SANS

network security 2014

PROGRAM GUIDE

Caesars Palace | Las Vegas, NV

October 19-27, 2014

@SANSInstitute | #SANSNetworkSecurity

TABLE OF CONTENTS

NETWARS
TOURNAMENTS

All students who register for a 5- or 6-day course will be eligible to play NetWars for FREE.

Register Now!
sans.org/event/network-security-2014/schedule

DFIR NETWARS TOURNAMENT

Hosted by Rob Lee
Thursday, October 23 and Friday, October 24
6:30pm-9:30pm | Roman IV

CORE NETWARS TOURNAMENT

Hosted by Ed Skoudis
Thursday, October 23 and Friday, October 24
6:30pm-9:30pm | Roman I and II

GENERAL INFORMATION

Registration and Courseware Pick-up Information

Location: Promenade Foyer

Sunday, October 19 (Short Courses Only) 8:00am-9:00am
Sunday, October 19 (Welcome Reception) 5:00pm-7:00pm
Monday, October 20 . . . . . 7:00am-5:30pm
Tuesday, October 21 - Saturday, October 25 . . . . . 8:00am-5:30pm
Sunday, October 26 . . . . . 8:00am-9:00am (Closes)

Internet Café *(WIRED & WIRELESS)*

Location: Promenade Foyer
Printer will be available for students' use

Monday, October 20 . . . . . Opens at noon - 24 hours
Tuesday, October 21 - Friday, October 24 . . . . . Open 24 hours
Saturday, October 25. . . . . Closes at 2:00pm

Course Times

All full-day courses will run 9:00am-5:00pm (unless noted)

Course Breaks

7:00am - 9:30am – Morning Coffee
10:30am-10:50am – Morning Break
12:15pm-1:30pm – Lunch (On your own)
3:00pm-3:20pm – Afternoon Break

First Time at SANS?

Please attend our ***Welcome to SANS*** briefing designed to help newcomers get the most from your SANS training experience. The talk is from **8:15am-8:45am** on **Monday, October 20** at the General Session in **Roman III**

GENERAL INFORMATION

Dining Options

We have assembled a short list of dining suggestions you may like to try during lunch breaks. See page 26 of this booklet.

Feedback Forms and Course Evaluations

The SANS planning committee wants to know what we should keep doing and what we need to improve – but we need your help! Please take a moment to fill out an evaluation form after each course and drop it in the evaluation box.

Social Board and Twitter

You can post open invites to lunch, dinner or other outings. Located on the Bulletin Board near the Registration Desk. Join the conversation on Twitter and use the hashtag #SANSNetworkSecurity for up-to-date information from fellow attendees!

Wear Your Badge Daily

To make sure you are in the right place, the SANS door monitors will be checking your badge for each course you enter. For your convenience, please wear your badge at all times.

Lead a BoF! (Birds of a Feather Session)

Whether you are an expert or just interested in keeping the conversation going, sign up and suggest topics at the BoF board near registration. If you have questions, leave a message with your contact information with someone at the registration desk in the Promenade Foyer.

Bootcamp Sessions and Extended Hours

The following classes have evening bootcamp sessions or extended hours. For specific times, please refer to pages 4-6.

Bootcamps (Attendance Mandatory)

MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam
SEC401: Security Essentials Bootcamp Style
SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking
SEC760: Advanced Exploit Development for Penetration Testers

Extended Hours:

MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™
SEC504: Hacker Tools, Techniques, Exploits and Incident Handling
SEC560: Network Penetration Testing and Ethical Hacking

COURSE SCHEDULE

START DATE: **Sunday, October 19**

Time: 9:00am-5:00pm (Unless otherwise noted)

MGT305: Technical Communication and Presentation Skills for Security Professionals
Instructor: David Hoelzer . . . . . Location: Pompeian I

MGT415: A Practical Introduction to Risk Assessment
Instructor: James Tarala. . . . . Location: Pompeian II

START DATE: **Monday, October 20**

Time: 9:00am-5:00pm (Unless otherwise noted)

SEC301: Intro to Information Security
Instructors: Fred Kerby, Keith Palmgren . . Location: Octavius 17/18

SEC401: Security Essentials Bootcamp Style
Instructor: Bryce Galbraith . . . . . .Location: Neopolitan I
Bootcamp Hours: 5:00pm-7:00pm (Course days 1-5)

SEC501: Advanced Security Essentials – Enterprise Defender
Instructor: Paul A. Henry . . . . . Location: Neopolitan II

SEC502: Perimeter Protection In-Depth
Instructor: Tanya Baccam . . . . . .Location: Neopolitan III

SEC503: Intrusion Detection In-Depth
Instructor: Mike Poor. . . . . Location: Milano VI

SEC504: Hacker Tools, Techniques, Exploits & Incident Handling
Instructor: John Strand. . . . . .Location: Milano VII/VIII
Extended Hours: 5:00pm-6:30pm (Course Day 1 only)

SEC505: Securing Windows with the Critical Security Controls
Instructor: Jason Fossen. . . . . .Location: Octavius 1/2

SEC506: Securing Linux/Unix
Instructor: Hal Pomeranz. . . . . Location: Octavius 3

SEC511: Continuous Monitoring and Security Operations
Instructor: Eric Conrad . . . . . Location: Octavius 14/15/16

SEC542: Web App Penetration Testing & Ethical Hacking
Instructor: Seth Misenar . . . . . Location: Octavius 5

SEC560: Network Penetration Testing and Ethical Hacking
Instructor: Ed Skoudis . . . . . Location: Roman II
Extended Hours: 5:00pm-6:30pm (Course Day 1 only)

SEC561: Intense Hands-on Pen Testing Skill Development (with SANS NetWars)
Instructor: Tim Medin . . . . . .Location: Pompeian IV

COURSE SCHEDULE

SEC566: Implementing and Auditing the Critical Security Controls – In-Depth
Instructor: James Tarala . . . . . .Location: Octavius 7/8

SEC573: Python for Penetration Testers
Instructor: Mark Baggett . . . . . .Location: Pompeian III

