methods of embedding security into orchestration, and every facet of the cloud life cycle. We'll explore tools and tactics that work, and even walk through several cutting-edge use cases where security can be automated entirely in both deployment and incident detection-and-response scenarios using APIs and scripting.

"SEC545 is excellent for cloud security understanding and overviews. I would definitely recommend this course for people looking at building a cloud security program."

-Justin Pyle, **Chan Zuckerberg Initiative**

Who Should Attend

- Security analysts
- Security architects
- Senior security engineers
- Technical security managers
- Security monitoring analysts
- Cloud security architects
- DevOps and DevSecOps engineers
- System administrators
- Cloud administrators

Dave Shackleford is the owner and principal consultant of Voodoo Security and a SANS analyst and course author. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering and is a VMware vExpert with extensive experience designing and configuring secure virtualized infrastructures. He has previously worked as CSO for Configuresoft, CTO for the Center for Internet Security, and as a security architect, analyst, and manager for several Fortune 500 companies. Dave is the author of the Sybex book *Virtualization Security: Protecting Virtualized Environments*, as well as the co-author of *Hands-On Information Security* from Course Technology. Recently Dave co-authored the first published course on virtualization security for the SANS Institute. Dave currently serves on the Board of Directors at the SANS Technology Institute and helps lead the Atlanta chapter of the Cloud Security Alliance.
@daveshackleford

Course Day Descriptions

Mon, Feb 3 – Fri, Feb 7
9:00am – 5:00pm
Hands-on labs

DAY 1: Cloud Security Foundations

The first day of the course starts out with an introduction to the cloud, including terminology, taxonomy, and basic technical premises. We also examine what is happening in the cloud today, and cover the spectrum of guidance available from the Cloud Security Alliance, including the Cloud Controls Matrix, the 14 major themes of cloud security, and other research available. Next we spend time on cloud policy and planning, delving into the changes an organization needs to make for security and IT policy to properly embrace the cloud. After all the legwork is done, we'll start talking about some of the main technical considerations for the different cloud models. We'll start by breaking down Software-as-a-Service (SaaS) and some of the main types of security controls available. A specialized type of Security-as-a-Service (SecaaS) known as Cloud Access Security Brokers (CASBs) will also be explained, with examples of what to look for in such a service. We'll wrap up with an introduction to Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) controls, which will set the stage for the rest of the course.

Topics: Introduction to the Cloud and Cloud Security Basics; Cloud Security Alliance Guidance; Cloud Policy and Planning; SaaS Security; Cloud Access Security Brokers; Intro to PaaS and IaaS Security Controls

DAY 2: Core Security Controls for Cloud Computing

The second day of SEC545 compares traditional in-house controls with those in the cloud today. Some controls are similar and mostly compatible, but not all of them. Since most cloud environments are built on virtualization technology, we walk through a short virtualization security primer, which can help teams building hybrid clouds that integrate with internal virtualized assets, and also help teams properly evaluate the controls cloud providers offer in this area. We'll then break down cloud network security controls and tradeoffs, since this is an area that is very different from what we've traditionally run in-house. For PaaS and IaaS environments, it's critical to secure virtual machines (instances) and the images we deploy them from, so we cover this next. At a high level, we'll also touch on identity and access management for cloud environments to help control and monitor who is accessing the cloud infrastructure, as well as what they're doing there. We also cover data security controls and types, including encryption, tokenization, and more. Specific things to look for in application security are laid out as the final category of overall controls. We then pull it all together to demonstrate how you can properly evaluate a cloud provider's controls and security posture.

Topics: Cloud Security: In-House versus Cloud; A Virtualization Security Primer; Cloud Network Security; Instance and Image Security; Identity and Access Management; Data Security for the Cloud; Application Security for the Cloud; Provider Security: Cloud Risk Assessment

DAY 3: Cloud Security Architecture and Design

Instead of focusing on individual layers of our cloud stack, we start day three by building the core security components. We'll break down cloud security architecture best practices and principles that most high-performing teams prioritize when building or adding cloud security controls and processes to their environments. We start with infrastructure and core component security – in other words, we need to look at properly locking down all the pieces and parts we covered on day two! This then leads to a focus on major areas of architecture and security design. The first is building various models of access control and compartmentalization. This involves breaking things down into two categories: identity and access management and network security. We delve into these in significant depth, as they can form the backbone of a sound cloud security strategy. We then look at architecture and design for data security, touching on encryption technologies, key management, and what the different options are today. We wrap up our third day with another crucial topic: availability. Redundant and available design is as important as ever, but we need to use cloud provider tools and geography to our advantage. At the same time, we need to make sure we evaluate the cloud provider's disaster recovery and continuity, and so this is covered as well.

Topics: Cloud Security Architecture Overview; Cloud Architecture and Security Principles; Infrastructure and Core Component Security; Access Controls and Compartmentalization; Confidentiality and Data Protection; Availability

DAY 4: Cloud Security – Offense and Defense

There are many threats to our cloud assets, so the fourth day of the course begins with an in-depth breakdown of the types of threats out there. We'll look at numerous examples. The class also shows students how to design a proper threat model focused on the cloud by using several well-known methods such as STRIDE and attack trees and libraries. Scanning and pen testing the cloud used to be challenging due to restrictions put in place by the cloud providers themselves. But today it is easier than ever. There are some important points to consider when planning a vulnerability management strategy in the cloud, and this class touches on how to best scan your cloud assets and which tools are available to get the job done. Pen testing naturally follows this discussion, and we talk about how to work with the cloud providers to coordinate tests, as well as how to perform testing yourself. On the defensive side, we start with network-based and host-based intrusion detection, and how to monitor and automate our processes to better carry out this detection. This is an area that has definitely changed from what we're used to in-house, so security professionals need to know what their best options are and how to get this done. Our final topics on day four include incident response and forensics (also topics that have changed significantly in the cloud). The tools and processes are different, so we need to focus on automation and event-driven defenses more than ever.

Topics: Threats to Cloud Computing; Vulnerability Management in the Cloud; Cloud Pen Testing; Intrusion Detection in the Cloud; Cloud IR and Event Management; Cloud Forensics

DAY 5: Cloud Security Automation and Orchestration

On our final day, we'll focus explicitly on how to automate security in the cloud, both with and without scripting techniques. We will use tools like the AWS CLI and AWS Lambda to illustrate the premises of automation, then turn our attention toward SecDevOps principles. We begin by explaining what that really means, and how security teams can best integrate into DevOps and cloud development and deployment practices. We'll cover automation and orchestration tools like Ansible and Chef, as well as how we can develop better and more efficient workflows with AWS CloudFormation and other tools. Continuing some of the topics from day four, we will look at event-driven detection and event management, as well as response and defense strategies that work. While we won't automate everything, some actions and scenarios really lend themselves to monitoring tools like CloudWatch, tagging assets for identification in security processes, and initiating automated response and remediation to varying degrees. We wrap up the class with a few more tools and tactics, followed by a sampling of real-world use cases.

Topics: Scripting and Automation in the Cloud; SecDevOps Principles; Creating Secure Cloud Workflows; Building Automated Event Management; Building Automated Defensive Strategies; Tools and Tactics; Real-World Use Cases; Class Wrap-Up

SEC555: **SIEM with Tactical Analytics**

GCDA
Detection Analyst
www.giac.org/gcda

6 Day Program | 46 CPEs | Laptop Required

You Will Be Able To

- Deploy the SANS SOF-ELK VM in production environments
- Demonstrate ways most SIEMs commonly lag current open-source solutions (e.g., SOF-ELK)
- Get up to speed on SIEM use, architecture, and best practices
- Know what type of data sources to collect logs from
- Deploy a scalable logs solution with multiple ways to retrieve logs
- Operationalize ordinary logs into tactical data
- Develop methods to handle billions of logs from many disparate data sources
- Understand best practice methods for collecting logs
- Dig into log manipulation techniques challenging many SIEM solutions
- Build out graphs and tables that can be used to detect adversary activities and abnormalities
- Combine data into active dashboards that make analyst review more tactical
- Utilize adversary techniques against them by using frequency analysis in large data sets
- Develop baselines of network activity based on users and devices
- Develop baselines of Windows systems with the ability to detect changes from the baseline
- Apply multiple forms of analysis such as long tail analysis to find abnormalities
- Correlate and combine multiple data sources to achieve more complete understanding
- Provide context to standard alerts to help understand and prioritize them

Mick Douglas
SANS Certified Instructor

Many organizations have logging capabilities but lack the people and processes to analyze them. In addition, logging systems collect vast amounts of data from a variety of data sources that require an understanding of those sources for proper analysis. This class is designed to provide students with the training, methods, and processes to enhance existing logging solutions. This class will also help you understand the when, what, and why behind the logs. This is a lab-heavy course that utilizes SOF-ELK, a SANS-sponsored free Security Information and Event Management (SIEM) solution, to provide hands-on experience and the mindset for large-scale data analysis.

Today, security operations do not suffer from a "Big Data" problem but rather a "Data Analysis" problem. Let's face it, there are multiple ways to store and process large amounts of data without any real emphasis on gaining insight into the information collected. Added to that is the daunting idea of an infinite list of systems from which one could collect logs. It is easy to get lost in the perils of data saturation. This class moves away from the typical churn-and-burn log systems and moves instead towards achieving actionable intelligence and developing a tactical Security Operations Center (SOC).

This course is designed to demystify the SIEM architecture and process by navigating the student through the steps of tailoring and deploying a SIEM to full SOC integration. The material will cover many bases in the "appropriate" use of a SIEM platform to enrich readily available log data in enterprise environments and extract actionable intelligence. Once the information is collected, the student will be shown how to present the gathered input into usable formats to aid in eventual correlation. Students will then iterate through the log data and events to analyze key components that will allow them to learn how rich this information is, how to correlate the data, how to start investigating based on the aggregate data, and finally, how to go hunting with this newly gained knowledge. They will also learn how to deploy internal post-exploitation tripwires and breach canaries to nimbly detect sophisticated intrusions. Throughout the course, the text and labs will not only show how to manually perform these actions, but also how to automate many of the processes mentioned so students can employ these tasks the day they return to the office.

The underlying theme is to actively apply Continuous Monitoring and analysis techniques by utilizing modern cyber threat attacks. Labs will involve replaying captured attack data to provide real-world results and visualizations.

"This course uses real-world events and hands-on training to allow me to immediately improve my organization's security stance. Day one back in the office I was implementing what I learned."

-Frank Giachino, **Bechtel**

Even when his job title has indicated otherwise, Mick Douglas has been doing information security work for over 10 years. He received a bachelor's degree in communications from Ohio State University. He is the managing partner for InfoSec Innovations. He is always excited for the opportunity to share with others so they do not have to learn the hard way! By studying with Mick, security professionals of all abilities will gain useful tools and skills that should make their jobs easier. When he's not "geeking out" you'll likely find Mick indulging in one of his numerous hobbies; photography, scuba diving, or hanging around in the great outdoors.
@BetterSafetyNet

Course Day Descriptions

Mon, Feb 3 – Sat, Feb 8
9:00am – 7:00pm (Days 1-5)
9:00am – 5:00pm (Day 6)
Evening bootcamp sessions; hands-on labs

This course is available via **Simulcast**. See page 64 for more information.

DAY 1: SIEM Architecture

This section will introduce free logging and analysis tools and focus on techniques to make sense of and augment traditional logs. It also covers how to handle the big data problem of handling billions of logs and how advances in free tools are starting to give commercial solutions a run for their money. Day one is designed to get them up to speed on SIEM concepts and to bring all students to a base level to carry them through the rest of the class. It is designed to also cover SIEM best practices. During day one we will be introducing Elasticsearch, Logstash, and Kibana within SOF-ELK and immediately go into labs to get students comfortable with ingesting, manipulating, and reporting on log data.

Topics: State of the SOC/SIEM; Log Monitoring; Logging Architecture; SIEM Platforms; Planning a SIEM; SIEM Architecture; Ingestion Techniques and Nodes; Data Queuing and Resiliency; Storage and Speed; Analytical Reporting

DAY 2: Service Profiling with SIEM

This section covers how to collect and handle this massive amount of data. Methods for collecting these logs through service logs such as from DNS servers will be covered, as will be passive ways of pulling the same data from the network itself. Techniques will be demonstrated to augment and add valuable context to the data as they are collected. Finally, analytical principles will be covered for finding the needles in the stack of needles. We will cover how, even if we have the problem of searching through billions of logs, we can surface only meaningful items of interest. Active dashboards will be designed to quickly find the logs of interest and to provide analysts with additional context for what to do next.

Topics: Detection Methods and Relevance to Log Analysis; Analyzing Common Application Logs that Generate Tremendous Amounts of Data; Applying Threat Intelligence to Generic Network Logs; Active Dashboards and Visualizations

Who Should Attend

- Security analysts
- Security architects
- Senior security engineers
- Technical security managers
- Security Operations Center analysts, engineers, and managers
- CND analysts
- Security monitoring specialists
- System administrators
- Cyber threat investigators
- Individuals working to implement Continuous Security Monitoring
- Individuals working in a hunt team capacity

DAY 3: Advanced Endpoint Analytics

The value in endpoint logs provides tremendous visibility in detecting attacks. In particular, with regard to finding post-compromise activity, endpoint logs can quickly become second to none. However, logs even on a single desktop can range in the tens if not hundreds of thousands of events per day. Multiply this by the number of systems in your environment and it is no surprise that organizations get overwhelmed. This section will cover the how and more importantly the why behind collecting system logs. Various collection strategies and tools will be used to gain hands-on experience and to provide simplification with handling and filtering the seemingly infinite amount of data generated by both servers and workstations. Workstation log strategies will be covered in depth due to their value in today's modern attack vectors. After all, modern-day attacks typically start and then spread from workstations.

Topics: Endpoint Logs

DAY 4: Baselining and User Behavior Monitoring

This section focuses on applying techniques to automatically maintain a list of assets and their configurations as well as methods to distinguish if they are authorized or unauthorized. Key locations to provide high-fidelity data will be covered and techniques to correlate and combine multiple sources of data together will be demonstrated to build a master inventory list. Other forms of knowing thyself will be introduced such as gaining hands-on experience in applying network and system baselining techniques. We will monitor network flows and identify abnormal activity such as C2 beaconing as well as look for unusual user activity. Finally, we will apply large data analysis techniques to sift through massive amounts of endpoint data. This will be used to find things such as unwanted persistence mechanisms, dual-homed devices, and more.

Topics: Identifying Authorized and Unauthorized Assets; Identifying Authorized and Unauthorized Software; Baseline Data

DAY 5: Tactical SIEM Detection and Post-Mortem Analysis

This section focuses on combining multiple security logs for central analysis. More importantly, we will cover methods for combining multiple sources to provide improved context to analysts. We will also show how providing context with asset data can help prioritize analyst time, saving money and addressing risks that matter. After covering ways to optimize traditional security alerts, we will jump into new methods to utilize logging technology to implement virtual tripwires. While it would be ideal to prevent attackers from gaining access to your network, it is a given that at some point you will be compromised. However, preventing compromise is the beginning, not the end goal. Adversaries will crawl your systems and network to achieve their own ends. Knowing this, we will implement logging-based tripwires—and if a single one is stepped on, we can quickly detect it and respond to the adversary.

Topics: Centralizing NIDS and HIDS Alerts; Analyzing Endpoint Security Logs; Augmenting Intrusion Detection Alerts; Analyzing Vulnerability Information; Correlating Malware Sandbox Logs with Other Systems to Identify Victims Across the Enterprise; Monitoring Firewall Activity; SIEM Tripwires; Post-Mortem Analysis

DAY 6: Capstone: Design, Detect, Defend

The course culminates in a team-based design, detect, and defend the flag competition. Powered by NetWars, day six provides a full day of hands-on work applying the principles taught throughout the week. Your team will progress through multiple levels and missions designed to ensure mastery of the modern cyber defense techniques promoted all week long. From building a logging architecture to augmenting logs, analyzing network logs, analyzing system logs, and developing dashboards to find attacks, this challenging exercise will reinforce key principles in a fun, hands-on, team-based challenge.

Topics: Defend-the-Flag Challenge – Hands-on Experience

"This course is as practical and real-world as it gets. SEC555 provides numerous quick wins and really stimulates thinking about the relative value of numerous ways to defend your organization."

-Mikhale Vitebskiy, **Lexington Partners**

SEC599: Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses

GDAT
Defending Advanced Threats
www.giac.org/gdat

6	36	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Understand how recent high-profile attacks were delivered and how they could have been stopped
- Implement security controls throughout the different phases of the Cyber Kill Chain and the MITRE ATT&CK framework to prevent, detect, and respond to attacks

Topics To Be Addressed

- Leveraging MITRE ATT&CK as a "common language" in the organization
- Building your own Cuckoo sandbox solution to analyze payloads
- Developing effective group policies to improve script execution (including PowerShell, Windows Script Host, VBA, HTA, etc.)
- Highlighting key bypass strategies for script controls (Unmanaged Powershell, AMSI bypasses, etc.)
- Stopping 0-day exploits using ExploitGuard and application whitelisting
- Highlighting key bypass strategies in application whitelisting (focus on AppLocker)
- Detecting and preventing malware persistence
- Leveraging the Elastic stack as a central log analysis solution
- Detecting and preventing lateral movement through Sysmon, Windows event monitoring, and group policies
- Blocking and detecting command and control through network traffic analysis
- Leveraging threat intelligence to improve your security posture

You just got hired to help our virtual organization "SYNCTECHLABS" build out a cybersecurity capability. On your first day, your manager tells you: "We looked at some recent cybersecurity trend reports and we feel like we've lost the plot. Advanced persistent threats, ransomware, denial of service... We're not even sure where to start!"

Cyber threats are on the rise: ransomware tactics are affecting small, medium, and large enterprises alike, while state-sponsored adversaries are attempting to obtain access to your most precious crown jewels. SEC599: Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses will arm you with the knowledge and expertise you need to overcome today's threats. Recognizing that a prevent-only strategy is not sufficient, we will introduce security controls aimed at stopping, detecting, and responding to your adversaries.

Course authors Stephen Sims and Erik Van Buggenhout (both certified as GIAC Security Experts) are hands-on practitioners who have built a deep understanding of how cyber attacks work through penetration testing and incident response. While teaching penetration testing courses, they were often asked the question: "How do I prevent or detect this type of attack?" Well, this is it! SEC599 gives students real-world examples of how to prevent attacks. The course features more than 20 labs plus a full-day Defend-the-Flag exercise during which students attempt to defend our virtual organization from different waves of attacks against its environment.

Our six-part journey will start off with an analysis of recent attacks through in-depth case studies. We will explain what types of attacks are occurring and introduce formal descriptions of adversary behavior such as the Cyber Kill Chain and the MITRE ATT&CK framework. In order to understand how attacks work, you will also compromise our virtual organization "SYNCTECHLABS" in section one exercises.

In sections two, three, four and five we will discuss how effective security controls can be implemented to prevent, detect, and respond to cyber attacks.

SEC599 will finish with a bang. During the Defend-the-Flag Challenge on the final course day, you will be pitted against advanced adversaries in an attempt to keep your network secure. Can you protect the environment against the different waves of attacks? The adversaries aren't slowing down, so what are you waiting for?

"SEC599 handles a lot of important aspects [of the entire Kill Chain]. It gives good insight into potential attacks and mitigation."

