SANS FIRE 2013

PROGRAM GUIDE

June 15-22, 2013
Washington, DC

Powered by

Table of Contents

SANS School Store Hours

Location: Columbia 1/2

Tuesday, June 18	10:30am-1:30pm & 3:00pm-6:00pm
Wednesday, June 19	10:30am-1:30pm & 3:00pm-6:00pm
Thursday, June 20	10:30am-1:30pm & 3:00pm-6:00pm
Friday, June 21	10:30am-1:30pm & 3:00pm-6:00pm
Saturday, June 22	10:30am-1:30pm (Closes)

Here are a few of the items you can find for sale in the School Store:

STI Fleece	ISC Messenger Bag	Baseball Caps
Travel Mugs	Water Bottles	Polos
Large Selection of Published Books	Mouse Pads	Sweatshirts
	Wireless Cards	Teensy 2.0 Development Board
T-shirts	Cable Locks	

RECEIVE A FREE GIFT!

Spend $100 or more and receive a free gift with your purchase while supplies last!

Registration Information

Location: Terrace Lobby

Saturday, June 15 (Short Courses Only) . . . . . 8:00am - 9:00am
Sunday, June 16 (Short Courses Only) . . . . . 8:00am - 9:00am
Sunday, June 16 (Early Popcorn Registration – Int'l Terrace Foyer) . . 5:00pm - 7:00pm
Monday, June 17 . . . . . 7:00am - 5:30pm
Tuesday, June 18 . . . . . 8:00am - 7:30pm
Wednesday, June 19 – Friday, June 21 . . . . . 8:00am - 5:30pm
Saturday, June 22 . . . . . 8:00am - 2:00pm (Closes)

Courseware Pick-up Information

Location: Columbia 1/2

Saturday, June 15 (Short Courses Only) . . . . . 8:00am - 9:00am
Sunday, June 16 (Short Courses Only) . . . . . 8:00am - 9:00am
Sunday, June 16 (Early Popcorn Registration – Int'l Terrace Foyer) . . 5:00pm - 7:00pm
Monday, June 17 (Int'l Terrace Foyer) . . . . . 7:00am - 5:30pm
Tuesday, June 18 . . . . . 10:30am-1:30pm & 3:00pm-6:00pm
Wednesday, June 19 . . . . . 10:30am-1:30pm & 3:00pm-6:00pm
Thursday, June 20 . . . . . 10:30am-1:30pm & 3:00pm-6:00pm
Friday, June 21 . . . . . 10:30am-1:30pm & 3:00pm-6:00pm
Saturday, June 22 . . . . . 10:30am-1:30pm (Closes)

SANS School Store Information

Location: Columbia 1/2

Tuesday, June 18 . . . . . 10:30am-1:30pm & 3:00pm-6:00pm
Wednesday, June 19 . . . . . 10:30am-1:30pm & 3:00pm-6:00pm
Wednesday, June 19 . . . . . 10:30am-1:30pm & 3:00pm-6:00pm
Thursday, June 20 . . . . . 10:30am-1:30pm & 3:00pm-6:00pm
Friday, June 21 . . . . . 10:30am-1:30pm & 3:00pm-6:00pm
Saturday, June 22 . . . . . 10:30am-1:30pm (Closes)

Internet Café *(WIRED & WIRELESS)*

Location: International Terrace Foyer
Printer will be available for students' use

Monday, June 17 . . . . . Opens at noon - 24 hours
Tuesday, June 18 – Friday, June 21 . . . . . Open 24 hours
Saturday, June 22 . . . . . 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

General Information

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 17, at the General Session in Int'l Ballroom Center .

Dining Options

We have assembled a short list of dining suggestions you may like to try during lunch breaks. See page 17 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

You can post open invites to lunch, dinner or other outings. Located on the bulletin board on the Terrace Level near the Registration Desk.

Wear Your Badge and Course Ticket Daily

To make sure you are in the right place, the SANS door monitors will be checking your badge and course tickets 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 Crystal Foyer.

Bootcamp Sessions and Extended Hours

The following classes have evening bootcamp sessions or extended hours. For specific times, please refer to pages 4-5.

Bootcamps (Attendance Mandatory)

MGT414: SANS® +S™ Training Program for the CISSP® Cert Exam
SEC401: Security Essentials Bootcamp Style
SEC660: Advanced Penetration Testing, Exploits & 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
Special: (ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program

Course Schedule

Six-Day Courses

Monday, June 17 – Saturday, June 22

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

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

DEV522: Defending Web Applications Security Essentials
Instructor: Jason Lam ..... Location: Oaklawn

FOR408: Computer Forensic Investigations – Windows In-Depth
Instructor: Paul A. Henry ..... Location: Jefferson West

FOR508: Advanced Computer Forensic Analysis & Incident Response
Instructor: Rob Lee ..... Location: Int'l Ballroom West

MGT414: SANS® +S™ Training Program for the CISSP® Cert Exam
Instructor: Eric Conrad ..... Location: Columbia Hall 4
Bootcamp Hours: 8:00am – 9:00am (Course days 2-6) &
5:15pm - 7:00pm (Course days 1-5)

MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep
Instructor: Jeff Frisk ..... Location: Columbia Hall 11

SEC401: SANS Security Essentials Bootcamp Style
Instructor: Dr. Eric Cole ..... Location: Lincoln
Bootcamp Hours: 5:15pm - 7:00pm (Course days 1-5)

SEC501: Advanced Security Essentials - Enterprise Defender
Instructor: Bryce Galbraith ..... Location: Columbia Hall 12

