SANS FIRE 2015

PROGRAM GUIDE

June 13-20

Hilton Baltimore

Baltimore, MD

@SANSInstitute | #SANSFIRE

SANS OnDemand Bundle

Add an OnDemand Bundle to your course to get an additional four months of intense training! OnDemand Bundles are just $629 when added to your live course, and include:

- Four months of OnDemand access to our custom e-learning platform
- Quizzes
- MP3s and Videos of lectures
- Labs
- Subject-Matter Expert support

OnDemand Bundle is available for these courses.

SEC301 – $629	SEC560 – $629	ICS410 – $629
SEC401 – $629	SEC566 –$629	LEG523 – $629
SEC501 – $629	SEC579 – $629	FOR408 – $629
SEC502 – $629	SEC617 – $629	FOR508 – $629
SEC503 – $629	SEC642 – $629	FOR526 – $629
SEC504 – $629	SEC660 – $629	FOR572 – $629
SEC505 – $629	AUD507 – $629	FOR585 – $629
SEC506 – $629	DEV522 – $629	FOR610 – $629
SEC511 – $629	DEV544 – $629	MGT414 – $629
SEC542 – $629		MGT512 – $629

Three ways to register!

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

TABLE OF CONTENTS

NETWARS TOURNAMENTS

All students who register for a 4-6 day course will be eligible to play NetWars for FREE.

Register Now!
sans.org/event/sansfire-2015/schedule

DFIR NETWARS TOURNAMENT

Hosted by Rob Lee and Chad Tilbury
Thursday, June 18 and Friday, June 19
6:30-9:30pm | Francis Scott Key 7

CORE NETWARS TOURNAMENT

Hosted by Jeff McJunkin
Thursday, June 18 and Friday, June 19
6:30-9:30pm | Francis Scott Key 5 and 6

GENERAL INFORMATION

Registration & Courseware Pick-up Information

Location: Francis Scott Key Foyer (2ND FLOOR)

Saturday, June 13 (Short Courses Only) 8:00-9:00am

Location: South Foyer (2ND FLOOR)

Sunday, June 14 (Welcome Reception) 5:00-7:00pm
Monday, June 15 . . . . . 7:00am-5:30pm
Tuesday, June 16 - Friday, June 19. . . . . 8:00am-5:00pm
Saturday, June 20 . . . . . 8:00am-Noon

Internet Café *(WIRED & WIRELESS)*

Location: Billie Holiday Foyer (2ND FLOOR)

Monday, June 15 . . . . . Opens at noon – 24 hours
Tuesday, June 16 - Friday, June 19 . . . . . Open 24 hours
Saturday, June 20 . . . . . Closes at 2:00pm

Course Times

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

Course Breaks

7:00-9:00am – Morning Coffee
10:30-10:50am – Morning Break
12:15-1:30pm – Lunch (On your own)
3:00-3:20pm – 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 **8:15-8:45am** on **Monday, June 15** at the ***General Session*** in **Francis Scott Key 5**.

GENERAL INFORMATION

Dining Options

We have assembled a short list of dining suggestions you may like to try during lunch breaks. See page 25 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.

Twitter

Join the conversation on Twitter and use the hashtag **#SANSFIRE** for up-to-date information from fellow attendees!

Wear Your Badge

To make sure you are in the right place, the SANS door monitors will be checking your badge for each course and evening event 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 South 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)

SEC401: Security Essentials Bootcamp Style
SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
SEC760: Advanced Exploit Development for Penetration Testers
MGT414: SANS Training Program for CISSP® Certification

Extended Hours:

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling
FOR408: Windows Forensic Analysis
FOR585: Advanced Smartphone Forensics
SEC560: Network Penetration Testing and Ethical Hacking
MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™

COURSE SCHEDULE

START DATE: **Saturday, June 13**

Time: 9:00am-5:00pm (Unless otherwise noted)
All locations are at the Hilton Baltimore (Unless noted Marriott)

SEC524: Cloud Security Fundamentals
Instructor: Dave Shackleford . . . . . .Location: Billie Holiday 5

SEC546: IPv6 Essentials
Instructor: Johannes Ullrich, Ph.D. . . . . .Location: Peale A

SEC580: Metasploit Kung Fu for Enterprise Pen Testing
Instructor: Eric Conrad . . . . . .Location: Billie Holiday 6

FOR578: Cyber Threat Intelligence
Instructors: Robert M. Lee,
Mike Cloppert . . . . . .Location: Billie Holiday 3

MGT415: A Practical Introduction to Cyber Security Risk Management
Instructor: James Tarala. . . . . .Location: Billie Holiday 2

MGT433: Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program
Instructor: Lance Spitzner . . . . . .Location: Billie Holiday 4

MGT535: Incident Response Team Management
Instructor: Alissa Torres . . . . . .Location: Billie Holiday 1

HOSTED: Physical Penetration Testing
Instructor: The CORE Group. . . . . Location: Peale B & C

START DATE: **Monday, June 15**

Time: 9:00am-5:00pm (Unless otherwise noted)
All locations are at the Hilton Baltimore (Unless noted Marriott)

SEC301: Intro to Information Security
Instructor: Keith Palmgren. . . . . Location: Francis Scott Key 12

SEC401: Security Essentials Bootcamp Style
Instructor: Dr. Eric Cole . . . . . .Location: Billie Holiday 6
Bootcamp Hours: 5:00-7:00pm (Course days 1-5)

SEC501: Advanced Security Essentials – Enterprise Defender
Instructor: Paul A. Henry . . . . . .Location: Billie Holiday 3

SEC502: Perimeter Protection In-Depth
Instructor: Tanya Baccam . . . . . .Location: Johnson B

