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

SANS Salt Lake City 2016

June 27 – July 2

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

"As always, SANS training is extremely valuable for any security professional. This course sits on top of the mountain of great SANS material."

-Doug Rodgers, Wells Fargo

SAVE $400

by registering and paying early!

See page 13 for more details.

Protect your company and advance your career with these crucial courses:

- Security Essentials Bootcamp Style
- Hacker Tools, Techniques, Exploits & Incident Handling
- Advanced Digital Forensics and Incident Response
- Defending Web Applications Security Essentials
- SANS Training Program for CISSP® Certification
- ICS/SCADA Security Essentials

GIAC Approved Training

REGISTER AT

sans.org/salt-lake-city-2016

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 Salt Lake City 2016 lineup of instructors includes:

David R. Miller
Certified Instructor

Michael Murr
Principal Instructor

Justin Searle
Certified Instructor

Bryan Simon
Certified Instructor

Chad Tilbury
Senior Instructor

Johannes Ullrich
Senior Instructor

Evening Bonus Sessions

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

KEYNOTE: ***Tales from the Battlefield: Lessons in Incident Response*** – Chad Tilbury

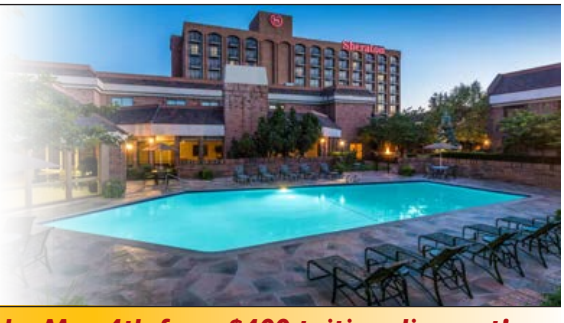
The Internet of Evil Things – Dr. Johannes Ullrich

The CISSP® Exam was Implemented on April 15, 2015 – David Miller

Continuous Ownage: Why You Need Continuous Monitoring – Bryan Simon

The training campus for SANS Salt Lake City 2016, the Sheraton Salt Lake City Hotel, is located in the heart of the downtown business and entertainment district.

PAGE 13



Be sure to register and pay by May 4th for a $400 tuition discount!

Courses-at-a-Glance

The Value of SANS Training & YOU

EXPLORE

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

RELATE

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

VALIDATE

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

SAVE

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

ADD VALUE

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

ALTERNATIVES

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

ACT

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

Return on Investment

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

REMEMBER

the SANS promise:

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

SEC401:
Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Jun 27 - Sat, Jul 2
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Bryan Simon

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"The success of this course rides on the delivery of the instructor. Bryan makes a 10 hour day go by very fast, and his teaching is stellar and his knowledge is amazing."
-Carroll Anne Smith, Analyst at DHS

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

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

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

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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

With the advanced persistent threat, 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.

Bryan Simon *SANS Certified Instructor*

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

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, Jun 27 - Sat, Jul 2
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Michael Murr

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8140

Bundle OnDemand
WITH THIS COURSE
sans.org/ondemand

"SEC504 was very structured, well-presented, interesting, and engaging for people new to the field as well as experienced professionals." -Ewa Konkolska, Prudential Insurance

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
- Penetration testers
- Ethical hackers
- 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

By helping you understand attackers' 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, this course helps you turn the tables on computer attackers. 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, detect, and respond to them. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a hands-on workshop that focuses on scanning 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 is foundational and core strength building in the most critical areas of incident handling. It reinforces and develops understanding around roles and TTPs of both adversary and defender." -Araceli Ari Gomes, Dell Secureworks

Michael Murr *SANS Principal Instructor*

Michael has been a forensic analyst with Code-X Technologies for over five years. He has conducted numerous investigations and computer forensic examinations, and performed specialized research and development. Michael has taught SANS SEC504 (Hacker Techniques, Exploits, and Incident Handling), SANS FOR508 (Computer Forensics, Investigation, and Response), and SANS FOR610 (Reverse-Engineering Malware). He has also led SANS@Home courses; and is a member of the GIAC Advisory Board. Currently, Michael is working on an open-source framework for developing digital forensics applications. Michael 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

