SANS

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

TYSONS CORNER FALL 2017

McLean, VA | October 14-21

Protect Your Business and Advance Your Career

Ten hands-on, immersion-style information security courses taught by real-world practitioners

CYBER DEFENSE
ETHICAL HACKING
PENETRATION TESTING
CYBER THREAT INTELLIGENCE
DIGITAL FORENSICS
MANAGEMENT
AUDIT

GIAC CERTIFICATIONS

"SANS provides the education that any and all security organizations absolutely must have to succeed."
-Thomas L., U.S. Air Force

SAVE $400

Register and pay by Aug 23rd – Use code **EarlyBird17**

www.sans.org/tysons-corner-2017

SANS Tysons Corner FALL 2017

OCTOBER 14-21

SANS Instructors

SANS instructors are real-world practitioners who specialize in the subjects they teach. All instructors undergo rigorous training and testing in order to teach SANS courses. This guarantees that what you learn in class will be up to date and relevant to your job. The SANS Tysons Corner Fall 2017 lineup of instructors includes:

Kevin Fiscus
Certified Instructor
@kevinbfiscus

Hassan El Hadary
Instructor
@hassan_hadary

G. Mark Hardy
Principal Instructor
@g_mark

Robert M. Lee
Certified Instructor
@RobertMLee

Keith Palmgren
Senior Instructor
@kpalmgren

Bryan Simon
Certified Instructor
@BryanOnSecurity

James Tarala
Senior Instructor
@isaudit

Joe Vest
Instructor

Joshua Wright
Senior Instructor
@joswr1ght

Eric Zimmerman
Certified Instructor
@EricRZimmerman

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 10.

KEYNOTE: ***Everything You Ever Learned About Passwords Is Wrong*** – Keith Palmgren

Industrial Control System Active Defense and Threat Intelligence – Robert M. Lee

Anti-Ransomware: How to Turn the Tables – G. Mark Hardy

Hunting Logic Attacks – Hassan El Hadary

Plumbing the Depths: ShellBags – Eric Zimmerman

Save $400 when you register and pay by August 23rd using code EarlyBird17

Courses at a Glance

		SAT 10-14	SUN 10-15	MON 10-16	TUE 10-17	WED 10-18	THU 10-19	FRI 10-20	SAT 10-21
SEC301	Intro to Information Security			Page 1					
SEC401	Security Essentials Bootcamp Style			Page 2					
SEC542	Web App Penetration Testing and Ethical Hacking			Page 3					
SEC564	Red Team Operations and Threat Emulation *BETA!*	Page 9							
SEC566	Implementing and Auditing the Critical Security Controls – In-Depth			Page 4					
SEC575	Mobile Device Security and Ethical Hacking			Page 5					
FOR508	Advanced Digital Forensics, Incident Response, and Threat Hunting			Page 6					
FOR578	Cyber Threat Intelligence			Page 7					
MGT512	SANS Security Leadership Essentials for Managers with Knowledge Compression™			Page 8					
SEC580	Metasploit Kung Fu for Enterprise Pen Testing	Page 9							

Register today for SANS Tysons Corner Fall 2017!
www.sans.org/tysons-corner-2017

@SANSInstitute
Join the conversation:
#SANSTysons

SEC301

Intro to Information Security

GISF Certification

Information Security Fundamentals

www.giac.org/gisf

Five-Day Program
Mon, Oct 16 - Fri, Oct 20
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Keith Palmgren

"Labs reinforced the security principles in a real-world scenario."
-Tyler Moore, Rockwell

"This is the perfect course for establishing a foundation of information security, and the instructor is very knowledgeable and well-versed in the topics."
-Stephen Pridmore, Protective Life

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

To determine if the SANS SEC301 course is right for you, ask yourself five simple questions:

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

If you answer yes to any of these questions, the **SEC301: Intro to Information Security** training course is for you. Jump-start your security knowledge by receiving insight and instruction from real-world security experts on critical introductory topics that are fundamental to information security. This completely revised five-day, comprehensive course covers everything from core terminology to the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles.

This course is designed for students who have a basic knowledge of computers and technology but no prior knowledge of cybersecurity. The hands-on, step-by-step teaching approach will enable you to grasp all of the information presented even if some of the topics are new to you. You'll learn the fundamentals of information security that will serve as the foundation of your InfoSec skills and knowledge for years to come.