-Kevin Giesekam, **Dutch Police**

Bryce Galbraith
SANS Principal Instructor

As a contributing author of the internationally bestselling book, *Hacking Exposed: Network Security Secrets & Solutions*, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. Bryce was a member of Foundstone's world-renowned penetration testing team and served as a co-author and senior instructor of Foundstone's groundbreaking, Ultimate Hacking: Hands-On course series. Bryce continues to provide highly specialized ethical hacking and cybersecurity consulting services to clients around the world and teaches thousands of cybersecurity professionals, from a who's who of top organizations, how to defend against advanced adversaries.
@brycegalbraith

Course Day Descriptions

Mon, Feb 3 – Sat, Feb 8
9:00am – 5:00pm
Hands-on labs

This course is available via **Simulcast**. See page 64 for more information.

DAY 1: Introduction and Reconnaissance

Our six-part journey starts with an analysis of recent attacks through in-depth case studies. We will explain what's happening in real situations and introduce the Cyber Kill Chain and MITRE ATT&CK framework as a structured approach to describing adversary tactics and techniques. We will also explain what purple teaming is, typical tools associated with it, and how it can be best organized in your organization. In order to understand how attacks work, students will also compromise our virtual organization "SYNCTECHLABS" during section one exercises.

Topics: Course Outline and Lab Setup; Adversary Emulation and the Purple Team; Reconnaissance

DAY 2: Payload Delivery and Execution

Section 2 will cover how the attacker attempts to deliver and execute payloads in the organization. We will first cover adversary techniques (e.g., creation of malicious executables and scripts), then focus on how both payload delivery (e.g., phishing mails) and execution (e.g., double-clicking of the attachment) can be hindered. We will also introduce YARA as a common payload description language and SIGMA as a vendor-agnostic use-case description language.

Topics: Common Delivery Mechanisms; Hindering Payload Delivery; Preventing Payload Execution

DAY 3: Exploitation, Persistence, and Command and Control

Section 3 will first explain how exploitation can be prevented or detected. We will show how security should be an integral part of the software development lifecycle and how this can help prevent the creation of vulnerable software. We will also explain how patch management fits in the overall picture. Next, we will zoom in on exploit mitigation techniques, both at compile-time (e.g., ControlFlowGuard) and at run-time (ExploitGuard). We will provide an in-depth explanation of what the different exploit mitigation techniques (attempt to) cover and how effective they are. We'll then turn to a discussion of typical persistence strategies and how they can be detected using Autoruns and OSQuery. Finally, we will illustrate how command and control channels are being set up and what controls are available to the defender for detection and prevention.

Topics: Protecting Applications from Exploitation; Avoiding Installation; Foiling Command and Control

DAY 4: Lateral Movement

Section 4 will focus on how adversaries move laterally throughout an environment. A key focus will be on Active Directory (AD) structures and protocols (local credential stealing, NTLMv2, Kerberosm, etc.). We will discuss common attack strategies, including Windows privilege escalation, UAC bypasses, (Over-) Pass-the-Hash, Kerberoasting, Silver Tickets, and others. We'll also cover how BloodHound can be used to develop attack paths through the AD environment. Finally, we will discuss how lateral movement can be identified in the environment and how cyber deception can be used to catch intruders red-handed!

Topics: Protecting Administrative Access; Key Attack Strategies against AD; How Can We Detect Lateral Movement?

DAY 5: Action on Objectives, Threat Hunting, and Incident Response

Section five focuses on stopping the adversary during the final stages of the attack:

- How does the adversary obtain "domain dominance" status? This includes the use of Golden Tickets, Skeleton Keys, and directory replication attacks such as DCSync and DCShadow.
- How can data exfiltration be detected and stopped?
- How can threat intelligence aid defenders in the Cyber Kill Chain?
- How can defenders perform effective incident response?

As always, theoretical concepts will be illustrated during the different exercises performed throughout the day.

Topics: Domain Dominance; Data Exfiltration; Leveraging Threat Intelligence; Threat Hunting and Incident Response

DAY 6: APT Defender Capstone

The course culminates in a team-based Defend-the-Flag competition. Section six is a full day of hands-on work applying the principles taught throughout the course. Your team will progress through multiple levels and missions designed to ensure mastery of the modern cybersecurity controls promoted all week long. This challenging exercise will reinforce key principles in a fun, hands-on, team-based challenge. Note that OnDemand students will enjoy this exercise on an individual basis. As always, SANS subject-matter experts are available to support every OnDemand student's experience.

Topics: Applying Previously Covered Security Controls In-depth; Reconnaissance; Weaponization; Delivery; Exploitation; Installation; Command and Control; Action on Objectives

Who Should Attend

- Security architects and security engineers
- Red teamers and penetration testers
- Technical security managers
- Security Operations Center analysts, engineers, and managers
- Individuals looking to better understand how persistent cyber adversaries operate and how the IT environment can be improved to better prevent, detect, and respond to incidents.

"The different topics covered in this course can bring eye-opening layers of defense to any organization."

-Mike Marx, **Carbon Black**

GIAC
The Highest Standard in Cybersecurity Certification

Job-Specific, Specialized Focus

Today's cyber attacks are highly sophisticated and exploit specific vulnerabilities. Broad and general InfoSec certifications are no longer enough. Professionals need the specific skills and specialized knowledge required to meet multiple and varied threats. That's why GIAC has more than 30 certifications, each focused on specific job skills and each requiring unmatched and distinct knowledge.

Deep, Real-World Knowledge

Theoretical knowledge is the ultimate security risk. Deep, real-world knowledge and hands-on skills are the only reliable means to reduce security risk. Nothing comes close to a GIAC certification to ensure that this level of real-world knowledge and skill has been mastered.

Most Trusted Certification Design

The design of a certification exam impacts the quality and integrity of a certification. GIAC exam content and question design are developed through a rigorous process led by GIAC's on-staff psychometrician and reviewed by experts in each area. More than 78,000 certifications have been issued since 1999. GIAC certifications meet ANSI standards.

"Earning 3 GIAC certifications after I graduated from college has enabled me to enter the InfoSec field. Not only did they set me apart from my peers, GIAC certs also made my resume more appealing to recruiters."

- Kim Ngoc, GuardSight, Inc.

GIAC

DEEPER KNOWLEDGE. ADVANCED SECURITY.

GIAC.ORG

"Attackers are always evolving, and having a GIAC cert prepares you to evolve with them. It allows you to implement the appropriate methods and best practices in your company while understanding it's a continuous fight."

– Jason Sevilla, Cyber Intelligence Analyst

SANS CYBER IMMERSION ACADEMY

"The SANS Institute is renowned and respected for its world-class cyber training. CACI is pleased to team with SANS on this critical workforce development initiative, which will help fill a pressing need for cybersecurity experts in industry and government."

– Mike Mourelatos
Vice President & CTO
CACI, National Services & Intelligence Solutions

Employ Top Cybersecurity Talent

Develop Your Own Cybersecurity Talent

You have great people. Invest in their skills and everyone wins. SANS Cyber Immersion Academies quickly and cost-effectively meet the specific needs of organizations and employers seeking to develop and retain top cybersecurity talent. Our immersive, accelerated training programs help you develop the best available talent on the market.

Hire Our Cybersecurity Professionals

The competition for top talent is intense. When you need to fill cybersecurity positions, the SANS Cyber Immersion Academies can help. Our qualified and diverse graduates include U.S. veterans and proven professionals. They are ready to join your team and work on day one!

Our Academy Graduates are Seeking Opportunities!

For more information, contact
IMMERSIONACADEMY@SANS.ORG or visit WWW.SANS.ORG/ACADEMY4EMPLOYERS

Cyber Workforce ACADEMY | VetSuccess ACADEMY | Women's ACADEMY | Diversity Cyber ACADEMY

SEC542: **Web App Penetration Testing and Ethical Hacking**

GWAPT
Web Application Penetration Tester
www.giac.org/gwapt

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Apply a detailed, four-step methodology to your web application penetration tests: reconnaissance, mapping, discovery, and exploitation
- Analyze the results from automated web testing tools to validate findings, determine their business impact, and eliminate false positives
- Manually discover key web application flaws
- Use Python to create testing and exploitation scripts during a penetration test
- Discover and exploit SQL Injection flaws to determine true risk to the victim organization
- Create configurations and test payloads within other web attacks
- Fuzz potential inputs for injection attacks
- Explain the impact of exploitation of web application flaws
- Analyze traffic between the client and the server application using tools such as the Zed Attack Proxy and Burp Suite to find security issues within the client-side application code
- Manually discover and exploit Cross-Site Request Forgery (CSRF) attacks
- Use the Browser Exploitation Framework (BeEF) to hook victim browsers, attack client software and the network, and evaluate the potential impact that XSS flaws have within an application
- Perform a complete web penetration test during the Capture-the-Flag exercise to bring techniques and tools together into a comprehensive test

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

SEC542 helps students move beyond push-button scanning to professional, thorough, and high-value web application penetration testing.

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

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

SEC542 enables students to assess a web application's security posture and convincingly demonstrate the impact of inadequate security that plagues most organizations.

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

In addition to high-quality course content, SEC542 focuses heavily on in-depth, hands-on labs to ensure that students can immediately apply all they learn.

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

Eric Conrad
SANS Faculty Fellow

Eric Conrad is the 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 GPEN, GCIH, GCIA, GCFA, GAWN, and GSEC certifications. Eric also blogs about information security at ericconrad.com.
@eric_conrad

Course Day Descriptions

Mon, Feb 3 – Sat, Feb 8
9:00am – 5:00pm
Hands-on labs

DAY 1: Introduction and Information Gathering

Understanding the attacker's perspective is key to successful web application penetration testing. The course begins by thoroughly examining web technology, including protocols, languages, clients and server architectures, from the attacker's perspective. We will also examine different authentication systems, including Basic, Digest, Forms and Windows Integrated authentication, and discuss how servers use them and attackers abuse them.

Topics: Overview of the Web from a Penetration Tester's Perspective; Exploring the Various Servers and Clients; Discussion of the Various Web Architectures; Discovering How Session State Works; Discussion of the Different Types of Vulnerabilities; WHOIS and DNS Reconnaissance; The HTTP Protocol; WebSocket; Secure Sockets Layer (SSL) Configurations and Weaknesses; Heartbleed Exploitation; Utilizing the Burp Suite in Web App Penetration Testing

DAY 2: Configuration, Identity, and Authentication Testing

The second day starts the actual penetration testing process, beginning with the reconnaissance and mapping phases. Reconnaissance includes gathering publicly available information regarding the target application and organization, identifying the machines that support our target application, and building a profile of each server, including the operating system, specific software and configuration. The discussion is underscored through several practical, hands-on labs in which we conduct reconnaissance against in-class targets.

Topics: Scanning with Nmap; Discovering the Infrastructure within the Application; Identifying the Machines and Operating Systems; Exploring Virtual Hosting and Its Impact on Testing; Learning Methods to Identify Load Balancers; Software Configuration Discovery; Learning Tools to Spider a Website; Brute Forcing Unlinked Files and Directories; Discovering and Exploiting Shellshock; Web Authentication; Username Harvesting and Password Guessing; Fuzzing; Burp Intruder

DAY 3: Injection

This section continues to explore our methodology with the discovery phase. We will build on the information started the previous day, exploring methods to find and verify vulnerabilities within the application. Students will also begin to explore the interactions between the various vulnerabilities.

Topics: Session Tracking; Authentication Bypass Flaws; Mutillidae; Command Injection; Directory Traversal; Local File Inclusion (LFI); Remote File Inclusion (RFI); SQL Injection; Blind SQL Injection; Error-Based SQL Injection; Exploiting SQL Injection; SQL Injection Tools; sqlmap

DAY 4: XXE and XSS

On day four, students continue exploring the discovery phase of the methodology. We cover methods to discover key vulnerabilities within web applications, such as Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF/XSRF). Manual discovery methods are employed during hands-on labs.

Topics: XML External Entity (XXE); Cross-Site Scripting (XSS); Browser Exploitation Framework (BeEF); AJAX; XML and JSON; Document Object Model (DOM); Logic Attacks; API Attacks; Data Attacks

DAY 5: CSRF, Logic Flaws, and Advanced Tools

On the fifth day, we launch actual exploits against real-world applications, building on the previous three steps, expanding our foothold within the application, and extending it to the network on which it resides. As penetration testers, we specifically focus on ways to leverage previously discovered vulnerabilities to gain further access, highlighting the cyclical nature of the four-step attack methodology.

Topics: Cross-Site Request Forgery (CSRF); Python for Web App Penetration Testing; WPScan; w3af; Metasploit for Web Penetration Testers; Leveraging Attacks to Gain Access to the System; How to Pivot Our Attacks Through a Web Application; Exploiting Applications to Steal Cookies; Executing Commands Through Web Application Vulnerabilities; When Tools Fail

DAY 6: Capture-the-Flag Challenge

On day six, students form teams and compete in a web application penetration testing tournament. This NetWars-powered Capture-the-Flag Challenge provides students an opportunity to wield their newly developed or further-honed skills to answer questions, complete missions, and exfiltrate data, applying skills gained throughout the course. The style of challenge and integrated-hint system allows students of various skill levels to both enjoy a game environment and solidify the skills learned in class.

Who Should Attend

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

"SEC542 shows a hands-on way of doing web app penetration testing – not just how to use this tool or that tool."

-Christopher J. Stover, **Infogressive Inc.**

"Knowing everything from the Internet is not enough. This class has a sequential structure to understand the basics of pen testing."

-Vinita Mhapsekar, **Kaiser Permanente**

SEC560: **Network Penetration Testing and Ethical Hacking**

GPEN
Penetration Tester
www.giac.org/gpen

6	37	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Develop tailored scoping and rules of engagement for penetration testing projects to ensure the work is focused, well defined, and conducted in a safe manner
- Conduct detailed reconnaissance using document metadata, search engines, and other publicly available information sources to build a technical and organizational understanding of the target environment
- Utilize a scanning tool such as Nmap to conduct comprehensive network sweeps, port scans, OS fingerprinting, and version scanning to develop a map of target environments
- Choose and properly execute Nmap Scripting Engine scripts to extract detailed information from target systems
- Configure and launch a vulnerability scanner such as Nessus so that it safely discovers vulnerabilities through both authenticated and unauthenticated scans, and customize the output from such tools to represent the business risk to the organization
- Analyze the output of scanning tools to eliminate false positive reduction with tools including Netcat and Scapy
- Utilize the Windows PowerShell and Linux bash command lines during post-exploitation to plunder target systems for vital information that can further overall penetration test progress, establish pivots for deeper compromise, and help determine business risks
- Configure an exploitation tool such as Metasploit to scan, exploit, and then pivot through a target environment

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.

SEC560 IS THE MUST-HAVE COURSE FOR EVERY WELL-ROUNDED SECURITY PROFESSIONAL

With comprehensive coverage of tools, techniques, and methodologies for network penetration testing, SEC560 truly prepares you to conduct high-value penetration testing projects 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 with great skill.

LEARN THE BEST WAYS TO TEST YOUR OWN SYSTEMS BEFORE THE BAD GUYS ATTACK

You'll 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.

EQUIPPING SECURITY ORGANIZATIONS WITH COMPREHENSIVE PENETRATION TESTING AND ETHICAL HACKING KNOW-HOW

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test and on the final day of the course you'll do just that. After building your skills in comprehensive and challenging labs, the course culminates with a final 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 skills you've gained in this course.

"SEC560 provides practical, how-to material that I can use daily in my penetration testing activities – not only technically, but also from a business perspective."

-Steve Nolan, **General Dynamics**

Jeff McJunkin
SANS Certified Instructor

Jeff McJunkin is a senior staff member at Counter Hack Challenges with more than nine years of experience in systems and network administration and network security. His greatest strength is his breadth of experience – from network and web application penetration testing to digital/mobile forensics, and from technical training to systems architecture. Jeff is a computer security/information assurance graduate of Southern Oregon University and holds many professional certifications. He has also competed in many security competitions, including taking first place at a regional NetWars competition and a U.S. Cyber Challenge capture-the-flag competition, as well as joining the Red Team for the Pacific Rim Collegiate Cyber Defense Competition. His personal blog can be found at http://jeffmcjunkin.com. **@jeffmcjunkin**

Course Day Descriptions

Mon, Feb 3 – Sat, Feb 8
9:00am – 7:15pm (Day 1)
9:00am – 5:00pm (Days 2-6)
Extended hours; hands-on labs

DAY 1: Comprehensive Pen Test Planning, Scoping, and Recon

In this course section, you'll develop the skills needed to conduct a best-of-breed, high-value penetration test. We'll go in-depth on how to build a penetration testing infrastructure that includes all the hardware, software, network infrastructure, and tools you will need to conduct great penetration tests, with specific low-cost recommendations for your arsenal. We'll then cover formulating a pen test scope and rules of engagement that will set you up for success, including a role-play exercise. We'll also dig deep into the reconnaissance portion of a penetration test, covering the latest tools and techniques, including hands-on document metadata analysis to pull sensitive information about a target environment, as well as a lab using Recon-ng to plunder a target's DNS infrastructure for information such as which anti-virus tools the target organization uses.

Topics: The Mindset of the Professional Pen Tester; Building a World-Class Pen Test Infrastructure; Creating Effective Pen Test Scopes and Rules of Engagement; Detailed Recon Using the Latest Tools; Effective Pen Test Reporting to Maximize Impact; Mining Search Engine Results; Document Metadata Extraction and Analysis; Interrogating DNS for Juicy Information

DAY 2: In-Depth Scanning

This course section focuses on the vital task of mapping the target environment's attack surface by creating a comprehensive inventory of machines, accounts, and potential vulnerabilities. We look at some of the most useful scanning tools freely available today and run them in numerous hands-on labs to help hammer home the most effective way to use each tool. We also conduct a deep dive into some of the most useful tools available to pen testers today for formulating packets: Scapy and Netcat. We finish the module covering vital techniques for false-positive reduction, so you can focus your findings on meaningful results and avoid the sting of a false positive. And we examine the best ways to conduct your scans safely and efficiently.

Topics: Tips for Awesome Scanning; Tcpdump for the Pen Tester; Nmap In-Depth: The Nmap Scripting Engine; Version Scanning with Nmap; Vulnerability Scanning with Nessus; False-Positive Reduction; Packet Manipulation with Scapy; Enumerating Users; Netcat for the Pen Tester; Monitoring Services during a Scan

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

DAY 3: Exploitation

In this section, we look at the many kinds of exploits that penetration testers use to compromise target machines, including client-side exploits, service-side exploits, and local privilege escalation. We'll see how these exploits are packaged in frameworks like Metasploit and its mighty Meterpreter. You'll learn in-depth how to leverage Metasploit and the Meterpreter to compromise target environments. We'll also analyze the topic of anti-virus evasion to bypass the target organization's security measures, as well as methods for pivoting through target environments, all with a focus on determining the true business risk of the target organization.