FOR508:

Advanced Digital Forensics and Incident Response

SANS

Six-Day Program
Mon, Jun 27 - Sat, Jul 2
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Chad Tilbury

DFIR
digital-forensics.sans.org

GCFA
giac.org

SANS Technology Institute
sans.edu

sans.org/cyber-guardian

sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

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

- How the breach occurred
- How systems were affected and compromised
- What attackers took or changed
- How to contain and mitigate the incident

DAY 0: A 3-letter government agency contacts you to say critical information was stolen through a targeted attack on your organization. They won't tell how they know, but they identify several breached systems within your enterprise. An Advanced Persistent Threat adversary, aka an APT, is likely involved – the most sophisticated threat you are likely to face in your efforts to defend your systems and data.

Who Should Attend

- Incident response team leaders and members
- Security Operations Center personnel and information security practitioners
- Experienced digital forensic analysts
- System administrators
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- SANS FOR408 and SEC504 graduates

Over 80% of all breach victims learn of a compromise from third-party notifications, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years.

"The instructor was beyond qualified and excellent! He took the time to answer questions and help the students, and the exercises flowed very well with the instruction." -Wilfredo Hernandez, FL Dept. of Law Enforcement

Incident response tactics and procedures have evolved rapidly over the past several years. Data breaches and intrusions are growing more complex. Adversaries are no longer compromising one or two systems in your enterprise; they are compromising hundreds. Your team can no longer afford antiquated incident response techniques that fail to properly identify compromised systems, provide ineffective containment of the breach, and ultimately fail to rapidly remediate the incident.

This in-depth incident response course provides responders with advanced skills to hunt down, counter, and recover from a wide range of threats within enterprise networks, including APT adversaries, organized crime syndicates, and hactivism. Constantly updated, FOR508 addresses today's incidents by providing hands-on incident response tactics and techniques that elite responders are successfully using in real-world breach cases.

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

Chad Tilbury *SANS Senior Instructor*

Chad Tilbury has been responding to computer intrusions and conducting forensic investigations since 1998. His extensive law enforcement and international experience stems from working with a broad cross-section of Fortune 500 corporations and government agencies around the world. During his service as a Special Agent with the U.S. Air Force Office of Special Investigations, he investigated and conducted computer forensics for a variety of crimes, including hacking, abduction, espionage, identity theft, and multi-million dollar fraud cases. He has led international forensic teams and was selected to provide computer forensic support to the United Nations Weapons Inspection Team. Chad has worked as a computer security engineer and forensic lead for a major defense contractor and as the Vice President of Worldwide Internet Enforcement for the Motion Picture Association of America. In that role, he managed Internet anti-piracy operations for the seven major Hollywood studios in over 60 countries. Chad is a graduate of the U.S. Air Force Academy and holds a B.S. and M.S. in Computer Science as well as GCFA, GCIH, GREM, and ENCE certifications. He is currently a consultant specializing in incident response, corporate espionage, and computer forensics. @chadtilbury

DEV522:
Defending Web Applications Security Essentials

SANS

Six-Day Program
Mon, Jun 27 - Sat, Jul 2
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor:
Johannes Ullrich, Ph.D.

giac.org

sans.edu

Bundle OnDemand
with this course
sans.org/ondemand

"This training has been very helpful in making me more aware and have a better understanding of vulnerabilities and what can be done to minimize them in future development projects."
-Lerma Winchell, VyStar Credit Union

"SANS has always provided exceptional training using solid coursework to labs, ratios, and formats."
-Darrell Marsh, ATFS, LLC

This is the course to take if you have to defend web applications!

The quantity and importance of data entrusted to web applications is growing, and defenders need to learn how to secure them. Traditional network defenses, such as firewalls, fail to secure web applications. DEV522 covers the OWASP Top 10 Risks and will help you better understand web application vulnerabilities, thus enabling you to properly defend your organization's web assets.

Mitigation strategies from an infrastructure, architecture, and coding perspective will be discussed alongside real-world implementations that really work. The testing aspect of vulnerabilities will also be covered so you can ensure your application is tested for the vulnerabilities discussed in class.