SEC503: Intrusion Detection In-Depth
Instructor: Mike Poor ..... Location: Columbia Hall 6

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

SEC505: Securing Windows and Resisting Malware
Instructor: Jason Fossen ..... Location: Columbia Hall 5

SEC506: Securing Linux/Unix
Instructor: Hal Pomeranz ..... Location: Kalorama

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

SEC560: Network Penetration Testing and Ethical Hacking
Instructor: Ed Skoudis ..... Location: Int'l Ballroom Center
Extended Hours: 5:00pm-6:30pm (Course Day 1 only)

SEC575: Mobile Device Security and Ethical Hacking
Instructors: Joshua Wright, Tim Medin .... Location: Columbia Hall 9/10

Course Schedule

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

SEC617: Wireless Ethical Hacking, Penetration Testing & Defenses
Instructor: Larry Pesce ..... Location: DuPont

SEC642: Advanced Web App Penetration Testing & Ethical Hacking
Instructor: Kevin Johnson ..... Location: Columbia Hall 3

SEC660: Advanced Penetration Testing, Exploits & Ethical Hacking
Instructor: Stephen Sims ..... Location: Fairchild
Bootcamp Hours: 5:00pm-7:00pm (Course days 1-5)

Five-Day Courses

Monday, June 17 – Friday, June 21

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

FOR526: Windows Memory Forensics In-Depth
Instructor: Alissa Torres ..... Location: L'Enfant

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Instructor: Lenny Zeltser ..... Location: Columbia Hall 8

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

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

MGT514: IT Security Strategic Planning, Policy and Leadership
Instructor: Stephen Northcutt ..... Location: Gunston

SEC301: Intro to Information Security
Instructor: Fred Kerby ..... Location: Georgetown East

SEC566: Implementing and Auditing the Twenty Critical Security Controls – In-Depth
Instructor: James Tarala ..... Location: Columbia Hall 7

SEC573: Python for Penetration Testers
Instructor: Mark Baggett ..... Location: Jay

HOSTED: (ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program
Instructor: Frank Shirmo ..... Location: Northwest
Extended Hours: 5:00pm – 6:00pm (Course days 1-5)

HOSTED: Critical Infrastructure and Control System Cybersecurity
Instructor: Matthew Luallen ..... Location: Independence

Course Schedule

Four-Day Courses

Monday, June 17 – Thursday, June 20
Time: 9:00am – 5:00pm

DEV541: Secure Coding in Java/JEE: Developing Defensible Apps
Instructor: Srinidhi Mallur .....Location: Embassy

DEV544: Secure Coding in .NET: Developing Defensible Apps
Instructor: James Jardine .....Location: Piscataway

Two-Day Courses

Saturday, June 15 – Sunday, June 16
Time: 9:00am – 5:00pm

MGT433: Securing the Human: Building and Deploying an Effective Security Awareness Program
Instructor: Lance Spitzner.....Location: Columbia Hall 4

SEC524: Cloud Security Fundamentals
Instructor: Dave Shackleford .....Location: Columbia Hall 8

SEC546: IPv6 Essentials
Instructor: Dr. Johannes Ullrich..... Location: Columbia Hall 9/10

SEC580: Metasploit Kung Fu for Enterprise Pen Testing
Instructor: Eric Conrad .....Location: Columbia Hall 3

HOSTED: Offensive Countermeasures: The Art of Active Defenses
Instructor: John Strand .....Location: Columbia Hall 6

HOSTED: Physical Penetration Testing - Introduction
Instructor: Deviant Ollam .....Location: Columbia Hall 7

One-Day Courses

Saturday, June 15
Time: 9:00am – 5:00pm

MGT535: Incident Response Team Management
Instructor: Christopher Crowley .....Location: Columbia Hall 5

Sunday, June 16
Time: 9:00am – 5:00pm

MGT305: Technical Communication and Presentation Skills for Security Professionals
Instructor: G. Mark Hardy .....Location: Columbia Hall 11

MGT415: A Practical Introduction to Risk Assessment
Instructor: James Tarala .....Location: Columbia Hall 12

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 16

Registration Popcorn Reception

Sunday, June 16 | 5:00pm - 7:00pm
Location: International Terrace Foyer

Register early and network with your fellow students!

MONDAY, JUNE 17

Welcome to SANS General Session

Speaker: Dr. Eric Cole
Monday, June 17 | 8:15am - 8:45am
Location: International Ballroom Center

KEYNOTE

State of the Internet Panel Discussion

Moderators: Dr. Johannes Ullrich & Marcus Sachs

Panelists: Richard Porter, Jim Clausing, Rob VandenBrink, Russ McRee, Manuel Humberto Santander Palaez, and Jason Lam
Monday, June 17 | 7:15pm - 9:15pm
Location: International Ballroom Center

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 18

Vendor Expo

Tuesday, June 18 | 12:00pm - 1:30pm and 5:00pm - 7:00pm
Location: International Terrace and Columbia 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

Tuesday, June 18 | 5:00pm - 7:00pm
Location: International Terrace

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 to win exciting prizes.

Book Signing – SANS Published Authors

Tuesday, June 18 | 6:00pm - 6:30pm
Location: International Terrace & Columbia Foyer

Dr. Eric Cole, Eric Conrad, Seth Misenar, Paul A. Henry, Dave Shackleford, Ed Skoudis, Josh Wright, and Lenny Zeltser are not only top SANS instructors and industry leaders – they are published authors too! Bring your own copy of their best-selling titles or purchase one on-site, and get the author's autograph during our SANS Author Book Signing.