Written by a security professional with over 30 years of experience in both the public and private sectors, SEC301 provides uncompromising real-world insight from start to finish. The course prepares you for the Global Information Security Fundamentals (GISF) certification test, as well as for the next course up the line, **SEC401: Security Essentials Bootcamp 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.***

Keith Palmgren *SANS Senior Instructor*

Keith Palmgren is an IT security professional with 26 years of experience 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 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 DoD and the National Security Agency. As security practice manager for both Sprint and Netigy, Keith built and ran the security consulting practice, responsible for all security consulting world-wide 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. As a trainer, Keith has satisfied the needs of nearly 5,000 IT professionals and authored 17 training courses. Keith currently holds the CISSP, GSEC, CEH, Security+, Network+, A+, and CTT+ certifications. **@kpalmgren**

SEC401

Security Essentials Bootcamp Style

GSEC Certification
Security Essentials

www.giac.org/gsec

Six-Day Program
Mon, Oct 16 - Sat, Oct 21
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Bryan Simon

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

"This course has been invaluable in refreshing my networking, Windows, and security knowledge."

-Ron Mason, SLT Expressway

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

STOP and ask yourself the following questions:

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

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

SEC401: 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.

SANS Technology Institute
www.sans.edu

www.sans.org/8140

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

Bryan Simon *SANS Certified Instructor*

Bryan Simon is an internationally recognized expert in cybersecurity and has been working in the information technology and security field since 1991. Over the course of his career, Bryan has held various technical and managerial positions in the education, environmental, accounting, and financial services sectors. Bryan speaks on a regular basis at international conferences and with the press on matters of cybersecurity. He has instructed individuals from organizations such as 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 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 Advisory Board for the SANS Institute, and his acceptance into the prestigious SANS Cyber Guardian program. Bryan is a SANS instructor for SEC401, SEC501, SEC505, and SEC511. **@BryanOnSecurity**

SEC542

GWAPT Certification

Web Application Penetration Tester

www.giac.org/gwapt

Web App Penetration Testing and Ethical Hacking

Six-Day Program
Mon, Oct 16 - Sat, Oct 21
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Hassan El Hadary

Who Should Attend

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

"Every day of SEC542 gives you invaluable information from real-world testing you cannot find in a book."

-David Fava, The Boeing Company

"As a non-penetration tester, I found SEC542 very informative and useful. The exercises proved invaluable to illustrating the topics."

-Keith McFarland, Intel

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 students 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.

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

Bundle OnDemand
with this course
www.sans.org/ondemand

Hassan El Hadary *SANS Instructor*

Hassan is currently a lead consultant at SecureMisr, where he heads the application security assessment and code review team. He is also responsible for performing penetration tests as well as advising customers in the areas of PCI-DSS and PCI-PIN Security Compliance Requirements. He started his career as a programmer, gradually developing a passion for information security. Hassan received his master's degree in computer science from the American University in Cairo with a thesis in the field of secure software engineering. He holds the GWAPT and GCIH certifications. Hassan is an active participant in bug bounty programs. He has been acknowledged and rewarded by several vendors such as Google, Apple, Facebook, Twitter, PayPal, eBay, Etsy, AT&T, Gift Cards, Cisco Meraki, and Groupon. Hassan has made presentations at numerous events, including the SANS Pen Test Berlin, U.S. – Egypt Cyber Security Workshop, Middle East Info Security Summit, ADPoly Cyber Security Bootcamp, OWASP Cairo Chapter, CSCAMP and SKLABS. **@hassan_hadary**

SEC566

Implementing and Auditing the Critical Security Controls – In-Depth

GCCC Certification
Critical Controls

www.giac.org/gccc

Five-Day Program
Mon, Oct 16 - Fri, Oct 20
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: James Tarala

Who Should Attend

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

"This training gets right to the point quickly, and the labs are very clear and concise."

-Duane Harper, Community Health Systems

SANS Technology Institute
www.sans.edu

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

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

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

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

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle. The British government's Center for the Protection of National Infrastructure describes the Controls as the "baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence."