SEC503: Intrusion Detection In-Depth
Instructor: Mike Poor. . . . . Location: Francis Scott Key 3

SEC504: Hacker Tools, Techniques, Exploits & Incident Handling
Instructor: John Strand. . . . . Location: Francis Scott Key 5
Extended Hours: 5:00-7:15pm (Course Day 1 only)

COURSE SCHEDULE

SEC505: Securing Windows with the Critical Security Controls
Instructor: Jason Fossen. . . . . Location: Francis Scott Key 11

SEC506: Securing Linux/Unix
Instructor: Hal Pomeranz. . . . . Location: University 2 (MARRIOTT)

SEC511: Continuous Monitoring and Security Operations
Instructor: Seth Misenar . . . . . Location: Francis Scott Key 4

SEC542: Web App Penetration Testing and Ethical Hacking
Instructor: Eric Conrad . . . . . Location: Tubman A & B

SEC560: Network Penetration Testing and Ethical Hacking
Instructor: Ed Skoudis . . . . . Location: Francis Scott Key 6
Extended Hours: 5:00-7:15pm (Course Day 1 only)

SEC562: CyberCity Hands-on Kinetic Cyber Range Exercise
Instructor: Tim Medin . . . . . .Location: Poe A & B

SEC566: Implementing and Auditing the Critical Security Controls – In-Depth
Instructor: James Tarala . . . . . .Location: Billie Holiday 4

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

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

SEC642: Advanced Web App Penetration Testing and Ethical Hacking
Instructor: Justin Searle . . . . . .Location: Billie Holiday 1

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
Instructor: James Lyne . . . . . .Location: Billie Holiday 2
Bootcamp Hours: 5:15pm-7:00pm (Course days 1-5)

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

DEV522: Defending Web Applications Security Essentials
Instructor: Jason Lam . . . . . Location: Promenade (MARRIOTT)

DEV544: Secure Coding in .NET: Developing Defensible Apps
Instructors: Aaron Cure,
Eric Johnson . . . . . Location: University 4 (MARRIOTT)

FOR408: Windows Forensic Analysis
Instructor: Rob Lee . . . . . Location: Francis Scott Key 7
Set-up time: 8:00-9:00am (Course Day 1 only)

FOR508: Advanced Digital Forensics and Incident Response
Instructor: Chad Tilbury . . . . . Location: Francis Scott Key 10

COURSE SCHEDULE

FOR526: Memory Forensics In-Depth
Instructors: Jake Williams . . . . . Location: Francis Scott Key 9

FOR572: Advanced Network Forensics and Analysis
Instructors: Philip Hagen . . . . . .Location: Billie Holiday 5

FOR585: Advanced Smartphone Forensics
Instructors: Heather Mahalik. . . . . .Location: Peale A
Set-up time: 8:00-9:00am (Course Day 1 only)

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Instructor: Lenny Zeltser . . . . . Location: Francis Scott Key 8

MGT414: SANS Training Program for CISSP® Certification
Instructor: Jonathan Ham . . . . . .Location: Carroll A & B
Bootcamp Hours: 8:00-9:00am (Course days 2-6) &
5:00-7:00pm (Course days 1-5)

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

MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep
Instructor: Jeff Frisk . . . . . Location: Francis Scott Key 2

AUD507: Auditing & Monitoring Networks, Perimeters, and Systems
Instructor: David Hoelzer. . . . . Location: Peale B & C

LEG523: Law of Data Security and Investigations
Instructor: Benjamin Wright . . . . . Location: University 3 (MARRIOTT)

ICS410: ICS/SCADA Security Essentials
Instructor: Graham Speake. . . . . Location: Paca A & B

HOSTED: (ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program
Instructor: Frank Shirmo . . . . . Location: University 1 (MARRIOTT)

START DATE: **Thursday, June 18**

DFIR NetWars Tournament
Hosts: Rob Lee & Chad Tilbury . . . . . Location: Francis Scott Key 7
Hours: 6:30-9:30pm

CORE NetWars Tournament
Host: Jeff McJunkin . . . . . Location: Francis Scott Key 5 and 6
Hours: 6:30-9:30pm

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 network and computer security.

SUNDAY, JUNE 14

Registration Welcome Reception

Sun, June 14 | 5:00-7:00pm | Location: Francis Scott Key South Foyer

Register early and network with your fellow students!

MONDAY, JUNE 15

General Session – Welcome to SANS

Speaker: Johannes Ullrich, PhD

Mon, June 15 | 8:15-8:45am | Location: Francis Scott Key 5

SANS Technology Institute Information Session

Speaker: Bill Lockhart

Mon, June 15 | 5:30-7:00pm | Location: Ruth

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.

Visit our Open House and learn more!

KEYNOTE

State of the Internet Panel Discussion

Speakers: Dr. Johannes Ullrich, ISC Director and Marcus Sachs, ISC Director Emeritus

Mon, June 15 | 7:15-9:15pm | Location: Francis Scott Key 5

SANSFIRE offers the greatest opportunity to meet ISC handlers from around the world, and our most popular bonus session is their "State of the Internet" panel discussion. During this session, you will have the chance to hear from our handlers and ask their opinions and insights on current threats. This is a unique opportunity you will only have at SANSFIRE – a dozen of the industry's brightest minds at your disposal for two intriguing hours!

SPECIAL EVENTS

TUESDAY, JUNE 16

GIAC Program Overview

Speaker: Jeff Frisk

Tue, June 16 | 6:15-7:15pm | Location: Francis Scott Key 8

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.

MASTER'S PRESENTATION

Faster than a Speeding Bullet: Can Geolocation Find Supervillains in Your Network?

