SANS FIRE 2014

PROGRAM GUIDE

Baltimore, MD

June 21-30, 2014

Powered by

INTERNET STORM CENTER

@SANSInstitute | #SANSFIRE

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!
www.sans.org/event/sansfire-2014/schedule

SANS DFIR

Hosted by Rob Lee
Thursday, June 26 and Friday, June 27
6:30pm-9:30pm | Francis Scott Key 7

CORE NETWARS TOURNAMENT

Hosted by Jeff McJunkin & Tim Medin
Thursday, June 26 and Friday, June 27
6:30pm-9:30pm | Francis Scott Key 5 & 6

GENERAL INFORMATION

Registration and Courseware Pick-up Information

Location: South Foyer (Level 2)

Saturday, June 21 (Short Courses Only) 8:00am-9:00am
Sunday, June 22 (Short Courses Only) 8:00am-9:00am
Sunday, June 22 (Welcome Reception) 5:00pm-7:00pm
Monday, June 23 . . . . . 7:00am-5:30pm
Tuesday, June 24 - Saturday, June 28 . . . . . 8:00am-5:30pm
Sunday, June 29 . . . . . 8:00am-9:00am
Monday, June 30 . . . . . 8:00am-9:00am (Closes)

Internet Café *(WIRED & WIRELESS)*

Location: West Foyer (Level 2)
Printer will be available for students' use

Monday, June 23 . . . . . Opens at noon - 24 hours
Tuesday, June 24 - Friday, June 27 . . . . . Open 24 hours
Saturday, June 28 . . . . . Closes at 2:00pm

Course Times

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

Course Breaks

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, June 23** at the General Session in **Billie Holiday 6**

GENERAL INFORMATION

Dining Options

We have assembled a short list of dining suggestions you may like to try during lunch breaks. See page 15 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 #SANSFIRE 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 and course ticket 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)

MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam

SEC401: Security Essentials Bootcamp Style

SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking

Extended Hours:

MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™

SEC504: Hacker Techniques, Exploits & Incident Handling

SEC560: Network Penetration Testing and Ethical Hacking

COURSE SCHEDULE

START DATE: **Saturday, June 21**

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

SEC546: IPv6 Essentials
Instructor: Johannes Ullrich, Ph.D. . . . . Location: Billie Holiday 1

MGT433: Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program
Instructor: Lance Spitzner . . . . . Location: Billie Holiday 2

HOSTED: Onapsis: Securing SAP Platforms – Hands-on Security Techniques to Protect Business-Critical Infrastructure from Cyber-attacks
Instructors:
Juan Perez-Etchegoyen, Marc Roy. . . . . Location: Billie Holiday 4

HOSTED: Physical Penetration Testing – Introduction
Instructor: Deviant Ollam. . . . . Location: Billie Holiday 5

START DATE: **Sunday, June 22**

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

MGT305: Technical Communication and Presentation Skills for Security Professionals
Instructor: David Hoelzer. . . . . Location: Peale A

MGT415: A Practical Introduction to Risk Assessment
Instructor: James Tarala. . . . . Location: Peale B & C

MGT535: Incident Response Team Management
Instructor: Christopher Crowley. . . . . Location: Billie Holiday 6

START DATE: **Monday, June 23**

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

SEC301: Intro to Information Security
Instructor: Fred Kerby . . . . . Location: Francis Scott Key 2

SEC401: Security Essentials Bootcamp Style
Instructor: Dr. Eric Cole . . . . . Location: Billie Holiday 4
Bootcamp Hours: 5:00pm-7:00pm (Course days 1-5)

SEC501: Advanced Security Essentials – Enterprise Defender
Instructor: Ted Demopoulos . . . . . Location: Francis Scott Key 10

SEC503: Intrusion Detection In-Depth
Instructor: Mike Poor. . . . . Location: Francis Scott Key 8

SEC504: Hacker Techniques, Exploits, and Incident Handling
Instructor: John Strand. . . . . Location: Francis Scott Key 6
Extended Hours: 5:00pm-6:30pm (Course Day 1 only)