SEC575: Mobile Device Security and Ethical Hacking
Instructor: Christopher Crowley . . . . . Location: Neopolitan IV

SEC579: Virtualization and Private Cloud Security
Instructor: Dave Shackleford . . . . . .Location: Pompeian I

SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses
Instructor: Larry Pesce . . . . . Location: Octavius 6

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
Instructor: James Lyne . . . . . .Location: Salerno
Bootcamp Hours: 5:15pm-7:00pm (Course days 1-5)

SEC760: Advanced Exploit Development for Penetration Testers
Instructor: Stephen Sims . . . . . Location: Messina
Bootcamp Hours: 5:15pm-7:00pm (Course days 1-5)

DEV522: Defending Web Applications Security Essentials
Instructor: Johannes Ullrich, Ph.D. . . . . Location: Octavius 9

DEV541: Secure Coding in Java/JEE: Developing Defensible Apps
Instructor: Gregory Leonard . . . . . Location: Sorrento

DEV544: Secure Coding in .NET: Developing Defensible Apps
Instructor: Eric Johnson . . . . . Location: Octavius 10

FOR408: Windows Forensic Analysis
Instructor: Chad Tilbury . . . . . .Location: Roman IV

FOR508: Advanced Computer Forensic Analysis and Incident Response
Instructor: Rob Lee . . . . . .Location: Florentine II/III

FOR526: Memory Forensics In-Depth
Instructor: Alissa Torres. . . . . Location: Octavius 12

FOR572: Advanced Network Forensics and Analysis
Instructor: Philip Hagen. . . . . .Location: Milano V

FOR585: Advanced Smartphone Forensics
Instructor: Heather Mahalik . . . . . Location: Capri

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Instructor: Lenny Zeltser . . . . . Location: Octavius 11

COURSE SCHEDULE

START DATE: **Monday, October 20** (CONTINUED)
Time: 9:00am-5:00pm (Unless otherwise noted)

MGT414: SANS® +S™ Training Program for the CISSP® Cert Exam
Instructor: Dr. Eric Cole . . . . . Location: Milano II
Bootcamp Hours: 8:00am – 9:00am (Course days 2-6) & 5:00pm-7:00pm (Course days 1-5)

MGT512: SANS Security Leadership Essentials for Managers with Knowledge Compression™
Instructor: G. Mark Hardy . . . . . Location: Milano III
Extended Hours: 5:00pm – 6:00pm (Course days 1-4)

MGT514: IT Security, Strategic Planning, and Leadership
Instructors: Stephen Northcutt, Frank Kim . . . Location: Milano I

MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep
Instructor: Jeff Frisk . . . . . Location: Milano IV

AUD507: Auditing & Monitoring Networks, Perimeters & Systems
Instructor: David Hoelzer . . . . . Location: Octavius 13

LEG523: Law of Data Security and Investigations
Instructor: Benjamin Wright . . . . . Location: Pompeian II

ICS410: ICS/SCADA Security Essentials
Instructor: Justin Searle. . . . . Location: Florentine IV

HOSTED: (ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program
Instructor: Mano Paul . . . . . Location: Anzio

START DATE: **Sunday, October 26**
Time: 9:00am-5:00pm (Unless otherwise noted)

SEC440: Critical Security Controls: Planning, Implementing, and Auditing
Instructor: James Tarala . . . . . .Location: Octavius 1/2

SEC546: IPv6 Essentials
Instructor: Johannes Ullrich, Ph.D.. . . . . Location: Octavius 3

SEC580: Metasploit Kung Fu for Enterprise Pen Testing
Instructor: Eric Conrad . . . . . Location: Octavius 5

MGT433: Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program
Instructor: Lance Spitzner . . . . . .Location: Octavius 7/8

HOSTED: Embedded Device Security Assessments For The Rest Of Us
Instructor: Paul Asadoorian . . . . . Location: Octavius 9

HOSTED: Offensive Countermeasures: The Art of Active Defenses
Instructors: Mick Douglas, John Strand. . . . Location: Octavius 10

HOSTED: Physical Penetration Testing - Introduction
Instructor: Deviant Ollam. . . . . Location: Octavius 6

SPECIAL EVENTS

Enrich your SANS experience!

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

SUNDAY, OCTOBER 19

Registration Welcome Reception

Sunday, October 19 | 5:00pm-7:00pm | Location: Promenade Foyer

Register early and network with your fellow students!

Women in Technology Meet and Greet

Sunday, October 19 | 7:00pm - 8:00pm | Location: Genoa

SANS is proud to host the Women in Technology Meet and Greet! From Jean Jennings Bartik to Diane Greene, women have always been a driving force in the field of information technology. Their experiences have been filled not only with stories of overcoming challenges but also ones of innovation and inspiration. Join us to hear some of these stories, come share your own and network with other conference attendees.

MONDAY, OCTOBER 20

General Session - Welcome to SANS

Speaker: Dr. Eric Cole

Monday, October 20 | 8:15am-8:45am | Location: Roman III

Breaking and Fixing Critical Infrastructure

Speaker: Justin Searle, Managing Partner, UtiliSec

Monday, October 20 | 12:30pm-1:15pm | Location: Roman III

New ICS technologies bring greater benefits for both providers and consumers of critical infrastructure, however often these benefits come at a cost from a security perspective. Unlike the over-hyped messages we usually hear from the media, the sky is NOT falling. However, just like any other technology, the systems and devices that make up the world's critical infrastructures will have weaknesses and vulnerabilities. It is important for us to understand these vulnerabilities, how they can be attacked, and what we need to do to defend against those attacks. This presentation will explore a testing methodology that owner/operators and vendors can use to perform penetration testing on their equipment to identify and remediate vulnerabilities before they are exploited by the bad guys.

SPECIAL EVENTS

SANS Technology Institute Open House

Speaker: Bill Lockhart

Monday, October 20 | 6:00pm-7:00pm | Location: Florentine I

SANS Technology Institute Master of Science degree programs offer candidates an unparalleled opportunity to excel in the two aspects of security that are most important to the success of their employer and their own careers: management skills and technical mastery.