TUESDAY, JUNE 18

SANS @NIGHT

Memory Analysis with Volatility

Speaker: Russ McRee

Tuesday, June 18 | 7:15pm - 8:15pm | Int'l Ballroom Center

This discussion will cover the complete life cycle of memory acquistion and analysis for forensics and incident response, using Volatility. Volatility has been referred to as the Python version of the Windows Internals book, given how much can be learned about Windows by reviewing how Volatility enumerates evidence. We'll conduct real-time analysis and examine Volatility's plug-in capabilities. The Volatility project shortens the amount of time it takes to put cutting-edge research into the hands of practitioners, while encouraging and pushing the technical advancement of the digital forensics field. Join us and learn more about this outstanding tool.

SANS @NIGHT

Offensive Digital Forensics

Speaker: Alissa Torres

Tuesday, June 18 | 7:15pm - 8:15pm | Int'l Ballroom East

Network intruders are utilizing sophisticated offensive forensic techniques to parse remote systems, obtain credentials, and locate and steal "target data". Incident responders and forensic examiners must be able to unravel the actions and intent of the adversary on their own networks in order to halt their progress, and anticipate future campaigns. From this session, attendees will gain a deeper understanding of today's offensive forensic strategies, how adversaries determine where key sensitive data and individuals reside and, most importantly, how to detect these techniques utilizing Windows and file system artifacts.

SANS @NIGHT

Introducing the CompTIA® CASP™ Exam

Speakers: Eric Conrad and Seth Misenar

Tuesday, June 18 | 8:15pm - 9:15pm | Int'l Ballroom East

Eric Conrad and Seth Misenar, coauthors of the ***CISSP Study Guide***, published by Syngress, will introduce you to the new CompTIA Advanced Security Practitioner certification, a hands-on technical exam with a mix of deeper technical questions, as well as higher-level management questions. The CASP was recently added to DoD 8570 for the following roles: IAT level III, IAM II, and IASAE level I and II. Will this cert be a valuable addition to your resume? Will this cert bleed significant market share from the CISSP? Now that it has been added to DoD8570, will CASP become the go to DoD cert? Come find out where CASP fits into the security certification landscape and see if Eric and Seth's new SANS prep course for the CASP is right for you.

Special Events

TUESDAY, JUNE 18

SANS @NIGHT

Avoiding Cyberterrorism Threats Inside Hydraulic Power Generation Plants

Speaker: Manuel Humberto Santander Palaez

Tuesday, June 18 | 8:15pm - 9:15pm | Int'l Ballroom Center

Hydroelectric generation plants possess a number of cyberterrorism risks, which could cause significant problems like interruptions in the power grid or water leaks from the reservoir, among others. This presentation will discuss the vulnerabilities in the infrastructure of hydroelectric generation plants, some tools to check for them and several remediation techniques to avoid materialization of problems.

WEDNESDAY, JUNE 19

Online Training Social Hour

Wednesday, June 19 | 6:00pm - 7:00pm | Int'l Patio

SANS Online Training invites you to a casual social hour. Join us on the International Patio to learn more about SANS' online training options. Enjoy a complimentary drink while you socialize with SANS instructors and network with fellow attendees. Reservations are highly recommended; email vlive@sans.org to reserve your spot!

GIAC Program Overview

Speaker: Jeff Frisk

Wednesday, June 19 | 6:30pm - 7:15pm | Columbia Hall 7

GIAC certification provides assurance that a certified individual meets a minimum level of ability and possesses the skills necessary to do the job. Find out why this is important to your career.

SANS Technology Institute Open House

Speaker: Toby R. Gouker - Provost

Wednesday, June 19 | 7:15pm - 8:15pm | Columbia Hall 7

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.

WEDNESDAY, JUNE 19

(ISC)² Reception

Wednesday, June 19 | 6:30pm-7:30pm | Cabinet

SANS is pleased to host a reception for (ISC)²® members and SANSFIRE students interested in memberships. This is a great opportunity for you to meet with fellow (ISC)² members, receive membership updates directly from Hord Tipton, Executive Director (ISC)², and hear Dr. Eric Cole discuss the latest cybersecurity trends.

Women in Technology Meet and Greet

Host: Karen Fioravanti

Wednesday, June 19 | 7:15pm - 8:15pm | Northwest

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 and come share your own. After the discussions, stay and network with other conference attendees.

SANS @NIGHT

Automated Analysis of Android Malware

Speaker: Jim Clausing

Wednesday, June 19 | 7:15pm - 8:15pm | Int'l Ballroom East

With the increasing volume of malware-targeting mobile devices, and the trend toward allowing BYOD (bring your own device), it is imperative that we detect it in our networks and determine its capabilities. This talk will describe an automated environment for analyzing malware-targeting Android devices, built from free and open source tools.

SANS @NIGHT

Fiber Channel - Your "Other" Datacenter Network

Speaker: Rob VandenBrink

Wednesday, June 19 | 8:15pm - 9:15pm | Int'l Ballroom East

The majority of large datacenter storage architectures in the world are currently based on Fiber Channel networks. Unfortunately, the emphasis on security, compliance, and audit remains on hosts and traditional Ethernet networks, leaving the Fiber Channel behind as "a storage thing" that for some reason is never secured. Unfortunately, abdicating this responsibility leaves the Fiber Channel network open as a conduit for unfettered, unmonitored recon and theft of data, without regard for security zones you may have defined on your IP network. In this presentation we'll explore commonly overlooked security settings in Fiber Channel security, how to audit, pentest, or attack fiber channel, and more importantly, how to secure your Fiber Channel network. Live demos of methods and tools are part of this presentation. More on these later as we build them!

