THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH

SANS Columbia, MD

June 26 - July 1, 2017

PROTECT YOUR COMPANY AND ADVANCE YOUR CAREER
WITH HANDS-ON, IMMERSION-STYLE

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

Seven courses in:

CYBER DEFENSE
PENETRATION TESTING
INCIDENT RESPONSE
CYBER THREAT INTELLIGENCE
ETHICAL HACKING
ICS/SCADA SECURITY

SAVE $400

Register and pay by May 3rd – Use code **EarlyBird17**

"The quality of SANS training was exceptional and exceeded my already high expectations. The instructor presented well, but his knowledge and real-world experiences were the true benefit. I am anxious to attend more courses."

-Doug Henderson, Binghamton University

GIAC CERTIFICATIONS
GIAC-Approved Training

www.sans.org/columbia

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 Columbia 2017 lineup of instructors includes:

Rebekah Brown
Instructor
@PDXBek

Paul A. Henry
Senior Instructor
@phenrycissp

Robert M. Lee
Certified Instructor
@RobertMLee

Michael Murr
Principal Instructor
@mikemurr

Chris Pizor
Certified Instructor
@chris_pizor

Dr. Johannes Ullrich
Senior Instructor
@johullrich
@sans_isc

J.D. Wegner
Instructor
@jdwegner

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 8.

KEYNOTE: ***Threat Intelligence and Attribution in a Political Climate***
Robert M. Lee

Opening a Can of Active Defense and Cyber Deception to Confuse and Frustrate Attackers
Chris Pizor

Evolving Threats
Paul Henry

Intro to Windows Computer Forensics – Finding Intrusions
Jacquelyn Blanchard

Save $400 when you register and pay by May 3rd using code EarlyBird17

Courses at a Glance

	MON 6-26	TUE 6-27	WED 6-28	THU 6-29	FRI 6-30	SAT 7-1
SEC301 Intro to Information Security	Page 1					
SEC401 Security Essentials Bootcamp Style	Page 2					
SEC503 Intrusion Detection In-Depth	Page 3					
SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	Page 4					
SEC560 Network Penetration Testing and Ethical Hacking	Page 5					
FOR578 Cyber Threat Intelligence	Page 6					
ICS515 ICS Active Defense and Incident Response	Page 7					

SEC301

Intro to Information Security

GISF Certification

Information Security Fundamentals

www.giac.org/gisf

Five-Day Program
Mon, June 26 - Fri, June 30
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: J.D. Wegner

Who Should Attend

- People who are new to information security 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 information security and need formal training/certification

"Labs reinforced the security principles in a real-world scenario."

-Tyler Moore, Rockwell

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 was the perfect blend of technical and practical information for someone new to the field, and I would recommend it!"

-Steve Mecco, Draper

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.***

J.D. Wegner *SANS Instructor*

J.D. Wegner has 40 years of experience in IT, half that spent teaching others how to excel in the industry. He describes himself as a Crypto-Geek and holds that "a little paranoia now and then is healthy." J.D. has taught over 10,000 students from industry, education, and the government how to build networks and make them more secure. He and his wife call Hickory, NC home and enjoy spending time with their grandchildren. **@jdwegner**

SEC401

Security Essentials Bootcamp Style

GSEC Certification
Security Essentials

www.giac.org/gsec

Six-Day Program
Mon, June 26 - Sat, July 1
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Paul A. Henry

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

"Everyone in cyber should attend this course because it covers many aspects of security and emerging trends."
-Pamela Livingston-Spruill, DOE/NNSA

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

STOP and ask yourself the following questions:

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

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

SEC401: 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:

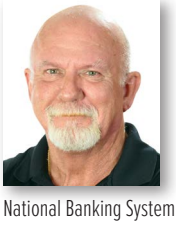
What is the risk? Is it the highest priority risk? What is the most cost-effective way to reduce the risk?

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



Paul A. Henry *SANS Senior Instructor*

Paul is one of the world's foremost global information security and computer forensic experts, with more than 20 years' experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principal at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security. Throughout his career, Paul has played a key strategic role in launching new network security initiatives to meet our ever-changing threat landscape. He also advises and consults on some of the world's most challenging and high-risk information security projects, including the National Banking System in Saudi Arabia, the Reserve Bank of Australia, the U.S. Department of Defense's Satellite Data Project, and both government and telecommunications projects throughout Southeast Asia. Paul is frequently cited by major publications as an expert on perimeter security, incident response, computer forensics, and general security trends, and serves as an expert commentator for network broadcast outlets such as FOX, NBC, CNN, and CNBC. In addition, Paul regularly authors thought leadership articles on technical security issues, and his expertise and insight help shape the editorial direction of key security publications such as the *Information Security Management Handbook*, to which he is a consistent contributor. Paul is a featured speaker at seminars and conferences worldwide, delivering presentations on diverse topics such as anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, perimeter security, and incident response. **@phenrycissp**

SEC503

Intrusion Detection In-Depth

GCIA Certification
Certified Intrusion Analyst

www.giac.org/gcia

Six-Day Program
Mon, June 26 - Sat, July 1
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Johannes Ullrich, Ph.D.

