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

SANS SOUTHERN CALIFORNIA Anaheim 2017

February 6-11

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

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

Eight courses on

Cyber Defense
Penetration Testing
Incident Response
Threat Hunting
Ethical Hacking
Management
ICS/SCADA Security

"SANS training is valuable to me both personally and professionally. It provided me with the tools to communicate better, and has sharpened my skills."
-Richard Branam, NSID

SAVE $400

Register and pay by Dec 14th – Use code **EarlyBird17**

GIAC
GIAC-Approved Training

www.sans.org/anaheim

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 Anaheim 2017 lineup of instructors includes:

Jason Fossen
Faculty Fellow
@JasonFossen

James Lyne
Certified Instructor
@jameslyne

Michael Murr
Principal Instructor
@mikemurr

Keith Palmgren
Senior Instructor
@kpalmgren

Billy Rios
SANS Instructor
@XSSniper

Stephen Sims
Senior Instructor
@Steph3nSims

Mark Williams
SANS Instructor
@securemdw

Eric Zimmerman
SANS Instructor
@EricRZimmerman

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 9.

KEYNOTE: ***What's New for Security in Windows Server 2016 and Windows 10?***
Jason Fossen

(Am)Cache Rules Everything Around Me
Eric Zimmerman

Birds of a Feather or...
Mark Williams

The 14 Absolute Truths of Security
Keith Palmgren

Save $400 when you register and pay by Dec 14th using code EarlyBird17

Courses-at-a-Glance

		MON 2-6	TUE 2-7	WED 2-8	THU 2-9	FRI 2-10	SAT 2-11
SEC301	Intro to Information Security	Page 1					
SEC401	Security Essentials Bootcamp Style	Page 2					
SEC504	Hacker Tools, Techniques, Exploits & Incident Handling	Page 3					
SEC505	Securing Windows and PowerShell Automation	Page 4					
SEC660	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	Page 5					
FOR508	Advanced Digital Forensics, Incident Response, and Threat Hunting	Page 6					
MGT514	IT Security Strategic Planning, Policy, and Leadership	Page 7					
ICS410	ICS/SCADA Security Essentials	Page 8					

SEC301:

Intro to Information Security

SANS

Five-Day Program
Mon, Feb 6- Fri, Feb 10
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Keith Palmgren

www.giac.org/gisf

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"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

"Keith is very engaging and he not only helped me greatly to understand the topics, but also made them interesting to learn."
-Jennifer Bakowski, John Hancock Financial Services

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: Introduction 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.

Authored 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**. 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 is an educational genius to have me grasping HEX and BIN in twenty minutes!"
-Lisa Bruere, LMI Aerospace Inc.

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

SANS

Six-Day Program
Mon, Feb 6- Sat, Feb 11
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Stephen Sims

www.giac.org/gsec

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"This course has been valuable both to me and my career – the course material and the instructor are an awesome match."
-Camille Crosby,
The William Carter Company

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.

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

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

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

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

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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

Who Should Attend

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

Stephen Sims *SANS Senior Instructor*

Stephen Sims is an industry expert with over 15 years of experience in information technology and security. Stephen currently works out of San Francisco as a consultant performing reverse engineering, exploit development, threat modeling, and penetration testing. Stephen has a master's of science degree in information assurance from Norwich University. He is the author of SANS' only 700-level course, SEC760: Advanced Exploit Development for Penetration Testers, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author of SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking. He holds the GIAC Security Expert (GSE) certification as well as the CISSP, CISA, Immunity NOP, and many other certifications. In his spare time, Stephen enjoys snowboarding and writing music. @Steph3nSims

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, Feb 6- Sat, Feb 11
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Michael Murr

www.giac.org/gcih

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

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

"This training caters to various levels of technical ability and relates actions and activities to real issues."
-Armando Nardo, Ernst & Young LLP

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.**

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

"Great instruction! SEC504 covered topics very thoroughly and gave great examples."
-Kevin H., U.S. Department of Homeland Security

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

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

"This course was well organized and the instructor presented the material in a clear and concise manner. You will learn something."
-Thomas C., Marine Corps Cyberspace Command

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 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

SEC505:

Securing Windows and PowerShell Automation

SANS

Six-Day Program
Mon, Feb 6- Sat, Feb 11
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jason Fossen

Hackers know how to use PowerShell for evil. Do you know how to use it for good? In SEC505 you will learn PowerShell and adaptive Windows security at the same time. SecOps requires automation, and Windows automation means PowerShell.