SEC505: Securing Windows with the Critical Security Controls
Instructor: Jason Fossen. . . . . Location: Francis Scott Key 12

COURSE SCHEDULE

SEC506: Securing Linux/Unix
Instructor: Hal Pomeranz. . . . . Location: Calloway A & B

SEC542: Web App Penetration Testing & Ethical Hacking
Instructor: Seth Misenar . . . . . Location: Billie Holiday 6

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

SEC561: Intense Hands-on Pen Testing Skill Development
Instructor: Joshua Wright. . . . . Location: Tubman A & B

SEC566: Implementing and Auditing the Critical Security Controls – In-Depth
Instructor: James Tarala . . . . . Location: MARRIOTT: University 1 & 2

SEC573: Python for Penetration Testers
Instructor: Mark Baggett . . . . . Location: Billie Holiday 3

SEC575: Mobile Device Security and Ethical Hacking
Instructor: Christopher Crowley . . Location: Francis Scott Key 4

SEC579: Virtualization and Private Cloud Security
Instructor: Dave Shackleford . . . . . Location: Caroll A & B

SEC642: Advanced Web App Penetration Testing and Ethical Hacking
Instructor: Justin Searle . . . . . Location: Peale A

SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking
Instructor: Stephen Sims . . . . . Location: Francis Scott Key 1
Bootcamp Hours: 5:15pm-7:00pm (Course days 1-5)

DEV522: Defending Web Applications Security Essentials
Instructor: Johannes Ullrich, Ph.D. . . . . Location: Johnson B

DEV541: Secure Coding in Java/JEE: Developing Defensible Applications
Instructors: Frank Kim, Megan Restuccia
Location: MARRIOTT: Grand Ballroom Salon DE

FOR408: Windows Forensic Analysis
Instructor: Rob Lee . . . . . Location: Francis Scott Key 7

FOR508: Advanced Computer Forensic Analysis and Incident Response
Instructor: Chad Tilbury . . . . . Location: Billie Holiday 5

FOR572: Advanced Network Forensics and Analysis
Instructor: Philip Hagen. . . . . Location: Peale B & C

FOR585: Advanced Smartphone Forensics
Instructor: Heather Mahalik . . . . . Location: Francis Scott Key 3

COURSE SCHEDULE

START DATE: **Monday, June 23** (CONTINUED)

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

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Instructor: Lenny Zeltser . . . . . Location: Francis Scott Key 9

MGT414: SANS® +S™ Training Program for the CISSP® Cert Exam
Instructor: Eric Conrad . . . . . .Location: Billie Holiday 1
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: Francis Scott Key 11
Extended Hours: 5:00pm – 6:00pm (Course days 1-4)

MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep
Instructor: Jeff Frisk . . . . . Location: MARRIOTT: University 3 & 4

AUD507: Auditing Networks, Perimeters, and Systems
Instructor: David Hoelzer. . . . . .Location: Johnson A

LEG523: Law of Data Security and Investigations
Instructor: Benjamin Wright . . . . . .Location: Billie Holiday 2

ICS410: ICS/SCADA Security Essentials
Instructor: Paul A. Henry . . . . . Location: Paca A & B

HOSTED: (ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program
Instructor: EJ Jones . . . . . .Location: Tilghman

START DATE: **Thursday, June 26**

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

DFIR NetWars Tournament
Host: Rob Lee . . . . . Location: Francis Scott Key 7
Hours: 6:30pm-9:30pm

Core NetWars Tournament
Hosts: Jeff McJunkin, Tim Medin . . . . . Location: Frances Scott Key 5 & 6
Hours: 6:30pm-9:30pm

START DATE: **Sunday, June 29**

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

SEC580: Metasploit Kung Fu for Enterprise Pen Testing
Instructor: Eric Conrad . . . . . Location: Peale B & C

SPECIAL576: CyberCity Hands-on Kinetic Cyber Range Exercise for the InfoSec Pro
Instructor: Tim Medin . . . . . .Location: Peale A

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, JUNE 22

Registration Welcome Reception

Sunday, June 22 | 5:00pm-7:00pm | Location: South Foyer

Register early and network with your fellow students!