Speaker: Tim Collyer

Tue, June 16 | 7:15-8:15pm | Location: Billie Holiday 1

Good logging provides the IP addresses of external connections to our network. This data can be compared against geolocation databases to provide the physical location of the IP source. By extracting physical location data from network logs, we can track user location and determine if a user would need to be a superhero (or supervillain) to travel quickly enough between two different logon locations. This sounds great, but how does it work in practice? This talk will explore the technical mechanics behind tracking geolocation as well where the kryptonite lies in this process.

SANS@NIGHT

The State of the Takedown: Disrupting Online Cybercrime

Speaker: John Bambenek

Tue, June 16 | 7:15-8:15pm | Location: Francis Scott Key 8

We have all seen the splashy headlines of large threats being subjected to takedowns only to re-emerge days (or hours) later. A few takedowns, however, have achieved long term results. This talk will focus on how recent successful operations were accomplished and cover such topics as:

- Developing automated intelligence and surveillance
- Techniques to enhance ability for attribution of threat actors
- Acquiring intelligence from otherwise "hostile" jurisdictions
- Working with law enforcement versus purely private-sector action

This talk will also discuss other disruptive techniques besides takedowns that can be used to protect your organizations.

SANS@NIGHT

The 13 Absolute Truths of Security

Speaker: Keith Palmgren

Tue, June 16 | 7:15-8:15pm | Location: Francis Scott Key 5

Keith Palmgren has identified 13 "Absolute Truths" of security – things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these 13 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 13 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

How to Run Linux Malware Analysis Apps as Docker Containers

Speaker: Lenny Zeltser

Tue, June 16 | 7:15-8:15pm | Location: Francis Scott Key 6

There are wonderful malware analysis applications out there that run well on Linux; however, installing and configuring them could be quite challenging. A relatively new approach using such tools involves running them as application containers. In this scenario, the application is packaged together with its dependencies as a Docker image, so you don't have to worry about setup or runtime problems that can occur when running the apps in a traditional manner. In this informative talk Lenny Zeltser, the lead author of SANS' malware analysis course, explains how you can use malware analysis tools that are already distributed as Docker images as part of the REMnux project. These tools include Thug, Viper, Rekall, JSDetox, and others. Lenny also offers tips for packaging your favorite apps in a similar manner. He will cover the following topics:

- What is Docker and how it is different from virtualization technologies?
- What malware analysis applications are available as Docker images?
- How can you launch and interact with malware analysis apps running as containers?
- How can you build Docker application images of your favorite applications?
- What are the security implications of running applications as containers?

Attend this presentation to start learning about Docker containers so you can not only use them when examining malicious software, but also so you better understand what application containers are and what role they might play alongside other infrastructure technologies.

SPECIAL EVENTS

SANS@NIGHT

Making Awareness Stick

Speaker: Lance Spitzner

Tue, June 16 | 7:15-8:15pm | Location: Francis Scott Key 7

One of the most common, long-term challenges faced by any awareness program is getting it to stick. How do you create an engaging program that people want to listen to, teaches them more, and ultimately changes behaviors? In this talk we explain what organizations are effectively doing around the world to emotionally engage and communicate to their employees. Key points you will learn include:

- Behavior modeling
- Defining your culture
- Self-education
- Ambassador/Champion programs
- Developing your engagement strategy

MASTER'S PRESENTATION

Practical Attack Detection Using Big Data, Semantics, and Kill Chains

Speaker: Brian Nafziger

Tue, June 16 | 8:15-9:15pm | Location: Billie Holiday 1

Traditional toolsets using atomic syntactic-based detection methods have slowly lost the ability, in and of themselves, to detect and respond to today's well-planned, multi-phased, multi-asset, and multi-day attacks thereby leaving a gap in detecting these attacks. Modern toolsets must rapidly detect and respond to attacks that are across multiple phases, across thousands of assets, across days of time, and across millions of events. Big data, semantics, and kill chains are, potentially, optimal choices for detecting modern attacks. The question is, do they live up to their potential? If true, then the security community must investigate these frameworks. The objective is to grow a framework using Splunk that begins to fill the gap and then share it.

SANS@NIGHT

Debunking the Complex Password Myth

Speaker: Keith Palmgren

Tue, June 16 | 8:15-9:15pm | Location: Francis Scott Key 5

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.

SPECIAL EVENTS

SANS@NIGHT

Attacks by BroBot Against the U.S. Financial Markets

Speaker: Donald Smith

Tue, June 16 | 8:15-9:15pm | Location: Francis Scott Key 8

BroBot, while fairly small for a botnet, was successfully used to demonstrate many layer 7 attacks that had varying degrees of success. We will discuss several of the techniques used and mitigation methods that were developed and deployed.

SANS@NIGHT

Enterprise PowerShell for Remote Security Assessment

Speaker: James Tarala

Tue, June 16 | 8:15-9:15pm | Location: Francis Scott Key 6

As organizations assess the security of their information systems, the need for automation has become more and more apparent. Not only are organizations attempting to automate their assessments, the need is becoming more pressing to perform assessments centrally against large numbers of enterprise systems. Forensic analysts, incident handlers, penetration testers, and auditors all regularly find themselves in situations where they need to remotely assess a large number of systems through an automated set of tools. Microsoft's PowerShell scripting language has become the defacto standard for many organizations looking to perform this level of distributed automation. In this presentation James Tarala, of Enclave Security, will describe to students the enterprise capabilities PowerShell offers and show practical examples of how PowerShell can be used to perform large scale Windows security assessments.

SANS@NIGHT

Securing The Kids

Speaker: Lance Spitzner

Tue, June 16 | 8:15-9:15pm | Location: Francis Scott Key 7

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.