You've run a vulnerability scanner and applied patches – *now what?* A major theme of this course is defensible design: we have to assume that there will be a breach, so we need to build in damage control from the beginning. Whack-a-mole incident response cannot be our only defensive strategy – we'll never win, and we'll never get ahead of the game. By the time your Security Information and Event Manager (SIEM) or monitoring system tells you a Domain Admin account has been compromised, it's TOO LATE.

Who Should Attend

- Security Operations (SecOps) engineers
- Windows endpoint and server administrators
- Anyone implementing the NSA top 10 mitigations
- Anyone who wants to learn PowerShell automation
- Anyone implementing the CIS Critical Security Controls
- Those deploying or managing a Public Key Infrastructure (PKI) or smart cards
- Anyone who needs to reduce malware infections

For the assume-breach mindset, we must carefully delegate *limited* administrative powers so that the compromise of one administrator account is not a total catastrophe. Managing administrative privileges is a tough problem, so this course devotes an entire day to just this one critical task.

Learning PowerShell is also useful for another kind of security: *job* security. Employers are looking for people with these skills. You don't have to know any PowerShell to attend the course, we will learn it together. About half the labs during the week are PowerShell, while the rest use graphical security tools. PowerShell is free and open source on GitHub for Linux and Mac OS, too.

This course is not a vendor show to convince you to buy another security appliance or to install yet another endpoint agent. The idea is to use built-in or free Windows and Active Directory security tools when we can (especially PowerShell and Group Policy) and then purchase commercial products only when absolutely necessary.

If you are an IT manager or CIO, the aim for this course is to have it pay for itself 10 times over within two years, because automation isn't just good for SecOps/DevOps, it can save money, too. Besides, PowerShell is also simply fun to use.

This course is designed for systems engineers, security architects, and the SecOps team. The focus of the course is on how to automate the NSA Top 10 Mitigations and the CIS Critical Security Controls related to Windows, especially the ones that are the difficult to implement in large environments.

This is a fun course and a real eye-opener, even for Windows administrators with years of experience. We don't cover patch management, share permissions, or other such basics – the aim is to go far beyond all that. Come have fun learning PowerShell and agile Windows security at the same time!

"This is a really great course for anyone involved in administration or securing of Windows environments."-David Hazar, Oracle

www.giac.org/gcwn

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

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

"This training was an excellent balance between theory and practical applications, extremely relevant to current trends, concepts, and technologies."
-Chris S., Naval Surface Warfare Center

Jason Fossen *SANS Faculty Fellow*

Jason Fossen is a principal security consultant at Enclave Consulting LLC, a published author, and a frequent public speaker on Microsoft security issues. He is the sole author of the SANS week-long Securing Windows course (SEC505), maintains the Windows day of Security Essentials (SEC401.5), and has been involved in numerous other SANS projects since 1998. He graduated from the University of Virginia, received his master's degree from the University of Texas at Austin, and holds a number of professional certifications. He currently lives in Dallas, Texas. @JasonFossen

SEC660:

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

SANS

Six-Day Program
Mon, Feb 6- Sat, Feb 11
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: James Lyne

www.giac.org/gxpn

www.sans.edu

www.sans.org/cyber-guardian

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"I'm very impressed at how well the instructor conveyed the information. This is a hard topic and I feel like I have a lot I can take home to practice. This material puts me at that next level." -Adam Logue, Spectrum Health

This course is designed as a logical progression point for those who have completed **SEC560: Network Penetration Testing and Ethical Hacking**, or for those with existing penetration testing experience.