Special Events

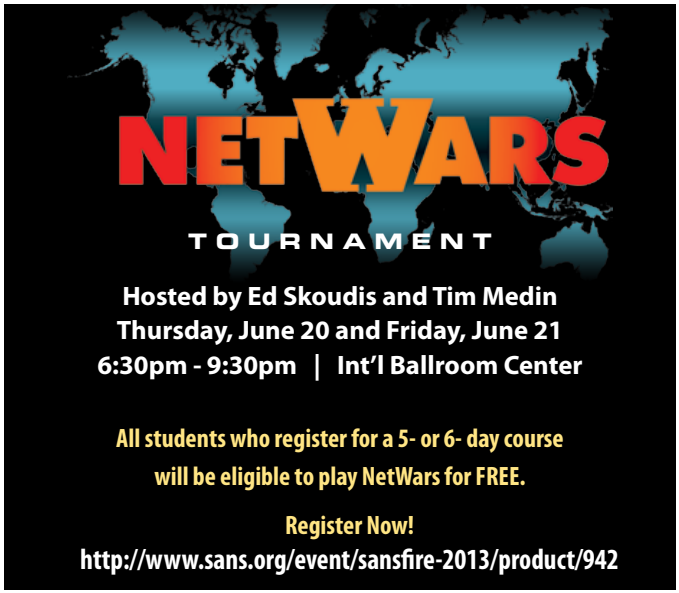
WEDNESDAY, JUNE 19

SANS @NIGHT

Securing the Human - Phishing Launch

Wednesday, June 19 | 7:30pm - 8:30pm | Int'l Ballroom Center

SANS STH.Phishing takes an innovative approach to advanced phishing attack prevention. Too often we focus on technical controls while ignoring the weakest link- the end user. STH.Phishing simulates phishing attacks to educate your end users on how to avoid getting compromised. Come join us for the product launch. Chat with the content developers and see a demo.



THURSDAY, JUNE 20

SANS @NIGHT

Active Defense, Crime and Punishment: New Tools to Find Bad People

Speaker: John Strand

Thursday, June 20 | 7:15pm - 8:15pm | Int'l Ballroom East

In this presentation we will discuss some new active defense tools which can be used to effectively locate attackers and bad guys, even if they are connecting through TOR. This presentation will be based on the Active Defense Harbinger Distribution and all attendees can follow along as John Strand walks through new and improved tools for geolocation and tracking of the bad guys. Oh, Yea.. And we will show you how to do it legally.

THURSDAY, JUNE 20

SANS @NIGHT

Defensive Reading: Understanding Online News

Speaker: Richard Porter

Thursday, June 20 | 8:15pm - 9:15pm | Int'l Ballroom East

The proliferation of social media has given mass media a whole new meaning. The depth of potential propaganda, biased news, and/or plain spin is vast. Understanding some of the nuances of what is written can help prepare you for defensive reading. This talk introduces the first stage in the development of a mental martial art, with the first technique being defensive reading. We will examine the core motives behind phrases like "condition of anonymity because talks were ongoing" or "the lawmaker spoke on condition of anonymity". This talk will briefly cover a world of perhaps total disclosure. We will also examine some techniques in which you can understand decision heuristics and how to defend against cognitive miserliness.

FRIDAY, JUNE 21

SANS @NIGHT

Special Operations and Infosec

Speaker: Gal Shpantzer

Friday, June 21 | 7:15pm - 8:15pm | Int'l Ballroom East

The Security Outliers project focuses on Layer 8 and the importance of leadership, teamwork, and communications in managing information security teams. The Outliers project kicked off with a presentation at RSA 2010, after a year of academic research, scouring journals and books as well as conducting interviews with leaders in high-risk professions, both in and out of infosec.

We will begin this entertaining yet educational session with a very quick explanation of who the SEALs are and what they are tasked with doing by the highest levels of the US government, then proceed through a synopsis of the course I completed and how I've used the lessons learned since then. This will include representative hilarious (and pathetic) visuals from the Extreme SEAL Experience, freezing in and out of the river then getting really dirty, jumping out of helicopters, rappelling, shooting, etc. Once the obligatory SEAL pr0n is presented, we'll dive into the general leadership and infosec-specific lessons learned from the academic research on the SEALs, as well as the experiential learning of how SEALs build teamwork and plan/rehearse/execute/debrief complex and risky missions. The session will close with practical advice on managing risk and burnout through teamwork, including some basic mind-hacks that are applicable on and off the job site.

Special Events

FRIDAY, JUNE 21

SANS @NIGHT

Securing the Kids

Speaker: Lance Spitzner

Friday, June 21 | 7:15pm - 8:15pm | Int'l Ballroom East

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.

Key take aways include:

- Why securing kids online is harder then securing kids in the physical world.
- Top three risks they face; strangers, friends and themselves.
- Use of education to inform and secure them.
- Use of a dedicated computer just for kids.
- Kids Acceptable Use Policy.
- Filtering and monitoring tools.
- Additional lessons learned and resources to learn more.

SANS @NIGHT

Securing the Human

Speaker: Lance Spitzner

Friday, June 21 | 8:15pm - 9:15pm | Int'l Ballroom East

Organizations have traditionally invested most of their security in technology, with little effort in protecting their employees. As a result, many attackers today target the weakest link, the human. Awareness, not just technology, has become key to reducing risk and remaining compliant. This high-level talk designed for management explains why humans are so vulnerable, how they are being actively exploited, and what organizations can do about it.