Who Should Attend

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

"This training directly correlates to my agency's mission of conducting network forensics/ intrusion investigations."

-Chris G., U.S. Air Force Office of Special Investigations

"I would recommend this to network/ security people who have some experience already but need to sharpen their skills."

-M.S., AOL

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

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

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

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

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

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

Johannes Ullrich, Ph.D. *SANS Senior Instructor*

As Dean of Research for the SANS Technology Institute, Johannes is currently responsible for the SANS Internet Storm Center (ISC) and the GIAC Gold program. In 2000, he founded DShield.org, which is now the data collection engine behind the ISC. His work with the ISC has been widely recognized, and in 2004, *Network World* named him one of the 50 most powerful people in the networking industry. Prior to working for SANS, Johannes worked as a lead support engineer for a web development company and as a research physicist. Johannes holds a PhD in physics from SUNY Albany and is based in Jacksonville, Florida. His daily podcast summarizes current security news in a concise format. **@johullrich** **@sans_isc**

SEC504

Hacker Tools, Techniques, Exploits, and Incident Handling

GCIH Certification
Incident Handler
www.giac.org/gcih

Six-Day Program
Mon, June 26 - Sat, July 1
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Chris Pizor

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

"This course fills the gap of 'here's what adversaries do and the evidence it leaves.'"
-Kevin Heithaus, JPMorgan Chase

"SEC504 helped me put many pieces of the puzzle together."
-Ian Trimble, Blue Cross Blue Shield

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or one or two disgruntled employees (and whose does not!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth. As defenders, it is essential we understand these hacking tools and techniques.

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

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

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

Chris Pizor *SANS Certified Instructor*

Chris Pizor is a civilian employee working for the U.S. Air Force as the lead curriculum designer for cyber warfare operations training. Chris served on active duty in the USAF as a Network Intelligence Analyst before retiring in 2010. He was part of the initial cadre of the NSA Threat Operations Center and helped develop tactics to discover and eradicate intrusions into U.S. government systems. Chris has worked in the intelligence community for more than 20 years, including 12 years focused on cybersecurity. Over the course of his active duty career, Chris received multiple individual and team awards. Chris is passionate about security and helping others advance their security knowledge, and he is continuously researching and refining his own skills so he can prepare U.S. airmen and women and other professionals defend their vital networks and critical infrastructure. Chris earned a bachelor's degree in intelligence studies and information operations from the American Military University and a master's of science in cybersecurity from University of Maryland University College. He holds the GSEC, GCIA, GCIH, GPEN, GXPN, GCFA, GISP, and CISSP certifications. When Chris isn't working, he enjoys spending time with his wife and two young children, woodworking, and spending time outdoors. **@chris_pizor**

SEC560

Network Penetration Testing and Ethical Hacking

GPEN Certification
Penetration Tester

www.giac.org/gpen

Six-Day Program
Mon, June 26 - Sat, July 1
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Michael Murr

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

"I learned more in one class than in years of self-study!"
-Bradley Milhorn, Compucom Inc.

"It introduces the whole process of pen testing from start of engagement to end."
-Barry Tsang, Deloitte

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 more than 30 detailed hands-on labs throughout. The course is chock-full of practical, real-world tips from some of the world's best penetration testers to help you do your job safely, efficiently...and masterfully.

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

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

You will bring comprehensive penetration testing and ethical hacking know-how back to your organization.

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

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian

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

Michael Murr *SANS Principal Instructor*

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

FOR578

Cyber Threat Intelligence

Five-Day Program
Mon, June 26 - Fri, June 30
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Rebekah Brown

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

"Outstanding course material and instructor presentation! FOR578 truly drills into the analytic process, while remaining technical. I highly recommend this course to anyone performing any level of intelligence support to defensive cyber operations."

-Thomas L., U.S. Air Force

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!