MONDAY, JUNE 23

General Session - Welcome to SANS

Speaker: Johannes Ullrich, Ph.D.

Monday, June 23 | 8:15am-8:45am | Location: Billie Holiday 6

SANS Technology Institute Open House

Speaker: William Lockhart

Monday, June 23 | 6:00pm-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. 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

State of the Internet Panel Discussion

Moderators: Johannes Ullrich, Ph.D. & Marcus Sachs

Panelists: Rob VandenBrink, Russ McRee, Manuel Humberto Santander Palaez, Richard Porter, and Adrien de Beaupre

Monday, June 23 | 7:15pm-9:15pm | Location: Billie Holiday 6

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 24

Online Reception

Tuesday, June 24 | 6:00pm-8:00pm | Location: Fitness Center Patio

Join the SANS Online Training team for a bird's eye view of the Orioles vs. White Sox game from the Hilton Fitness Center Patio on Tuesday night. Only 50 guests are allowed in this space, so we'll be giving away 'tickets' in the Registration area at noon on Monday. Swing by to put your name on the guest list!

SANS@NIGHT

Security Awareness Metrics: Measuring Human Behavior

Speaker: Lance Spitzner

Tuesday, June 24 | 7:15pm-8:15pm | Location: Billie Holiday 6

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

C3CM Defeating the Command, Control, and Communications of Digital Assailants

Speaker: Russ McRee

Tuesday, June 24 | 8:15pm-9:15pm | Location: Francis Scott Key 5

C3CM: the acronym for command, control, and communications countermeasures. Ripe for use in the information security realm, C3CM takes us past C2 analysis and to the next level. Initially, C3CM was most often intended to wreck the command and control of enemy air defense networks, a very specific military mission. We'll apply that mindset in the context of combating bots and other evil. Our version of C3CM therefore is to identify, interrupt, and counter the command, control, and communications capabilities of our digital assailants. The three phases of C3CM will utilize: Nfsight with Nfdump, Nfsen, and fprobe to conduct our identification phase, Bro with Logstash and Kibana for the interruption phase, and ADHD for the counter phase.

Converge these on one useful platform and you too might have a chance to deter those who would do you harm. We'll discuss each of these three phases (identify, interrupt, and counter) with tooling and tactics, complete with demonstrations and methodology attendees can put to use in their environments. Based on the three-part ISSA Journal Toolsmith series http://holisticinfosec.blogspot.com/search?q=c3cm&max-results=20&by-date=true

SPECIAL EVENTS

SANS@NIGHT

Avoiding Cyberterrorism Threats Inside Electrical Substations

Speaker: Manuel Humberto Santander Pelez

Tuesday, June 24 | 7:15pm-8:15pm | Location: Francis Scott Key 5

The IEC61850 protocol is widely used for automation of operation inside electrical substations and it is also used for replacement of the communications between protection relays by replacing the method of using analog inputs/outputs and wires for communications by GOOSE (Generic Object Oriented Substation Events) messages over Ethernet cables. Since most ICS/SCADA systems inside electrical substations are being modernized, protocols and devices use ethernet and IP and so are prone to several vulnerabilities. In this presentation we will discuss the vulnerabilities of protocol IEC 61850 and how to remediate them.

SANS@NIGHT

Securing The Kids

Speaker: Lance Spitzner

Tuesday, June 24 | 8:15pm-9:15pm | Location: Billie Holiday 6

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.

WEDNESDAY, JUNE 25

Vendor Solutions Expo

Wednesday, June 25 | 12:00pm-1:30pm | 5:00pm-7:00pm

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!

SPECIAL EVENTS

STI MASTER'S PRESENTATION

Setting up Splunk for Event Correlation in Your Home Lab

Speaker: Aron Warren – Master's Degree Candidate

Wednesday, June 25 | 7:15pm-7:55pm | Location: Francis Scott Key 12

Splunk is an ideal event correlation instrument for use in large enterprise environments down to small home laboratory networks such as those used by students. Splunk's appeal has grown over the past few years due to a number of factors: speed and amount of collectable data, a growing user base as well as new ways of exploiting its capabilities are discovered. This presentation will outline a student research home network Splunk installation including Internet taps, infrastructure used, query creation, and finally pulling multiple data sources together to track security events.