Over the next 20 years, information technology will become so central to all aspects of our lives, from recreation to warfare, that information security will rise in importance and scale. It will become a profession with more than 500,000, and perhaps as many as 1,000,000, people employed in positions in which they have significant roles in shaping the security of their employers' systems. Those people need managers, technical directors, and chief information security officers who are deeply skilled in the technology and who have excellent management skills.

If you aspire to help lead your organization's or your country's information security program and you have the qualifications, organizational backing, and personal drive to excel in these challenging degree programs, we will welcome you into the program.

KEYNOTE

APT: It is Time to Act

Speaker: Dr. Eric Cole

Monday, October 20 | 7:15pm-9:15pm | Location: Roman III

Albert Einstein said "We cannot solve our problems with the same thinking we used when we created them." With the new advanced and emerging threat vectors that are breaking into networks with relative ease, a new approach to security is required. The myth that these attacks are so stealthy they cannot be stopped is just not true. There is no such thing as an unstoppable adversary. It is time to act.

In this engaging talk one of the experts on APT, Dr. Cole, will outline an action plan for building a defensible network that focuses on the key motto that "Prevention is Ideal but Detection is a Must". Better understand what the APT really is and what organizations can do to be better prepared. The threat is not going away, so the more organizations can realign their thinking with solutions that actually work, the safer the world will become.

SPECIAL EVENTS

TUESDAY, OCTOBER 21

SANS@NIGHT

Malware Analysis Essentials Using REMnux

Speaker: Lenny Zeltser

Tuesday, October 21 | 7:15pm-8:15pm | Location: Roman I

Though some tasks for analyzing Windows malware are best performed on Windows laboratory systems, there is a lot you can do on Linux with the help of free and powerful tools. REMnux is an Ubuntu distribution that incorporates many such utilities. This practical session presents some of the most useful REMnux tools. Lenny Zeltser, who teaches SANS' reverse-engineering malware course, will share how you can use the utilities installed on REMnux to:

- Assess suspicious Windows executable files
- Explore infection artifacts in a network capture file
- Examine malicious document and media files

If you haven't experimented with Linux-based tools for malware analysis, you've been missing out. And if you've been meaning to begin exploring the field of malware analysis, this talk will help you get started.

SANS@NIGHT

An Introduction to PowerShell for Security Assessments

Speaker: James Tarala

Tuesday, October 21 | 7:15pm-8:15pm | Location: Roman III

With the increased need for automation in operating systems, every platform now provides a native environment for automating repetitive tasks via scripts. Since 2007, Microsoft has gone "all in" with their PowerShell scripting environment, providing access to every facet of the Microsoft Windows operating system and services via a scriptable interface. Administrators can completely administer and audit not only an operating system from this shell, but most all Microsoft services, such as Exchange, SQL Server, and SharePoint services as well. In this presentation James Tarala of Enclave Security will introduce students to using PowerShell scripts for assessing the security of these Microsoft services. Auditors, system administrators, penetration testers, and others will all learn practical techniques for using PowerShell to assess and secure these vital Windows services.

SPECIAL EVENTS

SANS@NIGHT

The 13 Absolute Truths of Security

Speaker: Keith Palmgren

Tuesday, October 21 | 7:15pm-8:15pm | Location: Florentine II/III

Keith Palmgren has identified thirteen "Absolute Truths" of security - things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these thirteen 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 thirteen absolute truths in turn, examine what they mean to the security manager, what they mean to the security posture, and how understanding them will lead to a successful security program.

SANS@NIGHT

The Great Browser Schism: How to Analyze IE10 & IE11

Speaker: Chad Tilbury

Tuesday, October 21 | 8:15pm-9:15pm | Location: Roman I

Changes to Internet Explorer have been slowly occurring since Windows 7, but the introduction of IE10 with Windows 8 and IE11 with Windows 8.1 has been nothing short of cataclysmic. Take everything you knew about Internet Explorer and file it away, because it won't help you now. This talk will cover Internet Explorer 10 & 11 artifact by artifact, giving you the tools and techniques necessary to do a full analysis. Learn to parse the ESE database, where your Index.dat files went, and why device synchronization will make browser forensics more important than ever.

SANS@NIGHT

Evolving Threats

Speaker: Paul A. Henry

Tuesday, October 21 | 8:15pm-9:15pm | Location: Roman III

For nearly two decades defenders have fallen into the "Crowd Mentality Trap" and 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 upon 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 $157 billion (USD) in data breach costs in only the past 6 years.

SPECIAL EVENTS

WEDNESDAY, OCTOBER 22

Vendor Solutions Expo

Wednesday, October 22 | 12:00pm-1:30pm | 5:30pm-7:30pm
Location: Octavius 25

All attendees are invited to meet with established and emerging solution providers as they reveal the latest tools and technologies critical to information security. The SANS Vendor Expo showcases product offerings from key technology providers in the commercial tools and services market. Vendors arrive prepared to interact with a technically savvy audience. You'll find demonstrations and product showcases that feature all the best that the security industry has to offer!

SANS@NIGHT

How Not to Suck at Pentesting

Speaker: John Strand
Wednesday, October 22 | 7:15pm-8:15pm | Location: Roman I

In this presentation, John will cover some key components that many penetration tests lack, including why it is important to get caught, why it is important to learn from real attackers and how to gain access to organizations without sending a single exploit. Additionally, John will show you how to bypass "all powerful" white listing applications that are often touted as an impenetrable defense. Bit9? Palo Alto? Yea, we will talk about bypassing those too.

SANS@NIGHT

Weaponizing Digital Currency

Speaker: G. Mark Hardy
Wednesday, October 22 | 7:15pm-8:15pm | Location: Roman III

Satoshi Nakamoto wasn't stupid. In the early days, he (they) mined over 1,000,000 Bitcoins when nobody really cared. If Bitcoin continues to increase in value at the rate it did last year, someone will be holding a massive currency weapon. George Soros destabilized the British Pound in 1992 and made over £1,000,000,000 profit. In the largest counterfeiting operation in history, Nazi Germany devised Operation Bernhard to destabilize the British economy by dropping millions of pounds from Luftwaffe aircraft. If the holder of the megabitcoin has a currency digital weapon that works frictionlessly in milliseconds, against whom will he target it? Can it destabilize an entire government? Can it be continuously reused for blackmail? What should governments be doing now to plan for this contingency and fight back? We'll discuss an entirely new class of information weapon – digital cryptocurrency – and how it might either change the course of history, or be relegated to the ash heap of failure.