Topics: Comprehensive Metasploit Coverage with Exploits, Stagers, and Stages; Strategies and Tactics for Anti-Virus Evasion; In-Depth Meterpreter Analysis, Hands-On; Implementing Port Forwarding Relays for Merciless Pivots; How to Leverage PowerShell Empire to Plunder a Target Environment

DAY 4: Post-Exploitation and Merciless Pivoting

Once you've successfully exploited a target environment, penetration testing gets extra exciting as you perform post-exploitation, gathering information from compromised machines and pivoting to other systems in your scope. This course section zooms in on pillaging target environments and building formidable hands-on command line skills. We'll cover Windows command line skills in-depth, including PowerShell's awesome abilities for post-exploitation. We'll see how we can leverage malicious services and the incredible WMIC toolset to access and pivot through a target organization. We'll then turn our attention to password guessing attacks, discussing how to avoid account lockout, as well as numerous options for plundering password hashes from target machines including the great Mimikatz Kiwi tool. Finally, we'll look at Metasploit's fantastic features for pivoting, including the msfconsole route command.

Topics: Windows Command Line Kung Fu for Penetration Testers; PowerShell's Amazing Post-Exploitation Capabilities; Password Attack Tips; Account Lockout and Strategies for Avoiding It; Automated Password Guessing with THC-Hydra; Retrieving and Manipulating Hashes from Windows, Linux, and Other Systems; Pivoting through Target Environments; Extracting Hashes and Passwords from Memory with Mimikatz Kiwi

DAY 5: In-Depth Password Attacks and Web App Pen Testing

In this course section, we'll go even deeper in exploiting one of the weakest aspects of most computing environments: passwords. You'll custom-compile John the Ripper to optimize its performance in cracking passwords. You'll look at the amazingly full-featured Cain tool, running it to crack sniffed Windows authentication messages. We'll use the incredible Hashcat tool for increased speed in cracking passwords, all hands-on. And we'll cover powerful "pass-the-hash" attacks, leveraging Metasploit, the Meterpreter, and more. We then turn our attention to web application pen testing, covering the most powerful and common web app attack techniques, with hands-on labs for every topic we address. We'll cover finding and exploiting cross-site scripting (XSS), cross-site request forgery (XSRF), command injection, and SQL injection flaws in applications such as online banking, blog sites, and more.

Topics: Password Cracking with John the Ripper; Sniffing and Cracking Windows Authentication Exchanges Using Cain; Using Hachcat for Maximum Effectiveness; Pass-the-Hash Attacks with Metasploit and More; Finding and Exploiting Cross-Site Scripting; Utilizing Cross-Site Request Forgery Flaws; Data Plundering with SQL Injection; Leveraging SQL Injection to Perform Command Injection; Maximizing Effectiveness of Command Injection Testing

DAY 6: Penetration Test and Capture-the-Flag Challenge

This lively session represents the culmination of the network penetration testing and ethical hacking course. You'll apply all of the skills mastered in the course in a comprehensive, hands-on workshop during which you'll conduct an actual penetration test of a sample target environment. We'll provide the scope and rules of engagement, and you'll work to achieve your goal of finding out whether the target organization's Personally Identifiable Information (PII) is at risk. As a final step in preparing you for conducting penetration tests, you'll make recommendations about remediating the risks you identify.

Topics: Applying Penetration Testing and Ethical Hacking Practices End-to-End; Detailed Scanning to Find Vulnerabilities and Avenues to Entry; Exploitation to Gain Control of Target Systems; Post-Exploitation to Determine Business Risk; Merciless Pivoting; Analyzing Results to Understand Business Risk and Devise Corrective Actions

SEC573: **Automating Information Security with Python**

GPYC
Python Coder
www.giac.org/gpyc

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Modify existing open-source tools to customize them to meet the needs of your organization.
- Manipulate log file formats to make them compatible with various log collectors.
- Write new tools to analyze log files and network packets to identify attackers in your environment.
- Develop tools that extract otherwise inaccessible forensic artifacts from computer systems of all types.
- Automate the collection of intelligence information to augment your security from online resources.
- Automate the extraction of signs of compromise and other forensics data from the Windows Registry and other databases.
- Write a backdoor that uses exception handling, sockets, process execution, and encryption to provide you with your initial foothold in a target environment. The backdoor will include features such as a port scanner to find an open outbound port, techniques for evading antivirus software and network monitoring, and the ability to embed a payload from tools such as Metasploit.

All security professionals, including penetration testers, forensic analysts, network defenders, security administrators, and incident responders, have one experience in common: CHANGE. Tools, technologies, and threats change constantly, but Python is a simple, user-friendly language that can help you keep pace with change, allowing you to write custom tools and automate tasks to effectively manage and respond to your unique threats.

Whether you are new to coding or have been coding for years, SEC573: Automating Information Security with Python will have you creating programs that make your job easier and your work more efficient. This self-paced course starts from the very beginning, assuming you have no prior experience with or knowledge of programming. We cover all of the essentials of the language up front. If you already know the essentials, you will find that the pyWars lab environment allows advanced developers to quickly accelerate to more advanced material in the course.

Technology, threats, and tools are constantly evolving. If we don't evolve with them, we'll become ineffective and irrelevant, unable to provide the vital defenses our organizations increasingly require. Maybe your chosen Operating System has a new feature that creates interesting forensic artifacts that would be invaluable for your investigation, if only you had a tool to access it. Often for new features and forensic artifacts, no such tool has yet been released. You could try moving your case forward without that evidence or hope that someone creates a tool before the case goes cold...or you can write a tool yourself.

Or perhaps an attacker bypassed your defenses and owned your network months ago. If existing tools were able to find the attack, you wouldn't be in this situation. You are bleeding sensitive data and the time-consuming manual process of finding and eradicating the attacker is costing you money and hurting your organization. The answer is simple if you have the skills: Write tools to automate various aspects of your defenses.

Or, as a penetration tester, you need to evolve as quickly as the threats you are paid to emulate. What do you do when "off-the-shelf" tools and exploits fall short? If you're good, you write your own tool or modify existing capabilities to make them perform as you need them to.

SEC573 is designed to give you the skills you need for tweaking, customizing, or outright developing your own tools. We put you on the path of creating your own tools, empowering you to better automate the daily routine of today's information security professional and to achieve more value in less time. Again and again, organizations serious about security emphasize their need for skilled tool builders. There is a huge demand for people who can understand a problem and then rapidly develop prototype code to attack or defend against it. Learn Python in-depth with us to become fully weaponized.

Mark Baggett
SANS Senior Instructor

Mark Baggett is the owner of Indepth Defense, an independent consulting firm that offers incident response and penetration testing services. Mark has more than 28 years of commercial and government experience ranging from software developer to chief information security officer. He is the author of the SEC573: Automating Information Security with Python course. Mark has a master's degree in information security engineering and many industry certifications, including being the 15th person in the world to receive the prestigious GIAC Security Expert certification (GSE). Mark is very active in the information security community. He is the founding president of The Greater Augusta ISSA (Information Systems Security Association) chapter, which has been extremely successful in bringing networking and educational opportunities to Augusta Information Technology workers. Since January 2011, Mark has served as the SANS Technical Advisor to the DoD, where he assists various entities in the development of information security capabilities.
@MarkBaggett

Course Day Descriptions

Mon, Feb 3 – Sat, Feb 8
9:00am – 5:00pm
Hands-on labs

This course is available via **Simulcast**. See page 64 for more information.

DAY 1: Essentials Workshop with pyWars

The course begins with a brief introduction to Python and the pyWars Capture-the-Flag challenge. We set the stage for students to learn at their own pace in the pyWars lab environment, which is 100 percent hands-on. As more advanced students take on Python-based Capture-the-Flag challenges, students who are new to programming will start from the very beginning with Python essentials.

Topics: Syntax; Variables; Math Operators; Strings; Functions; Modules; Control Statements; Introspection

DAY 2: Essentials Workshop with MORE pyWars

You will never learn to program by staring at PowerPoint slides. This section continues the hands-on, lab-centric approach established at the beginning of the course. It covers data structures and more detailed programming concepts. Next, we focus on invaluable tips and tricks to make you a better Python programmer and to show you how to debug your code.

Topics: Lists; Loops; Tuples; Dictionaries; The Python Debugger; Coding Tips; Tricks and Shortcuts; System Arguments; ArgParser Module

DAY 3: Defensive Python

In this section, we take on the role of a network defender with more logs to examine than there is time in the day. Attackers have penetrated the network and you will have to analyze the logs and packet captures to find them. We will discuss how to analyze network logs and packets to discover where the attackers are coming from and what they are doing. We will build scripts to empower continuous monitoring and disrupt the attackers before they exfiltrate your data. Forensicators and offensive security professionals won't be left out because reading and writing files and parsing data are also essential skills they will apply to their craft.

Topics: File Operations; Python Sets; Regular Expressions; Log Parsing; Data Analysis Tools and Techniques; Long Tail/Short Tail Analysis; Geolocation Acquisition; Blacklists and Whitelists; Packet Analysis; Packet Reassembly; Payload Extraction

DAY 4: Forensics Python

In our forensics-themed section, we will assume the role of a forensic analyst who has to carve evidence from artifacts when no tool exists to do so. Even if you don't do forensics, you will find that the skills covered in this section are foundational to every security role. We will discuss the process required to carve binary images, find appropriate data of interest in them, and extract those data. Once you have the artifact isolated, there is more analysis to be done. You will learn how to extract metadata from image files. Then, we will discuss techniques for finding artifacts in other locations, such as SQL databases, and interacting with web pages.

Topics: Acquiring Images from Disk; Memory and the Network; File Carving; The STRUCT Module; Raw Network Sockets and Protocols; Image Forensics and PIL; SQL Queries; HTTP Communications with Python Built in Libraries; Web Communications with the Requests Module

DAY 5: Offensive Python

During our offensive-themed section, we play the role of penetration testers whose normal tricks have failed. Their attempts to establish a foothold have been stopped by modern defenses. To bypass these defenses, you will build an agent to give you access to a remote system. Similar agents can be used for Incident response or systems administration, but our focus will be on offensive operations.

Topics: Network Socket Operations; Exception Handling; Process Execution; Blocking and Non-blocking Sockets; Using the Select Module for Asynchronous Operations; The Select Module; Python Objects; Argument Packing and Unpacking

DAY 6: Capture-the-Flag Challenge

In this final section you will be placed on a team with other students to apply the skills you have mastered in a series of programming challenges. Participants will exercise the new skills and the code they have developed throughout the course in a series of challenges. You will solve programming challenges, exploit vulnerable systems, analyze packets, parse logs, and automate code execution on remote systems. Test your skills! Prove your might!

Who Should Attend

- Security professionals who benefit from automating routine tasks so they can focus on what's most important
- Forensic analysts who can no longer wait on someone else to develop a commercial tool to analyze artifacts
- Network defenders who sift through mountains of logs and packets to find evil-doers in their networks
- Penetration testers who are ready to advance from script kiddie to professional offensive computer operations operator
- Security professionals who want to evolve from security tool consumer to security solution provider

You Will Receive

- A USB containing a virtual machine filled with sample code and working examples
- A copy of *The Python Pocket Reference* published by O'Reilly Press
- MP3 audio files of the complete course lecture

"Excellent class for learning how to construct automated and advanced discovery analytics for information systems."

-Mary Gutierrez, **Booz Allen Hamilton**

"SEC573 is excellent. I went from having almost no Python coding ability to being able to write functional and useful programs."

-Caleb Jaren, **Microsoft**

SEC642: **Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques**

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Perform advanced Local File Include (LFI)/Remote File Include (RFI), Blind SQL injection (SQLi), and Cross-Site Scripting (XSS) combined with Cross-Site Request Forger (XSRF) discovery and exploitation
- Exploit advanced vulnerabilities common to most backend language like Mass Assignments, Type Juggling, and Object Serialization
- Perform JavaScript-based injection against ExpressJS, Node.js, and NoSQL
- Understand the special testing methods for content management systems such as SharePoint and WordPress
- Identify and exploit encryption implementations within web applications and frameworks
- Discover XML Entity and XPath vulnerabilities in SOAP or REST web services and other datastores
- Use tools and techniques to work with and exploit HTTP/2 and Web Sockets
- Identify and bypass Web Application Firewalls and application filtering techniques to exploit the system

Who Should Attend

- Web and network penetration testers
- Red team members
- Vulnerability assessment personnel
- Security consultants
- Developers and QA testers
- System administrators and IT managers
- System architects

Can your web apps withstand the onslaught of modern advanced attack techniques?

Modern web applications are growing more sophisticated and complex as they utilize exciting new technologies and support ever more critical operations. Long gone are the days of basic HTML requests and responses. Even in the age of Web 2.0 and AJAX, the complexity of HTTP and modern web applications is progressing at breathtaking speed. With the demands of highly available web clusters and cloud deployments, web applications are looking to deliver more functionality in smaller packets, with a decreased strain on backend infrastructure. Welcome to an era that includes tricked-out cryptography, WebSockets, HTTP/2, and a whole lot more. Are your web application assessment and penetration testing skills ready to evaluate these impressive new technologies and make them more secure?

Are you ready to put your web apps to the test with cutting-edge skills?

This pen testing course is designed to teach you the advanced skills and techniques required to test modern web applications and next-generation technologies. The course uses a combination of lecture, real-world experiences, and hands-on exercises to teach you the techniques to test the security of tried-and-true internal enterprise web technologies, as well as cutting-edge Internet-facing applications. The final course day culminates in a Capture-the-Flag competition, where you will apply the knowledge you acquired during the previous five days in a fun environment based on real-world technologies.

This course offers hands-on learning of advanced web app exploitation skills.

We begin by exploring advanced techniques and attacks to which all modern-day complex applications may be vulnerable. We'll learn about new web frameworks and web backends, then explore encryption as it relates to web applications, digging deep into practical cryptography used by the web, including techniques to identify the type of encryption in use within the application and methods for exploiting or abusing it. We'll look at alternative front ends to web applications and web services such as mobile applications, and examine new protocols such as HTTP/2 and WebSockets. The final portion of the class will focus on how to identify and bypass web application firewalls, filtering, and other protection techniques.

"SEC642 is the perfect course for someone who has a background in web app pen testing, but wants to really gain advanced skills."

-Matthew Sullivan, **Webfilings**

Adrien de Beaupre
SANS Principal Instructor

Adrien de Beaupre works as an independent consultant in beautiful Ottawa, Ontario. His work experience includes technical instruction, vulnerability assessment, penetration testing, intrusion detection, incident response and forensic analysis. He is a member of the SANS Internet Storm Center (isc.sans.edu). He is the lead course author of SANS SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques and SEC460: Enterprise Threat and Vulnerability Assessment. He is actively involved with the information security community, and has been working with SANS since 2000. Adrien holds a variety of certifications including the GXPN, GPEN, GWAPT, GCIH, GCIA, GSEC, CISSP®, OPST, and OPSA. When not geeking out he can be found with his family, or at the dojo.
@adriendb

Course Day Descriptions

Mon, Feb 3 – Sat, Feb 8
9:00am - 5:00pm
Hands-on labs

DAY 1: Advanced Attacks

As applications and their vulnerabilities become more complex, penetration testers have to be able to handle advanced targets. We'll start the course with a warm-up pen test of a small application. After our review of this exercise, we will explore some of the more advanced techniques for LFI/RFI and SQLi server-based flaws. We will then take a stab at combined XSS and XSRF attacks, where we leverage the two vulnerabilities together for even greater effect. After discovering the flaws, we will then work through various ways to exploit these flaws beyond the typical means exhibited today. These advanced techniques will help penetration testers find ways to demonstrate these vulnerabilities to their organization through advanced and custom exploitation.

Topics: Review of the Testing Methodology; Using Burp Suite in a Web Penetration Test; Exploiting Local and Remote File Inclusions; Exploring Advanced Discovery Techniques for SQL Injection and Other Server-Based Flaws; Exploring Advanced Exploitation of XSS and XSRF in a Combined Attack; Learning Advanced Exploitation Techniques

DAY 2: Web Frameworks

We'll continue exploring advanced discovery and exploitation techniques for today's complex web applications. We'll look at vulnerabilities that could affect web applications written in any backend language, then examine how logic flaws in applications, especially in Mass Object Assignments, can have devastating effects on security. We'll also dig into assumptions made by core development teams of backend programming languages and learn how even something as simple as handling the data types in variables can be leveraged through the web with Type Juggling and Object Serialization. Next we'll explore various popular applications and frameworks and how they change the discovery techniques within a web penetration test. Part of this discussion will lead us to cutting-edge technologies like the MEAN stack, where JavaScript is leveraged from the browser, web server, and backend NoSQL storage. The final section of the class examines applications in content management systems such as SharePoint and WordPress, which have unique needs and features that make testing them both more complex and more fruitful for the tester.

Topics: Web Architectures; Web Design Patterns; Languages and Frameworks; Java and Struts; PHP-Type Juggling; Logic Flaws; Attacking Object Serialization; The MEAN Stack; Content Management Systems; SharePoint; WordPress

DAY 3: Web Cryptography

Cryptographic weaknesses are common, yet few penetration testers have the skill to investigate, attack and exploit these flaws. When we investigate web application crypto attacks, we typically target the implementation and use of cryptography in modern web applications. Many popular web programming languages or development frameworks make encryption services available to the developer, but do not inherently protect encrypted data from being attacked, or only permit the developer to use cryptography in a weak manner. These implementation mistakes are going to be our focus in this section, as opposed to the exploitation of deficiencies in the cryptographic algorithms themselves. We will also explore the various ways applications use encryption and hashing insecurely. Students will learn techniques ranging from identifying what the encryption technique is to exploiting various flaws within the encryption or hashing.

Topics: Identifying the Cryptography Used in the Web Application; Analyzing and Attacking the Encryption Keys; Exploiting Stream Cipher IV Sollisions; Exploiting Electronic Codebook (ECB) Mode Ciphers with Block Shuffling; Exploiting Cipher Block Chaining (CBC) Mode with Bit Flipping; Vulnerabilities in PKCS#7 Padding Implementations

DAY 4: Alternative Web Interfaces

Web applications are no longer limited to the traditional HTML-based interfaces. Web services and mobile applications have become more common and are regularly being used to attack clients and organizations. As such, it has become very important that penetration testers understand how to evaluate the security of these systems. We will examine Flash, Java, Active X, and Silverlight flaws. We will explore various techniques to discover flaws within the applications and backend systems. These techniques will make use of tools such as Burp Suite and other automated toolsets. We'll use lab exercises to explore the newer protocols of HTTP/2 and WebSockets, exploiting flaws exposed within each of them.

Topics: Intercepting Traffic to Web Services and from Mobile Applications; Flash, Java, ActiveX, and Silverlight Vulnerabilities; SOAP and REST Web Services; Penetration Testing Web Services; WebSocket Protocol Issues and Vulnerabilities; New HTTP/2 Protocol Issues and Penetration Testing

DAY 5: Web Application Firewall and Filter Bypass

Applications today are using more security controls to help prevent attacks. These controls, such as Web Application Firewalls and filtering techniques, make it more difficult for penetration testers during their testing. The controls block many of the automated tools and simple techniques used to discover flaws. On this day we'll explore techniques used to map the control and how that control is configured to block attacks. You'll be able to map out the rule sets and determine the specifics of how the Web Application Firewall detects attacks. This mapping will then be used to determine attacks that will bypass the control. You'll use HTML5, UNICODE, and other encodings that will enable your discovery techniques to work within the protected application.