SPECIAL EVENTS

WEDNESDAY, JUNE 17

MASTER'S PRESENTATION

Security Visibility in Enterprise

Speaker: Jim Hendrick

Wed, June 17 | 7:15-7:55pm | Location: Billie Holiday 1

Security Visibility. What is it? Don't we get that from our tools? We passed compliance, don't we have visibility? Often driven by regulatory and compliance efforts, security visibility means different things to organizations of all sizes. Many tools or services promise to provide protection, deliver insight, achieve compliance, and a host of other things. And, many projects that are run to implement "best practices" leave the customer feeling either unsure of what they got for the effort or completely overwhelmed and unable to see any real value. In this brief talk, the speaker will cover at a very high level one organization's journey to implement an internal SOC and SIEM, touching on the project structure itself but largely focused on key elements and decisions that can hopefully be instructive in your own organization.

SANS@NIGHT

"Network Security as Counterinsurgency" Replacing The Art of War with FM 3-24

Speaker: Kevin Liston

Wed, June 17 | 7:15-8:15pm | Location: Francis Scott Key 5

Growing tired of trying to turn "know yourself and lose 50 battles" into an actionable process? A sigma or two shy of six? Disappointed by the limited choices you have for the A in your OODA loop? Need a new set of metaphors and fancy-sounding language to motivate your managers and/or clients? Learn how to leverage lessons from the FM 3-24 Counterinsurgency manual to regain control of your network.

SANS@NIGHT

Windows Exploratory Surgery with Process Hacker

Speaker: Jason Fossen

Wed, June 17 | 7:15-8:45pm | Location: Francis Scott Key 8

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

Bueller... Bueller...: Smartphone Forensics Moves Fast. Stay Current or Miss Evidence

Speaker: Heather Mahalik

Wed, June 17 | 7:15-8:15pm | Location: Francis Scott Key 6

How have smartphone OS upgrades to iOS 8 and Lollipop changed the game of forensics? The goal of this talk will be to cover new locations for data storage, how the tools stand up to the changes and how to manually recover data that the tools miss. We will look at residual data from older OSs on Android and iOS (because an upgrade doesn't delete the old data) and determine how the data is parsed and decoded while staying within a limited budget.

SANS@NIGHT

Evolving Threats

Speaker: Paul A. Henry

Wed, June 17 | 8:15-9:15pm | Location: Francis Scott Key 6

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.

MASTER'S PRESENTATION

Creating a Baseline of Process Activity for Memory Forensics

Speaker: Gordon Fraser

Wed, June 17 | 8:15-9:15pm | Location: Billie Holiday 1

A component of memory forensics is the examination of running processes looking for anomalies. This assumes that the analyst can recognize what is expected so they can identify what does not belong. Knowledge of what is normal is valuable because it can be used as a filter so the analyst can quickly focus on the unusual. This presentation provides an approach for establishing a baseline that can be used to identify what is normal and discusses how this information can be used in memory analysis.

SANS@NIGHT

Offensive Countermeasures, Active Defenses, and Internet Tough Guys

Speaker: John Strand

Wed, June 17 | 8:15-9:15pm | Location: Francis Scott Key 5

In this presentation, John Strand will demonstrate the Active Defense Harbinger Distribution, a DARPA funded, free Active Defense virtual machine. He will debunk many of the myths, outright lies, and subtle confusions surrounding taking active actions against attackers. From this presentation, you will not only know how to take action against attackers, you will learn how to do it legally.

SANS@NIGHT

Unconventional Linux Incident Response

Speaker: Tom Webb

Wed, June 17 | 8:15-9:15pm | Location: Francis Scott Key 7

Responding to compromised servers in a homogeneous Linux environment is boring! What would you do if you had to collect data on a exotic processor, 10-year-old kernel or a rare file system? I will discuss specific examples of incidents, tools, and lessons learned from hundreds of collections in a widely diverse Linux environment.

THURSDAY, JUNE 18

Hosts: Rob Lee and Chad Tilbury

Thu, June 18 & Friday, June 19 | 6:30-9:30pm

Location: Francis Scott Key 7

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

Host: Jeff McJunkin
Thu, June 18 & Friday, June 19 | 6:30-9:30pm
Location: Francis Scott Key 5 and 6

SANS 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 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.

MASTER'S PRESENTATION

The Spy with a License to Kill

Speaker: Matthew Hosburgh
Thu, June 18 | 7:15-7:55pm | Location: Billie Holiday 1

Industrial espionage, malware, and targeted attacks bring about a certain stigma. These terms have been around for decades and in many cases become cliché. Yet, they bring a new meaning when dealing with Industrial Control Systems (ICS). ICS provide a myriad of functions such as pipeline control, monitoring of the fermentation process in a brewery, and traffic light control. These systems are no longer contained. They are connected, exposed, and vulnerable. One recent campaign has caught the attention of many security professionals. The Energetic Bear Campaign and more specifically, Havex, is a real and interesting threat that is targeting numerous control systems, but why?

SANS@NIGHT

Software Defined Networking – Attacker Defined Networking

Speaker: Rob Vandenbrink
Thu, June 18 | 7:15-8:15pm | Location: Francis Scott Key 8

It's becoming clear the future of enterprise, carrier, and "cloud" networking is becoming inextricably tied to Software Defined Networking (SDN). The promise of SDN is to present a network administrator with a high-level view of the network, and more importantly a high-level, vendor agnostic method of configuring a network – where a single construction or operation in the SDN controller might reconfigure multiple (or all) devices on the network to achieve the higher-level goal.