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

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

James Tarala *SANS Senior Instructor*

James Tarala is a principal consultant with Enclave Security and is based in Venice, Florida. He is a regular speaker for the SANS Institute as well as a courseware author and editor for many SANS auditing and security courses. As a consultant, he has spent the past few years developing large enterprise IT security and infrastructure architectures, specifically working with many Microsoft-based directory services, e-mail, terminal services, and wireless technologies. He has also spent a large amount of time consulting with organizations to assist them with their security management, operational practices, and regulatory compliance issues, and he often performs independent security audits and assists internal audit groups in developing their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University and his graduate work at the University of Maryland. He holds numerous professional certifications. **@isaudit**

SEC575

Mobile Device Security and Ethical Hacking

GMOB Certification
Mobile Device Security Analyst
www.giac.org/gmob

Six-Day Program
Mon, Oct 16 - Sat, Oct 21
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Joshua Wright

Who Should Attend

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

"The new lab format in SEC575 is fantastic."
-David Lavezzo, Capital One

"SEC575's material is excellent. Josh Wright is a top-notch instructor and brings passion to the material he teaches."
-Adam Kliarsky, Disney

SANS Technology Institute
www.sans.edu

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

Imagine an attack surface spread throughout your organization and in the hands of every user. It moves from place to place regularly, stores highly sensitive and critical data, and sports numerous different wireless technologies all ripe for attack. You don't need to imagine any further because this already exists today: **mobile devices**. These devices are the biggest attack surface in most organizations, yet these same organizations often don't have the skills needed to assess them.

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

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

Understanding and identifying vulnerabilities and threats to mobile devices is a valuable skill, but it must be paired with the ability to communicate the associated risks. Throughout the course, you'll review the ways in which we can effectively communicate threats to key stakeholders. You'll leverage tools including Mobile App Report Cards to characterize threats for management and decision-makers, while identifying sample code and libraries that developers can use to address risks for in-house applications as well.

You'll then use your new skills to apply a mobile device deployment penetration test in a step-by-step fashion. Starting with gaining access to wireless networks to implement man-in-the-middle attacks and finishing with mobile device exploits and data harvesting, you'll examine each step in conducting such a test with hands-on exercises, detailed instructions, and tips and tricks learned from hundreds of successful penetration tests. By building these skills, you'll return to work prepared to conduct your own test, and you'll be better informed about what to look for and how to review an outsourced penetration test.

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**

FOR508

Advanced Digital Forensics, Incident Response, and Threat Hunting

GCFA Certification
Forensic Analyst

www.giac.org/gcfa

Six-Day Program
Mon, Oct 16 - Sat, Oct 21
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Eric Zimmerman

Who Should Attend

- Incident response team members
- Threat hunters
- Experienced digital forensic analysts
- Information security professionals
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- SANS FOR500 (formerly FOR408) and SEC504 graduates

"Many people lack good forensics skills; being able to figure out what happened is sometimes more important than fixing it."

-Justin Davis, St. Jude Medical

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

- Detect how and when a breach occurred
- Identify compromised and affected systems
- Determine what attackers took or changed
- Contain and remediate incidents
- Develop key sources of threat intelligence
- Hunt down additional breaches using knowledge of the adversary

"SEC508 gives you the exact tools and information needed to modernize your Incident Response processes."

-Shaun Gatherum, NuScale Power

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.

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 hactivism. Constantly updated, **FOR508: Advanced Digital Forensics, 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.

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

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

www.sans.org/8140

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

Eric Zimmerman *SANS Certified Instructor*

As a former Special Agent with the FBI, Eric had responsibilities that included managing on-scene triage. He identified several gaps in an existing process and started creating solutions to address them. What began as building and expanding a few live response tools took Eric down a path that eventually led to him writing more than 50 programs that are now used by nearly 8,800 law enforcement officers in over 80 countries. Much of Eric's work involved designing and building software related to investigations of sexual abuse of children. In a single year, Eric's programs led to the rescue of hundreds of these children. As a result, in May 2012, Eric's was given a National Center for Missing and Exploited Children's Award, which honors outstanding law enforcement professionals who have performed above and beyond the call of duty. Eric was also presented with the U.S. Attorney Award for Excellence in Law Enforcement in 2013. Today, Eric serves as a Senior Director at Kroll in the company's cybersecurity and investigations practice. Eric's teaching philosophy focuses on the long-term gains achieved by not only understanding the nuts and bolts of how to run a tool and consume output, but also getting a deeper understanding of how tools work "under the hood." His focus on understating the big picture of digital forensics prepares students to perform better analysis, do new research of their own, and identify the best tools or techniques to perform successful investigations – all skills that will have a lifelong impact. **@EricRZimmerman**