SANS@NIGHT

An Introduction to PowerShell for Security Assessments

Speaker: James Tarala

Wednesday, June 25 | 7:15pm-8:15pm | Location: Billie Holiday 6

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.

SANS@NIGHT

Consulting from Virtual Island

Speaker: Rob VandenBrink

Wednesday, June 25 | 8:15pm-9:15pm | Location: Billie Holiday 6

In this session, we'll discuss using a virtualization in a consulting practice as well as how typical data center concerns "scale down" in this environment. The importance of change control and testing is doubly important in a small software defined data center such as this, even if the data center administrator is also the only user on the system – segregation of test and experimental functions from "production" will also be covered in some detail. In addition, we'll discuss considerations, workarounds, and pitfalls when splitting workload off for remote workload execution, using commodity server hardware, remote laptops or providing virtual appliances for execution within your customer's virtual environment.

THURSDAY, JUNE 26

CORE NETWARS TOURNAMENT

Hosts: Jeff McJunkin & Tim Medin

Thu, June 26 & Fri, June 27 | 6:30pm-9:30pm | Location: F.S. Key 5 & 6

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 DFIR NETWARS TOURNAMENT

Host: Rob Lee

Thu, June 26 & Fri, June 27 | 6:30pm-9:30pm | Location: F.S. 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.

SANS@NIGHT

Penetration Testing Corporate Mobile Applications and BYOD Environments

Speaker: Dmitry Dessiatnikov

Thursday, June 26 | 7:15pm-8:15pm | Location: Billie Holiday 6

The explosion of the mobile application market coupled with acceptance of "bring your own device" (BYOD) to enterprise environments comes with its unique security risks. While driven by a rise in productivity, convenience and overall user satisfaction BYOD increases the attack surface that most businesses are not prepared for. In this presentation we will cover the reasons for penetration testing BYOD environments along with a demonstration of a remote compromise of an Android phone in a corporate environment. We will also discuss the OWASP top 10 mobile risks and demonstrate some common issues with a vulnerable iOS mobile application. A free tool will be shared with the audience that can assist with assessing their corporate BYOD environments. Finally, we will cover some mitigating controls and what can be done to address raised issues.

SANS@NIGHT

How to Spy on your Employees with Memory Forensics

Speaker: Alissa Torres

Thursday, June 26 | 7:15pm-8:15pm | Location: Francis Scott Key 8

Many companies can't afford employee endpoint monitoring software such as SpectorPro, and yet still have the need to figure out how a rogue employee is spending his time on the job. Consider a cheaper solution for employee spying- one that makes use of native Windows services and an investigator's ninja memory analysis skills. Whether it be creating a scheduled task to send a machine to hibernate or instantiating an unsuspected memory dump, targeted employee spying can be done on the cheap. Through process enumeration, browsing history reconstruction and memory-mapped file extraction, watch as your presenters piece together what our trusted insider was doing on their company computer, unbeknownst to his boss. Even if you don't have the need to covertly investigate a rogue employee (yet), this talk will arm you the knowledge to know what is within the realm of the possible.

GIAC Program Overview

Speaker: Jeff Frisk

Thursday, June 26 | 8:15pm-8:45pm | 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.

SANS@NIGHT

Bust a Cap in a Web App With ZAP

Speaker: Adrien de Beaupre

Thursday, June 26 | 8:15pm-9:15pm | Location: Billie Holiday 6

The Zed Attack Proxy (ZAP) is the Open Web Application Security Project's (OWASP) flagship testing tool. This presentation will describe the why and how of attacking your own web-based applications with ZAP. The presentation will include a walk-through of the web application testing methodology where ZAP is used as the attack tool.