Who Should Attend

- Application developers
- Application security analysts or managers
- Application architects
- Penetration testers who are interested in learning about defensive strategies
- Security professionals who are interested in learning about web application security
- Auditors who need to understand defensive mechanisms in web applications
- Employees of PCI-compliant organizations who need to be trained to comply with payment card industry requirements

To maximize the benefit for a wider range of audiences, the discussions in this course will be programming-language agnostic. Focus will be maintained on security strategies rather than coding-level implementation.

DEV522: Defending Web Applications Security Essentials is intended for anyone tasked with implementing, managing, or protecting web applications. It is particularly well suited for application security analysts, developers, application architects, pen testers, and auditors who are interested in recommending proper mitigations to web security issues and for infrastructure security professionals who have an interest in better defending their web applications.

The course will also cover additional issues the authors have found to be important in their day-to-day web application development practices. The topics that will be covered include:

- Infrastructure security
- Server configuration
- Authentication mechanisms
- Application language configuration
- Application coding errors like SQL Injection and cross-site scripting
- Cross-site request forgery
- Authentication bypass
- Web services and related flaws
- Web 2.0 and its use of web services
- XPATH and XQUERY languages and injection
- Business logic flaws
- Protective HTTP headers

The course will make heavy use of hands-on exercises and will conclude with a large defensive exercise, reinforcing the lessons learned throughout the week.

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. He founded DShield.org in 2000, 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 located in Jacksonville, Florida. His daily podcast summarizes current security news in a concise format. @johullrich

MGT414:

SANS Training Program for CISSP® Certification

SANS

Six-Day Program
Mon, Jun 27 - Sat, Jul 2
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPEs
Laptop NOT Needed
Instructor: David R. Miller

giac.org

sans.org/8140

Bundle OnDemand
WITH THIS COURSE
sans.org/ondemand

"This course has been fantastic in terms of boiling down years of IT security trends and best practices into a week of learning."
-Eric Pavlov, InnoMark

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that has been specifically updated to prepare you to pass the 2015 version of the CISSP® exam.

Course authors Eric Conrad and Seth Misenar have revised MGT414 to take into account the 2015 updates to the CISSP® exam and prepare students to navigate all types of questions included in the new version.

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

Who Should Attend

- Security professionals who want to understand the concepts covered in the CISSP® exam as determined by (ISC)²
- Managers who want to understand the critical areas of network security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® eight domains
- Security professionals and managers looking for practical ways to apply the eight domains of knowledge to their current activities

You Will Be Able To:

- Understand the eight domains of knowledge that are covered on the CISSP® exam
- Analyze questions on the exam and be able to select the correct answer
- Apply the knowledge and testing skills learned in class to pass the CISSP® exam
- Understand and explain all of the concepts covered in the eight domains of knowledge
- Apply the skills learned across the eight domains to solve security problems when you return to work

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

Take advantage of the SANS CISSP® Get Certified Program currently being offered.
sans.org/special/cissp-get-certified-program

David R. Miller *SANS Certified Instructor*

David has been a technical instructor since the early 1980s and has specialized in consulting, auditing, and lecturing on information systems security, legal and regulatory compliance, and network engineering. David has helped many enterprises develop their overall compliance and security program, including through policy writing, network architecture design to include security zones, development of incident response teams and programs, design and implementation of public key infrastructures, security awareness training programs, specific security solution designs like secure remote access and strong authentication architectures, disaster recovery planning and business continuity planning, and pre-audit compliance gap analysis and remediation. He serves as a security lead and forensic investigator on numerous enterprise-wide IT design and implementation projects for Fortune 500 companies, providing compliance, security, technology, and architectural recommendations and guidance. Projects include Microsoft Windows Active Directory enterprise designs, Security Information and Event Management systems, Intrusion Detection and Protection Systems, endpoint protection systems, patch management systems, configuration monitoring systems, and enterprise data encryption for data at rest, in transit, in use, and within email systems. David is an author, lecturer and technical editor of books, curriculum, certification exams, and computer-based training videos.

ICS410:
ICS/SCADA Security Essentials

SANS

Five-Day Program
Mon, Jun 27 - Fri, Jul 1
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Justin Searle

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.