SPECIAL EVENTS

SANS@NIGHT

Debunking the Complex Password Myth

Speaker: Keith Palmgren
Wednesday, October 22 | 7:15pm-8:15pm | Location: Florentine II/III

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

SANS@NIGHT

SANS 8 Mobile Device Security Steps

Speaker: Chris Crowley
Wednesday, October 22 | 8:15pm-9:15pm | Location: Roman I

Every organization is challenged to rapidly deploy mobile device security. The SANS 8 Mobile Device Security Steps is a community-driven project to provide the most up-to-date information on the most effective strategies for securing mobile infrastructure. Chris Crowley will discuss the guidance provided in the 8 Steps, including: user authentication and restricting unauthorized access, OS and application management, device monitoring, and key operational components for mobile device management.

SANS@NIGHT

Know Thyself: Brian Krebs is a Nice Guy But You Don't Want Him Writing About You

Speaker: Ryan Johnson
Wednesday, October 22 | 8:15pm-9:15pm | Location: Roman III

We are often asked to come into an organization and answer the question, "Are we owned?" Many times when we try to answer that question, we're faced with the ultimate security and forensics dilemma – they don't have any data to help you answer the question. No firewall logs. No full packet capture. No idea what should be on their endpoint systems. No idea what should be transitting their network. Nothing. In this talk, Ryan will talk about a method that he uses to help answer that question. Ryan will describe how you can look across the entire organization and get a snapshot assessment of the compromise status of the enterprise using all your lethal forensicator knowledge, progressively narrowing down the massive dataset to something more manageable.

SPECIAL EVENTS

THURSDAY, OCTOBER 23

DFIR NetWars Tournament

Host: Rob Lee

Thu, Oct 23 & Fri, Oct 24 | 6:30pm-9:30pm | Location: Roman IV

SANS DFIR NetWars Tournament is an incident simulator packed with a vast amount of forensic and incident response challenges covering host forensics, network forensics, and malware and memory analysis. It is developed by incident responders and analysts who use these skills daily to stop data breaches and solve crimes. Sharpen your team's skills prior to being involved in a real incident.

CORE NetWars Tournament

Hosts Ed Skoudis

Thu, Oct 23 & Fri, Oct 24 | 6:30pm-9:30pm | Location: Roman I/II

Core NetWars is a computer and network security challenge designed to test a participant's experience and skills in a safe, controlled environment while having a little fun with your fellow IT security professionals. Many enterprises, government agencies, and military bases are using NetWars OnSites to help identify skilled personnel and as part of extensive hands-on training. With Core NetWars, you'll build a wide variety of skills while having a great time.

SANS@NIGHT

Compli-promised: Balancing with Risk Mgt

Speaker: My-Ngoc Nguyen

Thursday, October 23 | 7:15pm-8:15pm | Location: Florentine IV

Many of the organizations recently breached were said to be compliant to their respective regulatory requirements (e.g PCI, FISMA, SOX, HIPAA, etc.). Because it has been mistakenly implied that compliant means secure, compliance bodies just increase the requirements and repercussions for noncompliance. In a knee jerk reaction, organizations focus on compliance at the expense of real security. It then becomes a numbers game and organizations compromise (pun intended) quality of security controls for checking the box on the audit list. The number of controls (ranging from 105 to 612 depending on the mandate) is daunting and so organizations end up becoming less secure. As Alan Paller (SANS) quoted, "If you have everything to do, you do nothing." The compromise to just comply leads to the compromise of the organization.

Don't be like those firms and compromise. Become securer by addressing the controls of your highest risk and most prioritized risk and as a by-product, compliant. This talk will provide an overview of security trends and breaches, the threat landscape, commonalities in the vulnerabilities of the compromised organizations, and relate it all to a risk perspective.

SPECIAL EVENTS

SANS@NIGHT

Windows Exploratory Surgery with Process Hacker

Speaker: Jason Fossen

Thursday, October 23 | 7:15pm-8:45pm | Location: Florentine II/III

In this talk we'll rummage around inside the guts of Windows while on the lookout for malware, using a free tool named Process Hacker (similar to Process Explorer). Understanding processes, threads, drivers, handles, and other OS internals is important for analyzing malware, doing forensics, troubleshooting, and hardening the OS. If you have a laptop, get Process Hacker from SourceForge.net and together we'll take a peek under the GUI to learn about Windows internals and how to use Process Hacker for combating malware. http://processhacker.sourceforge.net

SANS@NIGHT

The Law of Offensive Countermeasures, Active Defense or Whatever You Wanna Call It

Speaker: Benjamin Wright

Thursday, October 23 | 7:15pm-8:15pm | Location: Roman III

The range of steps that a good guy might take relative to a bad guy is limited only by imagination. As our imagination invents new steps, we use metaphors like 'honeypot,' 'sinkhole' and 'hacking back' to describe what's going on. But when we try to fit these metaphors into law, confusion erupts. This presentation will only compound the confusion. Come join the raucous discussion.

GIAC Program Overview

Speaker: Jeff Frisk

Thursday, October 23 | 8:15pm-8:45pm | Location: Florentine IV

GIAC is the leading provider and developer of Information Security Certifications. GIAC tests and validates the ability of practitioners in information security, forensics, and software security. GIAC certification holders are recognized as experts in the IT industry and are sought after globally by government, military, and industry to protect the cyber environment.

SANS@NIGHT

Sushi-grade Smartphone Forensics on a Ramen Noodle Budget

Speaker: Heather Mahalik

Thursday, October 23 | 8:15pm-9:15pm | Location: Pompeian III

One of the biggest questions we get in FOR585 is "What can I do with open source tools because my lab can't afford to buy all of this equipment?" This talk will answer those questions specific to Android forensics. Acquisition, analysis, and memory capture are possible using open source methods and tools. Is data missed if the examiner relies on open source tools for Android forensics? A comparison of what is recovered from an Android using open source and popular commercial tools will be discussed.

