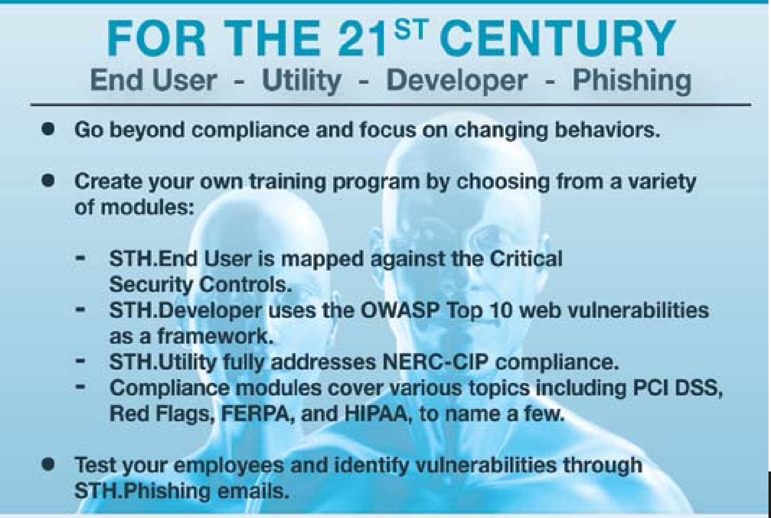
# Program Guide

*December 12-19, 2013 | Washington, DC*

SANS

CYBER DEFENSE INITIATIVE



## Table of Contents

**SANS Technology Institute, an independent subsidiary of SANS, is now accredited by The Middle States Commission on Higher Education!**

3624 Market Street | Philadelphia, PA 19104 | 267.285.5000
an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

*Two unique, respected master's degree programs:*

MASTER OF SCIENCE IN INFORMATION SECURITY ENGINEERING

MASTER OF SCIENCE IN INFORMATION SECURITY MANAGEMENT

*Learn more at* www.sans.edu | info@sans.edu

## General Information

### Registration Information

*Location: International Terrace Foyer*

| | |
|---|---|
| Wednesday, December 11 (Popcorn Reception) | 5:00pm-7:00pm |
| Thursday, December 12 | 7:00am-5:30pm |
| Friday, December 13-Wednesday, December 18 | 8:00am-5:30pm |
| Thursday, December 19 | 8:00am-9:00am (Closes) |

### Courseware Pick-up Information

*Location: International Terrace Foyer*

| | |
|---|---|
| Wednesday, December 11 | 5:00pm-7:00pm |
| Thursday, December 12 | 7:00am-9:00am |
| Wednesday, December 18 | 8:00am-9:00am |

### Internet Café *(WIRED & WIRELESS)*

*Location: Concourse Foyer*
*Printer will be available for students' use*

| | |
|---|---|
| Thursday, December 12 | Opens at noon – 24 hours |
| Friday, December 13-Monday, December 16 | Open 24 hours |
| Tuesday, December 17 | 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 Thursday, December 12 at the General Session in Jefferson.

## General Information

### Dining Options

We have assembled a short list of dining suggestions you may like to try during lunch breaks. See page 20 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 at the end of each day 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 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 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.

### 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

*Extended Hours:*

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

**SEC504:** Hacker Techniques, Exploits & Incident Handling

# Course Schedule

## Six-Day Courses

*Thursday, December 12-Tuesday, December 17*
*Time: 9:00am - 5:00pm (Unless otherwise noted)*

**AUD507: Auditing Networks, Perimeters, and Systems**
Instructor: David Hoelzer . . . . . . . . . . . . . . . . Location: Columbia Hall 12

**FOR408: Computer Forensic Investigations – Windows In-Depth**
Instructor: Chad Tilbury. . . . . . . . . . . . . . . . . . . Location: Columbia Hall 8

**FOR508: Advanced Computer Forensic Analysis and Incident Response**
Instructor: Rob Lee . . . . . . . . . . . . . . . . . . . . . . Location: Columbia Hall 6

**FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques**
Instructor: Lenny Zeltser . . . . . . . . . . . . . . . .Location: Columbia Hall 9/10

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

**SEC401: SANS Security Essentials Bootcamp Style**
Instructor: Seth Misenar . . . . . . . . . . . . . . . . .Location: Columbia Hall 1/2
*Bootcamp Hours: 5:00pm - 7:00pm (Course days 1-5)*

**SEC501: Advanced Security Essentials – Enterprise Defender**
Instructor: Dr. Eric Cole . . . . . . . . . . . . . . . . . . . . . . . Location: Jefferson

**SEC503: Intrusion Detection In-Depth**
Instructor: Mike Poor. . . . . . . . . . . . . . . . . . . . . Location: Columbia Hall 5

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

**SEC505: Securing Windows and Resisting Malware**
Instructor: Jason Fossen. . . . . . . . . . . . . . . . . . . . . . . . Location: Gunston

**SEC542: Web App Penetration Testing & Ethical Hacking**
Instructor: Kevin Johnson . . . . . . . . . . . . . . . . . . . . . . . .Location: Monroe