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

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
- A license to Windows 10 and a hardware PLC for students to use in class and take home with them

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 training really opens you up to possibilities and issues that otherwise you wouldn't really think about." -Alfonso Barreiro, Panama Canal Authority

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

GICSP
giac.org

SANS Technology Institute
sans.edu

Bundle OnDemand
with this course
sans.org/ondemand

"Very satisfied with ICS410, and the instructor was very knowledgeable and great at balancing group backgrounds (IT vs. SCADA)."
-Chad Slater,
The Dow Chemical Company

Justin Searle *SANS Certified Instructor*

Justin Searle is a Managing Partner of UtiliSec, specializing in Smart Grid security architecture design and penetration testing. Justin led the Smart Grid Security Architecture group in the creation of NIST Interagency Report 7628 and played key roles in the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG). He currently leads the testing group at National Electric Sector Cybersecurity Organization Resources (NESCOR). Justin has taught courses in hacking techniques, forensics, networking, and intrusion detection for multiple universities, corporations, and security conferences. In addition to electric power industry conferences, Justin frequently presents at top international security conferences such as Black Hat, DEFCON, OWASP, Nullcon, and AusCERT. He co-leads prominent open-source projects including the Samurai Web Testing Framework (SamuraiWTF), the Samurai Security Testing Framework for Utilities (SamuraiSTFU), Middler, Yokoso!, and Laudanum. Justin has an MBA in International Technology and is a CISSP and SANS GIAC certified Incident Handler (GCIH), Intrusion Analyst (GCIA), and Web Application Penetration Tester (GWAPT). @meeas

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:

Tales from the Battlefield: Lessons in Incident Response – *Chad Tilbury*

As more organizations face off against advanced adversaries, classic incident response processes are being adapted and updated to address new threats and speed up the recovery process. "Tales from the Battlefield" will illustrate multiple real-world case studies demonstrating some exciting new approaches to incident response. Learn how incident response teams are detecting, responding, and attributing attacks from targeted attackers and get a taste for the future of incident response.

The Internet of Evil Things – *Dr. Johannes Ullrich*

Embedded systems are the new target. As our networks grow, uncontrolled and unsupervised, forgotten machines will take over and rule us all soon. Analyzing the embedded malware that comes with this presents a number of challenges. Current debuggers and virtualization techniques that mimic these systems are incomplete and will not allow us to completely analyze malware the way we are used to in good-old desktop malware environments. These malware blackboxes need different instrumentations and techniques. We will present some ideas on how to analyze these malware samples, and introduce you to embedded system analysis (unless your bot is removing this event from your smart watch's reminder list!).

The CISSP® Exam was Implemented on April 15, 2015 – *David Miller*

Are you interested in CISSP® certification? How might it improve your career? Or your résumé? In getting a new job? On your business card? In maintaining your career and moving you up the ladder. In developing your skill set? How about helping with that pay raise? This talk will look at how management views this much sought-after certification. Have you been studying for it? Do you plan to take the exam soon? On January 15, 2015, the ISC^2, the certifying body for the CISSP® certification exam, released a new set of exam objectives for the exam. These changes were implemented on the CISSP® certification exam beginning April 15, 2015. This new set of exam objectives is a major change from the previous version of the exam. ISC^2 has moved and merged content to form eight Domains of the Common Body of Knowledge, down from 10 Domains in the previous exam. They have also added numerous new topics to the objectives. You will need to know about the new material you will be tested on. This talk will examine the new shape and the new topics of the 2015 CISSP® certification exam.

Continuous Ownage: Why You Need Continuous Monitoring – *Bryan Simon*

Repeat after me: I will be breached. Most organizations realize this fact too late, usually after a third party informs them months after the initial compromise. Treating security monitoring as a quarterly auditing process means most compromises will go undetected for weeks or months. The attacks are continuous, and the monitoring must match. This talk will help you face this problem and explain how to move your organization to a more defensible security architecture that enables continuous security monitoring. The talk will also give you a hint at the value you and your organization will gain from attending the new course designed by Seth Misenar and Eric Conrad: SANS SEC511: Continuous Monitoring and Security Operations.