SPECIAL EVENTS

SANS@NIGHT

Logs, Logs, Every Where – Nor Any Byte to Grok

Speaker: Phil Hagen

Thursday, October 23 | 8:15pm-9:15pm | Location: Roman III

In the practice of Network Forensics, we frequently lack the ultimate evidence – a full packet capture. Instead, we must seek other Artifacts of Communication, which provide insight to system communications that have long since concluded. These artifacts often come from log events created along the path of communication – switches, routers, firewalls, intrusion detection systems, proxy servers, and a myriad of other devices.

The skilled network forensicator will aggregate these different sources, then apply sound analytic processes to the consolidated evidence. Only then can we build a comprehensive understanding of those network communication events and establish the best possible sequence of events around the incident in question.

In this talk, we will discuss one tool that can be very effective in practice: Logstash. This is a free and open-source solution primarily intended for system and network administrators to observe live data. However, it can also provide great value to the forensicator, who must integrate disparate data sources and formats. New developments around Logstash also make it an ideal tool for the system-based forensicator as well, since supertimeline data can be integrated to the broader view of evidence.

FRIDAY, OCTOBER 24

SANS@NIGHT

The Bot Inside the Machine

Speaker: Johannes Ullrich, Ph.D.

Friday, October 24 | 7:15pm-8:15pm | Location: Florentine II/III

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).

SPECIAL EVENTS

SANS@NIGHT

Security Awareness Metrics: Measuring Human Behavior

Speaker: Lance Spitzner

Friday, October 24 | 7:15pm-8:15pm | Location: Roman III

Security awareness is nothing more than another control designed to reduce risk, specifically human risk. This session will discuss the different ways organizations are effectively measuring human risk, which methods are proving to be the most successful, and steps you can take to have successful metrics for your awareness program.

SANS@NIGHT

Securing The Kids

Speaker: Lance Spitzner

Friday, October 24 | 8:15pm-9:15pm | Location: Roman III

Technology is an amazing tool. It allows our kids to access a tremendous amount of information, meet new people, and communicate with friends around the world. In addition, for them to be successful in the 21st century they have to know and understand how to leverage these new tools. However, with all these capabilities come a variety of new risks, risks that as parents you may not understand or even be aware of. In this one-hour presentation we cover the top three risks to kids online and the top five steps you can take to protect them. This course is based on the experiences and lessons learned from a variety of SANS top instructors who not only specialize in security, but are parents just like you. This talk is sponsored and delivered by SANS Securing The Human program.

SANS@NIGHT

Into the DOM: Hacking Web 2.0

Speaker: Doug Logan

Friday, October 24 | 8:15pm-9:15pm | Location: Florentine II/III

Today's websites increasingly rely on JavaScript to implement core functionality. This often opens up the possibility for unique and creative application specific vulnerabilities, IF you can find the right place to hook into the code. Within this presentation we'll discuss how to use Firebug and other tools to find and break into the functions you're interested in. This will include a brief description on the various event handling options available in JavaScript, and a detailed look at a few of the ways Firebug, and a few other tools make it easier to intercept these events.

VENDOR EVENTS

Vendor Solutions Expo

Wednesday, October 22 | 12:00pm-1:30pm | 5:30pm-7:30pm
Location: Octavius 25

All attendees are invited to meet with established and emerging solution providers as they reveal the latest tools and technologies critical to information security. The SANS Vendor Expo showcases product offerings from key technology providers in the commercial tools and services market. Vendors arrive prepared to interact with a technically savvy audience. You'll find demonstrations and product showcases that feature all the best that the security industry has to offer!

Vendor Welcome Reception: PRIZE GIVEAWAYS!!! – Passport to Prizes

Wednesday, October 22 | 5:30pm-7:30pm | Location: Octavius 25

This informal reception allows you to visit exhibits and participate in some exciting activities. This is a great time to mingle with your peers and experience firsthand the latest in information security tools and solutions with interactive demonstrations and showcase discussions. Enjoy appetizers and beverages and compare experiences with other attendees regarding the solutions they are using to address security threats in their organization. Attendees will receive a Passport to Prizes entry form. Visit each sponsor to receive a stamp, and then enter to win exciting prizes.

Vendor-Sponsored Lunch Session

Wednesday, October 22 | 12:00pm-1:30pm | Location: Octavius 25

Sign-up at SANS Registration to receive a ticket for a free lunch brought to you by sponsoring vendors. Please note, by accepting a lunch ticket your badge will be scanned and your information shared with the sponsoring vendors. Join these sponsoring vendors and others on the expo floor for an introduction to leading solutions and services that showcase the leading options in information security. Take time to browse the show floor and get introduced to providers and their solutions that align with the security challenges being discussed in class.

Luncheon sponsors are:

BeyondTrust
Certes Networks
Click Security
Codenomicon
Corero
CyberSponse
EiQnetworks
FireEye
ForeScout Technologies
General Dynamics Fidelis Cybersecurity
iBoss
LogRhythm
Narus, Inc.
Palo Alto
PhishMe
Pwnie Express
Qualys
Rapid7 Inc.
Sourcefire, now a part of Cisco
Spikes Security

VENDOR EVENTS

Vendor-Sponsored Lunch & Learns

Since SANS course material is product neutral, these presentations provide the opportunity to evaluate vendor tools in an interactive environment to increase your effectiveness, productivity, and knowledge gained from the conference. These sessions feature a light meal or refreshments provided by the sponsor. Sign-Up Sheets for the events below are located on the Community Bulletin Board at Student Registration.