Topics: Understanding Web Application Firewalling and Filtering Techniques; Determining the Rule Sets Protecting the Application; Fingerprinting the Defense Techniques Used; Learning How HTML5 Injections Work; Using UNICODE, CTYPEs, and Data URIs to Bypass Restrictions; Bypassing a Web Application Firewall's Best-Defended Vulnerabilities, XSS and SQLi

DAY 6: Capture-the-Flag Challenge

On this final course day you will be placed on a network and given the opportunity to complete an entire penetration test. The goal of this exercise is for you to explore the techniques, tools, and methodology you will have learned over the last five days. You'll be able to use these skills against a realistic extranet and intranet. At the end of the day, you will provide a verbal report of the findings and methodology you followed to complete the test. Students will be provided with a virtual machine that contains the Samurai Web Testing Framework (SamuraiWTF). You will be able to use this both in the class and after leaving and returning to your jobs.

FOR500: **Windows Forensic Analysis**

GCFE
Forensic Examiner
www.giac.org/gcfe

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Perform proper Windows forensic analysis by applying key techniques focusing on Windows 7/8/10
- Use full-scale forensic tools and analysis methods to detail nearly every action a suspect accomplished on a Windows system, including who placed an artifact on the system and how, program execution, file/folder opening, geo-location, browser history, profile USB device usage, and more
- Uncover the exact time that a specific user last executed a program through Registry and Windows artifact analysis, and understand how this information can be used to prove intent in cases such as intellectual property theft, hacker-breached systems, and traditional crimes
- Determine the number of times files have been opened by a suspect through browser forensics, shortcut file analysis (LNK), e-mail analysis, and Windows Registry parsing
- Identify keywords searched by a specific user on a Windows system in order to pinpoint the files and information the suspect was interested in finding and accomplish detailed damage assessments
- Use Windows shellbags analysis tools to articulate every folder and directory that a user opened up while browsing local, removable, and network drives
- Determine each time a unique and specific USB device was attached to the Windows system, the files and folders that were accessed on it, and who plugged it in by parsing key Windows artifacts such as the Registry and log files
- Use event log analysis techniques to determine when and how users logged into a Windows system, whether via a remote session, at the keyboard, or simply by unlocking a screensaver

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

FOR500: Windows Forensic Analysis will teach you to:

- Conduct in-depth forensic analysis of Windows operating systems and media exploitation focusing on Windows 7, Windows 8/8.1, Windows 10, and Windows Server 2008/2012/2016
- Identify artifact and evidence locations to answer critical questions, including application execution, file access, data theft, external device usage, cloud services, geolocation, file download, anti-forensics, and detailed system usage
- Focus your capabilities on analysis instead of on how to use a particular tool
- Extract critical answers and build an in-house forensic capability via a variety of free, open-source, and commercial tools provided within the SANS Windows SIFT Workstation

All organizations must prepare for cyber-crime occurring on their computer systems and within their networks. Demand has never been greater for analysts who can investigate crimes such as fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover vital 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 experts capable of piecing together what happened on computer systems second by second.

FOR500: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of 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. You will learn how to recover, analyze, and authenticate forensic data on Windows systems, track particular user activity on your network, and organize findings for use in incident response, internal investigations, and civil/criminal litigation. You will be able to 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 unbelievable amount of data about you and your users. FOR500 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR500 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7, Windows 8/8.1, Windows 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 7 systems to just-discovered Windows 10 artifacts.

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."

@robtlee

Course Day Descriptions

Mon, Feb 3 – Sat, Feb 8
9:00am – 5:00pm
Hands-on labs

DAY 1: Windows Digital Forensics and Advanced Data Triage

The Windows forensics course starts with an examination of digital forensics in today's interconnected environments and discusses challenges associated with mobile devices, tablets, cloud storage, and modern Windows operating systems. We will discuss how modern hard drives, such as Solid State Devices (SSD), can affect the digital forensics acquisition process and how analysts need to adapt to overcome the introduction of these new technologies.

Topics: Windows Operating System Components; Core Forensic Principles; Live Response and Triage-Based Acquisition Techniques; Acquisition Review with Write Blocker; Advanced Acquisition Challenges; Windows Image Mounting and Examination; NTFS File System Overview; Document and File Metadata; File Carving; Custom Carving Signatures; Memory, Pagefile, and Unallocated Space Analysis

DAY 2: Core Windows Forensics Part 1 – Windows Registry Forensics and Analysis

Our journey continues with the Windows Registry, where the digital forensic investigator will learn how to discover critical user and system information pertinent to almost any investigation. Each examiner will learn how to navigate and examine the Registry to obtain user-profile data and system data. The course teaches forensic investigators how to prove that a specific user performed key word searches, ran specific programs, opened and saved files, perused folders, and used removable devices. Throughout the section, investigators will use their skills in a real hands-on case, exploring the evidence and analyzing evidence.

Topics: Registry Basics; Profile Users and Groups; Core System Information; User Forensic Data; Tools Utilized

DAY 3: Core Windows Forensics Part 2 – USB Devices and Shell Items

Being able to show the first and last time a file or folder was opened is a critical analysis skill. Utilizing shortcut (LNK), jump list, and Shellbag databases through the examination of SHELL ITEMS, we can quickly pinpoint which file or folder was opened and when. The knowledge obtained by examining SHELL ITEMS is crucial in tracking user activity in intellectual property theft cases internally or in tracking hackers. Removable storage device investigations are often an essential part of performing digital forensics. We will show you how to perform in-depth USB device examinations on Windows 7, 8/8.1, and 10. You will learn how to determine when a storage device was first and last plugged in, its vendor/make/model, and even the unique serial number of the device used.

Topics: Shell Item Forensics; USB and Bring Your Own Device (BYOD) Forensic Examinations

DAY 4: Core Windows Forensics Part 3 – Email, Key Additional Artifacts, and Event Logs

Depending on the type of investigation and authorization, a wealth of evidence can be unearthed through the analysis of email files. Recovered email can bring excellent corroborating information to an investigation, and its informality often provides very incriminating evidence. It is common for users to have an email that exists locally on their workstation, on their company email server, in a private cloud, and in multiple webmail accounts. Windows event log analysis has solved more cases than possibly any other type of analysis. Understanding the locations and content of these files is crucial to the success of any investigator. Many researchers overlook these records because they do not have adequate knowledge or tools to get the job done efficiently. This section arms each investigator with the core knowledge and capability to maintain this crucial skill for many years to come.

Topics: Email Forensics; Forensicating Additional Windows OS Artifacts; Windows Event Log Analysis

DAY 5: Core Windows Forensics Part 4 – Web Browser Forensics: Firefox, Internet Explorer, and Chrome

With the increasing use of the web and the shift toward web-based applications and cloud computing, browser forensic analysis has become a critical skill. During this section, the investigator will comprehensively explore web browser evidence created during the use of Internet Explorer, Edge, Firefox, and Google Chrome. The analyst will learn how to examine every significant artifact stored by the browser and how to analyze some of the more obscure (and powerful) browser artifacts, such as session restore, tracking cookies, zoom levels, predictive site prefetching, and private browsing remnants.

Topics: Browser Forensics: History, Cache, Searches, Downloads, Understanding Browser Timestamps, Internet Explorer; Edge; Firefox; Chrome; Examining of Browser Artifacts; Tools Used

DAY 6: Windows Forensic Challenge

This complex case will involve an investigation into one of the most recent versions of the Windows Operating System. The evidence is real and provides the most realistic training opportunity currently available. Solving the case will require that students use all of the skills gained from each of the previous sections.

Topics: Digital Forensic Case; Windows 10 Forensic Challenge

Who Should Attend

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

"Excellent and engaging course that provides in-depth knowledge taught by true professionals."

-Callum Wilson, **Grant Thornton**

"This course has really helped me gain critical and useful knowledge that I can use directly at my work."

-Daniel Frasure, **KPMG**

FOR508: **Advanced Incident Response, Threat Hunting, and Digital Forensics**

GCFA
Forensic Analyst
www.giac.org/gcfa

6	36	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Learn and master the tools, techniques, and procedures necessary to effectively hunt, detect, and contain a variety of adversaries and remediate incidents
- Detect and hunt unknown live, dormant, and custom malware in memory across multiple Windows systems in an enterprise environment
- Hunt through and perform incident response across hundreds of unique systems simultaneously using F-Response Enterprise and the SIFT Workstation
- Identify and track malware beaconing outbound to its command and control (C2) channel via memory forensics, registry analysis, and network connection residue
- Determine how the breach occurred by identifying the beachhead and spear phishing attack mechanisms
- Target advanced adversary anti-forensics techniques like hidden and time-stomped malware, along with utility-ware used to move in the network and maintain an attacker's presence
- Use memory analysis, incident response, and threat hunting tools in the SIFT Workstation to detect hidden processes, malware, attacker command lines, rootkits, network connections, and more
- Track user and attacker activity second-by-second on the system you are analyzing through in-depth timeline and super-timeline analysis
- Recover data cleared using anti-forensics techniques via Volume Shadow Copy and Restore Point analysis
- Identify lateral movement and pivots within your enterprise, showing how attackers transition from system to system without detection

Hal Pomeranz
SANS Faculty Fellow

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics will help you to:

- Detect how and when a breach occurred
- Identify compromised and affected systems
- Perform damage assessments and determine what was stolen or changed
- Contain and remediate incidents
- Develop key sources of threat intelligence
- Hunt down additional breaches using knowledge of the adversary

DAY 0: A 3-letter government agency contacts you to say an advanced threat group is targeting organizations like yours, and that your organization is likely a target. They won't tell how they know, but they suspect that there are already several breached systems within your enterprise. An advanced persistent threat, aka an APT, is likely involved. This is the most sophisticated threat that you are likely to face in your efforts to defend your systems and data, and these adversaries may have been actively rummaging through your network undetected for months or even years.

This is a hypothetical situation, but the chances are very high that hidden threats already exist inside your organization's networks. Organizations can't afford to believe that their security measures are perfect and impenetrable, no matter how thorough their security precautions might be. Prevention systems alone are insufficient to counter focused human adversaries who know how to get around most security and monitoring tools.

The key is to constantly look for attacks that get past security systems, and to catch intrusions in progress, rather than after attackers have completed their objectives and done significant damage to the organization. For the incident responder, this process is known as "threat hunting." Threat hunting uses known adversary behaviors to proactively examine the network and endpoints in order to identify new data breaches.

Threat hunting and Incident response tactics and procedures have evolved rapidly over the past several years. Your team can no longer afford to use antiquated incident response and threat hunting techniques that fail to properly identify compromised systems, provide ineffective containment of the breach, and ultimately fail to rapidly remediate the incident. Incident response and threat hunting teams are the keys to identifying and observing malware indicators and patterns of activity in order to generate accurate threat intelligence that can be used to detect current and future intrusions.

This in-depth incident response and threat hunting course provides responders and threat hunting teams with advanced skills to hunt down, identify, counter, and recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, organized crime syndicates, and hactivists. Constantly updated, FOR508: Advanced Incident Response and Threat Hunting addresses today's incidents by providing hands-on incident response and threat hunting tactics and techniques that elite responders and hunters are successfully using to detect, counter, and respond to real-world breach cases.

ADVANCED THREATS ARE IN YOUR NETWORK – IT'S TIME TO GO HUNTING!

Hal Pomeranz is an independent digital forensic investigator who has consulted on cases ranging from intellectual property theft to employee sabotage, organized cybercrime, and malicious software infrastructures. He has worked with law enforcement agencies in the United States and Europe and with global corporations. Equally at home in the Windows or Mac environment, Hal is recognized as an expert in the analysis of Linux and Unix systems. His research on EXT4 file system forensics provided a basis for the development of open-source forensic support for this file system. His EXT3 file recovery tools are used by investigators worldwide. Hal is a SANS Lethal Forensicator, and is the creator of the SANS Linux/Unix Security track (GCUX). He holds the GCFA and GREM certifications and teaches the related courses in the SANS Forensics curriculum. He is a respected author and speaker at industry gatherings worldwide. Hal is a regular contributor to the SANS Computer Forensics blog and co-author of the Command Line Kung Fu blog.
@hal_pomeranz

Course Day Descriptions

Mon, Feb 3 – Sat, Feb 8
9:00am – 5:00pm
Hands-on labs

This course is available via **Simulcast**. See page 64 for more information.

DAY 1: Advanced Incident Response and Threat Hunting

Incident responders and threat hunters should be armed with the latest tools, memory analysis techniques, and enterprise methodologies to identify, track, and contain advanced adversaries and remediate incidents. Incident response and threat hunting analysts must be able to scale their analysis across thousands of systems in their enterprise. This section examines the six-step incident response methodology as it applies to incident response for advanced threat groups. We will show the importance of developing cyber threat intelligence to impact the adversaries' "kill chain" and demonstrate live response techniques and tactics that can be applied to a single system and across the entire enterprise.

Topics: Real Incident Response Tactics; Threat Hunting; Threat Hunting in the Enterprise; Incident Response and Hunting across Endpoints; Malware Defense Evasion and Identification; Malware Persistence Identification; Investigating WMI-Based Attacks

DAY 2: Intrusion Analysis

Cyber defenders have a wide variety of tools and artifacts available to identify, hunt, and track adversary activity in a network. Each attacker action leaves a corresponding artifact, and understanding what is left behind as footprints can be critical to both red and blue team members. Attacks follow a predictable pattern, and we focus our detective efforts on immutable portions of that pattern. As an example, at some point attackers will need to run code to accomplish their objectives. We can identify this activity via application execution artifacts. Attackers will also need one or more accounts to run code. Consequently, account auditing is a powerful means of identifying malicious actions. Attackers also need a means to move throughout the network, so we look for artifacts left by the relatively small number of ways there are to accomplish this part of their mission. In this section, we cover common attacker tradecraft and discuss the various data sources and forensic tools you can use to identify malicious activity in the enterprise.

Topics: Stealing and Utilization of Legitimate Credentials; Advanced Evidence of Execution Detection; Lateral Movement Adversary Tactics, Techniques, and Procedures (TTPs); Log Analysis for Incident Responders and Hunters

Who Should Attend

- Incident response team members
- Threat hunters
- Security Operations Center analysts
- Experienced digital forensic analysts
- Information security professionals
- Federal agents and law enforcement personnel
- Red team members, penetration testers, and exploit developers
- SANS FOR500 and SEC504 graduates

"FOR508 was outstanding. The breadth and depth of the content was impressive."

-Al Sears, **Skechers, USA**

DAY 3: Memory Forensics in Incident Response and Threat Hunting

Now a critical component of many incident response and threat hunting teams that regularly detect advanced adversaries in their organization, memory forensics has come a long way in just a few years. Memory forensics can be extraordinarily effective at finding evidence of worms, rootkits, PowerShell, and advanced malware used by APT attackers. In fact, some attacks may be nearly impossible to unravel without memory analysis. Memory analysis was traditionally the domain of Windows internals experts, but the recent development of new tools and techniques makes it accessible today to all investigators, incident responders, and threat hunters. Better tools, interfaces and detection heuristics have greatly leveled the playing field. Understanding attack patterns in memory is a core analyst skill applicable across a wide range of endpoint detection and response products. This extremely popular section will cover many of the most powerful memory analysis capabilities available and give you a solid foundation of advanced memory forensic skills to super-charge investigations, regardless of the toolset employed.

Topics: Remote and Enterprise Incident Response; Triage and Enpoint Detection and Reponse; Memory Acquisition; Memory Forensics Analysis Process for Response and Hunting; Memory Forensics Examinations; Memory Analysis Tools

DAY 4: Timeline Analysis

Learn advanced incident response and hunting techniques uncovered via timeline analysis directly from the authors who pioneered timeline analysis tradecraft. Temporal data are located everywhere on a computer system. Filesystem modified/access/creation/change times, log files, network data, registry data, and Internet history files all contain time data that can be correlated into critical analysis to successfully solve cases. Pioneered by Rob Lee in 2001, timeline analysis has become a critical incident response, hunting, and forensics technique. New timeline analysis frameworks provide the means to conduct simultaneous examinations of a multitude of time-based artifacts. The analysis that once took days now takes minutes. This section will step you through the two primary methods of building and analyzing timelines created during advanced incident response, threat hunting, and forensic cases. Exercises will show analysts how to create a timeline and also how to introduce the key methods to help you use those timelines effectively in your cases.

Topics: Timeline Analysis Overview; Memory Analysis Timeline Creation; Filesystem Timeline Creation and Analysis; Super Timeline Creation and Analysis

DAY 5: Incident Response & Hunting Across the Enterprise – Advanced Adversary and Anti-Forensics Detection

Over the years, we have observed that many incident responders and threat hunters have a challenging time finding threats without pre-built indicators of compromise or threat intelligence gathered before a breach. This is especially true in APT adversary intrusions. This advanced session will demonstrate techniques used by first responders to identify malware or forensic artifacts when very little information exists about their capabilities or hidden locations. We will discuss techniques to help funnel possibilities down to the candidates most likely to be evil malware trying to hide on the system.

Topics: Cyber Threat Intelligence; Malware and Anti-Forensic Detection; Anti-Forensic Detection Methodologies; Identifying Compromised Hosts without Active Malware

DAY 6: The APT Threat Group Incident Response Challenge

This incredibly rich and realistic enterprise intrusion exercise is based on a real-world advanced persistent threat (APT) group. It brings together techniques learned earlier in the week and tests your newly acquired skills in a case that simulates an attack by an advanced adversary. The challenge brings it all together using a real intrusion into a complete Windows enterprise environment. You will be asked to uncover how the systems were compromised in the initial intrusion, find other systems the adversary moved to laterally, and identify intellectual property stolen via data exfiltration. You will walk out of the course with hands-on experience investigating realistic attacks, curated by a cadre of instructors with decades of experience fighting advanced threats from attackers ranging from nation-states to financial crime syndicates and hactivist groups.

Topics: Identification and Scoping; Containment and Threat Intelligence Gathering; Remediation and Recovery

FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

GNFA
Network Forensic Analyst
www.giac.org/gnfa

6	36	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Extract files from network packet captures and proxy cache files, allowing for follow-on malware analysis or definitive data loss determination
- Use historical NetFlow data to identify relevant past network occurrences, allowing for accurate incident scoping
- Reverse-engineer custom network protocols to identify an attacker's command-and-control abilities and actions
- Decrypt captured SSL traffic to identify attackers' actions and what data they extracted from the victim
- Use data from typical network protocols to increase the fidelity of the investigation's findings
- Identify opportunities to collect additional evidence based on the existing systems and platforms within a network architecture
- Examine traffic using common network protocols to identify patterns of activity or specific actions that warrant further investigation
- Incorporate log data into a comprehensive analytic process, filling knowledge gaps that may be far in the past
- Learn how attackers leverage man-in-the-middle tools to intercept seemingly secure communications
- Examine proprietary network protocols to determine what actions occurred on the endpoint systems
- Analyze wireless network traffic to find evidence of malicious activity
- Learn how to modify configuration on typical network devices such as firewalls and intrusion detection systems to increase the intelligence value of their logs and alerts during an investigation

Philip Hagen
SANS Senior Instructor

This course will help you take your system-based forensic knowledge onto the wire. Incorporate network evidence into your investigations, provide better findings, and get the job done faster.

It is exceedingly rare to work any forensic investigation that doesn't have a network component. Endpoint forensics will always be a critical and foundational skill for this career, but overlooking a perpetrator's network communications is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, employee misuse scenario, or are engaged in proactive adversary discovery, the network often provides an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, uncover attackers that have been active for months or longer, or even prove useful in definitively proving a crime actually occurred.