Key points include:

- How humans are nothing more than another type of operating system, albeit a highly vulnerable one.
- Why humans are so bad at judging risk and how attackers exploit these vulnerabilities.
- How an effective awareness program patches these vulnerabilities and reduces risk.
- How to develop a modular and flexible program that reaches multi-cultures.
- How to create and effectively use metrics.

Dining Options

Sample the tastes and sounds of the capital city without ever leaving the hotel. The Washington Hilton features several Washington DC dining options, each offering a uniquely Washingtonian atmosphere and featuring some of the most savory cuisine in the nation's capital. From casual dining to a relaxing cocktail, we do our best to cater to your every taste!

In-Room Dining

Experience restaurant dining in the comfort of your room. Enjoy breakfast, lunch, dinner or a late night snack carefully prepared by Washington Hilton's renowned culinary team. Whether its food or a selection from our extensive wine list, In Room Dining is quick, convenient and delicious!

McClellan's Sports Bar

McClellan's Sports Bar is the perfect place to watch the game and unwind after a long day of travel and meetings. We offer a wide selection of draft and bottle beers and a knowledgeable bar staff that will prepare your favorite cocktails. McClellan's is the perfect Washington DC dining option with great food, the perfect beverage, comfortable seating and 15 flat screen televisions that will allow you to enjoy the evening.

TDL Bar

Situated in the heart of Washington Hilton's lobby, TDL Bar is the ideal spot to meet, mingle or unwind. Enjoy refreshing handcrafted cocktails, regional wines and draft beers, complimented with a selection of locally-inspired dishes, signature flatbreads and small plates perfect for sharing. Large stone-top communal tables, easy-access electric outlets and complimentary wi-fi provide the perfect place to spread out and stay connected, while more intimate seating scattered throughout is great for networking.

The Coffee Bean & Tea Leaf

Start the day with a java to go, whether it's hot brewed or blended with ice. The Coffee Bean & Tea Leaf provides the perfect place to grab your favorite gourmet coffee, loose-leaf tea, flaky pastry or filling sandwich in a relaxed setting with cozy seating, complimentary Wi-Fi and TVs featuring the latest in news, sports and entertainment.

The District Line Restaurant

Enjoy an authentic, contemporary urban neighborhood gathering place, serving up handcrafted cocktails, chalkboard specials and a host of hearty American comfort foods with a local twist. The menu features a variety of regionally-inspired comfort foods and seasonal dishes with high-quality, fresh ingredients from farmers within 150 miles of Washington, D.C. Semi-private dining for up to 60 guests is available. The District Line Restaurant is open for breakfast, including the signature Hilton Breakfast buffet, as well as lunch and dinner.

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.

AUD507 – $449	SEC503 – $449
DEV541 – $449	SEC505 – $449
DEV544 – $239	SEC506 – $449
FOR610 – $449	SEC542 – $449
LEG523 – $449	SEC566 –$449
MGT414 – $449	SEC579 – $449
SEC501 – $449	SEC617 – $449

Three ways to register!

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

Vendor Events

Vendor Expo

Tuesday, June 18 | 12:00pm - 1:30pm and 5:00pm - 7:00pm
Location: International Terrace and Columbia 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

Tuesday, June 18 | 5:00pm - 7:00pm
Location: International Terrace

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

Tuesday, June 18 | 12:00pm - 1:30pm
Location: International Terrace and Columbia 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:

ForeScout Technologies	Palo Alto Networks	Guidance Software
GE	Paragon Technology Group	HP Enterprise Security
General Dynamics/Fidelis	Arbor Networks	LogRhythm
PhishMe	Aramco	McAfee
StoneSoft	BeyondTrust	Rapid7
Brocade	EventTracker	SourceFire
Fusion-io		Beyond Trust

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***

Infogressive, Inc.
Aggressive Information Security

FORTINET

Fortinet: Next Generation Firewalls

Speaker: Troy Brueckner, CISSP, GISP,
VP of Sales and Marketing for Infogressive
Monday, June 17 | 12:30pm – 1:15pm | Columbia Hall 7

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.

FIREMON

Building Risk Visibility into Your Firewall Management Process

Speaker: Richard Porter, Senior Systems Engineer, FireMon
Monday, June 17 | 12:30pm – 1:15pm | Int'l Ballroom West

Firewall deployments in large organizations can easily get out of control – and become rife with unnecessary risk. Inappropriate access is granted readily. Constant change complicates policy implementation. A real-time, enterprise-wide picture of network security posture is a distant dream. Only by automating tedious manual processes at the operations, management and compliance levels of the organization can security teams regain control and better protect their information. This requires consolidated, real-time data of the security infrastructure and a scalable, distributed solution that provides fast, flexible analysis and reporting.

FIDELIS SECURITY SYSTEMS

GENERAL DYNAMICS
Fidelis Cybersecurity Solutions

Connecting the Dots: Protecting Your Enterprise and Your Career

Speaker: Mike Nichols, Technical Product Manager
Monday, June 17 | 12:30pm – 1:15pm | Columbia Hall 8

Attacks do not happen in isolation, and often finding or preventing one attempt at infiltration does not mean you stemmed the tide. Recent news stories have shown us that a lack of deep analysis will result in a serious loss of revenue for a company and probably the loss of your job. Don't get lost in the details, thinking the single alert signifies the attackers goal. Connect the dots, save your company, and save your career.