Breaking and Fixing Critical Infrastructure

Speaker: Justin Searle, Managing Partner, UtiliSec
Monday, October 20 | 12:30pm-1:15pm | Location: Roman III

New ICS technologies bring greater benefits for both providers and consumers of critical infrastructure, however often these benefits come at a cost from a security perspective. Unlike the over-hyped messages we usually hear from the media, the sky is NOT falling. However, just like any other technology, the systems and devices that make up the world's critical infrastructures will have weaknesses and vulnerabilities. It is important for us to understand these vulnerabilities, how they can be attacked, and what we need to do to defend against those attacks. This presentation will explore a testing methodology that owner/operators and vendors can use to perform penetration testing on their equipment to identify and remediate vulnerabilities before they are exploited by the bad guys.

Beyond the Breach - A Look Into the Latest Threat Trends

Speaker: Marshall Heilman, Managing Director – Mandiant, a FireEye Company
Tuesday, October 21 | 12:30pm-1:15pm | Location: Pompeian II

This session will review FireEye Labs' findings and analysis on the diverse threat group activity we've been tracking over the last year, and what it means for organizations. We will review shifts in the threat landscape, threat groups' techniques, and the activity's impact. We will also cover what these trends mean for organizations, and how they can prepare accordingly.

VENDOR EVENTS

Continuous Security Intelligence with the SANS Critical Security Controls

Speaker: Vijay Basani, President/CEO, EiQ Networks
Tuesday, October 21 | 12:30pm-1:15pm | Location: Pompeian IV

Organizations of all sizes, and across almost every industry, face significant challenges protecting critical IT assets from an exponentially increasing threat landscape. And, of course, serious vulnerabilities continue to be discovered in both legacy and emerging IT systems. Implementing effective security controls has been shown to significantly reduce the risk of information breach. In this session, Vijay Basani, President and CEO at EiQ Networks, will discuss an approach for delivering continuous security intelligence through the intersection of the right people. process and technology. He will also provide a case study on how EiQ's solutions can increase information security, improve operational efficiency, and lower cost for an organization through automation of many of the top Critical Security Controls recommended by SANS.

Continuous Monitoring & Mitigation

Speaker: Eric Vanderbur, Systems Engineer, ForeScout Technologies
Tuesday, October 21 | 12:30pm-1:15pm | Location: Pompeian III

You've already invested in multiple kinds of security systems, but are they working together effectively? Do they share intelligence? Do they coordinate their responses? Are all your remediations automated? This session examines a reference architecture for continuous monitoring and mitigation, based on next-generation network access control and open standards-based information sharing architecture.

VENDOR EVENTS

Fortinet Next Generation Firewalls

Speaker: Justin Kallhoff, Founder, Infogressive
Tuesday, October 21 | 12:30pm-1:15pm | Location: Roman I

Infogressive, a Fortinet platinum partner, will discuss next generation firewall technology. Learn how Fortinet products can improve your organization's security and simplify your network for a fraction of the cost of other manufacturers.

Simplify Your Security Operations with One Solution for Detecting Advanced Malware and Exploitable Vulnerabilities

Speaker: Narayan Makaram,
Product Marketing Manager, Tenable Network Security, Inc.
Tuesday, October 21 | 12:30pm-1:15pm | Location: Roman III

When it comes to closing gaps in security operations, added complexity is your enemy. Yet, enterprises persist in buying point solutions for managing vulnerabilities and detecting advanced threats (malware). With shrinking IT budgets and fewer trained professionals in security operations, the time is right for a smarter, more streamlined approach to both vulnerability and threat management.

Join us for lunch and you will learn how Tenable Network Security enables:

- Comprehensive identification of vulnerabilities across all asset types (physical/virtual, mobile/cloud)
- Effective detection of advanced threats on endpoints using threat intelligence from internal/external sources
- Correlation of anomalous network activity associated with compromised endpoints

VENDOR EVENTS

corero
FIRST LINE OF DEFENSE

Connecting your Business to the Unsecured Internet – The DDoS Threat

Speaker: Stephen Gates, Security Evangelist
Thursday, October 23 | 12:30pm-1:15pm | Location: Pompeian II

Today's breed of DDoS Attacks and Cyber Threats are not only incredibly sophisticated and designed to wreak havoc on your business, they are challenging to identify, and defend against. Without the proper technology in place to detect, analyze mitigate, any online business is vulnerable to effects of a DDoS attack. This session examines key steps to consider in your DDoS protection plan to enhance your existing defense in depth security strategy and the Corero approach to helping customers respond to the wide variety of attacks we see today.

beyondtrust®
Beyond Traditional Security

Retina Vulnerability Management: The Best-Kept Secret in Security

Speaker: Jason Williams, Security Engineer, BeyondTrust
Thursday, October 23 | 12:30pm-1:15pm | Location: Roman I

Some vendors expend a lot of energy on, well, being loud. At BeyondTrust, we focus on R&D, making Retina one of the fastest, most complete vulnerability management solutions available (and you have to see the reports). Come have lunch on us, and see a "secret" weapon that's been deployed hundreds of thousands of times since 1998.

skybox®
security

Automated Attack Simulation – Network Pen-Testing the Easy Way

Speaker: Sean Keef, Director, Sales Engineering, Skybox Security
Thursday, October 23 | 12:30pm-1:15pm | Location: Pompeian IV

When the goal is vulnerability prioritization and understanding how existing network security devices are mitigating the risk of vulnerability exploitation, Skybox is the answer. Find out how Skybox Security can prioritize vulnerabilities and focus remediation efforts through automated attack simulation. We'll look at the pieces of information necessary to setup attack simulation and explore the output of the system.

VENDOR EVENTS

GENERAL DYNAMICS
Fidelis Cybersecurity Solutions

Stay Ahead of the Adversary with Network Security Analytics

Speaker: H. Michael Nichols, Senior Manager, Sales Engineering
Thursday, October 23 | 12:30pm-1:15pm | Location: Roman III

Threat actors often modify their tactics, or the tools they use to attack, but their techniques, or methods, have a much longer lifecycle. Much like the way the antivirus industry learned signature-based detection of malware was a perfect method of detection, the network security community is learning that detecting threats by looking at a single event in time does not provide total protection. If network defenses are to evolve and defeat new attacks, we must look for the attackers' ingrained behavior, not their constantly changing tactics. Network security analytics allows us to track attacks over time, alerting when a series of events is determined to be a method of attack, and empowering us with the ability to stay one step ahead of the adversary.