FOR572 was designed to cover the most critical skills needed for the increased focus on network communications and artifacts in today's investigative work, including numerous use cases. Many investigative teams are incorporating proactive threat hunting, in which existing evidence is used with newly-acquired threat intelligence to uncover evidence of previously-unidentified incidents. Other teams focus on post-incident investigations and reporting. Still others engage with an adversary in real time, seeking to contain and eradicate the attacker from the victim's environment. In these situations and more, the artifacts left behind from attackers' communications can provide an invaluable view into their intent, capabilities, successes, and failures.

In FOR572, we focus on the knowledge necessary to examine and characterize communications that have 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-based dissection, 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 under way.

FOR572 is truly an advanced course – we hit the ground running on day one. Bring your entire bag of skills: forensic techniques and methodologies, full-stake networking knowledge (from the wire all the way up to user-facing services), Linux shell utilities, and everything in between. They will all benefit you throughout the course as you hone your skills to fight crime.

UNRAVEL INCIDENTS...ONE BYTE (OR PACKET) AT A TIME.

Phil Hagen began his studies at the U.S. Air Force Academy's Computer Science Department, where he focused on network security and was an inaugural member of the computer security extracurricular group. He served in the Air Force as a communications officer at Beale AFB and the Pentagon. Today, Phil's career has spanned the full attack life cycle – tool development, deployment, operations, and the investigative aftermath – giving him rare and deep insight into the artifacts left behind. Phil has covered deep technical tasks, managed an entire computer forensic services portfolio, and handled executive responsibilities. He has supported systems that demanded 24x7x365 functionality, managed a team of 85 computer forensic professionals in the national security sector, and provided forensic consulting services for law enforcement, government, and commercial clients. All of that brings Phil to his role today as the DFIR strategist at Red Canary, where he supports the firm's managed threat detection service. Phil also spends time developing and maintaining the SOF-ELK distribution, a virtual appliance free for the DFIR Community.
@PhilHagen

Course Day Descriptions

Mon, Feb 3 – Sat, Feb 8
9:00am – 5:00pm
Hands-on labs

DAY 1: Off the Disk and Onto the Wire

Although many fundamental network forensic concepts align with those of any other digital forensic investigation, the network presents many nuances that require special attention. Today you will learn how to apply what you already know about digital forensics and incident response to network-based evidence. You will also become acclimated to the basic tools of the trade.

Topics: Web Proxy Server Examination; Foundational Network Forensics Tools: tcpdump and Wireshark; Network Evidence Acquisition; Network Architectural Challenges and Opportunities

DAY 2: Core Protocols & Log Aggregation/Analysis

There are countless network protocols that may be in use in a production network environment. We will cover those that are most likely to benefit the forensicator in typical casework, as well as several that help demonstrate analysis methods useful when facing new, undocumented, or proprietary protocols. By learning the "typical" behaviors of these protocols, we can more readily identify anomalies that may suggest misuse of the protocol for nefarious purposes. These protocol artifacts and anomalies can be profiled through direct traffic analysis as well as through the log evidence created by systems that have control or visibility of that traffic. While this affords the investigator with vast opportunities to analyze the network traffic, efficient analysis of large quantities of source data generally requires tools and methods designed to scale.

Topics: Hypertext Transfer Protocol (HTTP): Protocol and Logs; Domain Name Service (DNS): Protocol and Logs; Firewall, Intrusion Detection System, and Network Security Monitoring Logs; Logging Protocol and Aggregation; ELK Stack and the SOF-ELK Platform

Who Should Attend

- Incident response team members and forensicators
- Hunt team members
- 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

DAY 3: NetFlow and File Access Protocols

Network connection logging, commonly called NetFlow, may be the single most valuable source of evidence in network investigations. Many organizations have extensive archives of flow data due to its minimal storage requirements. Since NetFlow does not capture any content of the transmission, many legal issues with long-term retention are mitigated. Even without content, NetFlow provides an excellent means of guiding an investigation and characterizing an adversary's activities from pre-attack through operations. Whether within a victim's environment or for data exfiltration, adversaries must move their quarry around through the use of various file access protocols. By knowing some of the more common file access and transfer protocols, a forensicator can quickly identify an attacker's theft actions.

Topics: NetFlow Collection and Analysis; Open-Source Flow Tools; File Transfer Protocol (FTP); Microsoft Protocols

DAY 4: Commercial Tools, Wireless, and Full-Packet Hunting

Commercial tools are a mainstay in the network forensicator's toolkit. We'll explore the various roles that commercial tools generally fill, as well as how they can be best integrated into an investigative workflow. With the runaway adoption of wireless networking, investigators must also be prepared to address the unique challenges this technology brings to the table. However, regardless of the protocol being examined or budget used to perform the analysis, having a means of exploring full-packet capture is a necessity, and having a toolkit to perform this at scale is critical.

Topics: Simple Mail Transfer Protocol (SMTP); Commercial Network Forensics; Wireless Network Forensics; Automated Tools and Libraries; Full-Packet Hunting with Moloch

DAY 5: Encryption, Protocol Reversing, OPSEC, and Intel

Advancements in common technology have made it easier to be a bad guy and harder for us to track them. Strong encryption methods are readily available and custom protocols are easy to develop and employ. Despite this, there are still weaknesses even in the most advanced adversaries' methods. As we learn what the attackers have deliberately hidden from us, we must operate carefully to avoid tipping our hats regarding the investigative progress – otherwise the attacker can quickly pivot, nullifying our progress.

Topics: Encoding, Encryption, and SSL/TLS; Meddler-in-the-Middle; Network Protocol Reverse Engineering; Investigation OPSEC and Threat Intel

DAY 6: Network Forensics Capstone Challenge

This section will combine all of what you have learned prior to and during this week. In groups, you will examine network evidence from a real-world compromise by an advanced attacker. Each group will independently analyze data, form and develop hypotheses, and present findings. No evidence from endpoint systems is available – only the network and its infrastructure.

Topics: Network Forensic Case

"Excellent tools and strategies to bring back to the workplace."

-Branco Jacob, **NCDOC**

"Essential to any investigator's skill set, this course makes the advanced network forensics techniques easily graspable."

-Casey Brooks, **Leidos Cyber**

FOR578: **Cyber Threat Intelligence**

GCTI
Cyber Threat Intelligence
www.giac.org/gcti

5 Day Program	30 CPEs	Laptop Required

Who Should Attend

- Security practitioners
- Incident response team members
- Threat hunters
- Security Operations Center personnel and information security practitioners
- Digital forensic analysts and malware analysts
- Federal agents and law enforcement officials
- Technical managers
- SANS alumni looking to take their analytical skills to the next level

"This course does a great job of teaching a sound methodology and an evidence-based approach to IT, and in breaking down biases and reconstructing analytical pathways."

-Sveva Vittoria Scenarreli, **PwC UK**

Security practitioners should attend FOR578: Cyber Threat Intelligence because it is unlike any other technical training. It focuses on structured analysis in order to establish a solid foundation for any security skill set and to amplify existing skills. The course will help practitioners from across the security spectrum to:

- Develop analysis skills to better comprehend, synthesize, and leverage complex scenarios
- Identify and create intelligence requirements through practices such as threat modeling
- Understand and develop skills in tactical, operational, and strategic-level threat intelligence
- Generate threat intelligence to detect, respond to, and defeat focused and targeted threats
- Learn about the different sources from which to collect adversary data and how to exploit and pivot off of those data
- Validate information received externally to minimize the costs of bad intelligence
- Create Indicators of Compromise (IOCs) in formats such as YARA, OpenIOC, and STIX
- Move security maturity past IOCs into understanding and countering the behavioral tradecraft of threats
- Establish structured analytical techniques to be successful in any security role

It is common for security practitioners to call themselves analysts. But how many of us have taken structured analysis training instead of simply attending technical training? Both are important, but very rarely do analysts focus on training on analytical ways of thinking. This course exposes analysts to new mindsets, methodologies, and techniques that will complement their existing knowledge as well as establish new best practices for their security teams. Proper analysis skills are key to the complex world that defenders are exposed to on a daily basis.

The analysis of an adversary's intent, opportunity, and capability to do harm is known as cyber threat intelligence. Intelligence is not a data feed, nor is it something that comes from a tool. Intelligence is actionable information that answers a key knowledge gap, pain point, or requirement of an organization. This collection, classification, and exploitation of knowledge about adversaries gives defenders an upper hand against adversaries and forces defenders to learn and evolve with each subsequent intrusion they face.

Cyber threat intelligence thus represents a force multiplier for organizations looking to establish or update their response and detection programs to deal with increasingly sophisticated threats. Malware is an adversary's tool, but the real threat is the human one, and cyber threat intelligence focuses on countering those flexible and persistent human threats with empowered and trained human defenders.

Knowledge about the adversary is core to all security teams. The red team needs to understand adversaries' methods in order to emulate their tradecraft. The Security Operations Center needs to know how to prioritize intrusions and quickly deal with those that need immediate attention. The incident response team needs actionable information on how to quickly scope and respond to targeted intrusions. The vulnerability management group needs to understand which vulnerabilities matter most for prioritization and the risk that each one presents. The threat hunting team needs to understand adversary behaviors to search out new threats.

In other words, cyber threat intelligence informs all security practices that deal with adversaries. FOR578: Cyber Threat Intelligence will equip you, your security team, and your organization with the tactical, operational, and strategic-level cyber threat intelligence skills and tradecraft required to better understand the evolving threat landscape and to accurately and effectively counter those threats.

Peter Szczepankiewicz
SANS Certified Instructor

In his past work with the military, Peter responded to network attacks and worked with both defensive and offensive red teams. Currently, Peter is a Senior Security Engineer with IBM. Peter believes that people lead technology, not the other way around. He works daily to bring actionable intelligence out of disparate security devices for customers, making systems interoperable. As Peter explains, "Putting together networks only to tear them apart is just plain fun, and allows students to take the information learned from books and this hands-on experience back to their particular work place."
@_s14

Course Day Descriptions

Mon, Feb 3 – Fri, Feb 7
9:00am – 5:00pm
Hands-on labs

DAY 1: Cyber Threat Intelligence and Requirements

Cyber threat intelligence is a rapidly growing field. However, intelligence was a profession long before the word "cyber" entered the lexicon. Understanding the key points regarding intelligence terminology, tradecraft, and impact is vital to understanding and using cyber threat intelligence. This section introduces students to the most important concepts of intelligence, analysis tradecraft, and levels of threat intelligence, as well as the value they can add to organizations. It also focuses on getting your intelligence program off to the right start with planning, direction, and the generation of intelligence requirements. As with all sections, the day includes immersive hands-on labs to ensure that students have the ability to turn theory into practice.

Topics: Case Study: Carbanak, The Great Bank Robbery; Understanding Intelligence; Understanding Cyber Threat Intelligence; Threat Intelligence Consumption; Positioning the Team to Generate Intelligence; Planning and Direction (Developing Requirements)

DAY 2: The Fundamental Skill Set: Intrusion Analysis

Intrusion analysis is at the heart of threat intelligence. It is a fundamental skill set for any security practitioner who wants to use a more complete approach to addressing security. Two of the most commonly used models for assessing adversary intrusions are the "kill chain" and the "Diamond Model." These models serve as a framework and structured scheme for analyzing intrusions and extracting patterns such as adversary behaviors and malicious indicators. In this section students will participate in and be walked through multi-phase intrusions from initial notification of adversary activity to the completion of analysis of the event. The section also highlights the importance of this process in terms of structuring and defining adversary campaigns.

Topics: Primary Collection Source: Intrusion Analysis; Kill Chain Courses of Action; Kill Chain Deep Dive; Handling Multiple Kill Chains; Collection Source: Malware

DAY 3: Collection Sources

Cyber threat intelligence analysts must be able to interrogate and fully understand their collection sources. Analysts do not have to be malware reverse engineers, as an example, but they must at least understand that work and know what data can be sought. This section continues from the previous one in identifying key collection sources for analysts. There is also a lot of available information on what is commonly referred to as open-source intelligence (OSINT). In this course section students will learn to seek and exploit information from Domains, External Datasets, Transport Layer Security/Secure Sockets Layer (TLS/SSL) Certificates, and more while also structuring the data to be exploited for purposes of sharing internally and externally.

Topics: Case Study: Axiom; Collection Source: Domains; Case Study: GlassRAT; Collection Source: External Datasets; Collection Source: TLS Certificates; Case Study: Trickbots; Exploitation: Storing and Structuring Data

DAY 4: Analysis and Dissemination of Intelligence

Many organizations seek to share intelligence but often fail to understand its value, its limitations, and the right formats to choose for each audience. Additionally, indicators and information shared without analysis are not intelligence. Structured analytical techniques such as the Analysis of Competing Hypotheses can help add considerable value to intelligence before it is disseminated. This section will focus on identifying both open-source and professional tools that are available for students as well as on sharing standards for each level of cyber threat intelligence both internally and externally. Students will learn about YARA and generate YARA rules to help incident responders, security operations personnel, and malware analysts. Students will gain hands-on experience with STIX and understand the CybOX and TAXII frameworks for sharing information between organizations. Finally, the section will focus on building the singular intrusions into campaigns and being able to communicate about those campaigns.

Topics: Analysis: Exploring Hypotheses; Analysis: Building Campaigns; Dissemination: Tactical; Case Study: Sony Attack; Dissemination: Operational

DAY 5: Higher-Order Analysis and Attribution

A core component of intelligence analysis at any level is the ability to defeat biases and analyze information. The skills required to think critically are exceptionally important and can have an organization-wide or national-level impact. In this course section, students will learn about logical fallacies and cognitive biases as well as how to defeat them. They will also learn about nation-state attribution, including when it can be of value and when it is merely a distraction. Students will also learn about nation-state-level attribution from previously identified campaigns and take away a more holistic view of the cyber threat intelligence industry to date. The class will finish with a discussion on consuming threat intelligence and actionable takeaways for students to make significant changes in their organizations once they complete the course.

Topics: Logical Fallacies and Cognitive Biases; Dissemination Strategies; Case Study: Stuxnet; Fine-Tuning Analysis; Case Study: Sofacy; Attribution

"This training summarizes CTI very well and connects all the dots. The training gives you clear answers to the following questions: what is CTI, how important is it, what is it built upon, and how can it be applied in practice?"

-Nikita Martynov, **NNIT A/S**

"I could take this course five times more and get something new each time! So much valuable info to take back to my organization."

-Charity Willhoite, **Armor Defense, Inc.**

FOR585: **Smartphone Forensic Analysis In-Depth**

GASF
Advanced Smartphone Forensics
www.giac.org/gasf

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Select the most effective forensic tools, techniques, and procedures for critical analysis of smartphone data
- Reconstruct events surrounding a crime using information from smartphones, including manual timeline development and link analysis (e.g., who communicated with whom, where, and when) without relying on a tool
- Understand how smartphone file systems store data, how they differ, and how the evidence will be stored on each device
- Interpret file systems on smartphones and locate information that is not generally accessible to users
- Identify how the evidence got onto the mobile device – we'll teach you how to know if the user created the data, which will help you avoid the critical mistake of reporting false evidence obtained from tools
- Incorporate manual decoding techniques to recover deleted data stored on smartphones and mobile devices
- Tie a user to a smartphone at a specific date/time and at various locations
- Recover hidden or obfuscated communication from applications on smartphones
- Decrypt or decode application data that are not parsed by your forensic tools
- Detect smartphones compromised by malware and spyware using forensic methods
- Decompile and analyze mobile malware using open-source tools
- Handle encryption on smartphones and bypass, crack, and/or decode lock codes manually recovered from smartphones, including cracking iOS backup files that were encrypted with iTunes

FOR585: Smartphone Forensic Analysis In-Depth will help you understand:

- Where key evidence is located on a smartphone
- How the data got onto the smartphone
- How to recover deleted mobile device data that forensic tools miss
- How to decode evidence stored in third-party applications
- How to detect, decompile, and analyze mobile malware and spyware
- Advanced acquisition terminology and free techniques to gain access to data on smartphones
- How to handle locked or encrypted devices, applications, and containers

SMARTPHONES HAVE MINDS OF THEIR OWN. DON'T MAKE THE MISTAKE OF REPORTING SYSTEM EVIDENCE, SUGGESTIONS, OR APPLICATION ASSOCIATIONS AS USER ACTIVITY. IT'S TIME TO GET SMARTER!

A smartphone lands on your desk and you are tasked with determining if the user was at a specific location at a specific date and time. You rely on your forensic tools to dump and parse the data. The tools show location information tying the device to the place of interest. Are you ready to prove the user was at that location? Do you know how to take this further to place the subject at the location of interest at that specific date and time? Tread carefully, because the user may not have done what the tools are showing!

Mobile devices are often a key factor in criminal cases, intrusions, IP theft, security threats, accident reconstruction, 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: Smartphone Forensic Analysis In-Depth 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. Examination and interpretation of 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 31 hands-on labs, a forensic challenge, and a bonus take-home case that allow students to analyze different datasets from smart devices and leverage the best forensic tools, methods, 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.

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 smartphone activity can and will be used against them!

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

Heather Mahalik
SANS Senior Instructor

Heather has worked on high-stress and high-profile cases, investigating everything from child exploitation to Osama Bin Laden's media. She has helped law enforcement, eDiscovery firms, and the federal government extract and manually decode artifacts used in solving investigations around the world. All told she has more than 14 years of experience in digital forensics, including eight years focused on mobile forensics—there's hardly a device or platform she hasn't researched or examined or a commercial tool she hasn't used. These days Heather is the Senior Director of Digital Intelligence at Cellebrite. Heather previously led the mobile device team for Basis Technology, where she focused on mobile device exploitation in support of the federal government. She also worked as a forensic examiner at Stroz Friedberg and the U.S. State Department Computer Investigations and Forensics Lab, where she handled a number of high-profile cases. She has also developed and implemented forensic training programs and standard operating procedures.
@HeatherMahalik

Course Day Descriptions

Mon, Feb 3 – Sat, Feb 8
9:00am – 5:00pm
Hands-on labs

This course is available via **Simulcast**. See page 64 for more information.

DAY 1: Smartphone Overview, Misfit Devices, SQLite Introduction, and Android Forensics Overview

Although smartphone forensic concepts are similar to those of digital forensics, smartphone file system structures differ and require specialized decoding skills to correctly interpret the data acquired from the device. On this first course day, students will apply what they know to smartphone forensic handling, device capabilities, acquisition methods, misfit devices, SQLite database examination, and query development. They'll also gain an overview of Android devices and manually crack locked Androids. Students will become familiar with the forensic tools required to complete comprehensive examinations of smartphone data structures. We realize that not everyone examines BlackBerry and knock-off devices, which is why we offer "choose your own adventure" labs, meaning that students can select the labs most relevant to them. BlackBerry 10 smartphones are designed to protect user privacy, but techniques taught on this course day will enable the investigator to go beyond what the tools decode and manually recover data residing in database files of BlackBerry 10 device file systems. Knock-off devices are another outlier than can be parsed and decoded once you become familiar with the file system structures.