Who Should Attend

- Network and systems penetration testers
- Incident handlers
- Application developers
- Intrusion detection system engineers

Students with the prerequisite knowledge to take this course will walk through dozens of real-world attacks used by the most seasoned penetration testers. The methodology of a given attack is discussed, followed by exercises in a real-world lab environment to solidify advanced concepts and allow for the immediate application of techniques in the workplace. **Each day includes a two-hour evening bootcamp to allow for additional mastery of the techniques discussed and even more hands-on exercises.** A sample of topics covered includes weaponizing Python for penetration testers, attacks against network access control (NAC) and VLAN manipulation, network device exploitation, breaking out of Linux and Windows restricted environments, IPv6, Linux privilege escalation and exploit-writing, testing cryptographic implementations, fuzzing, defeating modern OS controls such as ASLR and DEP, return-oriented programming (ROP), Windows exploit-writing, and much more!

"I learned a lot from taking this course, and it has motivated me to learn more about exploit writing." -Daniel Alvarez, UBS AG

Attackers are becoming more clever and their attacks more complex. In order to keep up with the latest attack methods, you need a strong desire to learn, the support of others, and the opportunity to practice and build experience. **SEC660 provides attendees with in-depth knowledge of the most prominent and powerful attack vectors and an environment to perform these attacks in numerous hands-on scenarios.** This course goes far beyond simple scanning for low-hanging fruit, and shows penetration testers how to model the abilities of an advanced attacker to find significant flaws in a target environment and demonstrate the business risk associated with these flaws.

James Lyne *SANS Certified Instructor*

James is the Director of EMEA at SANS and Director of Technology Strategy at the security firm Sophos. He comes from a background in cryptography but over the years has worked in a wide variety of security problem domains including anti-malware and hacking. James spent many years as a hands-on analyst dealing with deep technical issues and is a self-professed "massive geek." Eventually James escaped dark rooms and learned some social skills, and today he is a keen presenter at conferences and industry events. He has a wide range of experience working in a technical and a strategic capacity from incident response to forensics with some of the world's largest and most paranoid organizations. James participates in industry panels and policy groups, and is a frequently-called-upon expert advisor all over the world. He is a frequent guest lecturer and often appears in the media including national TV. As a young spokesperson for the industry James is extremely passionate about talent development and participates in initiatives to identify and develop new talent. Ask James to show you his best geek party trick. @jameslyne

FOR508:

Advanced Digital Forensics, Incident Response, and Threat Hunting

SANS

Six-Day Program
Mon, Feb 6- Sat, Feb 11
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Eric Zimmerman

www.giac.org/gcfa

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

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

- 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

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 FOR408 and SEC504 graduates

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

This is a hypothetical situation, but the chances are very high that hidden threats already exist inside your organization's networks. Organizations can't afford to believe that their security measures are perfect and impenetrable, no matter how thorough their security precautions might be. Prevention systems alone are insufficient to counter focused human adversaries who know how to get around most security and monitoring tools. The key is to catch intrusions in progress, rather than after attackers have completed their objectives and done worse damage to the organization. For the incident responder, this process is known as "threat hunting."

"This was a great course. I learned some great techniques and this will lead to some changes in our incident response process." -Rick, Syngenta

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, this course 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!

Eric Zimmerman *SANS Instructor*

Eric Zimmerman is a senior director in Kroll's Cyber Security and Investigations practice. Eric has tremendous depth and breadth of expertise in the cyber realm, spanning complex law enforcement investigations, computer forensics, expert witness testimony, computer systems design and application architecture. He has received widespread recognition for his work, is an award-winning author, and is a frequently sought-after instructor and presenter on cyber-related topics. Before joining Kroll, Eric was a Special Agent with the Federal Bureau of Investigation, specializing in investigating criminal and national security-related computer intrusions, crimes against children (production, distribution and possession of child pornography), intellectual property theft and related crimes. During his tenure with the FBI, Eric wrote over 50 programs that include forensic utilities and response tools that today are in use by nearly 8,800 law enforcement officers in 82 countries. Over the course of his career, Eric has led or participated in a wide range of cyber-focused classes, seminars and conferences. He is a two-time winner of the SANS DFIR NetWars Tournament (2015, 2014). In addition to his many speaking engagements, Eric is the co-author of *X-Ways Forensics Practitioner's Guide*, which was a Forensic 4Cast 2014 Digital Forensics Book-of-the-Year winner. @EricRZimmerman

MGT514:

IT Security Strategic Planning, Policy, and Leadership

SANS

Five-Day Program
Mon, Feb 6- Fri, Feb 10
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: Mark Williams

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

This course teaches security professionals how to do three things:

Who Should Attend

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

SANS Technology Institute
www.sans.edu

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

"Mark did a great job engaging the students. This is a tough course, however he pulls participation out of everyone."
-Todd Wagner, Caterpillar Inc.