SPECIAL EVENTS

FRIDAY, JUNE 27

SANS@NIGHT

The "Insider Threat" Revised: Crime, Understanding, and Prediction

Speaker: Richard Porter

Friday, June 27 | 7:15pm-8:15pm | Location: Billie Holiday 6

In a world of continuous breaches by outsiders where have all the insiders gone? Most security professionals have always stated: Insiders are the worst threat! Are insiders still a threat? Using current literature and research as a foundation, this talk will discuss the current insider threat and risks. We will also discuss more human topics that relate to insider risks such as loyalty, trustworthiness, and betrayal. This talk will focus on motivations, risks, and potential warnings.

SANS@NIGHT

Creating a Covert Channel in WiFi

Speaker: Ronald Hamann

Friday, June 27 | 7:15pm-8:15pm | Location: Francis Scott Key 8

Most covert channels appear somewhere – firewall logs, IDSs, PCAP files, etc. This session will focus on using untracked, unlogged wifi packets to communicate with other devices and transport data all under IDS radar.

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

VENDOR EVENTS

Vendor Solutions Expo

Wed, June 25 | 12:00pm-1:30pm | 5:00pm-7:00pm
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 25 | 5:00pm-7:00pm | 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 25 | 12:00pm-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:

Beyond Trust
Duo Security
Emulex
Event Tracker
FireEye
Forescout
General Dynamics Fidelis Cybersecurity
iScanOnline
LogRhythm
PhishMe
Rapid7
Threat Track

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.

Looking Beyond Layers: Why Authentication Security Matters Most

Tuesday, June 24 | 12:30pm-1:15pm | Location: Francis Scott Key 11

Traditionally, "tried-and-true" security wisdom tells us that tough perimeter controls, defense-in-depth, threat-intelligence feeds, and all manner of security-point products are the solutions to all our problems. However, as we've seen time and time again, breaches still happen, credentials still get lifted, and chaos ensues. Yet there's still hope – authentication security is a viable avenue for making a huge impact against an attacker's sphere of influence and lateral movement capabilities. In this presentation, we will highlight some examples where two-factor authentication provided the key defense for disrupting attacks.

Understanding the Threat: A Model to Enable Active Response

Speaker: Finn Ramsland, Solutions Architect, Federal
Tuesday, June 24 | 12:30pm-1:15pm | Location: Francis Scott Key 8

With the ever growing volume and complexity of modern cyber attacks, defenders increasingly find themselves playing catch up. During this session we will dive into several recent campaigns uncovered by FireEye (to include the Digital Quartermaster and Operation Clandestine Fox) in an effort to better understand adversary techniques and methods. Following the campaign review, findings will be pulled together into a cohesive vision and data analytics model which helps facilitate active defense.

Using Intelligence Methods in Mobile Forensic Exams

Speaker: Lee Papathanasiou, Sales Engineer, Cellebrite
Tuesday, June 24 | 12:30pm-1:15pm | Location: Francis Scott Key 6

Investigators benefit from knowing their suspects' and victims' key patterns of life, including timelines, locations and people, before, during and after an incident. Discerning these patterns can be painstaking as you conduct your interviews. In this session, learn what mobile device usage can reveal about victims, suspects, and where their paths cross.

VENDOR EVENTS

EMULEX

The Power of Lossless Packet Capture (1G-100G) & Real-Time Netflow

Speaker: Sam Cook, Senior Sales Engineer

Tuesday, June 24 | 12:30pm-1:15pm | Location: Francis Scott Key 9

With network speeds of 10G, 40G, and even 100G now deployed in many production environments, organizations are finding it harder than ever to maintain the level of network visibility they were used to seeing at 1G. Furthermore, many commercial and open source network & security tools do not scale well at these higher data rates. Finding the root cause problem to security and network issues is now taking longer and incident response times are increasing, not decreasing. This Endace presentation will cover the benefits of a security architecture that incorporates a high-speed loss-less packet capture fabric and the generation of real-time Netflow data to improve network visibility, decrease incident response time, and better aid in the identification of root cause issues many organizations are facing today.

ForeScout
BE A GAME CHANGER

Continuous Monitoring & Mitigation

Speaker: Tim Jones, Systems Engineer

Tuesday, June 24 | 12:30pm-1:15pm | Location: Francis Scott Key 10

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.