SANS@NIGHT

Cyber Counter Intelligence and Deception: Toward Adaptive Defense

Speaker: Gadi Evron
Thu, June 18 | 8:15-9:15pm | Location: Francis Scott Key 8

In cyber, defenders operate from a static standpoint while the attacker has complete control over both attack space and the time dimension. This asymmetry causes breaches to be inevitable, and only be detected hundreds to thousands of days after the fact – and then often by a third party. This is a systematic failure in how security is done. By adopting an attacker-based rather than an attack-based approach, breaches can be detected and immunized against, making defence dynamic, and taking away the attacker's advantage.

SANS@NIGHT

Outsharing the Bad Guys. How to get Involved with the Internet Storm Center

Speaker: Dr. Johannes Ullrich
Thu, June 18 | 8:15-9:15pm | Location: Billie Holiday 6

In this informal session, we will talk about how to best share and contribute to the Internet Storm Center, as well as how to use our various data feeds and APIs. Bring your specific problem and suggestion and talk to the people who "run the place." You may walk out with a solution that works for you or a great idea about how to make collaborative information security work better for all of us struggling to keep up with the bad guys.

FRIDAY, JUNE 19

SANS@NIGHT

Continuous Monitoring and Real-World Analysis

Speaker: Seth Misenar
Fri, June 19 | 7:15-8:15pm | Location: Billie Holiday 8

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. Modern threats require a paradigm shift in the way we perform analysis and monitoring. This talk will help you face the problem and describe how to move your organization to a more defensible security architecture that enables continuous security monitoring.

SPECIAL EVENTS

SANS@NIGHT

Defending Control Systems in an Enterprise Environment

Speaker: Robert M. Lee

Fri, June 19 | 7:15-8:15pm | Location: Billie Holiday 4

Many organizations have control systems in their environments and do not know it. Sometimes these are as simple as heating ventilation and cooling systems (HVAC) and sometimes they are as complex as operational industrial control system (ICS) or supervisory control and data acquisition (SCADA) networks connected to the enterprise. In this presentation the course author of ICS515 and co-author of FOR578, Robert M. Lee, will give a talk on identifying control systems and what methods are available to monitor them and perform incident response when needed. The model presented can be used locally or from an enterprise-wide perspective in a security operations center (SOC) setup. Control systems are vulnerable and found in many environments but monitoring for and responding to adversaries is doable with existing methodologies and tools.

VENDOR EVENTS

Vendor Solutions Expo

Wed, June 17 | 12:00-1:30pm | 5:30-7:30pm
Location: Francis Scott Key Foyer

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

Wed, June 17 | 5:30-7:30pm | Location: Francis Scott Key Foyer

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

Wed, June 17 | 12:00-1:30pm | Location: Francis Scott Key Foyer

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:

Alert Logic	Event Tracker	PhishMe
Bit9 & Carbon Black	Fidelis Cybersecurity	Pwnie Express
Carahsoft	Forescout	Rapid7
Cellebrite	Guidance Software	Splunk
Domain Tools	Lancope	ThreatSTOP
ESVA	LogRhythm	Vectra Networks
	Palo Alto Networks	

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.

tenable network security

LUNCH AND LEARN

Tell It Like It Is – Managing Business Risk with Assurance Report Cards

Speaker: Bill Olson, Product Manager for SecurityCenter
Tue, June 16 | 12:30-1:15pm | Location: Francis Scott Key 3

Join Bill Olson exploring the challenge of defining and communicating security program objectives in clear, concise, and meaningful terms. You will learn ways to aligning security operations with business objectives so that you can effectively engage and inform line of business colleagues, C-level executives and corporate directors anytime they need insight into cyber risks. You will gain insight into Assurance Report Cards (ARCs), a new security reporting system introduced in Tenable SecurityCenter 5. Using ARCs, you can define your own security policies, which are then continually assessed for compliance. ARCs also provide on-demand, highly visual reports that enable effective communication with non-technical executives who need to know how network health aligns with high-level business objectives.

ForeScout
BE A GAME CHANGER

LUNCH AND LEARN

An Architecture for Continuous Monitoring and Mitigation

Speaker: Shane Stephens, Federal Systems Engineer
Tue, June 16 | 12:30-1:15pm | Location: Francis Scott Key 6

Why are cyber attackers still easily penetrating enterprise defenses? What can be done to close security gaps? What can be done to make legacy security systems work together more effectively so they can rapidly respond to cyber attacks? This session examines a reference architecture for continuous monitoring and mitigation, based on next-generation network access control, and a standards-based architecture to share information between and among legacy security systems.

VENDOR EVENTS

DOMAINTOOLS

LUNCH AND LEARN

Connect the Dots with Domain Name Intelligence from DomainTools

Speaker: Mark Kendrick, Director of Solution Engineering
Tue, June 16 | 12:30-1:15pm | Location: Francis Scott Key 1

The best incident responders know attribution can be a proxy for risk. Even when you don't know who's behind an attack, simply knowing what's linked to it can give you tremendous insight. This session will explore specific techniques for enumerating an attacker's online infrastructure and revealing patterns in the history of their domain names and IP addresses. We'll dig deep into published reports on various advanced persistent threats (APTs) and recreate the analysis which lead to their conclusions with resources you can put to immediate use. Plus, you'll get a sneak peak into DomainTools' upcoming investigation product and discover a hidden source for actor attribution.

ThreatSTOP™

LUNCH AND LEARN

Protecting the Things, Including the Ones You Already Have (and don't know about)

Speaker: John Thompson, Director, Systems Engineering, ThreatSTOP
Tue, June 16 | 12:30-1:15pm | Location: Francis Scott Key 5

The Internet Of Things is already here. Printers, Medical Devices, Cameras, Alarm systems; and more ALREADY connect to the network, and are Pwned. These systems typically are deployed and managed by people with little to no understanding of security, and are almost never patched. In this session we will show actual infections, and demonstrate protection that works for the Things on your network.