Rebekah Brown *SANS Instructor*

Rebekah Brown is the threat intelligence lead for Rapid7, supporting incident response, analytic response, global services and product support. She is a former NSA network warfare analyst, U.S. Cyber Command training and exercise lead, and Marine Corps crypto-linguist who has helped develop threat intelligence programs at the federal, state, and local levels as well as in the private sector at a Fortune 500 company. She has an associate's degree in Chinese Mandarin, a B.A. in international relations, and is wrapping up a M.A. in homeland security with a cybersecurity focus and a graduate certificate in intelligence analysis. **@PDXBek**

ICS515

ICS Active Defense and Incident Response

GRID Certification
Industrial Response and Defense
www.giac.org/grid

Five-Day Program
Mon, June 26 - Fri, June 30
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Robert M. Lee

Who Should Attend

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

"Awesome!! This course was my sixth SANS course, and Robert M. Lee demonstrated and reiterated the fact that SANS has the world's best instructors."
-Srinath Kannan, Accenture

"Very powerful tools and concepts!"
-Randy Wagner, Basin Electric

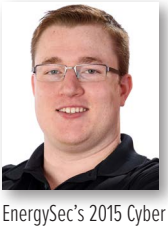
Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

ICS515: ICS Active Defense and Incident Response will help you deconstruct cyber attacks on industrial control systems (ICS), leverage an active defense to identify and counter threats, and use incident response procedures to maintain the safety and reliability of operations.

This course will empower students to understand their networked industrial control system environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security. This process of monitoring, responding to, and learning from threats internal to the network is known as active defense. An active defense is the approach needed to counter advanced adversaries targeting ICS, as has been seen with malware such as Stuxnet, Havex, and BlackEnergy2. Students can expect to come out of this course with the ability to deconstruct targeted ICS attacks and fight these adversaries and others. The course uses a hands-on approach and real-world malware to break down cyber attacks on ICS from start to finish. Students will gain a practical and technical understanding of leveraging active defense concepts such as using threat intelligence, performing network security monitoring, and utilizing malware analysis and incident response to ensure the safety and reliability of operations. The strategy and technical skills presented in this course serve as a basis for ICS organizations looking to show that defense is do-able.

This course will prepare you to:

- **Examine ICS networks and identify the assets and their data flows in order to understand the network baseline information needed to identify advanced threats**
- **Use active defense concepts such as threat intelligence consumption, network security monitoring, malware analysis, and incident response to safeguard the ICS**
- **Build your own Programmable Logic Controller using a CYBATIworks Kit and keep it after the class ends**
- **Gain hands-on experience with samples of Havex, BlackEnergy2, and Stuxnet through engaging labs while de-constructing these threats and others**
- **Leverage technical tools such as Shodan, Security Onion, TCPDump, NetworkMiner, Foremost, Wireshark, Snort, Bro, SGUIL, ELSA, Volatility, Redline, FTK Imager, PDF analyzers, malware sandboxes, and more**
- **Create indicators of compromise (IOCs) in OpenIOC and YARA while understanding sharing standards such as STIX and TAXII**
- **Take advantage of models such as the Sliding Scale of Cybersecurity, the Active Cyber Defense Cycle, and the ICS Cyber Kill Chain to extract information from threats and use it to encourage the long-term success of ICS network security**



Robert M. Lee *SANS Certified Instructor*

Robert M. Lee is the CEO and founder of the critical infrastructure cybersecurity company Dragos Security LLC, where he has a passion for control system traffic analysis, incident response, and threat intelligence research. He is the course author of SANS ICS515: Active Defense and Incident Response and the co-author of SANS FOR578: Cyber Threat Intelligence. Robert is also a non-resident National Cyber Security Fellow at New America focusing on policy issues relating to the cybersecurity of critical infrastructure and a PhD candidate at Kings College London. For his research and focus areas, he was named one of Passcode's Influencers and awarded EnergySec's 2015 Cyber Security Professional of the Year. Robert obtained his start in cybersecurity in the U.S. Air Force, where he served as a Cyber Warfare Operations Officer. He has performed defense, intelligence, and attack missions in various government organizations, and he established a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Robert routinely writes articles in publications such as *Control Engineering* and the *Christian Science Monitor's Passcode* and speaks at conferences around the world. He is also the author of SCADA and Me and the weekly web-comic **www.LittleBobbyComic.com**. **@RobertMLee**

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.

Threat Intelligence and Attribution in a Political Climate

Robert M. Lee

The business of security has never been as central to politics and mainstream media as it was during the 2016 election. Threat intelligence and attribution were particularly on display and many members of the information security community became part of the policy process as a result of their assessments. This presentation will break down these topics in order to help attendees understand how attribution works and what to watch out for in a highly political climate that revolves around security. To better understand the process, we'll examine case studies from 2016.