"Mark was great, actively engaging and thorough. His industry examples were great, and the conversation was well led."
-Jason Popp, Nordstrom Inc.

Develop Strategic Plans

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

Create Effective Information Security Policy

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

Develop Management and Leadership Skills

Leadership is a capability that must be learned, exercised and developed to better ensure organizational success. Strong leadership is brought about primarily through selfless devotion to the organization and staff, tireless effort in setting the example, and the vision to see and effectively use available resources toward the end goal. Effective leadership entails persuading team members to accomplish their objectives while removing obstacles and maintaining the well-being of the team in support of the organization's mission. Learn to utilize management tools and frameworks to better lead, inspire, and motivate your teams.

Mark Williams *SANS Instructor*

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

ICS410:
ICS/SCADA Security Essentials

SANS

Five-Day Program
Mon, Feb 6- Fri, Feb 10
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Billy Rios

GICSP
www.giac.org/gicsp

SANS Technology Institute
www.sans.edu

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

Who Should Attend

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

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

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

The course will provide you with:

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

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

"This course was a great introduction into the ICS landscape and associated security concerns. The ICS material presented will provide immediate value relative to helping secure my company." -Mike Poulos, Coca-Cola Enterprises

Given the dynamic nature of industrial control systems, many engineers do not fully understand the features and risks of many devices. In addition, IT support personnel who provide the communications paths and network defenses do not always grasp the systems' operational drivers and constraints. This course is designed to help traditional IT personnel fully understand the design principles underlying control systems and how to support those systems in a manner that ensures availability and integrity. In parallel, the course addresses the need for control system engineers and operators to better understand the important role they play in cybersecurity.

Billy Rios *SANS Instructor*

An accomplished author and speaker, Billy is recognized as one of the world's most respected experts on emerging threats related to industrial control systems (ICS), critical infrastructure, and medical devices. He has discovered thousands of security vulnerabilities in hardware and software supporting ICS and critical infrastructure. He has been publically credited by the Department of Homeland Security (DHS) over 50 times for his support to the DHS ICS Cyber Emergency Response Team (ICS-CERT). Billy was a Lead at Google, where he led the front-line response to externally reported security issues and incidents. Prior to Google, Billy was the Security Program Manager at Internet Explorer (Microsoft). During his time at Microsoft, Billy led the company's response to several high-profile incidents, including the response for Operation Aurora. Before Microsoft, Billy worked as a penetration tester, an intrusion detection analyst, and served as an active-duty Marine Corps Officer. He holds an MBA and a master's of science degree in information systems. He was a contributing author for several publications including *Hacking, the Next Generation* (O'Reilly), *Inside Cyber Warfare* (O'Reilly), and *The Virtual Battle Field* (IOS Press). @XSSniper

SANS@NIGHT EVENING TALKS

Enrich your SANS training experience!

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

KEYNOTE:

What's New for Security in Windows Server 2016 and Windows 10?

Jason Fossen

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

(Am)Cache Rules Everything Around Me

Eric Zimmerman

Amcache is a valuable artifact for forensic examiners because it contains a wealth of information related to evidence of execution of programs, including installed applications and other executables that have been run on a computer, the SHA-1 value of the program, and several time stamps of interest that include the last modified time as well as the first time a program was run. By understanding the data available in the Amcache hive, examiners will be able to build better timelines, create whitelists and blacklists of programs to exclude or look for on other systems, and quickly find outliers in the vast amount of data contained in Amcache hives. People attending this session will come away with an understanding of how data are structured and interrelated in the different parts of an Amcache. Attendees will receive free open-source tools that can process these hives quickly and efficiently.

Birds of a Feather or...