Topics: The SIFT Workstation; Forensic Acquisition Concepts of Smartphones; Smartphone Components; Introduction to SQLite; Android Forensic Overview; Handling Locked Android Devices

DAY 2: Android Forensics

Android devices are among the most widely used smartphones in the world, which means they will surely be part of an investigation that will come across your desk. Unfortunately, gaining access to these devices isn't as easy as it used to be. Android devices contain substantial amounts of data that can be decoded and interpreted into useful information. However, without honing the appropriate skills to bypass locked Androids and correctly interpret the data stored on them, you will be unprepared for the rapidly evolving world of smartphone forensics. Android backups can be created for forensic analysis or by a user. Smartphone examiners need to understand the file structures and how to parse these data. Additionally, Android and Google cloud data store tons of valuable information. You will find Google artifacts from iOS users as well.

Topics: Android Acquisition Considerations; Android File System Structures; Android Evidentiary Locations; Traces of User Activity on Android Devices; Android Backup Files; Google Cloud Data and Extractions

Who Should Attend

- Experienced digital forensic analysts
- Media exploitation analysts
- Information security professionals
- Incident response teams
- Law enforcement officers, federal agents, and detectives
- Accident reconstruction investigators
- IT auditors
- Graduates of SANS SEC575, SEC563, FOR500, FOR508, FOR572, FOR526, FOR610, or FOR518 who want to take their skills to the next level

"This course addresses the ever-increasing challenges that continually emerge in smartphone forensics."

-Hilary Tiony,
Directorate of E-govt Kenya

DAY 3: iOS Device Forensics

Apple iOS devices contain substantial amounts of data (including deleted records) that can be decoded and interpreted into useful information. Proper handling and parsing skills are needed for bypassing locked iOS devices and correctly interpreting the data. Without iOS instruction, you will be unprepared to deal with the iOS device that will likely be a major component in a forensic investigation.

Topics: iOS Forensic Overview and Acquisition; iOS File System Structures; iOS Evidentiary Locations; Handling Locked iOS Devices; Traces of User Activity on iOS Devices

DAY 4: iOS Backups, Malware and Spyware Forensics, and Detecting Evidence Destruction

iOS backups are extremely common and are found in the cloud and on hard drives. Users create backups, and we often find that our best data can be derived from creating an iOS backup for forensic investigation. This section will cover methodologies to extract backups and cloud data and analyze the artifacts for each. Malware affects a plethora of smartphone devices. We will examine various types of malware, how it exists on smartphones, and how to identify and analyze it. Most commercial smartphone tools help you identify malware, but none of them will allow you to tear down the malware to the level we cover in class. Up to five labs will be conducted on this day alone! The day ends with the students challenging themselves using tools and methods learned throughout the week to recover user data from a wiped smartphone.

Topics: iOS Backup File Forensics; Locked iOS Backup Files; iCloud Data Extraction and Analysis; Malware and Spyware Forensics; Detecting Evidence Destruction

DAY 5: Third-Party Application Analysis

This day starts with third-party applications across all smartphones and is designed to teach students how to leverage third-party application data and preference files to support an investigation. The rest of the day focuses heavily on secure chat applications, recovery of deleted application data and attachments, mobile browser artifacts, and knock-off phone forensics. The skills learned in this section will provide you with advanced methods for decoding data stored in third-party applications across all smartphones. We will show you what the commercial tools miss and teach you how to recover these artifacts yourself.

Topics: Third-Party Applications Overview; Third-Party Application Artifacts; Messaging Applications and Recovering Attachments; Mobile Browsers; Secure Chat Applications

DAY 6: Smartphone Forensics Capstone Exercise

This final course day will test all that you have learned during the course. Working in small groups, students will examine three smartphone devices and solve a scenario relating to a real-world smartphone forensic investigation. Each group will independently analyze the three smartphones, manually decode data, answer specific questions, form an investigation hypothesis, develop a report, and present findings.

Topics: Identification and Scoping; Forensic Examination; Forensic Reconstruction

"With so many security measures put in place by O/S devs and app devs, the analysis techniques taught in this course are an absolute necessity. If the good guys want to stay ahead of the bad guys, this course is a must."

-Luis Martinez, **Westchester District Attorney's Office**

MGT414: SANS Training Program for CISSP® Certification

GISP
Information Security Professional
www.giac.org/gisp

6	46	Laptop
Day Program	CPEs	Not Needed

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

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that is specifically designed to prepare students to successfully pass the CISSP® exam.

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

After completing the course students will have:

- Detailed coverage of the eight domains of knowledge
- The analytical skills required to pass the CISSP® exam
- The technical skills required to understand each question
- The foundational information needed to become a Certified Information Systems Security Professional (CISSP®)

External Product Notice:

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

"This [course] really pulls a lot together for me and it has been hugely valuable. I know parts of this are going to impact my approach to my work from the first day back."

-Merewyn Boak, **Apple**

Seth Misenar
SANS Faculty Fellow

Seth Misenar is the founder of and lead consultant for Context Security, a Jackson, Mississippi-based company that 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 a physical and network security consultant for Fortune 100 companies, as well as 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 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 the CISSP®, GPEN, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE. **@sethmisenar**

Course Day Descriptions

Mon, Feb 3 – Sat, Feb 8
9:00am – 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am – 5:00pm (Day 6)
Evening bootcamp sessions

DAY 1: Introduction; Security and Risk Management

On the first day of training for the CISSP® exam, MGT414 introduces the specific requirements needed to obtain certification. The exam update will be discussed in detail. We will cover the general security principles needed to understand the eight domains of knowledge, with specific examples for each domain. The first of the eight domains, Security and Risk Management, is discussed using real-world scenarios to illustrate the critical points.

Topics: Overview of CISSP® Certification; Introductory Material; Overview of the Eight Domains; Domain 1: Security and Risk Management

DAY 2: Asset Security and Security Engineering – Part 1

Understanding asset security is critical to building a solid information security program. The Asset Security domain, the initial focus of today's course section, describes data classification programs, including those used by both governments and the military as well as the private sector. We will also discuss ownership ranging from business/mission owners to data and system owners. We will examine data retention and destruction in detail, including secure methods for purging data from electronic media. We then turn to the first part of the Security Engineering domain, including new topics for the 2019 exam such as the Internet of Things, Trusted Platform Modules, Cloud Security, and much more.

Topics: Domain 2: Asset Security; Domain 3: Security Engineering (Part 1)

DAY 3: Security Engineering – Part 2; Communication and Network Security

This course section continues the discussion of the Security Engineering domain, including a deep dive into cryptography. The focus is on real-world implementation of core cryptographic concepts, including the three types of cryptography: symmetric, asymmetric, and hashing. Salts are discussed, as well as rainbow tables. We will round out Domain 3 with a look at physical security before turning to Domain 4, Communication and Network Security. The discussion will cover a range of protocols and technologies, from the Open Systems Interconnection (OSI) model to storage area networks.

Topics: Domain 3: Security Engineering (Part 2); Domain 4: Communication and Network Security

DAY 4: Identity and Access Management

Controlling access to data and systems is one of the primary objectives of information security. Domain 5, Identity and Access Management, strikes at the heart of access control by focusing on identification, authentication, and authorization of accounts. Password-based authentication represents a continued weakness, so Domain 5 stresses multi-factor authentication, biometrics, and secure credential management. The CISSP® exam underscores the increased role of external users and service providers, and mastery of Domain 5 requires an understanding of federated identity, SSO, SAML, and third-party identity and authorization services like Oauth and OpenID.

Topics: Domain 5: Identity and Access Management

DAY 5: Security Assessment and Testing; Security Operations

This course section covers Domain 6 (Security Assessment) and Domain 7 (Security Operations). Security Assessment covers types of security tests, testing strategies, and security processes. Security Operations covers investigatory issues, including eDiscovery, logging and monitoring, and provisioning. We will discuss cutting-edge technologies such as the cloud, and we'll wrap up day five with a deep dive into disaster recovery.

Topics: Domain 6: Security Assessment; Domain 7: Security Operations

DAY 6: Software Development Security

Domain 8 (Software Development Security) describes the requirements for secure software. Security should be "baked in" as part of network design from day one, since it is always less effective when it is added later to a poor design. We will discuss classic development models, including waterfall and spiral methodologies. We will then turn to more modern models, including agile software development methodologies. New content for the CISSP® exam update will be discussed, including DevOps. We will wrap up this course section by discussing security vulnerabilities, secure coding strategies, and testing methodologies.

Topics: Domain 8: Software Development Security

Who Should Attend

- Security professionals who are interested in understanding the concepts covered on the CISSP® exam as determined by (ISC)²
- Managers who want to understand the critical areas of information 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 the eight domains of knowledge can be applied to their current job

"Great discussions and examples that provide a clear understanding and relate material to examples."

-Kelley O'Neil, **Wells Fargo**

MGT514: **Security Strategic Planning, Policy, and Leadership**

GSTRT
Strategic Planning, Policy & Leadership
www.giac.org/gstrt

5 Day Program | 30 CPEs | Laptop Not Needed

You Will Be Able To

- Develop security strategic plans that incorporate business and organizational drivers
- Develop and assess information security policy
- Use management and leadership techniques to motivate and inspire your teams

"The knowledge gained in class will directly translate to an increased maturity in my organization's security policy as topics and principles discussed are implemented."

-Mike Parkin, **Chapters Health System**

As security professionals we have seen the landscape change. Cybersecurity is now more vital and relevant to the growth of your organization than ever before. As a result, information security teams have more visibility, more budget, and more opportunity. However, with this increased responsibility comes more scrutiny.

This course teaches security professionals how to do three things:

- Develop Strategic Plans
  Strategic planning is hard for people in IT and IT security because we spend so much time responding and reacting. We almost never get to practice until we get promoted to a senior position and then we are not equipped with the skills we need to run with the pack. Learn how to develop strategic plans that resonate with other IT and business leaders.
- Create Effective Information Security Policy
  Policy is a manager's opportunity to express expectations for the workforce, set the boundaries of acceptable behavior, and empower people to do what they ought to be doing. It is easy to get wrong. Have you ever seen a policy and your response was, "No way, I am not going to do that!"? Policy must be aligned with an organization's culture. We will break down the steps to policy development so that you have the ability to develop and assess policy to successfully guide your organization.
- Develop Management and Leadership Skills
  Leadership is a capability that must be learned, exercised and developed to better ensure organizational success. Strong leadership is brought about primarily through selfless devotion to the organization and staff, tireless effort in setting the example, and the vision to see and effectively use available resources toward the end goal. Effective leadership entails persuading team members to accomplish their objectives while removing obstacles and maintaining the well-being of the team in support of the organization's mission. Learn to utilize management tools and frameworks to better lead, inspire, and motivate your teams.

Using case studies from Harvard Business School, team-based exercises, and discussions that put students in real-world scenarios, students will participate in activities that they can then carry out with their own team members when they return to work.

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

Mark Williams
SANS Certified Instructor

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

Course Day Descriptions

Mon, Feb 3 – Fri, Feb 7
9:00am – 5:00pm

DAY 1: Strategic Planning Foundations

On this first day we will introduce the key elements of strategic security plans and lay the groundwork for the rest of the course. Creating strategic plans for security requires a fundamental understanding of the business and a deep understanding of the threat landscape.

Topics: Vision and Mission Statements; Stakeholder Management; PEST Analysis; Porter's Five Forces; Threat Actors; Asset Analysis; Threat Analysis

DAY 2: Strategic Roadmap Development

With a firm understanding of business drivers as well as the threats facing the organization, you will develop a plan to analyze the current situation, identify the target situation, perform gap analysis, and develop a prioritized roadmap. In other words, you will be able to determine (1) what you do today, (2) what you should be doing in the future, (3) what you don't do, and (4) what you should do first. With this plan in place you will learn how to build and execute your plan by developing a business case, defining metrics for success, and effectively marketing your security program.

Topics: Historical Analysis; Values and Culture; SWOT Analysis; Vision and Innovation; Security Framework; Gap Analysis; Roadmap Development; Business Case Development; Metrics and Dashboards; Marketing and Executive Communications

DAY 3: Security Policy Development and Assessment

Policy is one of the key tools that security leaders have to influence and guide the organization. Security managers must understand how to review, write, assess, and support security policy and procedure. Using an instructional delivery methodology that balances lecture, exercises, and in-class discussion, this course section will teach techniques to create successful policy that users will read and follow and business leaders will accept. Learn key elements of policy, including positive and negative tone, consistency of policy bullets, how to balance the level of specificity to the problem at hand, the role of policy, awareness and training, and the SMART approach to policy development and assessment.

Topics: Purpose of Policy; Policy Gap Analysis; Policy Development; Policy Review; Awareness and Training

DAY 4: Leadership and Management Competencies

Learn the critical skills you need to lead, motivate, and inspire your teams to achieve the goal. By establishing a minimum standard for the knowledge, skills, and abilities required to develop leadership you will understand how to motivate employees and develop from a manager into a leader.

Topics: Leadership Building Blocks; Creating and Developing Teams; Coaching and Mentoring; Customer Service Focus; Conflict Resolution; Effective Communication; Leading Through Change; Relationship Building; Motivation and Self-Direction; Teamwork; Leadership Development

DAY 5: Strategic Planning Workshop

Using the case study method, students will work through real-world scenarios by applying the skills and knowledge learned throughout the course. Case studies are taken directly from Harvard Business School, the pioneer of the case-study method, and focus specifically on information security management and leadership competencies. The Strategic Planning Workshop serves as a capstone exercise for the course, allowing students to synthesize and apply concepts, management tools, and methodologies learned in class.

Topics: Creating a Security Plan for the CEO; Understanding Business Priorities; Enabling Business Innovation; Working with BYOD; Effective Communication; Stakeholder Management

Who Should Attend

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

"This training is valuable because it shines a light on the many business aspects of security, while also providing excellent guidance for applying learnings in real life."

-Alyssa DeVita, **Marriott**

MGT516: **Managing Security Vulnerabilities: Enterprise and Cloud** | **NEW!**

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Create, implement, or improve your vulnerability management program
- Establish a secure and defensible enterprise and cloud computing environment
- Build an accurate and useful inventory of IT assets in the enterprise and cloud
- Identify existing vulnerabilities and understand the severity level of each
- Prioritize vulnerabilities for treatment
- Effectively report and communicate vulnerability data within your organization
- Engage treatment teams and make vulnerability management fun

Vulnerabilities are everywhere. There are new reports of weaknesses within our systems and software every time we turn around. Directly related to this is an increase in the quantity and severity of successful attacks against these weaknesses.

Managing vulnerabilities in any size organization is challenging. Enterprise environments add scale and diversity that overwhelm many IT security and operations organizations. Add in the cloud and the increasing speed with which all organizations must deliver systems, applications, and features to both their internal and external customers, and security may seem unachievable.

This course highlights why many organizations are still struggling with vulnerability management today and shows students how to solve these challenges. How do we manage assets successfully and analyze and prioritize vulnerabilities? What reports are most effective? How do we deal with vulnerabilities in our applications, and how do we treat them? We'll examine how the answers to these questions change as we move to the cloud or implement a private cloud or DevOps within our organizations. How do we make vulnerability management fun and get everyone to engage in the process? These are just some of the important topics we will cover in this course.

The primary goal of this course is to help you succeed where many are failing and to present solutions to the problems many are experiencing or will experience. Whether your vulnerability management program is well established or just starting, this course will help you mature your program and think differently about vulnerability management.

By understanding common issues and the solutions to them, you will be better prepared to meet the challenges you are facing or will face, and to determine what works best for your organization. Through class discussions and other exercises, you will learn specific analysis and reporting techniques so that you will be able to discuss the problems you and your peers are facing and how to solve those problems.

The course is based on the Prepare, Identify, Analyze, Communicate, and Treat (PIACT) Model:

- Prepare: Define, build, and continuously improve the program
- Identify: Identify vulnerabilities present in our operating environments
- Analyze: Analyze and prioritize identified vulnerabilities and other program metrics to provide meaningful assistance and guidance to stakeholders and program participants
- Communicate: Present the findings from analysis appropriately and efficiently for each stakeholder group
- Treat: Implement, test, and monitor solutions to vulnerabilities, vulnerability groups, and broader issues identified by the program

Knowing that our environments are adopting cloud services and becoming more tightly integrated with them, we look at both cloud and non-cloud environments simultaneously throughout the course, highlighting the tools, processes, and procedures that can be leveraged in each environment and presenting new and emerging trends.

David Hazar
SANS Instructor

David has over 19 years of broad, deep technical experience gained from a variety of hands-on roles serving the financial, healthcare, and technology industries. Currently, he focuses primarily on vulnerability management, application security, cloud security, and secure DevOps, helping his clients understand how to move from scanning to an effective, integrated, and holistic vulnerability management program. He also helps automate and integrate existing processes and toolsets related to vulnerability management and secure DevOps both on-premise and in the cloud. In addition to being a coauthor and instructor of MGT516, he is an instructor for DEV40: Secure DevOps and Cloud Application Security. David completed a bachelor of science in information systems and a master of information systems management at Brigham Young University, and currently holds the following certifications: CISSP®, GWAPT, GWEB, GMOB, GCIA, GCIH, GCUX, GCWN, and GSSP-.NET. He is located in Salt Lake City, UT and enjoys spending time with his family, skiing, and snowboarding. **@DavidHazar**

Course Day Descriptions

Mon, Feb 3 – Fri, Feb 7
9:00am – 5:00pm

DAY 1: Overview and Identify

Day 1 begins with a discussion of how to make vulnerability management fun and improve engagement within your organization. Then, we dive into the cloud and discuss how cloud design and architecture can impact vulnerability management. We discuss how to discover and manage assets and what context is critical to the success of the program. Finally, we begin our discussion of how to find or identify vulnerabilities in our environments.

Topics: Introduction and Identify

DAY 2: Identify and Analyze

Day 2 wraps up our discussion on how to identify vulnerabilities and then moves into how to deal with all of the results. We will go over a variety of analysis and prioritization techniques that can be used to more effectively and efficiently deal with the data that are generated during identification.

Topics: Identify and Analyze

DAY 3: Communicate and Treat

Day 3 begins with how to communicate vulnerabilities, including what metrics are common or useful, and how to generate meaningful reports. We'll examine communication strategies and the different types of meetings that can facilitate communication and program participation. Then, we dive into how to treat vulnerabilities by discussing how change and patch management programs can impact vulnerability management.

Topics: Communicate and Treat

DAY 4: Treatment, Buy-in, and Program

Day 4 discusses the treat phase of the PIACT model. Successful treatment of vulnerabilities should be the primary goal of vulnerability management. Throughout the day we will discuss the common operational processes that are used to treat vulnerabilities. We will also look at some of the technology solutions available to assist with some of these processes, and discuss different and emerging operating models that may impact our treatment methodology.

Topics: Treatment, Buy-in, and Program

DAY 5: Managing Vulnerabilities: Capstone Lab Exercise

Day 5 begins with a review of a scenario that triggers the group capstone exercise. The day is broken up into various sections and scenarios that stem from the main case study, which enables students to delve into various aspects of the PIACT model. A review of findings and conclusions will follow each section of the exercise, allowing each team to present its findings to the other teams and to engage in class discussions on the topics covered. The instructor will also present a potential solution for the scenarios discussed.

Who Should Attend

- CISOs
- Information security managers, officers, and directors
- Information security architects, analysts, and consultants
- Aspiring information security leaders
- Risk management professionals
- Business continuity and disaster recovery planners and staff members
- IT managers and auditors
- IT project managers
- IT/system administration/network administration professionals
- Operations managers
- Cloud service managers and administrators
- Cloud service security and risk managers
- Cloud service integrators, developers, and brokers
- IT security professionals managing vulnerabilities in the enterprise or cloud
- Government IT professionals who manage vulnerabilities in the enterprise or cloud (FedRAMP)
- Security or IT professionals who have team lead or management responsibilities
- Security or IT professionals who use or are planning to use cloud services

"Great course, great content. MGT516 is essential for both well-established and developing vulnerability management teams."