Guidance® SOFTWARE

LUNCH AND LEARN

Tue, June 16 | 12:30-1:15pm | Location: Francis Scott Key 8

VENDOR EVENTS

FIDELIS CYBERSECURITY™

LUNCH AND LEARN

Advanced Threats Need Comprehensive Defense

Speaker: Gerald Mancini, Vice President of Engineering
Tue, June 16 | 12:30-1:15pm | Location: Francis Scott Key 4

Join Fidelis Cybersecurity and learn more about:

- Why enterprises need a comprehensive defense against advanced threats
- The current threat landscape and approaches to advance threat defense
- How a security product detects advanced threats
- How you can empower the security team to detect and prevent threats across the network with actionable visibility over your network
- How to improve visibility in your network and endpoints with a comprehensive advanced threat defense solution

SOPHOS Infogressive, Inc. *Aggressive Information Security*

LUNCH AND LEARN

Prevent – Detect – Respond

Speaker: Rob Frickel, Security Analyst, Infogressive
Thu, June 18 | 12:30-1:15pm | Location: Francis Scott Key 11

We all want to prevent 100% of attacks, however most SANS attendees know that isn't realistic given today's threat landscape. We will discuss technologies and services that increase prevention rates, help with detection when your defenses fail, and how we respond when it really hits the fan. #BOOM

Bit9+ CARBON BLACK

ARM YOUR ENDPOINTS.

LUNCH AND LEARN

Real-time Detection, Prevention in Seconds: Make Attackers Part of Your Defense

Speaker: Jonathon Ross, Systems Engineer
Thu, June 18 | 12:30-1:15pm | Location: Francis Scott Key 12

Please join us to see how Bit9+Carbon Black work together, along with your existing controls, to arm your endpoints with defenses that minimize your endpoints' attack surface, detect new indicators of compromise, and maintain actionable intelligence that can automatically update your defenses as well as support your investigations from the moment you realize that an event is truly an incident.

PHISHME

LUNCH AND LEARN

Thu, June 18 | 12:30-1:15pm | Location: Francis Scott Key 8

VENDOR EVENTS

Lancope®

LUNCH AND LEARN

Combating Insider Threats – Protecting Your Agency from the Inside Out

Speaker: TK Keanini – CTO, Lancope, Inc

Thu, June 18 | 12:30-1:15pm | Location: Francis Scott Key 10

When Edward Snowden leaked classified information to the mainstream media, it brought the dangers posed by insider threats to the forefront of public consciousness, and not without reason. Today's agencies are drowning in fears surrounding sophisticated cyber attacks but perhaps the most concerning type of attack out there – the insider threat. According to Forrester, abuse by malicious insiders makes up 25% of data breaches, and another 36% of breaches are caused by the inadvertent misuse of data by insiders. Unfortunately, conventional security tools like firewalls, antivirus, and IDS/IPS are powerless in the face of the insider threat. Learn about the best practices and technologies you should be implementing now to avoid becoming the next victim of a high-profile attack.

ALERT LOGIC®
Security. Compliance. Cloud.

LUNCH AND LEARN

Anatomy of an Attack: It Takes an Expert to Stop Attackers

Speaker: Stephen Coty, Chief Security Evangelist

Thu, June 18 | 12:30-1:15pm | Location: Francis Scott Key 9

Attacks have advanced far beyond the early threats of tech-savvy kids wreaking havoc on computer networks. Today's attackers are fast, well-funded, and organized. Our discussion will take you into the world of cybercrime and give you an insider's look into how attackers operate and what you can do to protect your information in the cloud.

paloalto networks®

LUNCH AND LEARN

Crack the Code and Defeat the Advanced Adversary

Speaker: Brian O'Neil, SE Manager, Palo Alto Networks

Thu, June 18 | 12:30-1:15pm | Location: Francis Scott Key 7

Cybersecurity can sometimes feel like a puzzle – a code to crack. This isn't how it should be. Adversaries don't need to win. Stopping them doesn't require endless time and resources because most just take the path of least resistance for the easiest win. Your objective as a security practitioner is to raise the total cost of a successful attack, to make your organization a less appealing target. Join Palo Alto Networks for a lunch and learn that will take a detailed look at real attacks and how you can crack the code to defend your organization.

DINING OPTIONS

The Hilton Baltimore offers our guests the best dining in Baltimore while delivering the ultimate in charm city style. Our culinary team has created a new American cuisine for our ***Diamond Tavern*** restaurant while giving it a unique, urban twist for you to enjoy. Open for breakfast, lunch and dinner, it boasts 20 high-definition televisions ideal for celebrating game day at Camden Yards or catching your favorite sporting event throughout the year.

The ***Lobby Bar*** is an intimate, yet vibrant setting serving your favorite adult beverages while you relax and people watch in our spacious lobby. As a hotel guest, you can enjoy some of the same tempting creations from our ***Diamond Tavern*** while in your guest room through ***In-Room Dining*** services.