PHISHME

All Your Metadatas Are Belong To Me: Reverse Engineering Emails on an Enterprise Level

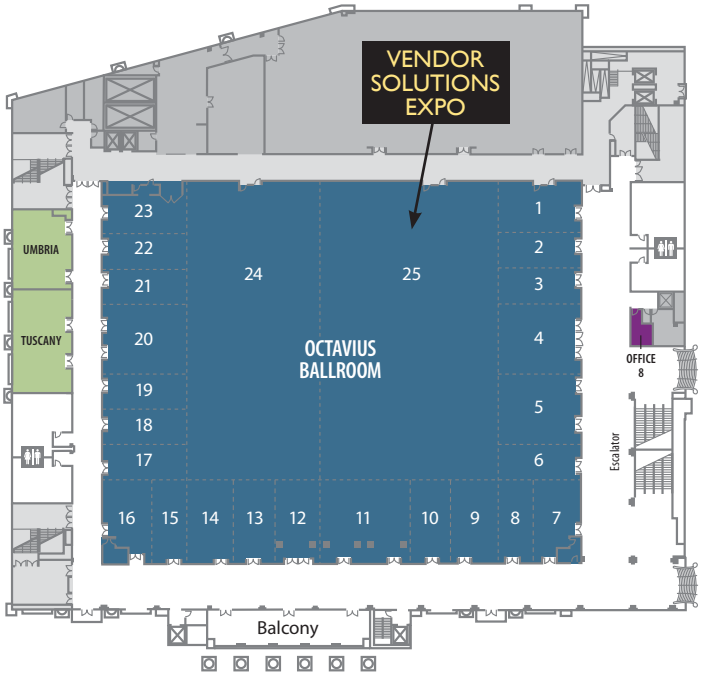
Speaker: Ronnie Tokazowski, Senior Researcher, PhishMe
Thursday, October 23 | 12:30pm-1:15pm | Location: Pompeian III

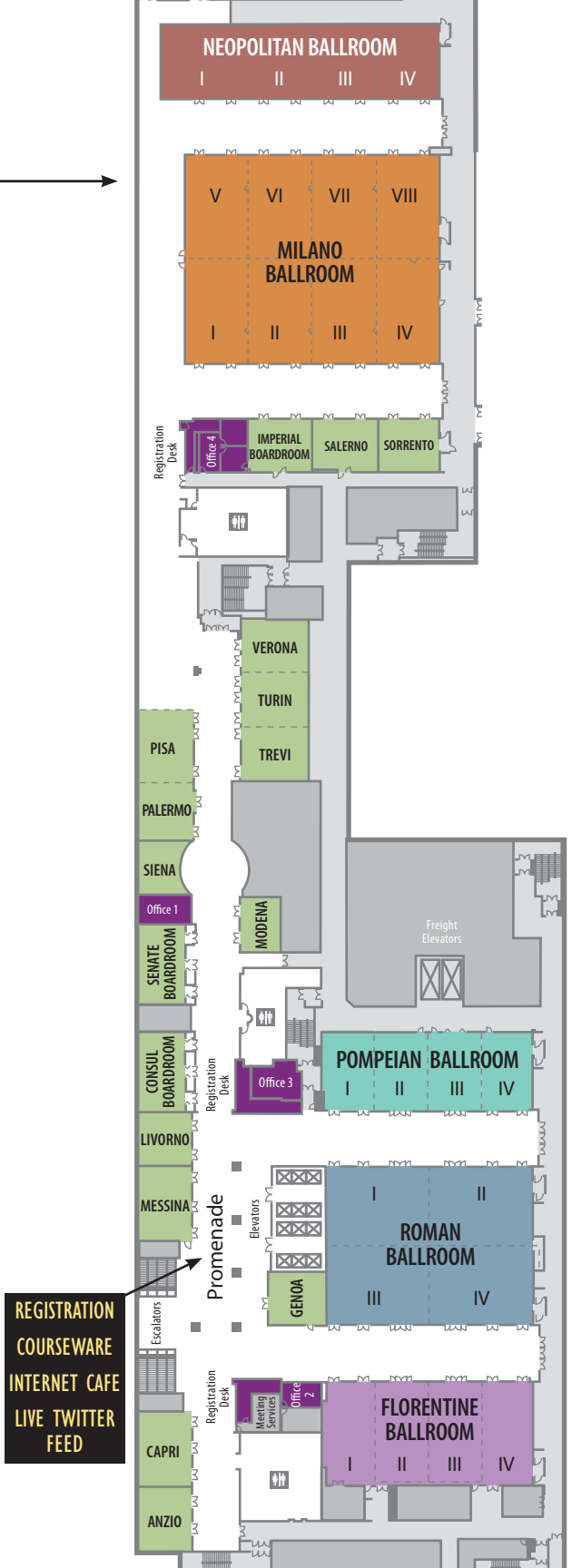
Although enterprises receive high volumes of phishing emails daily, many still lack the ability to effectively analyze them. Performing reverse engineering will allow companies to quickly answer questions about phishing emails they receive. In this presentation, I will detail new reverse engineering techniques that show how to parse and pivot on metadata within an email, use custom signatures to detect malicious logic, and provide general visibility into phishing emails. Performing these techniques will provide answers to questions such as "Have I ever seen this MD5 sent to me in email over the last year?" or "Have the bad guys ever used this domain against us?" that will allow organizations to proactively respond to phishing attacks.

HOTEL FLOORPLANS

PROMENADE LEVEL →

PROMENADE SOUTH





DINING OPTIONS

BACCHANAL BUFFET
Bacchanal Buffet features more than 500 items prepared by a team of master chefs in nine globally-inspired open kitchens.

UPSCALE ITALIAN

RAO'S
Come experience simple, honest, home cooking at Rao's at Caesars Palace, voted one of the best Italian restaurants in Las Vegas.

UPSCALE JAPANESE

NOBU
The ideal destination to be seen, socialize, and enjoy the unique cuisine of celebrated Chef Nobu Matsuhisa.