PHISHME

Resurrection of the Data Entry Attack

Speaker: Aaron Higbee, Chief Technology Officer & Co-Founder

Tuesday, June 24 | 12:30pm-1:15pm | Location: Francis Scott Key 12

Since the 1990's, data entry-based attacks have been utilized to social engineer credentials from users for network access. There was a period of time when they were forgotten or overlooked by information security teams due to the prevalence of Trojans, worms, DDoS, and other malware attacks. Well, data entry attacks are back in fashion as reported in recent high-profile breaches. This session will provide some history, highlight examples, and demonstrate the latest techniques to develop and detect data entry-based phishing attacks.

TANIUM™

Thursday, June 26 | 12:30pm-1:15pm | Location: Francis Scott Key 10

tripwire

Thursday, June 26 | 12:30pm-1:15pm | Location: Francis Scott Key 12

VENDOR EVENTS

FORTINET Infogressive, Inc. Aggressive Information Security

Fortinet Next Generation Firewalls

Speaker: Jeff Eckley, Sales Manager, Infogressive

Thursday, June 26 | 12:30pm-1:15pm | Location: Billie Holiday 4

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.

beyondtrust
Beyond Traditional Security

Vile Vulnerabilities, Rampant Rights, and Pervasive Passwords

Speaker: Paul Harper, Product Manager

Thursday, June 26 | 12:30pm-1:15pm | Location: Billie Holiday 2

Come scarf down a sandwich, and see a symbiotic suite of solutions for tackling this trifecta of threats! You'll see BeyondTrust's Retina and PowerBroker solutions for vulnerability, privilege and password management – and learn how they work together to pinpoint security exposures, enforce least-privilege policies, and control account access.

GENERAL DYNAMICS
Fidelis Cybersecurity Solutions

Operationalize Open Intelligence – YARA + Fidelis XPS

Speaker: Mike Nichols

Thursday, June 26 | 12:30pm-1:15pm | Location: Billie Holiday 6

Yara is an excellent content identification and classification system used by malware analysts and reverse engineers to apply signatures to data-at-rest and identify or discover malicious files. A new way of discovery and detection can be harnessed by using a granular application of Yara signatures to data-in-motion as it transits your network to prevent the threat from reaching the end user.

tenable network security

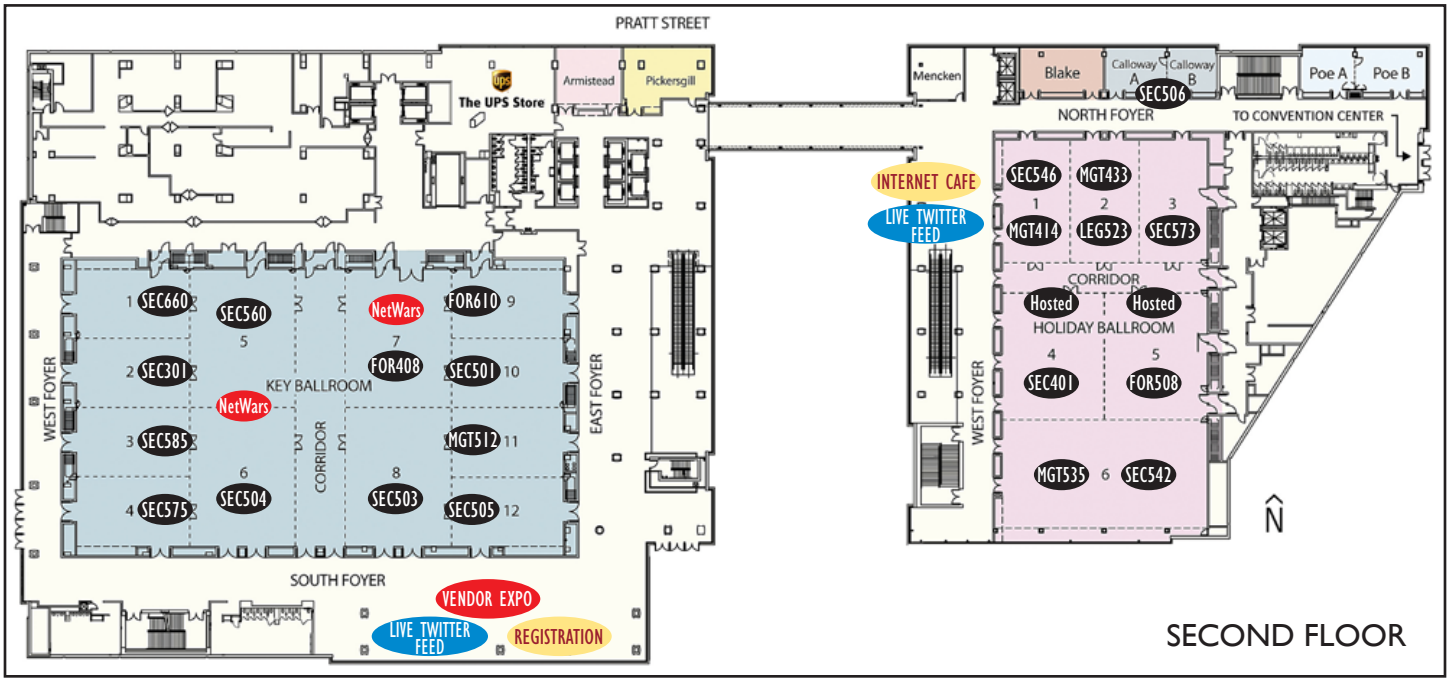
Effective Forensics Analytics for Actionable Incident Response