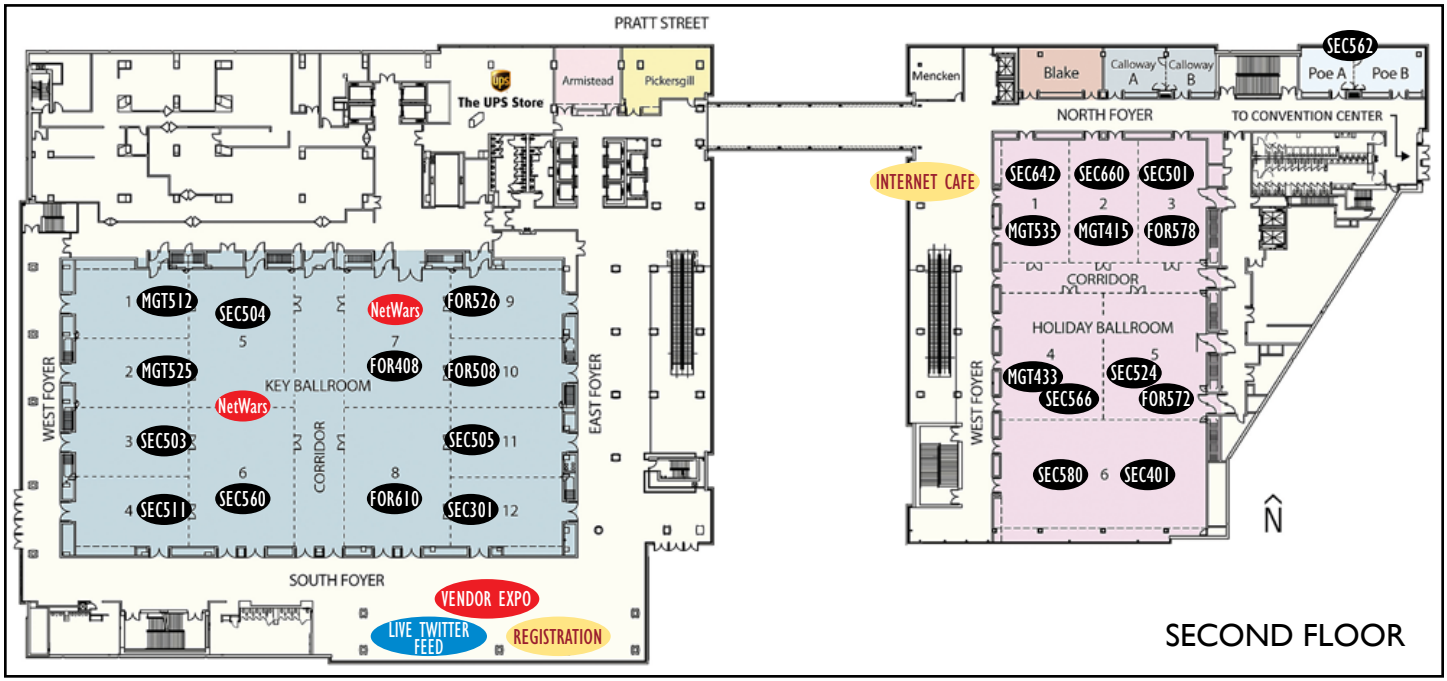
Diamond Tavern *(6:30am-10:00pm)*
The Diamond Tavern offers casual upscale dining in a lively sophisticated atmosphere, serving delicious American cuisine. All-day dining with a la carte breakfast, luncheon and dinner menus is available. The restaurant seats 240 people, outdoor patio seats an additional 80 people!

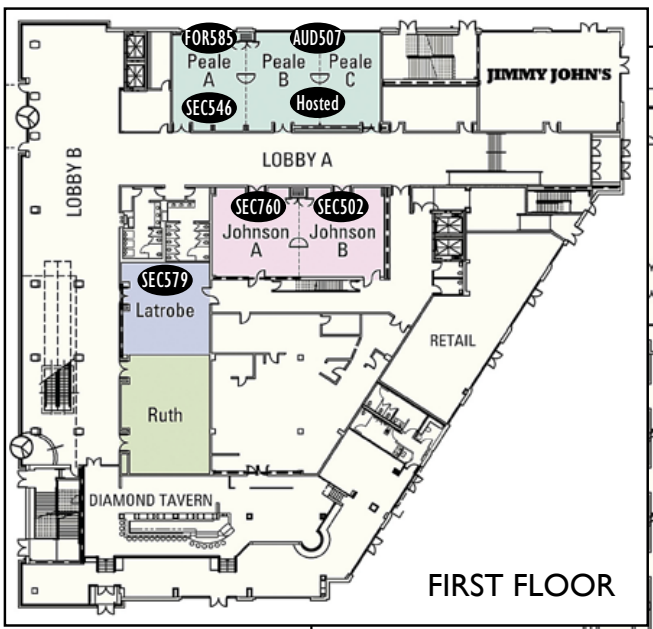
Lobby Bar *(5:00pm-1:00am)*
With its art décor layout and chic, metropolitan feel, the Lobby Bar is the ideal spot for cocktail hour, a casual meeting, or just people watching. Treat yourself to our specialty martinis and cocktails, made with the finest spirits and freshest ingredients, or a glass of wine from our esteemed selection. Cheers!