UPSCALE STEAKHOUSE

OLD HOMESTEAD STEAKHOUSE
Old Homestead Steakhouse at Caesars Palace offers fine dining in a Las Vegas restaurant inspired by the original Old Homestead, one of NYC's most historic restaurants.

UPSCALE FRENCH

PAYARD PATISSERIE & BISTRO
The Payard Patisserie & Bistro at Caesars Palace, unique among Las Vegas restaurants, contains an upscale bistro as well as a chocolate and pastry shop.

RESTAURANT GUY SAVOY
Restaurant Guy Savoy at Caesars Palace has been called the best restaurant in Las Vegas, serving elegant French Cuisine in a fine dining environment.

UPSCALE CONTEMPORARY SOUTHWESTERN

MESA GRILL
Brought to Caesars Palace Las Vegas by celebrity chef Bobby Flay, Mesa Grill Southwestern Restaurant features bold flavors and specialty margaritas.

UPSCALE CHINESE

EMPRESS COURT
Dine on authentic Cantonese seafood at the Empress Court Chinese Restaurant, a premium Las Vegas restaurant at Caesars Palace Las Vegas.

CASUAL CHINESE

BEIJING NOODLE NO. 9
Beijing Noodle No. 9 offers Northern Chinese cuisine in a friendly, casual atmosphere. The best restaurants in Las Vegas can only be found at Caesars.

CASUAL AMERICAN

MUNCHBAR
Come take a break at Munchbar, a Las Vegas restaurant and pub where you can find all your favorite comfort foods on a menu created by renowned Chef Bryan Ogden.

SERENDIPITY 3
Serendipity 3, one of the great Las Vegas restaurants at Caesars Palace, serves fun and whimsical entrees and delectable desserts.

CENTRAL BY MICHEL RICHARD
At Central, Chef Michel Richard serves American food with a French twist in a casual dining environment. For all the best restaurants in Las Vegas, try Caesars Palace.

CASUAL CAFE/VARIETY

GORDON RAMSAY PUB & GRILL
Gordon Ramsay Pub & Grill is the neighborhood restaurant conceptualized by the award-winning chef. The 290 seat restaurant is the most authentic English pub experience in Las Vegas, as only a native UK chef can provide.

CYPRESS STREET MARKETPLACE
Casual dining at Cypress Street Marketplace offers a wide variety of cuisines and specialty food. Find all the best Las Vegas restaurants at Caesars Palace.

OnDemand Bundles

Supplement Your Live Training with a SANS OnDemand Bundle

Register by the end of this training event to get these discounted prices!

Note: Only the course(s) that you are taking at this event are eligible to be bundled.

SEC301 – $599	SEC566 –$599	FOR508 – $599
SEC401 – $599	SEC575 – $599	FOR526 – $599
SEC501 – $599	SEC579 – $599	FOR585 – $599
SEC502 – $599	SEC617 – $599	FOR610 – $599
SEC503 – $599	SEC660 – $599	ICS410 – $599
SEC504 – $599	AUD507 – $599	LEG523 – $599
SEC505 – $599	DEV522 – $599	MGT414 – $599
SEC506 – $599	DEV541 – $599	MGT512 – $599
SEC542 – $599	DEV544 – $599	MGT514 – $599
SEC560 –$599	FOR408 – $599	MGT525 – $599

Three ways to register!

Visit the registration desk on-site
Call (301) 654-SANS
Write to ondemand@sans.org

Washington, DC | December 10-19, 2014

SANS CYBER DEFENSE INITIATIVE

Choose from these popular courses:

SECURITY

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Web App Penetration Testing and Ethical Hacking

Intrusion Detection In-Depth

FORENSICS

Memory Forensics In-Depth NEW!

Windows Forensic Analysis

REM: Malware Analysis Tools and Techniques

MANAGEMENT

SANS Security Leadership Essentials For Managers

Training Program for the CISSP® Cert Exam

INDUSTRIAL CONTROL SYSTEMS

ICS/SCADA Security Essentials NEW!

And more!

10TH ANNUAL

ICS SECURITY

SUMMIT & TRAINING

Orlando, FL

SUMMIT: Feb 23-24, 2015 | TRAINING: Feb 25 - Mar 2, 2015

For SCADA, Industrial Automation, and Control System Security

Choose from these popular courses

CyberCity Hands-on Kinetic Cyber Range Exercise

ICS/SCADA Security Essentials

Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program

Critical Infrastructure Protection

Assessing and Exploiting Control Systems

Critical Infrastructure and Control System Cybersecurity

NetWars – CyberCity

sans.org/event/ics-security-summit-2015

Future SANS Training Events

SANS **Cyber Defense San Diego** 2014
San Diego, CA | November 3-8 | #CyberDefSD

SANS **DFIRCON East** 2014
Fort Lauderdale, FL | November 3-8 | #DFIRCon

Pen Test Hackfest 2014
Washington, DC | November 13-20 | #HackFestSummit

Healthcare Cyber Security SUMMIT 2014
San Francisco, CA | December 3-10 | #HealthcareSummit

SANS **Cyber Defense Initiative** 2014
Washington, DC | December 10-19 | #SANSCDI

SANS **Security East** 2015
New Orleans, LA | January 16-21 | #SecurityEast

SANS **Cyber Threat Intelligence** SUMMIT & TRAINING 2015
Washington, DC | February 2-9 | #CTISummit

SANS **Scottsdale** 2015
Scottsdale, AZ | February 16-21 | #SANSScottsdale

10TH ANNUAL **ICS Security** SUMMIT – ORLANDO 2015
Orlando, FL | February 23 - March 2 | #SANSICS

SANS **DFIRCON West** 2015
Monterey, CA | February 23-28 | #DFIRCon

SANS **Cyber Guardian** 2015
Baltimore, MD | March 2-7 | #CyberGuardian

SANS **Northern Virginia** 2015
Reston, VA | March 9-14 | #SANSNoVA

SANS 2015
Orlando, FL | April 11-20 | #SANS2015

SANSFIRE 2015
Baltimore, MD | June 11-22 | #SANSFIRE

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