-Robert Adams, **CBC**

SEC540: **Cloud Security and DevOps Automation**

5 Day Program	38 CPEs	Laptop Required

You Will Be Able To

- Build a Secure DevOps workflow in your organization
- Create automated security tasks in Continuous Integration/Continuous Delivery (CI/CD) systems
- Configure and run scanners from the Secure DevOps Toolchain
- Perform cloud infrastructure security audits for common misconfiguration vulnerabilities
- Perform secure secrets management using on-premise and cloud-hosted secrets management tools
- Audit microservice architectures for security vulnerabilities in containers, serverless, and API gateway appliances
- Leverage cloud automation to automate patching and software deployments without downtime
- Build serverless functions to monitor, detect and actively defend cloud services and configurations

SEC540 provides development, operations, and security professionals with a methodology to build and deliver secure infrastructure and software using DevOps and cloud services. Students will explore how the principles, practices, and tools of DevOps can improve the reliability, integrity, and security of on-premise and cloud-hosted applications.

Starting with on-premise deployments, the first two days of the course examine the Secure DevOps methodology and its implementation using lessons from successful DevOps security programs. Students will gain hands-on experience using popular open-source tools such as Puppet, Jenkins, GitLab, Vault, Grafana, and Docker to automate Configuration Management ("infrastructure as Code"), Continuous Integration (CI), Continuous Delivery (CD), containerization, micro-segmentation, automated compliance ("Compliance as Code"), and Continuous Monitoring. The lab environment starts with a CI/CD pipeline that automatically builds, tests, and deploys infrastructure and applications. Leveraging the Secure DevOps toolchain, students perform a series of labs injecting security into the CI/CD pipeline using a variety of security tools, patterns, and techniques.

After laying the DevSecOps foundation, the final three days move DevOps workloads to the cloud, build secure cloud infrastructure, and deliver secure software. SEC540 provides in-depth analysis of the Amazon Web Services (AWS) toolchain, while lightly covering comparable services in Microsoft Azure. Using the CI/CD toolchain, students build a cloud infrastructure that can host containerized applications and microservices. Hands-on exercises analyze and fix cloud infrastructure and application vulnerabilities using security services and tools such as API Gateway, Identity and Access Management (IAM), CloudFront Signing, Security Token Service (STS), Key Management Service (KMS), managed WAF services, serverless functions, CloudFormation, AWS Security Benchmark, and much more.

Authors' Statement

"DevOps and the cloud are radically changing the way that organizations design, build, deploy, and operate online systems. Leaders like Amazon, Etsy, and Netflix are able to deploy hundreds or even thousands of changes every day, continuously learning, improving, and growing—and leaving their competitors far behind. Now DevOps and the cloud are making their way from Internet 'Unicorns' and cloud providers into enterprises.

"Traditional approaches to security can't come close to keeping up with this rate of accelerated change. Engineering and operations teams that have broken down the 'walls of confusion' in their organizations are increasingly leveraging new kinds of automation, including Infrastructure as Code, Continuous Delivery and Continuous Deployment, microservices, containers, and cloud service platforms. The question is: can security take advantage of the tools and automation to better secure its systems?

"Security must be reinvented in a DevOps and cloud world."

-Ben Allen, Jim Bird, Eric Johnson, and Frank Kim

Eric Johnson
SANS Principal Instructor

Eric Johnson is a Principal Security Consultant at Cypress Data Defense, where he leads secure software development lifecycle consulting, web and mobile application penetration testing, secure code review assessments, static source code analysis, security research, and security tools development. He also founded the Puma Scan static analysis open-source project, which allows software engineers to run security-focused .NET static analysis rules during development and in continuous integration pipelines. At the SANS Institute, Eric authors application security courses on DevOps, cloud security, secure coding, and defending mobile apps. He serves on the advisory board for the SANS Securing The Human Developer awareness training program, delivers security training around the world, and has presented his security research at conferences including BlackHat, OWASP, BSides, JavaOne, UberConf, and ISSA. Eric completed a bachelor of science degree in computer engineering and a master of science degree in information assurance at Iowa State University, and currently holds the CISSP®, GWAPT, GSSP-.NET, and GSSP-Java certifications. He is based in West Des Moines, Iowa and outside the office enjoys spending time with his family, attending Iowa State athletic events, and playing golf. **@emjohn20**

Course Day Descriptions

Mon, Feb 3 – Fri, Feb 7
9:00am – 7:00pm (Days 1-4)
9:00am – 5:00pm (Day 5)
Extended hours; hands-on labs

This course is available via **Simulcast**. See page 64 for more information.

DAY 1: Introduction to Secure DevOps

The first day is an introduction to DevOps practices, principles and tooling, how DevOps works, and how work is done in DevOps. We'll look at the importance of culture, collaboration, and automation in DevOps. Using case studies of DevOps "Unicorns" – the Internet tech leaders who have created the DNA for DevOps – we'll show you how and why they succeeded. This includes the keys to their DevOps security programs. Then you'll learn Continuous Delivery – the automation engine in DevOps – and how to build up a Continuous Delivery or Continuous Deployment pipeline. This includes how security controls can be folded into or wired into the CD pipeline, and how to automate security checks and tests in CD.

Topics: Introduction to DevOps; Case Studies on DevOps Unicorns; Working in DevOps; Security Challenges in DevOps; Building a CD Pipeline; DevOps Deployment Data; Secure Continuous Delivery; Security in Pre-Commit; Security in Commit; Security in Acceptance

DAY 2: Moving to Production

Building on the ideas and frameworks developed in the first course section, you will learn how secure Infrastructure as code, using modern automated configuration management tools like Puppet, Chef and Ansible, allows you to quickly and consistently deploy new infrastructure and manage configurations. Because the automated CD pipeline is so critically important to DevOps, you'll also learn to secure the pipeline, including RASP and other run-time defense technologies. As the infrastructure and application code moves to production, we'll spend the second half of the day exploring container security issues associated with tools such as Docker and Kubernetes, as well as how to protect secrets using Vault and how to build continuous security monitoring using Graphana, Graphite, and StatsD. Finally, we'll discuss how to build compliance into Continuous Delivery, using the security controls and guardrails that have been built in the DevOps toolchain.

Topics: Secure Configuration Management Using Infrastructure as Code; Securing Configuration Management and Continuous Integration/Continuous Delivery Pipelines; Container Security, Hardening, and Orchestration; Continuous Monitoring and Feedback Loops; Secure Secrets Management; Automating Compliance as Code

DAY 3: Moving to the Cloud

Observing DevOps principles, you'll learn to deploy infrastructure, applications, and the CI/CD toolchain into the cloud. This section provides an overview of Amazon Web Services (AWS) and introduces the foundational tools and practices you'll need to securely deploy your applications in the cloud.

Topics: Introduction to the Cloud; Cloud Architecture Overview; Secure Cloud Deployment; Security Scanning in CI/CD

DAY 4: Cloud Application Security

In this section, you'll learn to leverage cloud application security services to ensure that applications have appropriate encryption, authentication, authorization, and access control, while also maintaining functional and high-availability systems.

Topics: Data Protection; Secure Content Delivery; Microservice Security; Serverless Security; Security Automation with Lambda

DAY 5: Cloud Security Automation

Expanding on the foundation of the previous sections, we'll now focus on leveraging cloud services to automate security tasks such as deploying application patches to blue/green environments, deploying and configuring cloud web application firewalls, enabling cloud security monitoring, and automating cloud compliance scanning.

Topics: Blue/Green Deployment Options; Security Automation; Security Monitoring; Compliance

Who Should Attend

- Anyone working in or transitioning to a DevOps environment
- Anyone who wants to understand where to add security checks, testing, and other controls to DevOps and Continuous Delivery
- Anyone interested in learning to migrate DevOps workflows to the cloud, specifically Amazon Web Services (AWS)
- Anyone interested in leveraging cloud application security services provided by AWS
- Developers
- Software architects
- Operations engineers
- System administrators
- Security analysts
- Security engineers
- Auditors
- Risk managers
- Security consultants

"Mind-blowing! If you are a traditional security architect, tip-toeing around DevOps, get into SEC540. It takes you into the depths of DevSecOps and sets you up for the future!"

-Jatin Sachdeva, Cisco

ICS410: **ICS/SCADA Security Essentials**

GICSP
Industrial Cyber Security Professional
www.giac.org/gicsp

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Better understand various industrial control systems and their purpose, application, function, and dependencies on network IP and industrial communications
- Work with control network infrastructure design (network architecture concepts, including topology, protocols, and components) and their relation to IEC 62443 and the Purdue Model.
- Run Windows command line tools to analyze the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat, ect) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Work with operating systems (system administration concepts for Unix/Linux and/or Windows operating systems)
- Better understand the systems' security lifecycle
- Better understand information assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)
- Use your skills in computer network defense to detect host and network-based intrusions via intrusion detection technologies
- Implement incident response and handling methodologies
- Map different ICS technologies, attacks, and defenses to various cybersecurity standards including the NIST Cyber Security Framework, ISA/IEC 62443, ISO/IEC 27001, NIST SP 800-53, the Center for Internet Security Critical Security Controls, and COBIT 5

Monta Elkins
SANS Certified Instructor

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

The course will provide you with:

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

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

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

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

Monta Elkins is currently "Hacker-in-Chief" for FoxGuard Solutions, an ICS patch provider. A security researcher and consultant; he was formerly Security Architect for Rackspace, and the first ISO for Radford University. He has been a speaker at DEFCON, Homeland Security's ICSJWG (Industrial Control Systems Joint Working Group), EnergySec's Security Summit, VASCAN, GE Digital Energy's Annual Software Summit, Educause Security Professionals Conference, Toshiba's Industrial Control Systems Conference, NERC's GridSecCon, ICS CyberSecurity by Security Week, UTC Telecom and other security conferences. Monta was also the recipient of the EnergySec's Cyber Security Professional of the Year Award for 2018, and was recognized by the Industrial Control System (ICS) community and staff at EnergySec for his exceptional contributions to ICS security. Monta is the author and instructor of the "Defense against the Dark Arts" hands-on, hacker tools and techniques classes. He is also a guest lecturer for Virginia Tech University and teaches rapid prototyping and Arduino classes with Let's Code Blacksburg.
@montaelkins

Course Day Descriptions

Mon, Feb 3 – Fri, Feb 7
9:00am - 5:00pm
Hands-on labs

DAY 1: ICS Overview

Students will develop and reinforce a common language and understanding of industrial control system (ICS) cybersecurity as well as the important considerations that come with cyber-to-physical operations within these environments. Each student will receive programmable logic controller (PLC) hardware to keep. The PLC contains physical inputs and outputs that will be programmed in class and mapped to an operator interface, or HMI, also created in class. This improved hardware-enabled approach provides the necessary cyber-to-physical knowledge that allows students to better understand important ICS operational drivers and constraints that require specific safety protection, communications needs, system management approaches, and cybersecurity implementations. Essential terms, architectures, methodologies, and devices are all covered to build a common language for students from a variety of different roles.

Topics: Global Industrial Cybersecurity Professional (GICSP) Overview; Overview of ICS; Purdue Levels 0 and 1; Purdue Levels 2 and 3; DCS and SCADA; IT & ICS Differences; Physical and Cyber Security; Secure ICS Network Architectures

DAY 2: Field Devices and Controllers

If you know the adversary's approaches to attacking an ICS environment, you will be better prepared to defend that environment. Numerous attack vectors exist within an ICS environment. Some are similar to traditional IT systems, while others are more specific to ICS. During day 2, students will develop a better understanding of where these specific attack vectors exist and how to block them, starting at the lowest levels of the control network. Students will look at different technologies and communications used in Purdue Levels 0 and 1, the levels that are the most different from an IT network. Students will capture fieldbus traffic from the PLCs they programmed on day 1 and look at what other fieldbus protocols are used in the industry. Later in the day, students will analyze network captures containing other control protocols that traverse Ethernet-only networks and TCP/IP networks, set up a simulated controller, and interact with it through a control protocol.

Topics: ICS Attack Surface; Purdue Levels 0 and 1; Ethernet and TCP/IP

DAY 3: Supervisory Systems

Day 3 will take students through the middle layers of control networks. Students will learn about different methods to segment and control the flow of traffic through the control network. Students will explore cryptographic concepts and how they can be applied to communications protocols and on devices that store sensitive data. Students will learn about the risks of using wireless communications in control networks, which wireless technologies are commonly used, and available defenses for each. After a hands-on network forensics exercise where students follow an attacker from phishing campaign to HMI breach, students will look at HMI, historian, and user interface technologies used in the middle to upper levels of the control network, namely Purdue Levels 2 and 3, while performing attacks on HMI web technologies and interfaces susceptible to password brute force attacks.

Topics: Enforcement Zone Devices; Understanding Basic Cryptography; Wireless Technologies; Wireless Attacks and Defenses; Exercise: Network Forensics of an Attack; Purdue Level 2 and 3 Attacks

DAY 4: Workstations and Servers

Students will learn essential ICS-related server and workstation operating system capabilities, implementation approaches, and system management practices. Students will receive and work with both Windows- and Linux-based virtual machines in order to understand how to monitor and harden these hosts from attack. Students will examine concepts that benefit ICS systems such as system hardening, log management, monitoring, alerting, and audit approaches, then look at some of the more common applications and databases used in ICS environments across multiple industries. Finally, students will explore attacks and defenses on remote access for control systems.

Topics: Patching ICS Systems; Defending Microsoft Windows; Defending Unix and Linux; Endpoint Security Software; Event Logging and Analysis; Remote Access Attacks

DAY 5: ICS Security Governance

Students will learn about the various models, methodologies, and industry-specific regulations that are used to govern what must be done to protect critical ICS systems. Key business processes that consider risk assessments, disaster recovery, business impact analysis, and contingency planning will be examined from the perspective of ICS environments. On this final course day, students will work together on an incident response exercise that places them squarely in an ICS environment that is under attack. This exercise ties together key aspects of what has been learned throughout the course and presents students with a scenario to review with their peers. Specific incident-response roles and responsibilities are considered, and actions available to defenders throughout the incident response cycle are explored. Students will leave with a variety of resources for multiple industries and will be well prepared to pursue the GICSP, an important ICS-focused professional certification.

Topics: Building an ICS Cybersecurity Program; Creating ICS Cybersecurity Policy; Disaster Recovery; Measuring Cybersecurity Risk; Incident Response; Exercise: Incident Response Tabletop Exercise; Final Thoughts and Next Steps

Who Should Attend

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

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

"Good comprehensive content with dynamic instructor really made this course good. This is the best training course I've taken in 25+ years."

-**Curt Imanse**, Accenture

SEC440: **Critical Security Controls: Planning, Implementing, and Auditing**

2 Day Course | 12 CPEs | Laptop Not Needed

Sat, Feb 1 – Sun, Feb 2
9:00am – 5:00pm

Instructor:
Randy Marchany

This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS). The Critical Security Controls are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all serious and sensitive organizations. These controls were selected and defined by the U.S. military and other government agencies (including the NSA, DHS, GAO, and many others) and private organizations that are the most respected experts on how attacks actually work and what can be done to stop them. They defined these controls as their consensus for the best way to block known attacks and find and mitigate damage from the attacks that get through. For security professionals, the course enables you to see how to put the controls in place in your existing network through effective and widespread use of cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the controls are effectively implemented. SEC440 does not contain any labs. Students looking for hands-on labs involving the Critical Controls should take SEC566.

One of the best features of the course is that it uses offense to inform defense. In other words, you will learn about the actual attacks that you'll be stopping or mitigating. That makes the defenses very real, and it makes you a better security professional. SEC440 will provide you with the skills to start implementing and auditing each of the Critical Security Controls on your first day back on the job.

"Gives specific direction for understanding risks and building a program to address them."
-Eric Pierce, **Mindbody**

SEC455: **SIEM Design and Implementation**

2 Day Course | 14 CPEs | Laptop Required

Sat, Feb 1 – Sun, Feb 2
Extended hours
9:00am - 6:00pm (Day 1)
8:00am – 5:00pm (Day 2)

Instructor:
John Hubbard

Security Information and Event Management (SIEM) can be an extraordinary benefit to an organization's security posture, but understanding and maintaining it can be difficult. Many solutions require complex infrastructure and software that necessitate professional services for installation, but using those services can leave security teams feeling as if they do not truly own or understand how their SIEM operates. Combine this situation of complicated solutions with a shortage of available skills, a lack of simple documentation, and the high costs of software and labor, and it is not surprising that deployments often fail to meet expectations. A SIEM can be the most powerful tool a cyber defense team can wield, but only when it is used to its fullest potential. This course is designed to address this problem by demystifying SIEMs and simplifying the process of implementing a solution that is usable, scalable, and simple to maintain.

The goal of this course is to teach students how to build a SIEM from the ground up using the Elastic Stack. Throughout the course, students will learn about the required stages of log collection. We will cover endpoint agent selection, logging formats, parsing, enrichment, storage, and alerting, and we will combine these components to make a flexible, high-performance SIEM solution. Using this approach empowers SIEM engineers and analysts to understand the complete system, make the best use of technology purchases, and supplement current underperforming deployments. This process allows organizations to save money on professional services, increase the efficiency of internal labor, and develop a nimbler solution than many existing deployments. For example, many organizations pay thousands of dollars in consulting fees when a unique log source needs a custom parser. This course will train students how to easily parse any log source themselves, saving their organizations both time and money, and facilitating faster collection and use of new log sources.

SEC455 serves as an important primer to those who are unfamiliar with the architecture of an Elastic-based SIEM. Students who have taken or plan to take additional cyber defense courses may find SEC455 to be a helpful supplement to the advanced concepts in courses such as SEC555. In addition, the material discussed in this course will enable students to not only build a new SIEM, but improve and supplement their already existing implementations, producing a more efficient solution that provides the answers they need more quickly and at a lower cost. The overall goal is to show students how to design and modify a SIEM, improve upon their current solution, and reach their original defensive goal – catching adversary activity in their environment.

"SEC455 has made me rethink how I do event log monitoring and what I can do to improve."
-Roger Christopher,
Bureau of Land Management

SEC564: **Red Team Exercises & Adversary Emulation**

2 Day Course | 12 CPEs | Laptop Required

Sat, Feb 1 – Sun, Feb 2
9:00am – 5:00pm

Instructor:
Jorge Orchilles

Red Teaming is the process of using tactics, techniques, and procedures (TTPs) to emulate real-world adversaries in order to train and measure the effectiveness of the people, processes, and technology used to defend organizations. SEC564 will provide you with the skills to manage and operate a Red Team, conduct Red Team exercises and adversary emulations, and understand the role of the team and its importance in security testing.

Built on the fundamentals of penetration testing, Red Team exercises use a comprehensive approach to gain a holistic view of an organization's security posture in order to improve its ability to detect, respond, and recover from an attack. When properly conducted, Red Team exercises significantly improve an organization's security posture and controls, hone its defensive capabilities, and measure the effectiveness of its security operations.