Vendor Events

cellebrite
delivering mobile expertise

Smartphone Drill-Down: OS Extraction, Decoding & Analysis

Speaker: Ronen Engler, Cellebrite
Monday, June 17 | 12:30pm – 1:15pm | Columbia Hall 6

Locked devices, encrypted and deleted content, databases, and applications are just some of the complications investigators may encounter when examining a smartphone. In this session, learn the proper procedures for:

- iPhone passcode bypass, decoding and keychain decryption
- Android pattern lock bypass and decoding, and extraction methods: logical, file system and physical from both rooted and non-rooted devices
- BlackBerry physical extraction, decryption and decoding: full flash memory, not just the mass storage or IPD dumps
- Blackberry Messenger decoding (BBM)
- Applications decoding
- SQLite database extraction and viewing including deleted records
- Image carving from physical extractions

Learn how to build these pieces of evidence into your overall case, what they mean, how to analyze them, and how to explain your actions and interpretations in your documentation and case reporting.

Guidance® SOFTWARE
The World Leader in Digital Investigations™

Security Intelligence Through Endpoint Analytics: Deriving Insight from Chaos

Speaker: Roger Andras, Sr. Solutions Consultant, Guidance
Monday, June 17 | 12:30pm – 1:15pm | Columbia Hall 8

Every day, massive activity is being generated by the endpoint and servers across your enterprise. Employees are creating, deleting and editing files; individual devices are connecting to other devices both inside and outside the firewall; programs are opening and closing throughout the day; and malware is silently propagating beneath it all.

In this session we will discuss how this vast wealth of ever-changing data from the endpoints and servers scattered across the enterprise can be harnessed as a source for big data security analytics. We will demonstrate how this data can be captured and leveraged for security analytic purposes in order to expose hidden threats lurking underneath the deluge of endpoint activity. By the end of this session, you will understand:

- How complex relationships across disparate pieces of endpoint data can be used to expose a breach
- Requirements to ensure a high degree of accuracy and value in this approach to data-centric security
- Examples of various artifacts that – by themselves – present no insight into risk, but when combined with seemingly unassociated data through an analytic capability present use cases enabling you to expose a potential data breach before damage can be done.

Vendor Events

tenable network security

Tenable, the SANS 20 Critical Security Controls, and you – the basics and beyond.

Speaker: Jack Daniel, Technical Product Manager, Tenable Network Security

Monday, June 17 | 12:30pm – 1:15pm | Int'l Ballroom Center

SANS'20 Critical Security Controls are being adopted across enterprises and government agencies. In this Lunch and Learn session we will discuss the 20 controls as well as some of the challenges and roadblocks to implementation, and how Tenable Network Security can help you reach your security goals through discovery, inventory, assessment, and audit of your environment.

BROCADE

Securing the Virtual Datacenter

Speaker: Chip Copper, Global Solutions Architect

Wednesday, June 19 | 12:30pm – 1:15pm | Int'l Ballroom Center

Within the physical datacenter, a multi-layer security architecture is critical to establishing IT security posture and for compliance to regulatory standards. The virtual datacenter is no different. Virtual datacenters must adhere to the same strict security requirements as the physical networks. Join this interactive discussion to learn how the Brocade Vyatta 5400 vRouter enables a multi-layer security approach in the virtual datacenter.

IBM

Security Analytics: What Matters in Your Chatter

Speaker: Westley McDuffie, CISSP, Security Evangelist, IBM ISS Federal

Wednesday, June 19 | 12:30pm – 1:15pm | Int'l Ballroom East

Billions of security events and anomalous activity occur each day. How much of that is useful, or actionable? Understaffed, and under budgeted, spending the day looking for less than thirty events that matter in an endless sea of chatter...Sound familiar?

ForeScout Access ability.

Continuous Diagnostics & Mitigation (CDM); How to Achieve Cyber Security Readiness

Wednesday, June 19 | 12:30pm – 1:15pm | Georgetown East

Legacy systems, broad access, diverse devices and network dynamics, and resource constraints all impact the means to satisfy Command Cyber Readiness Inspections. Learn how to optimize processes and effectuate controls that eliminate intrusions, protect sensitive information and reduce attack exposure using a pragmatic approach to Continuous Diagnostics & Mitigation (CDM).

Vendor Events

hp

Good COP, Bad COP

Speaker: Rob Mathieson, CISSP ECSA, Solutions Architect, Intel / DoDHP, Enterprise Security Products, ArcSight - TippingPoint - Fortify

Wednesday, June 19 | 12:30pm – 1:15pm | Columbia Hall 6

During this session, attendees will explore what makes a good COP, why most COPs are considered bad (or at the very least...not entirely operational or relevant), and how to conceptualize, develop, and ultimately operationalize a picture that will matter. The scenarios during this session will be based on real-world COP developments and applications within the DoD, with an emphasis on mission impact assessment and decision making using intelligent source feed correlations through ArcSight ESM.

GE

GE – Incident Response

Speaker: Sean Mason, GE- Director, Incident Response

Wednesday, June 19 | 12:30pm – 1:15pm | Columbia Hall 8

Incident Response is regarded by many to be a black box, mythical art, full of voodoo and mystery. This talk will seek to change that preconception and educate the audience on what really goes on behind the mystical curtain.