FOR578

Cyber Threat Intelligence

GCTI Certification
Available Late 2017

Five-Day Program
Mon, Oct 16 - Fri, Oct 20
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Robert M. Lee

Who Should Attend

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

"This course gives a very smart and structured approach to cyber threat intelligence, something that the global community has been lacking to date."
-John Geary, Citigroup

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

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

FOR578: Cyber Threat Intelligence will help network defenders, threat hunting teams, and incident responders to:

- **Understand and develop skills in tactical, operational, and strategic-level threat intelligence**
- **Generate threat intelligence to detect, respond to, and defeat advanced persistent threats (APTs)**
- **Validate information received from other organizations to minimize resource expenditures on bad intelligence**
- **Leverage open-source intelligence to complement a security team of any size**
- **Create Indicators of Compromise (IOCs) in formats such as YARA, OpenIOC, and STIX**

The collection, classification, and exploitation of knowledge about adversaries – collectively known as cyber threat intelligence – gives network defenders information superiority that is used to reduce the adversary's likelihood of success with each subsequent intrusion attempt. Responders need accurate, timely, and detailed information to monitor new and evolving attacks, as well as methods to exploit this information to put in place an improved defensive posture.

Cyber threat intelligence thus represents a force multiplier for organizations looking to update their response and detection programs to deal with increasingly sophisticated advanced persistent threats. 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.

During a targeted attack, an organization needs a top-notch and cutting-edge threat hunting or incident response team armed with the threat intelligence necessary to understand how adversaries operate and to counter the threat. **FOR578: Cyber Threat Intelligence** will train you and your team in the tactical, operational, and strategic-level cyber threat intelligence skills and tradecraft required to make security teams better, threat hunting more accurate, incident response more effective, and organizations more aware of the evolving threat landscape.

THERE IS NO TEACHER BUT THE ENEMY!

Robert M. Lee *SANS Certified Instructor*

Robert M. Lee brings one of the most valuable and respected credentials to the classroom: real-world experience. Robert is the CEO and founder of his own company, Dragos, Inc., which provides cybersecurity solutions for industrial control system networks. In 2015, after the Ukranian power grid went down due to an intentional cyber attack, Robert helped to establish a specialized team to analyze the event. He then shared that information with the impacted parties as well as the U.S. government and private sector. Robert got his start in information security making small control systems for humanitarian missions. He joined the United States Air Force and became a cyberspace warfare operations officer in the U.S. intelligence community. In that role, he created and led a mission examining nation-states targeting industrial control systems, the first mission of its kind in the U.S. intelligence community. Robert has a master's degree in cybersecurity and computer forensics from Utica College as well as cyber and warfare training through the U.S. Air Force, and he's pursuing his doctorate in war studies from King's College London. He was named one of Forbes' 30 under 30 in Enterprise Technology in 2016, awarded EnergySec's 2015 Cyber Security Professional of the Year, and named one of Passcode's "Influencers." **@RobertMLee**

MGT512

GSLC Certification
Security Leadership

www.giac.org/gslc

SANS Security Leadership Essentials for Managers with Knowledge Compression™

Five-Day Program
Mon, Oct 16 - Fri, Oct 20
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop Recommended
Instructor: G. Mark Hardy

Who Should Attend

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

"I have some very specific achievable things I can do right away suggested by the course that will benefit my organization and me. That's valuable training."

-William E. Weyandt, American Orthodontics

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

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

Knowledge Compression™

Maximize your learning potential!

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

SANS Technology Institute
www.sans.edu

www.sans.org/8140

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

G. Mark Hardy *SANS Principal Instructor*

G. Mark Hardy is founder and president of National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for over 35 years, and is an internationally recognized expert and keynote speaker who has presented at over 250 events worldwide. He provides consulting services as a virtual CISO, expert witness testimony, and domain expertise in blockchain and cryptocurrency. G. Mark serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. He is a retired U.S. Navy captain and was entrusted with nine command assignments, including responsibility for leadership training for 70,000 sailors. A graduate of Northwestern University, he holds a BS in computer science, a BA in mathematics, a masters in business administration, and a masters in strategic studies, and holds the GSLC, CISSP, CISM and CISA certifications. @g_mark

SEC580 Metasploit Kung Fu for Enterprise Pen Testing

Two-Day Program
Sat, Oct 14 - Sun, Oct 15
9:00am - 5:00pm
12 CPEs
Laptop Required
Instructor: Kevin Fiscus

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 confirm 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.