Opening a Can of Active Defense and Cyber Deception to Confuse and Frustrate Attackers

Chris Pizor

You're convinced that something just isn't right in your environment and you're tired of hearing that there haven't been any A/V, IDS, IPS, or firewall alerts. It's time to smash the easy button and take a more proactive approach to security. To do this, you decide to employ Active Defense and Cyber Deception techniques to get better visibility. Join us as we discuss some practical approaches to deploying these techniques and the OPSEC considerations associated with them. We will talk about how we can increase the visibility of attacker actions in the lower levels of our network. Lastly, we will discuss Honeypot OPSEC and some common pitfalls you need to avoid, as well as some easy changes that can be made to improve their likelihood of success in identifying attacker activity. It's time to take back your house!

Evolving Threats

Paul Henry

For nearly two decades defenders have fallen into the "Crowd Mentality Trap." They have simply settled on doing the same thing everyone else was doing, while at the same time attackers have clearly evolved both in terms of malware delivery vectors and attack methodology. Today our defenses focus primarily on the gateway and on attempting to outwit attackers' delivery methods. This leaves us woefully exposed and according to a recent Data Breach Report has resulted in 3,765 incidents, 806 million records exposed, and US$157 billion in data breach costs in only the past six years.

Intro to Windows Computer Forensics – Finding Intrusions

Jacquelyn Blanchard

We hear about breaches and attacks in the news daily. Once an attack is discovered, a Digital Forensic & Incident Response (DFIR) professional is normally contacted and asked to assist. During this presentation, Jacquelyn Blanchard will share some basic tools and methods you can use to analyze a forensic image of a host after a compromise.

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.

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, and 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 expense into their employment agreements even before joining a company. Some offer to stay for a year after they complete the training.

SANS Training Formats

Whether you choose to attend a training class live or online, the entire SANS team is dedicated to ensuring your training experience exceeds expectations.

Live Classroom Instruction

Premier Training Events

Our most recommended format, live SANS training events deliver SANS' top instructors teaching multiple courses at a single time and location. This allows for:

- Focused, immersive learning without the distractions of your office environment
- Direct access to SANS Certified instructors
- Interacting with and learning from other professionals
- Attending SANS@Night events, NetWars tournaments, vendor presentations, industry receptions, and many other activities

Our premier live training events in North America, serving thousands of students, are held in Orlando, Washington DC, Las Vegas, New Orleans, and San Diego. Regional events with hundreds of students are held in most major metropolitan areas during the year. See page 12 for upcoming Training Events in North America.

Summits

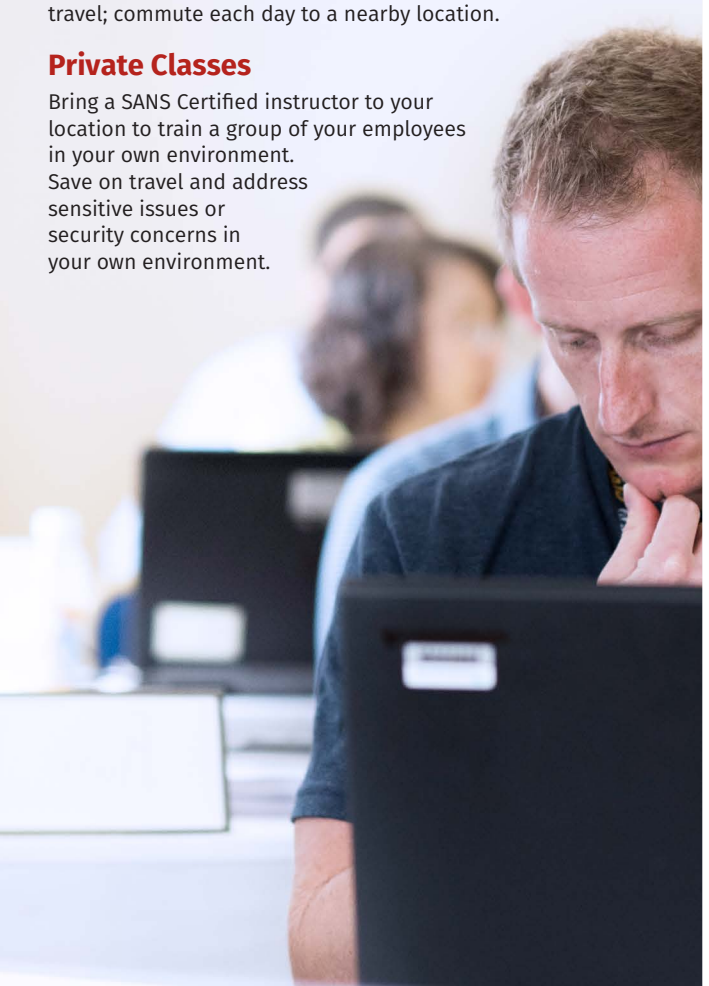
SANS Summits focus one or two days on a single topic of particular interest to the community. Speakers and talks are curated to ensure the greatest applicability to participants.