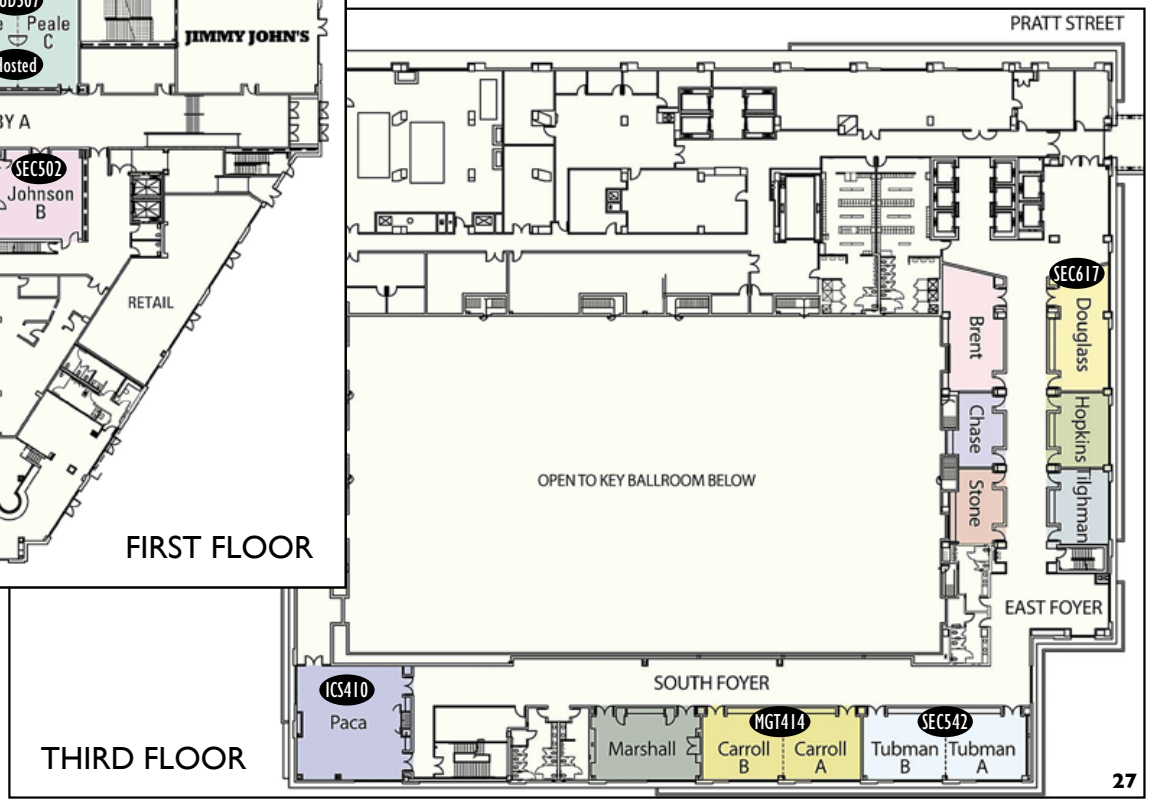
In-Room Dining *(6:00am-11:00pm)*
Experience restaurant dining in the comfort of your room. Enjoy breakfast, lunch, dinner or a late night snack carefully prepared by Hilton Baltimore's renowned culinary team. Whether it's food or a selection from our extensive wine list, In-Room Dining is quick, convenient and delicious!

Jimmy Johns
401 W Pratt St
Baltimore, MD 21201
Jimmyjohns.com
(410) 685-3377

HOTEL FLOORPLAN







Crystal City 2015

September 8-13 | sans.org/crystalcity

Courses offered:

SEC301: Intro to Information Security

SEC401: Security Essentials Bootcamp Style

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling

SEC566: Implementing and Auditing the Critical Security Controls

FOR408: Windows Forensic Analysis

MGT512: SANS Security Leadership Essentials For Managers

AUD507: Auditing & Monitoring Networks, Perimeters, and Systems

ICS410: ICS/SCADA Security Essentials

Baltimore 2015

September 21-26 | sans.org/baltimore

Courses offered:

SEC401: Security Essentials Bootcamp Style

SEC503: Intrusion Detection In-Depth

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling

SEC550: Active Defense, Offensive Countermeasures, and Cyber Deception

FOR526: Memory Forensics In-Depth

Save $400 by registering and completing payment early!

Tysons Corner 2015

October 12-17 | sans.org/tysonscorner

Courses offered:

SEC401: Security Essentials Bootcamp Style

SEC501: Advanced Security Essentials – Enterprise Defender

SEC503: Intrusion Detection In-Depth

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling

FOR508: Advanced Digital Forensics and Incident Response

FOR585: Advanced Smartphone Forensics

MGT414: SANS Training Program for CISSP® Certification

MGT514: IT Security Strategic Planning, Policy, and Leadership

Future SANS Training Events

SANS **Capital City** 2015
Washington, DC | July 6-11 | #SANSCapitalCity

SANS **Digital Forensics & Incident Response** SUMMIT
Austin, TX | July 7-14 | #DFIRSummit

SANS **San Jose** 2015
San Jose, CA | July 20-25 | #SANSSJ

SANS **Minneapolis** 2015
Minneapolis, MN | July 20-25 | #SANSmpls

SANS **Boston** 2015
Boston, MA | Aug 3-8 | #SANSBoston

SANS **Cyber Defense** SUMMIT & TRAINING
Nashville, TN | Aug 11-18 | #CyberDefenseSummit

SANS **San Antonio** 2015
San Antonio, TX | Aug 17-22 | #SANSSATX

SANS **Security Awareness** SUMMIT & TRAINING
Philadelphia, PA | Aug 17-25 | #SecAwareSummit

SANS **Virginia Beach** 2015
Virginia Beach, VA | Aug 24 - Sept 4 | #SANSVaBeach

SANS **Chicago** 2015
Chicago, IL | Aug 30 - Sept 4 | #SANSChicago

SANS **Crystal City** 2015
Crystal City, VA | Sept 8-13 | #SANSCrystalCity

SANS **Network Security** 2015
Las Vegas, NV | Sept 12-21 | #SANSNetworkSecurity

SANS **Baltimore** 2015
Baltimore, MD | Sept 21-26

SANS **Cyber Crime** SUMMIT & TRAINING
Dallas, TX | Sept 21-26

SANS **Seattle** 2015
Seattle, WA | Oct 5-10 | #SANSSeattle

SANS **Tysons Corner** 2015
Tysons Corner, VA | Oct 12-17 | # SANSTysonsCorner

SANS **Cyber Defense San Diego** 2015
San Diego, CA | Oct 19-24 | #CyberDefSD

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