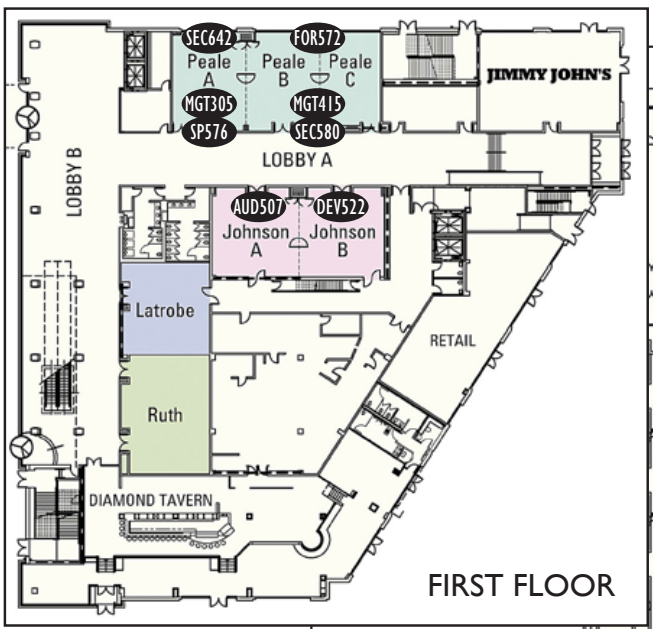
Speaker: Mr. Narayan Makaram

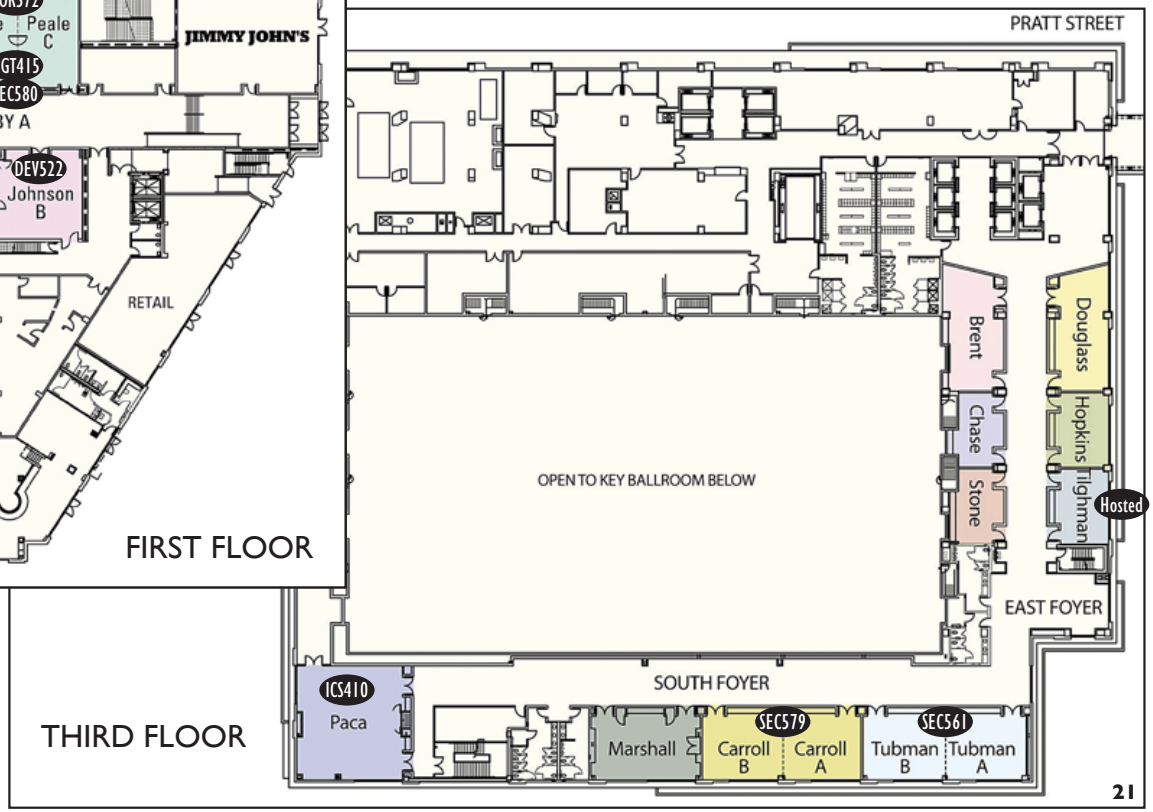
Thursday, June 26 | 12:30pm-1:15pm | Location: Billie Holiday 3

Advanced targeted attacks can easily go undetected without continuous visibility into vulnerabilities and real-time threats to your IT infrastructure. Detecting such attacks can be difficult, and even when they are detected you need the right information to respond to these security incidents. In this presentation, you will learn about the digital forensics data and analytics required at the host and network level to respond to such attacks, and how Tenable's comprehensive network security solutions enables you to gather actionable digital forensics to respond to security incidents.

HOTEL FLOORPLAN







Future SANS Training Events

SANS **Capital City** 2014
Washington, DC | July 7-12 | #SANSCapitalCity

SANS **San Francisco** 2014
San Francisco, CA | July 14-19 | #SANSsf

ICS Security Training – Houston
Houston, TX | July 21-25 | #SANSICSHouston