Red Team exercises require a different approach from a typical security test and rely heavily on well-defined TTPs, which are critical to successfully emulate a realistic adversary. The Red Team exercises and adversary emulation results exceed a typical list of penetration test vulnerabilities, provide a deeper understanding of how an organization would perform against a real adversary, and identify where security strengths and weaknesses exist across people, processes, and technology.

Whether you support a defensive or offensive role in security, understanding how Red Team exercises can be used to improve security is extremely valuable. This intensive two-day course will explore Red Team concepts in-depth, provide the required fundamentals of adversary emulation, and help you improve your organization's security posture.

"The content from SEC564 is great and I will be able to implement it in my organization right away!"
-Kirk Hayes, **Rapid 7**

SEC580: **Metasploit Kung Fu for Enterprise Pen Testing**

2 Day Course | 12 CPEs | Laptop Required

Sat, Feb 1 – Sun, Feb 2
9:00am – 5:00pm

Instructor:
Jeff McJunkin

Many enterprises today face regulatory or compliance requirements that mandate regular penetration testing and vulnerability assessments. Commercial tools and services for performing such tests can be expensive. While really solid free tools such as Metasploit are available, many testers do not understand the comprehensive feature sets of such tools and how to apply them in a professional-grade testing methodology. Metasploit was designed to help testers with confirming vulnerabilities using an open-source and easy-to-use framework. This course will help students get the most out of this free tool.

This class will show students how to apply the incredible capabilities of the Metasploit Framework in a comprehensive penetration testing and vulnerability assessment regimen, according to a thorough methodology for performing effective tests. Students who complete the course will have a firm understanding of how Metasploit can fit into their penetration testing and day-to-day assessment activities. The course will provide an in-depth understanding of the Metasploit Framework far beyond simply showing attendees how to exploit a remote system. The class will cover exploitation, post-exploitation reconnaissance, token manipulation, spear-phishing attacks, and the rich feature set of the Meterpreter, a customized shell environment specially created for exploiting and analyzing security flaws.

The course will also cover many of the pitfalls that a tester may encounter when using the Metasploit Framework and how to avoid or work around them, making tests more efficient and safe.

"SEC580 reinforces the tools, methodologies, and techniques the Advanced Persistent Threats (APTs) are using against me. It arms me for the battle."
-Nathan Gibson, **ADT, LLC**

Management | **2-Day Course**

MGT415: **A Practical Introduction to Cyber Security Risk Management**

2 Day Course | 12 CPEs | Laptop Required

In this course students will learn the practical skills necessary to perform regular risk assessments for their organizations. The ability to perform risk management is crucial for organizations hoping to defend their systems. There are simply too many threats, too many potential vulnerabilities that could exist, and not enough resources to create an impregnable security infrastructure. Therefore all organizations, whether they do so in an organized manner or not, will make priority decisions on how to best defend their valuable data assets. Risk management should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.

Sat, Feb 1 – Sun, Feb 2
9:00am – 5:00pm

Instructor:
Russell Eubanks

You Will Learn:

- How to perform a risk assessment step by step.
- How to map an organization's business requirements to implemented security controls.
- The elements of risk assessment and the data necessary for performing an effective risk assessment.
- What in-depth risk management models exist for implementing a deeper risk management program in an organization.

"Our company is creating a formal cyber risk and controls assessment program. This class was a perfect introduction to the topic."
-Jim Schleske, **Ball Aerospace**

DevSecOps | **2-Day Course**

SEC534: **Secure DevOps: A Practical Introduction**

2 Day Course | 12 CPEs | Laptop Required

This course explains the fundamentals of DevOps and how DevOps teams can build and deliver secure software. You will learn DevOps principles, practices, and tools and how they can be leveraged to improve the reliability, integrity, and security of systems.

Using lessons from successful DevOps security programs, we will explain how Secure DevOps can be implemented. Students will gain hands-on experience using popular open-source tools such as Puppet, Jenkins, GitLab, Vault, Grafana, and Docker to automate Configuration Management ("Infrastructure as Code"), Continuous Integration (CI), Continuous Delivery (CD), containerization, micro-segmentation, automated compliance ("Compliance as Code"), and Continuous Monitoring. The lab environment starts with a CI/CD pipeline that automatically builds, tests, and deploys infrastructure and applications. Leveraging the Secure DevOps toolchain, students perform a series of labs injecting security into the CI/CD pipeline using a variety of security tools, patterns, and techniques.

Sat, Feb 1 – Sun, Feb 2
9:00am – 5:00pm

Instructor:
Ben Allen

You Will Learn:

- Foundations and principles of DevOps, Continuous Delivery, and Continuous Deployment
- The security risks and challenges posed by DevOps
- The keys to successful DevOps security programs
- How to build security into Continuous Delivery and Continuous Deployment
- The tools, patterns, and techniques of security automation in DevOps
- How to secure your build and deployment environment and tool chain
- How to leverage Infrastructure as Code for secure configuration management and provisioning
- How manual security practices (risk assessments, audits, and pen tests) can be adapted to continuously changing environments, and the important role that they still play
- Security risks and challenges posed by containers, and how to secure container technology
- How to automate compliance in DevOps, using the DevOps Audit Defense Toolkit

"A fast-paced and illustrative two days on the current state of security for DevOps. It was well worth the time invested to take the class."
-Michael Machado, **Ring Central**

Kick off your **SANS Security East 2020** experience at the

Welcome Networking Reception

Sunday, February 2
6:00pm – 9:00pm

Fulton Alley
600 Fulton Street
New Orleans, LA 70130

Join your peers for a fun evening of bowling, shuffleboard, and darts while watching Super Bowl LIV. Food and beverages will be served.

Pick up event badges during pre-registration: Sunday, Feb. 2 from 4:00pm - 6:00pm.
Event badges are required for admission and the reception is for all registered Security East 2020 attendees.

Bonus Sessions

Please check for the schedule of night talks and updates at
www.sans.org/security-east/bonus-sessions

Welcome Reception at Fulton Alley

Kick off SANS Security East at the Welcome Reception

Sunday, February 2nd, 6:00pm – 9:00pm
Location: Fulton Alley, 600 Fulton Street

Network with industry peers and SANS instructors, and find out how to make the most of your week at Security East. Choose from bowling, shuffleboard, and darts while watching Super Bowl LIV.

Food and beverages will be served.

General Session – Welcome to SANS

Bryan Simon

Join us for a 30-minute overview to help you get the most out of your SANS training experience. You will receive event information and learn about programs and resources offered by SANS. This brief session will answer many questions and get your training experience off to a great start. This session will be valuable to all attendees but is highly recommended for first-time attendees.

KEYNOTE:
Everything You Ever Learned About Passwords Is Wrong

Keith Palmgren

Perhaps the worst advice you can give a user is "choose a complex password." The result is the impossible-to-remember password requiring the infamous sticky note on the monitor. In addition, that password gets used at a dozen sites at home, AND the very same password gets used at work. The final result ends up being the devastating password compromise. In this one-hour talk, we will look at the technical and non-technical (human nature) issues behind passwords. Attendees will gain a more complete understanding of passwords and receive solid advice on creating more easily remembered AND significantly stronger passwords at work and at home, for their users, for themselves and even for their children.

Who's in Your Wallet? Capital One Debrief and Post Mortem

Eric Johnson

Join Eric Johnson for a walk-through of the Capital One breach. We will demonstrate how the attacker compromised Amazon Web Services virtual machine credentials, gained access to privileged resources, and exfiltrated data from the account. The conversation then shifts to a post mortem discussion about cloud security controls that could have prevented or limited the blast radius of the attack.

Machine Learning and Network Monitoring: Welcome to the Machine

David Hoelzer

Is machine learning all just snake oil today, or are there practical applications that can be made that make your life easier? In this presentation, David Hoelzer will talk about the current trends and then walk you through demonstrations of machine learning methods applied to real network monitoring problems.

Web Apps Dripping with Honey

Mick Douglas

Web applications are under constant attack. To make matters worse, the defenses have been relatively static for years. Couple that in with known frameworks and you have the relative dumpster fire that web app security has become. Attendees of this talk will learn various defenses that are low-cost/low-risk yet highly effective.

Virtuous Cycles: Rethinking the SOC for Long-Term Success

John Hubbard

Many Security Operations Centers (SOCs) have a burnout problem that leads to negativity and constant turnover. With the cybersecurity talent shortage, keeping the people we have will only become increasingly important. The problem is that "Tier 1" and other SOC roles historically seem to quickly burn people out. So what do we do? While the field of psychology understands the factors that cause burnout, many SOCs do not take the time to do the research and create an environment to fight it. Though meticulously defined process and analyst tiering may be the norm, does it lead to sacrificing quality and happiness in the long term? Using science-backed research on intrinsic motivation and studies on SOC burnout factors, this talk will make the case that it's time to reconsider how we structure SOCs in order to create long-term success that benefits both the individual and the organization.

Coffee & Donuts with the College Students

Join us for coffee, donuts, and conversation with SANS.edu staff and current students. Learn about SANS' regionally accredited master's degree and graduate certificate programs for InfoSec professionals and undergraduate certificate program for people who want to launch a career in cybersecurity. Find out if the class you're taking this week or GIAC certifications you've earned may be applied towards a graduate or undergraduate program. Visit www.sans.edu for complete information on curriculum, admissions, and funding options.

Exhibitor-Sponsored Events

Lunch & Learns

Monday, February 3 | 12:30pm – 1:15pm

Since SANS course material is product neutral, these presentations provide the opportunity to evaluate vendor tools in an interactive environment to increase your effectiveness, productivity, and knowledge gained from the conference. These sessions feature a light meal or refreshments provided by the sponsor.

Upcoming SANS Training Events

DFIRCON	Coral Gables, FL	Nov 4-9
Atlanta Fall	Atlanta, GA	Nov 18-23
Austin	Austin, TX	Nov 18-23
Nashville	Nashville, TN	Dec 2-7
San Francisco Winter	San Francisco, CA	Dec 2-7

Cyber Defense Initiative®	Washington, DC	Dec 10-17

Austin Winter	Austin, TX	Jan 6-11
Miami	Miami, FL	Jan 13-18
Anaheim	Anaheim, CA	Jan 20-25
Las Vegas	Las Vegas, NV	Jan 27 – Feb 1
San Francisco East Bay	Emeryville, CA	Jan 27 – Feb 1

Security East	New Orleans, LA	Feb 1-8

Northern VA – Fairfax	Fairfax, VA	Feb 10-15
New York City	New York, NY	Feb 10-15
Scottsdale	Scottsdale, AZ	Feb 17-22
San Diego	San Diego, CA	Feb 17-22

Upcoming SANS Summit Events

Cloud & DevOps Security	Denver, CO	Nov 4-11
Pen Test HackFest	Washington, DC	Nov 18-25
Cyber Threat Intelligence	Washington, DC	Jan 20-27
Open-Source Intelligence	Washington, DC	Feb 18-24
ICS Security	Orlando, FL	Mar 2-8
Blue Team	Louisville, KY	Mar 2-9

Future Community SANS Events

Local, single-course events are also offered throughout the year via SANS Community.
Visit **www.sans.org/community** for up-to-date Community course information.

SANS OnDemand

Take SANS Training Anytime, Anywhere with OnDemand

More than 30 of the most popular SANS courses are available in our online training format OnDemand with no travel required. All OnDemand courses include:

- Four months of online access to your course
- Subject-matter-expert support
- Training with SANS top instructors
- All printed books and materials
- Labs and quizzes to reinforce your learning

Visit www.sans.org/ondemand to learn more about your OnDemand training options.

Hotel Information

Hilton New Orleans Riverside
Two Poydras Street | New Orleans, LA 70130
504-561-0500
www.sans.org/security-east/location

It's all about location in New Orleans, and the Hilton New Orleans Riverside places you at the center of it all. Nestled against the banks of the Mississippi, guests can watch the ships come sailing in or dive into the city life just steps away. Grab a beignet, listen to live jazz, ride a streetcar, or hop into a parade, you never know what you'll experience in the vibrant culture and excitement of New Orleans just outside the front door.

Special Hotel Rates Available

A special discounted rate of $214 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID. These rates include high-speed Internet in your room and are only available through **January 10, 2020**.

Top three reasons to stay at the Hilton New Orleans Riverside

1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Hilton New Orleans Riverside, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
3. SANS schedules morning and evening events at the Hilton New Orleans Riverside that you won't want to miss!

Registration Information

Register online at **www.sans.org/security-east**

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

Select your course 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.

An email confirmation will be sent to you once the registration form has been completed. If you have not received this email confirmation within two business days of registering, please call **301-654-7267** or contact **registration@sans.org** for assistance.

Pay Early and Save*

Use code **EarlyBird20** when registering early

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code by	**Dec 11**	**$300**	**Jan 1**	**$150**

*Some restrictions apply. Early bird discounts do not apply to Hosted courses.

SANS SIMULCAST

Live stream content directly from the classroom and interact with peers and in-class moderators. Simulcast includes four months of access to your course recordings, labs, and unlimited SME support. Visit **www.sans.org/security-east/attend-remotely** for more details.

SANS Voucher Program

Expand your training budget!

For organizations with multiple employees taking SANS training courses, the SANS Voucher Program is an easy-to-use, flexible training management solution. Based on the number of anticipated students and investment, you may be eligible to receive bonus funds from SANS. Your investment and bonus funds can be used for classroom and online training, and can also be used to pay for GIAC certification exams. Contact SANS for more detailed information about our Voucher Program. **www.sans.org/vouchers**

Cancellation & Access Policy

If an attendee must cancel, a substitute may attend instead. Substitution requests can be made at any time prior to the event start date. Processing fees will apply. All substitution requests must be submitted by email to **registration@sans.org** If an attendee must cancel and no substitute is available, a refund can be issued for any payments received by **January 15, 2020**. A credit memo can be requested up to the event start date. All cancellation requests must be submitted in writing by mail or fax and received by the stated deadlines. Payments will be refunded by the method that they were submitted. Processing fees will apply.

Registration Fees

Register online at **www.sans.org/security-east**

If you don't wish to register online, please call 301-654-SANS (7267) 9:00am-8:00pm (Mon-Fri) EST and we will fax or mail you an order form.

Courses – 5-6 Days		Paid before 12-11-19	Paid before 1-1-20	Paid after 1-1-20	Add GIAC Cert*	Add OnDemand*	Add NetWars Continuous
☐ SEC301	Introduction to Cyber Security	$5,790	$5,940	$6,090	☐ $799	☐ $799	☐ $1,420
☐ SEC401	Security Essentials Bootcamp Style	$6,720	$6,870	$7,020	☐ $799	☐ $799	☐ $1,420
☐ SEC450	Blue Team Fundamentals: Security Operations and Analysis ***NEW!***	$6,720	$6,870	$7,020		☐ $799	☐ $1,420
☐ SEC503	Intrusion Detection In-Depth	$6,720	$6,870	$7,020	☐ $799	☐ $799	☐ $1,420
☐ SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling	$6,720	$6,870	$7,020	☐ $799	☐ $799	☐ $1,420
☐ SEC530	Defensible Security Architecture and Engineering	$6,720	$6,870	$7,020	☐ $799	☐ $799	☐ $1,420
☐ SEC540	Cloud Security and DevOps Automation	$6,300	$6,450	$6,600		☐ $799	☐ $1,420
☐ SEC542	Web App Penetration Testing and Ethical Hacking	$6,720	$6,870	$7,020	☐ $799	☐ $799	☐ $1,420
☐ SEC545	Cloud Security Architecture and Operations	$5,790	$5,940	$6,090		☐ $799	☐ $1,420
☐ SEC555	SIEM with Tactical Analytics	$6,720	$6,870	$7,020	☐ $799	☐ $799	☐ $1,420
☐ SEC560	Network Penetration Testing and Ethical Hacking	$6,720	$6,870	$7,020	☐ $799	☐ $799	☐ $1,420
☐ SEC573	Automating Information Security with Python	$6,720	$6,870	$7,020	☐ $799	☐ $799	☐ $1,420
☐ SEC599	Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses	$6,720	$6,870	$7,020	☐ $799	☐ $799	☐ $1,420
☐ SEC642	Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques	$6,720	$6,870	$7,020	☐ $799		☐ $1,420
☐ FOR500	Windows Forensic Analysis	$6,720	$6,870	$7,020	☐ $799	☐ $799	☐ $1,420
☐ FOR508	Advanced Incident Response, Threat Hunting, and Digital Forensics	$6,720	$6,870	$7,020	☐ $799	☐ $799	☐ $1,420
☐ FOR572	Advanced Network Forensics: Threat Hunting, Analysis & Incident Response	$6,720	$6,870	$7,020	☐ $799	☐ $799	☐ $1,420
☐ FOR578	Cyber Threat Intelligence	$5,790	$5,940	$6,090	☐ $799	☐ $799	☐ $1,420
☐ FOR585	Smartphone Forensic Analysis In-Depth	$6,720	$6,870	$7,020	☐ $799	☐ $799	☐ $1,420
☐ MGT414	SANS Training Program for CISSP® Certification	$6,720	$6,870	$7,020	☐ $799	☐ $799	☐ $1,420
☐ MGT514	Security Strategic Planning, Policy, and Leadership	$6,300	$6,450	$6,600	☐ $799	☐ $799	☐ $1,420
☐ MGT516	Managing Security Vulnerabilities: Enterprise and Cloud ***NEW!***	$6,300	$6,450	$6,600			☐ $1,420
☐ ICS410	ICS/SCADA Security Essentials	$6,720	$6,870	$7,020	☐ $799	☐ $799	☐ $1,420

Skill-Based Short Courses		Course fee if taking a 4-6 day course	Course fee	Add OnDemand
☐ SEC440	Critical Security Controls: Planning, Implementing, and Auditing	$2,100	$2,800	☐ $315
☐ SEC455	SIEM Design & Implementation	$2,100	$2,800	
☐ SEC534	Secure DevOps: A Practical Introduction	$2,100	$2,800	
☐ SEC564	Red Team Exercises & Adversary Emulation	$2,100	$2,800	
☐ SEC580	Metasploit Kung Fu for Enterprise Pen Testing	$2,100	$2,800	
☐ MGT415	A Practical Introduction to Cyber Security Risk Management	$2,100	$2,800	
☐ SPECIAL	Core NetWars Tournament – Tournament Entrance Fee	**FREE**	$1,795	
☐ SPECIAL	Cyber Defense NetWars Tournament – Tournament Entrance Fee	**FREE**	$1,795	
☐ SPECIAL	DFIR NetWars Tournament – Tournament Entrance Fee	**FREE**	$1,795	

EARLY BIRD DISCOUNTS

Pay for any long course using the code **EarlyBird20** at checkout by **December 11th to get $300 OFF** or by **January 1st to get $150 OFF***

*Some restrictions apply. Early bird discounts do not apply to Hosted courses.

SANS
5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407

AFCEA Corporate Member

As the leading provider of information defense, security, and intelligence training to military, government, and industry groups, the SANS Institute is proud to be a Corporate Member of the AFCEA community.

Join the SANS.org community today to enjoy these ***free*** resources at **www.sans.org/join**

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 newly discovered attack vectors, vulnerabilities with active new exploits, how recent attacks worked, and other valuable data.

Webcasts

Ask the Experts 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 how a vendor's commercial tool can be used to solve or mitigate that problem.

Other Free Resources *(SANS.org account not required)*

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

SAVE $300 Register and pay by **Dec 11th** Use code **EarlyBird20**

www.sans.org/security-east