Mark Williams

In this talk, Mark Williams will explore the divide between privacy and security, and how it has influenced structure within the security and privacy programs. We will also discuss what is needed to move ahead in a world where privacy and security must learn to not only coexist but to build a more synergistic relationship if we are to accomplish the objectives of both. Where do operational paths cross for these two high-profile programs, and how can the paths be negotiated so that they parallel one another as closely as possible? This talk will discuss:

- Legislation for privacy and how it impacts security
- Security touchstones and best practices and how they impact privacy
- How to bring security and privacy together, and what are the basic steps required?
- How to meet operational needs of the organization and still have both privacy and security?

The 14 Absolute Truths of Security

Keith Palmgren

Keith Palmgren has identified 14 absolute truths of security – things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these 14 absolute truths and how they affect a security program can lead to the success of that program. Failing to recognize these truths will spell almost certain doom. Here we will take a non-technical look at each of the 14 absolute truths in turn, examine what they mean to the security manager and the security posture, and see how understanding them will lead to a successful security program.

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 Certification

- 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.

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

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

Community SANS www.sans.org/community
Live Training in Your Local Region with Smaller Class Sizes

Private Training www.sans.org/private-training
Live Onsite Training at Your Office Location. Both In-person and Online Options Available

Mentor www.sans.org/mentor
Live Multi-Week Training with a Mentor

Summit www.sans.org/summit
Live IT Security Summits and Training

ONLINE TRAINING

OnDemand www.sans.org/ondemand
E-learning Available Anytime, Anywhere, at Your Own Pace

vLive www.sans.org/vlive
Online Evening Courses with SANS' Top Instructors

Simulcast www.sans.org/simulcast
Attend a SANS Training Event without Leaving Home

OnDemand Bundles www.sans.org/ondemand/bundles
Extend Your Training with an OnDemand Bundle Including Four Months of E-learning

FUTURE SANS TRAINING EVENTS

San Francisco 2016
San Francisco, CA | Nov 27 - Dec 2

Cyber Defense Initiative 2016
Washington, DC | Dec 10-17

Security East 2017
New Orleans, LA | Jan 9-14

Las Vegas 2017
Las Vegas, NV | Jan 23-28

Cyber Threat Intelligence
SUMMIT & TRAINING 2017
Arlington, VA | Jan 25 - Feb 1

Scottsdale 2017
Scottsdale, AZ | Feb 20-25

Dallas 2017
Dallas, TX | Feb 27 - Mar 4

San Jose 2017
San Jose, CA | Mar 6-11

Tysons Corner Spring 2017
McLean, VA | Mar 20-25

ICS Security
SUMMIT & TRAINING 2017
Orlando, FL | Mar 20-27

Pen Test Austin 2017
Austin, TX | Mar 27 - Apr 1

SANS 2017
Orlando, FL | Apr 7-14

Threat Hunting & IR
SUMMIT & TRAINING 2017
New Orleans, LA | Apr 18-25

Baltimore Spring 2017
Baltimore, MD | Apr 24-29

Information on all events can be found at
www.sans.org/security-training/by-location/all

SANS ANAHEIM 2017

Hotel Information

Training Campus

Anaheim Majestic Garden Hotel

900 South Disneyland Drive
Anaheim, CA 92870
714-234-2413
www.sans.org/event/anaheim-2017/location

Located across the street from the Disneyland® Resort, Anaheim Majestic Garden Hotel is situated on 13 acres of strolling gardens with courtyards, a fountain, rose garden and koi pond. Unwind next to their sparkling outdoor heated pool and whirlpool or raise your energy level in the fitness center, family game room or video arcade/billiard room.

Special Hotel Rates Available

A special discounted rate of $148.00 S/D will be honored based on space availability. Government per diem rooms are available with proper ID. These rates include high-speed Internet in your room and are only available through January 18, 2017.

Top 5 Reasons to Stay at the Anaheim Majestic Garden Hotel

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 Anaheim Majestic Garden Hotel, 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 Anaheim Majestic Garden Hotel that you won't want to miss!
5. Everything is in one convenient location!

SANS ANAHEIM 2017

Registration Information

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

Register online at www.sans.org/anaheim

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.

Use code **EarlyBird17** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**12-14-16**	**$400.00**	**1-4-17**	**$200.00**

Some restrictions apply.

SANS Voucher Program

Expand your training budget!

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

www.sans.org/vouchers

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by January 18, 2017 – processing fees may 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