FireEye

LUNCH & LEARN

Wednesday, June 19 | 12:30pm – 1:15pm | Int'l Ballroom West

invincea

Stop Spear-Phishing and Watering Hole Attacks - Put the User in a Bubble

Speakers: Nick Keller and Jason Shupp of Invincea

Wednesday, June 19 | 12:30pm – 1:15pm | Columbia Hall 7

Join Nick Keller and Jason Shupp of Invincea for an informative discussion that will cover:

- Recent examples of user targeted attacks and thoughts on why they've succeeded
- How advances in virtualization enable the creation of segregated environments for your users to run highly targeted applications such as the web browser, PDF reader, Office suite, etc.
- How behavioral based malware detection is being used in these segregated environments to spot and kill zero-days - including the recently announced Java 7 exploit
- Methods for turning thwarted attacks into rich forensic information that can feed your entire infrastructure and extend its usefulness

Vendor Events

Phishing your employees: Lessons learned from phishing over 3.5 million people

Speaker: Jim Hansen

Thursday, June 20 | 12:30pm – 1:15pm | Columbia Hall 7

Cyber crime and electronic espionage, most commonly, initiate with an employee clicking a link to a website hosting malware, opening a file attached to an email and laden with malware, or just simply giving up corporate credentials when solicited via phishing websites. Phishing has been used to hijack online brokerage accounts to aid pump n' dump stock scams, compromise government networks, sabotage defense contracts, steal proprietary information on oil contracts worth billions, and break into the world's largest technology companies to compromise their intellectual property. Technical controls presented as silver bullets provide false hope and a false sense of security to employees, promoting dangerous behaviors. Learn how to build a scalable and effective program to educate your staff and change behavior from experts at PhishMe.

Accelerating Speed to Intelligence with ioMemory

Speaker: Christian Shrauder, CTO, Fusion-io Federal

Thursday, June 20 | 12:30pm – 1:15pm | Columbia Hall 5

In this talk we will explore challenges of exploding datasets and the requirements to analyze them. We will examine key architectural issues around data processing and how the introduction of NAND flash has changed the game. Fusion-io has brought to market a new memory tier that allows its customers to process greater volumes of data in a fraction of the time and cost.

STONESOFT

Active Security Strategies for Destructive Malware and Advanced Persistent Threats

Speaker: Brian Vosburgh, Principle Security Architect

Thursday, June 20 | 12:30pm – 1:15pm | Columbia Hall 7

Cyber strategy in 2013 requires a response to new kinds of advanced, sophisticated threats. Join this session to learn how new malware evades current firewall, IPS and A/V technologies and what you can do to stop it. The session will also review the use of offensive methodologies, creating baselines for proactive security, and the use of correlation for situational and tactical awareness. The session will conclude with a live demonstration of an APT evasion.

Vendor Events

"Big Data" & Security: How to Apply Advanced Analytics to Solve Mission Challenges

Speakers: Kiran Rathod, Chief Technology Officer, Paragon Technology Group (Moderator)

- Michael Carleton, Former Chief Information Officer, Department of Health & Human Services (HHS) and General Services Administration (GSA)
- Dr. Peter Aiken, President, Data Blueprint & Data Management Association (DAMA)
- Matt Pledger, Data Scientist, Paragon Technology Group
- Peter Frometa, Predictive Analytics Solutions Architect, IBM

Friday, June 21 | 12:30pm – 1:15pm | Columbia Hall 7

Data growth continues to outpace human capacity to monitor and understand its meaning and relevance. In 2009, the US Government generated more than 840 petabytes of data and the US healthcare data alone reached 150 exabytes. New technologies and techniques have emerged that can help agencies take more control over their data assets, but many are struggling with how to apply these data science concepts to address their critical mission challenges. An expert panel will tackle the most pressing big data security concerns and opportunities. How can you use data management best practices to keep your data safe? How can you make the most of text mining, time series & forecasting, and advanced modeling techniques to gain new insights for your agency? What common use cases can by repeated across government? What's working now in the real-world in both government and commercial environments?

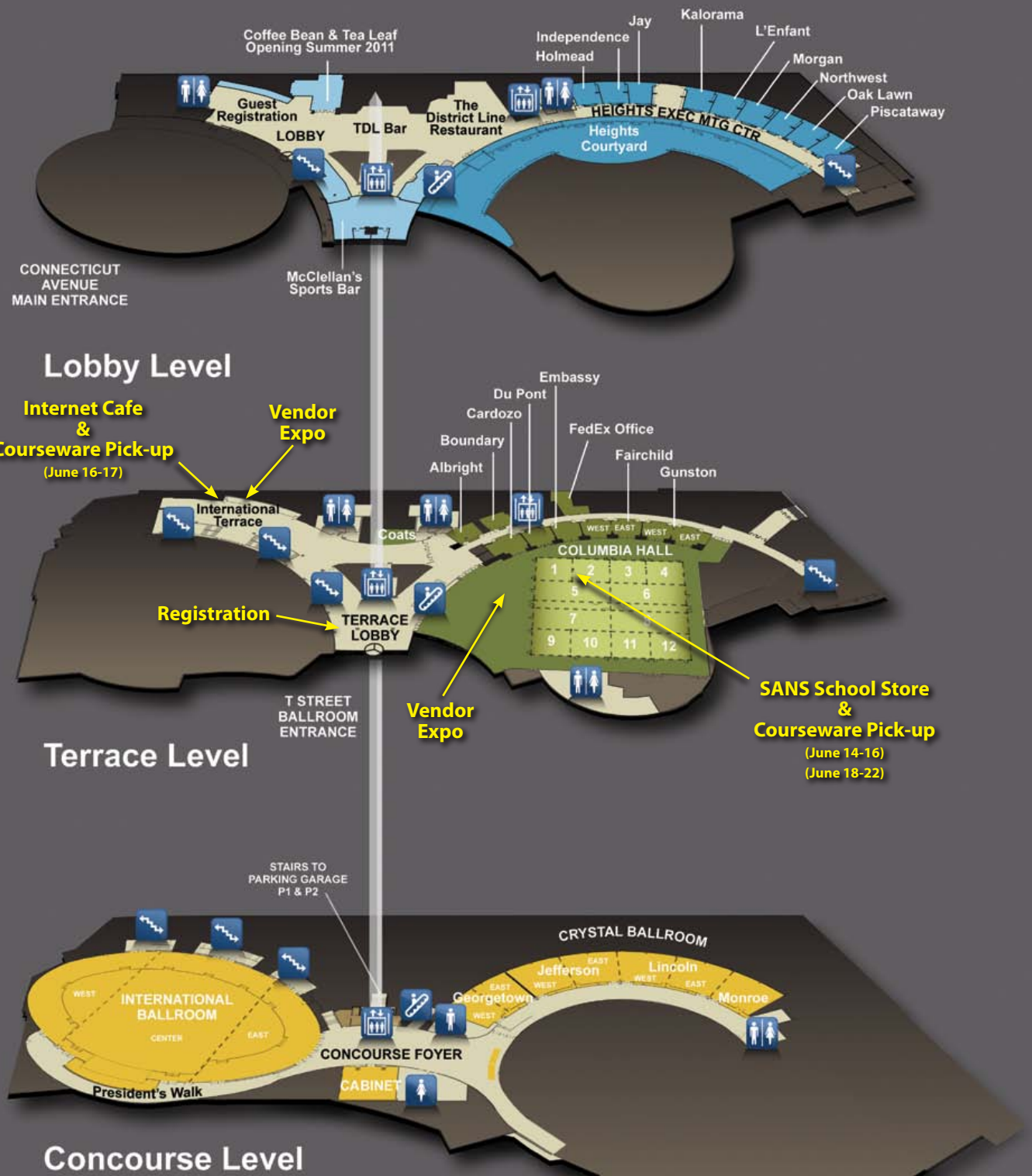
Emerging Technology: WildFire enables organizations to detect and prevent advanced persistent threats