SEC564 Red Team Operations and Threat Emulation

BETA!

Two-Day Program
Sat, Oct 14 - Sun, Oct 15
9:00am - 5:00pm
12 CPEs
Laptop Required
Instructor: Joe Vest

This course provides the foundation needed to manage and operate a Red Team and conduct Red Team engagements. What is Red Teaming? **Red Teaming is the process of using tactics, techniques, and procedures (TTPs) to emulate a real-world threat with the goals of training and measuring the effectiveness of people, processes and technology used to defend an environment.**

Red Teaming is built on the fundamentals of penetration testing, yet focuses on specific scenarios and goals used to evaluate and measure an organization's overall security defense posture. That posture includes people, processes, and technology. This course will explore Red Teaming concepts in depth to provide a clear understanding of what a Red Team is and its role in Security Testing.

Organizations spend a great deal of time and money on the security of their systems. Red Teaming uses a comprehensive approach to gain insight into an organization's overall security. Red Teams have a unique goal of testing an organization's ability to detect, respond to, and recover from an attack. When properly conducted, Red Team activities significantly improve an organization's security controls, help hone defensive capabilities, and measure the effectiveness of security operations.

The Red Team concept requires a different approach from a typical security test, and it relies heavily on well-defined TTPs. These are critical if a Red Team is to successfully emulate a realistic threat or adversary. Red Team results exceed a typical list of penetration test vulnerabilities, provide a deeper understanding of how an organization would perform against an actual threat, and identify where security strengths and weaknesses exist.

Bonus Sessions

Enrich your SANS training experience! Evening talks by our instructors and selected subject-matter experts help you broaden your knowledge, hear from the voices that matter in computer security, and get the most for your training dollar.

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.

Industrial Control System Active Defense and Threat Intelligence

Robert M. Lee

Industrial control systems (ICS) are some of the most defensible environments on the planet. Sure, ICS tend to have legacy equipment and numerous vulnerabilities, but if you really want to make the lights blink it's going to take more than an exploit. In this presentation, Robert M. Lee, the course author for ICS515 and FOR578, will talk about what it means to make a defensible environment a defended one by leveraging active defense best practices such as threat hunting and network security monitoring. In addition, the presentation will cover the types of threat intelligence that are applicable to such environments, with use-cases highlighting lessons learned for both good and bad practices. Ultimately, defending these industrial environments requires a human focus.

Anti-Ransomware: How to Turn the Tables

G. Mark Hardy

"OMG! We just got hit with ransomware!" What you don't usually hear next is "LOL!" You can build defenses that prevent ransomware from paralyzing your organization – we'll show you how. Ransomware is a billion dollar industry, and it's growing tremendously. Lost productivity costs far more than the average ransom, so executives just say, "Pay the darn thing." But what if you could stop ransomware in its tracks? We'll demonstrate tools and methodologies that are battle-proven and ACTUALLY WORK as evidenced by fully contained ransomware "explosions" that went nowhere. We'll offer insights into the future of this attack vector and venture predictions on how this industry will evolve and what to expect next.

Hunting Logic Attacks

Hassan El Hadary

One of the most challenging problems for developers these days is to design secure applications. Development platforms are protected from common attacks such as Cross-Site Scripting, SQL injection, and others by several provided techniques. However, logic attacks are still the trickiest to discover and the most difficult to stop. Logic attacks can allow an attacker to gain access to sensitive data or get control of unauthorized systems. In the era of IoT and complex applications, logic attacks will have higher impact. In this talk, we will present several logic attack scenarios of how attackers broke developer defenses. All of the scenarios are based on findings discovered in real-life professional experience and bug bounty programs. Finally, we will discuss the future of such attacks and its application to IoT systems.