Build Your Best Career

WITH

SANS

Add an

OnDemand Bundle & GIAC Certification Attempt*

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

SPECIAL PRICING

OnDemand Bundle

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

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

-Robert Jones, Team Jones, Inc.

GIAC Certification

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

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

-Christina Ford, Department of Commerce

MORE INFORMATION

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

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

Employers need good talent. Veterans need good jobs. SANS VetSuccess Immersion Academy delivers both.

Introducing the SANS VetSuccess Immersion Academy, an intensive, accelerated program that provides the real-world training and certifications needed to fill critical jobs in cybersecurity.

For employers, the academy is a faster, more reliable, and less expensive way to find, train, certify, and employ highly qualified cybersecurity talent.

For transitioning veterans, the academy provides free accelerated training and certifications to quickly and effectively launch careers in cybersecurity.

Find out how your organization can benefit from hiring graduates or launching an academy to meet your specific talent needs.

Read the Pilot Program Results Report
Visit sans.org/vetsuccess

SANS | CyberTalent IMMERSION ACADEMY

Read the Pilot Program Results Report
Visit sans.org/vetsuccess

Women's Academy Pilot
1st cohort graduation
Spring 2016

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events 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 sans.org/community
Live Training in Your Local Region with Smaller Class Sizes

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

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

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

ONLINE TRAINING

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

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

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

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

FUTURE SANS TRAINING EVENTS

Threat Hunting and Incident Response
SUMMIT & TRAINING 2016
New Orleans, LA | Apr 12-19

Pen Test Austin 2016
Austin, TX | Apr 18-23

Security West 2016
San Diego, CA | Apr 29 - May 6

Baltimore Spring 2016
Baltimore, MD | May 9-14

Houston 2016
Houston, TX | May 9-14

Security Operations Center
SUMMIT & TRAINING 2016
Crystal City, VA | May 19-26

SANSFIRE 2016
Washington, DC | Jun 11-18

Digital Forensics & Incident Response
SUMMIT & TRAINING 2016
Austin, TX | Jun 23-30

Rocky Mountain 2016
Denver, CO | Jul 11-16

Minneapolis 2016
Minneapolis, MN | Jul 18-23

San Antonio 2016
San Antonio, TX | Jul 18-23

ICS Security & Training – Houston 2016
Houston, TX | Jul 25-30

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

SANS SALT LAKE CITY 2016

Hotel Information

Training Campus

Sheraton Salt Lake City Hotel

150 West 500 South
Salt Lake City, UT 84101
801-401-2000
sans.org/event/salt-lake-city-2016/location

Sheraton Salt Lake City Hotel is perfectly located in the heart of the downtown business and entertainment district and three blocks from the Salt Palace Convention Center. Whether you want to visit Temple Square, cheer on your favorite team or shop at City Creek Mall, you'll find them all within walking distance of this downtown hotel or via the complimentary downtown TRAX.

Special Hotel Rates Available

A special discounted rate of $109.00 S/D will be honored based on space availability.
Should the prevailing government per diem rate fall below the SANS group rate, government per diem rooms will be made 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 5:00pm MST on June 3, 2016.

Top 5 reasons to stay at the Sheraton Salt Lake City 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 Sheraton Salt Lake City 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 Sheraton Salt Lake City Hotel that you won't want to miss!
5. Everything is in one convenient location!

SANS SALT LAKE CITY 2016

Registration Information

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

Register online at sans.org/salt-lake-city-2016/courses

Select your course or courses and indicate whether you plan to test for GIAC certification.

If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

Use code **EarlyBird16** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**5-4-16**	**$400.00**	**5-25-16**	**$200.00**

Some restrictions apply.

Group Savings (Applies to tuition only)

10% discount if 10 or more people from the same organization register at the same time
5% discount if 5-9 people from the same organization register at the same time

To obtain a group discount, complete the discount code request form at sans.org/security-training/discounts prior to registering.

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 June 8, 2016 – processing fees may apply.

SANS Voucher Credit Program

Expand your training budget! Extend your Fiscal Year. The SANS Voucher Discount Program pays you credits and delivers flexibility.
sans.org/vouchers

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

WEBCASTS

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

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

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

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

NEWSLETTERS

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

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

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

OTHER FREE RESOURCES

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

sans.org/security-resources