Speaker: Alfred Lee

Friday, June 21 | 12:30pm – 1:15pm | Columbia Hall 6

WildFire compliments the application, user, and content-based network security policies enabled by Palo Alto Networks next-generation firewalls with an ability to detect and prevent modern malware (sometimes referred to as APT). While the next-generation firewall enables the solution by seeing all traffic, the WildFire cloud-based virtualized desktop environment analyzes unknown executable content and determines maliciousness. Once determined, true payload-based signatures are created, tested, and delivered to all subscribers within 30 to 60 minutes. The in-line nature of the firewall enables detection across all traffic, as well as prevention of the infecting file, command-and-control traffic, as well as malicious DNS requests. All other technology focuses on a subset of the traffic, and is typically deployed out of line.

Hotel Floorplans



SANSFIRE 2013 | Washington, DC | June 15-22, 2013

FUTURE SANS TRAINING EVENTS

SANS CyberCon 2013

Online Training Event

Intense courses. Top instructors. No travel.

September 9-14, 2013

Seven of our top courses being offered:

SEC401: Security Essentials Bootcamp Style

SEC504: Hacker Techniques, Exploits, and Incident Handling

SEC575: Mobile Device Security and Ethical Hacking

FOR408: Computer Forensic Investigations – Windows In-Depth

LEG523: Law of Data Security and Investigations

AUD444: Auditing Security & Controls of Active Directory & Windows

AUD445: Auditing Security and Controls of Oracle Databases

Register at
www.sans.org/event/cybercon-fall-2013

Upcoming Summits & Training Courses

Digital Forensics and Incident Response Summit & Training
Austin, TX | July 9-16

ICS Security Training DC
Washington, DC | August 12-16

Critical Security Controls Summit
Washington, DC | August 12-18

Digital Forensics and Incident Response Summit & Training
Prague | October 6-12

ICS Security Training Seattle
Seattle, WA | October

Healthcare Summit
San Francisco, CA | October

Securing the Internet of Things Summit
San Francisco, CA | October

Pen Test Hackfest Summit & Training
Washington, DC | November 7-14

Asia Pacific ICS Security Summit
Singapore | December 2-7

For a full list of training events, please visit www.sans.org/summit.
Dates and locations are subject to change.

SANS Virginia Beach 2013

Virginia Beach, VA • August 19-30, 2013

The right security training for your staff,
at the right time, in the right location.

www.sans.org/event/virginia-beach-2013

SANS
THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

NETWORK SECURITY

Las Vegas | September 14-23, 2013

REGISTER AND PAY BY JULY 31ST

SAVE $500

www.sans.org/event/network-security-2013

Future SANS Training Events

Rocky Mountain
Denver, CO | July 14-20

San Francisco
San Francisco, CA | July 29 - August 3

Boston
Boston, MA | August 5-10

Virginia Beach
Virginia Beach, VA | August 19-30

Capital City
Washington, DC | September 3-8

CyberCon Fall
Online | September 9-14

Network Security
Las Vegas, NV | September 14-23

Seattle
Seattle, WA | October 7-12

Baltimore
Baltimore, MD | October 14-19

Chicago
Chicago, IL | October 28 - November 2

South Florida
Fort Lauderdale, FL | November 4-9

San Diego
San Diego, CA | November 18-25

San Antonio
San Antonio, TX | December 3-8

Cyber Defense Initiative
Washington, DC | December 11-19

San Francisco
San Francisco, CA | December 16-21

Security East
New Orleans, LA | January 18-27

Cyber Guardian
Baltimore, MD | March 3-8

For a full list of training events, please visit www.sans.org.
Dates and locations are subject to change.

Call us with any questions 301-654-SANS (7267)