Plumbing the Depths: ShellBags

Eric Zimmerman

This presentation will explore the most common ShellBag types (directories, GUIDs, control panel items, etc.) and the kinds of data contained therein, including timestamps, usernames, changing program associations, file system info, user searches, access to network resources (UNC paths and FTP), and so on. The discussion will also cover extension blocks and the kinds of data they contain. The discussion will start at the hex level, work toward higher levels of abstraction, and culminate with examples of using ShellBags Explorer (SBE) to streamline the review of ShellBags data. This will include showing how SBE can be used to accelerate the investigation of unlimited amounts of ShellBag data, including working with individual registry hives as well as deduplicating multiple hives for a user. The presentation will also demonstrate how Dan Pullega's research has been incorporated and expanded upon, including first and last explored dates. The information contained in ShellBags and exposed via SBE is relevant to FEs, incident response teams, and law enforcement as it quickly and easily provides context around a user's actions as well as the user's interaction with a computer and its associated resources.

Enhance Your Training Experience

Add an
OnDemand Bundle & GIAC Certification Attempt* to your course within seven days of this event for just $689 each.

SPECIAL 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

"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

"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.

Future Training Events

SANSFIRE — Washington, DC — July 22-29

San Antonio	San Antonio, TX	Aug 6-11
Boston	Boston, MA	Aug 7-12
New York City	New York, NY	Aug 14-19
Salt Lake City	Salt Lake City, UT	Aug 14-19
Chicago	Chicago, IL	Aug 21-26
Virginia Beach	Virginia Beach, VA	Aug 21 - Sep 1
Tampa – Clearwater	Clearwater, FL	Sep 5-10
San Francisco Fall	San Francisco, CA	Sep 5-10

Network Security — Las Vegas, NV — Sep 10-17

Baltimore Fall	Baltimore, MD	Sep 25-30
Rocky Mountain Fall	Denver, CO	Sep 25-30
Phoenix-Mesa	Mesa, AZ	Oct 9-14
Tysons Corner Fall	McLean, VA	Oct 16-21
San Diego	San Diego, CA	Oct 30 - Nov 4
Seattle	Seattle, WA	Oct 30 - Nov 4
Miami	Miami, FL	Nov 6-11
San Francisco Winter	San Francisco, CA	Nov 27 - Dec 2
Austin Winter	Austin, TX	Dec 4-9

Cyber Defense Initiative — Washington, DC — Dec 12-19

Future Summit Events

ICS & Energy	Houston, TX	July 10-15
Security Awareness	Nashville, TN	July 31 - Aug 9
Data Breach	Chicago, IL	Sep 25 - Oct 2
Secure DevOps	Denver, CO	Oct 10-17
SIEM & Tactical Analytics	Scottsdale, AZ	Nov 28 - Dec 5
Cyber Threat Intelligence	Washington, DC	Jan 27 - Feb 6

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.

Hotel Information

Hilton McLean Tysons Corner
7920 Jones Branch Drive
McLean, VA 22102
Phone: 703-847-5000
www.sans.org/event/tysons-corner-2017/location

Experience impeccable service at the Hilton McLean Tysons Corner hotel near Washington, DC. This contemporary hotel is located in the center of Tysons Corner's technology corridor, between Ronald Reagan National Airport and Washington Dulles International Airport. It is also just minutes from world-class shopping at Tysons Corner Center and the Galleria Mall. Take the Silver Line Metro from the McLean Station into downtown Washington, DC. A complimentary shuttle servicing a one-mile radius of the hotel is also provided.

Special Hotel Rates Available

A special discounted rate of $204.00 S/D will be honored based on space availability.

The group rate is currently lower than the government per diem rate. Should this change, a government rate will be available. The group rate includes high-speed Internet in your room and is only available through September 22, 2017.

Top 5 reasons to stay at the Hilton McLean Tysons Corner

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

Registration Information

Register online at **www.sans.org/tysons-corner-2017**

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.

Pay Early and Save*

Use code **EarlyBird17** when registering early

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code by	**8-23-17**	**$400.00**	**9-13-17**	**$200.00**

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

SANS Voucher Program

Expand your training budget!

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

www.sans.org/vouchers

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 received payments by **September 20, 2017**. 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.

Open a **SANS Account** today to enjoy these FREE resources:

WEBCASTS

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

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

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

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

NEWSLETTERS

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

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

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

OTHER FREE RESOURCES

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

www.sans.org/account