Community SANS Courses

Same SANS courses, courseware, and labs, taught by up-and-coming instructors in a regional area. Smaller classes allow for more extensive instructor interaction. No need to travel; commute each day to a nearby location.

Private Classes

Bring a SANS Certified instructor to your location to train a group of your employees in your own environment. Save on travel and address sensitive issues or security concerns in your own environment.



Online Training

SANS Online successfully delivers the same measured learning outcomes to students at a distance that we deliver live in classrooms. More than 30 courses are available for you to take whenever or wherever you want. Thousands of students take our courses online and achieve certification each year.

Top reasons to take SANS courses online:

- **Learn at your own pace, over four months**
- **Spend extra time on complex topics**
- **Repeat labs to ensure proficiency with skills**
- **Save on travel costs**
- **Study at home or in your office**

Our SANS OnDemand, vLive, Simulcast, and SelfStudy formats are backed by nearly 100 professionals who ensure we deliver the same quality instruction online (including support) as we do at live training events.

> **"I am thoroughly pleased with the OnDemand modality. From a learning standpoint, I lose nothing. In fact, the advantage of setting my own pace with respect to balancing work, family, and training is significant, not to mention the ability to review anything that I might have missed the first time."**
>
> -Kevin E., U.S. Army

> **"The decision to take five days away from the office is never easy, but so rarely have I come to the end of a course and had no regret whatsoever. This was one of the most useful weeks of my professional life."**
>
> -Dan Trueman, Novae PLC

Future Training Events

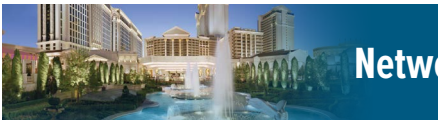
Baltimore Spring . . . . . Baltimore, MD . . . . . April 24-29

Security West . . . . . San Diego, CA . . . May 9-18

Northern Virginia – Reston . . . . Reston, VA . . . . . May 21-26
Atlanta . . . . . Atlanta, GA . . . . . May 30 - June 4
Houston . . . . . Houston, TX . . . . . June 5-10
San Francisco Summer . . . . . San Francisco, CA . . . . . June 5-10
Rocky Mountain . . . . . Denver, CO . . . . . June 12-17
Charlotte . . . . . Charlotte, NC . . . . . June 12-17
Minneapolis . . . . . Minneapolis, MN . . . . . June 19-24
Columbia . . . . . Columbia, MD . . . . . June 26 - July 1
Los Angeles – Long Beach . . . . Long Beach, CA . . . . . July 10-15

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 9-16

Baltimore September . . . . . Baltimore, MD . . . . . Sep 25-30
Rocky Mountain Fall . . . . . Denver, CO . . . . . Sep 25-30

Future Summit Events

Threat Hunting and IR . . . . . New Orleans, LA . . . . . April 18-25
Automotive Cybersecurity . . . . Detroit, MI . . . . . May 1-8
Security Operations Center . . . Washington, DC . . . . . June 5-12
Digital Forensics . . . . . Austin, TX . . . . . June 22-29
ICS & Energy . . . . . Houston, TX . . . . . July 10-14
Security Awareness . . . . . Nashville, TN . . . . . July 31 - Aug 9
Data Breach . . . . . Chicago, IL . . . . . Sep 25 - Oct 2

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

Sheraton Columbia Town Center
10207 Wincopin Circle
Columbia, MD 21044
Phone: 410-730-3900
www.sans.org/event/columbia-2017/location

Centrally located between Baltimore and Washington D.C., this prime location in Columbia's unique city center offers all the sophistication of downtown within the serenity of 12 wooded acres. Enjoy seasonal activities on the shores of Lake Kittamaqundi or walk over to the nearby 200-store upscale mall in Columbia and shop 'til you drop.

Special Hotel Rates Available

A special discounted rate of $135.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through **June 5, 2017**. To make reservations, please call **888-627-8318** and ask for the SANS group rate or SANS government rate

Top 5 reasons to stay at the Sheraton Columbia Town Center

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 Sheraton Columbia Town Center 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 Sheraton Columbia Town Center that you won't want to miss!
5. Everything is in one convenient location!

Registration Information

Register online at **www.sans.org/columbia**

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 before	**5-3-17**	**$400.00**	**5-24-17**	**$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. 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 **June 7, 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