SANS **Boston** 2014
Boston, MA | July 28 - August 2 | #SANSBoston

SANS **DHS Continuous Diagnostics and Mitigation**
WORKSHOP WITH TRAINING
Washington, DC | August 1-8

SANS **San Antonio** 2014
San Antonio, TX | August 11-16 | #SANSSanAntonio

Cyber Defense SUMMIT & TRAINING
Nashville, TN | August 13-20 | #CyberDefSummit

SANS **Virginia Beach** 2014
Virginia Beach, VA | August 18-29 | #SANSVaBeach

SANS **Chicago** 2014
Chicago, IL | August 24-29 | #SANSChicago

SANS **Crystal City** 2014
Crystal City, VA | September 8-13 | #SANSCrystalCity

Retail Cyber Security SUMMIT & TRAINING
Dallas, TX | September 8-17

Security Awareness SUMMIT & TRAINING
Dallas, TX | September 8-17

SANS **Albuquerque** 2014
Albuquerque, NM | September 15-20 | #SANSABQ

SANS **Baltimore** 2014
Baltimore, MD | September 22-27 | #SANSBaltimore

SANS **Seattle** 2014
Seattle, WA | Sept 29 - Oct 6 | #SANSSeattle

SANS **Network Security** 2014
Las Vegas, NV | October 19-27 | #SANSNetworkSecurity

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