**SEC575: Mobile Device Security and Ethical Hacking**
Instructor: Christopher Crowley . . . . . . . . . . Location: Columbia Hall 11

**SEC579: Virtualization and Private Cloud Security**
Instructor: Paul A. Henry . . . . . . . . . . . . . . . . . . . . . . . . Location: Fairchild

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

# Course Schedule

## Five-Day Courses

*Thursday, December 12-Monday, December 16*
*Time: 9:00am - 5:00pm (Unless otherwise noted)*

**FOR526: Windows Memory Forensics In-Depth**
Instructor: Alissa Torres . . . . . . . . . . . . . . . . . . . Location: Columbia Hall 4

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

**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 3

**HOSTED: (ISC)$^{2}$® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program**
Instructor: E. J. Jones. . . . . . . . . . . . . . . . . . . . . . . . . . . .Location: Holmead

## Three-Day Courses

*Thursday, December 12-Saturday, December 14*
*Time: 9:00am - 5:00pm*

**AUD444: Auditing Security and Controls of Active Directory and Windows**
Instructor: Tanya Baccam . . . . . . . . . . . . . . . . . . . . Location: Independence

*Sunday, December 15-Tuesday, December 17*
*Time: 9:00am - 5:00pm*

**AUD445: Auditing Security and Controls of Oracle Databases**
Instructor: Tanya Baccam . . . . . . . . . . . . . . . . . . . . Location: Independence

## Two-Day Courses

*Wednesday, December 18-Thursday, December 19*
*Time: 9:00am - 5:00pm*

**MGT433: Securing the Human: Building and Deploying an Effective Security Awareness Program**
Instructor: Lance Spitzner . . . . . . . . . . . . . . . Location: Georgetown West

**SEC434: Log Management In-Depth: Compliance, Security, Forensics, and Troubleshooting**
Instructor: Dr. Eric Cole . . . . . . . . . . . . . . . . . . . .Location: Jefferson West

**SEC580: Metasploit Kung Fu for Enterprise Pen Testing**
Instructor: Eric Conrad . . . . . . . . . . . . . . . . . . . . . .Location: Lincoln West

## One-Day Courses

*Wednesday, December 18 | Time: 9:00am - 5:00pm*

**MGT415: A Practical Introduction to Risk Assessment**
Instructor: David Hoelzer . . . . . . . . . . . . . . . . . . . Location: Jefferson East

**MGT535: Incident Response Team Management**
Instructor: Christopher Crowley . . . . . . . . . . Location: Georgetown East

# 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.*

## WEDNESDAY, DECEMBER 11

### Registration Popcorn Reception

Wed, Dec 11 | 5:00pm-7:00pm | Location: Int'l Terrace

***Register early and network with your fellow students!***

## THURSDAY, DECEMBER 12

### Welcome to SANS General Session

Speaker: Dr. Eric Cole

Thu, Dec 12 | 8:15am-8:45am | Location: Jefferson

### SANS Technology Institute Open House

Speaker: Alan Paller

Thu, Dec 12 | 6:00pm-7:15pm | Location: Georgetown East

Impact your career and learn about the cybersecurity master's degree program that has graduated some of America's most impressive cybersecurity leaders—the only program from an accredited graduate school focused solely on cybersecurity, built on SANS Institute material, granting a Master of Science degree upon graduation and more than five widely respected GIAC certifications even before you graduate.

This is the first major Open House since The SANS Technology Institute announced it was accredited by The Middle States Commission of Higher Education (3624 Market Street – Philadelphia, PA 19104 – 267.284.5000) an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

President Alan Paller of the SANS Technology Institute will provide authoritative information about SANS master's degree programs, their potential impact on your career, and how they might qualify for your employer's tuition reimbursement plan. Graduates and current students will be available to answer your questions.

Are you qualified to be one of the 100 new students we will accept into the programs in 2014? Join us at the Open House to learn more.

# Special Events

KEYNOTE

### *APT: It is Time to Act*

Speaker: Dr. Eric Cole

Thu, Dec 12 | 7:15pm-9:15pm | Location: Jefferson

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

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

## FRIDAY, DECEMBER 13

### Vendor Solutions Expo

Fri, Dec 13 | 12:00pm-1:30pm & 5:00pm-7:00pm

Location: Columbia Hall 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

Fri, Dec 13 | 5:00pm-7:00pm | Location: Columbia Hall 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.

SANS@NIGHT

### *Windows Exploratory Surgery with Process Hacker*

Speaker: Jason Fossen

Fri, Dec 13 | 7:15pm-8:45pm | Location: Georgetown East

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.

## Special Events

SANS@NIGHT

### *Have no fear - DFIR is here!*

Speakers: Rob Lee, Chad Tilbury, Alissa Torres, and Lenny Zeltser
Fri, Dec 13 | 7:15pm-8:45pm | Location: Jefferson

In an age of darkness, at a time of evil... When the cyberworld needed heros, what it got was this team. In less time than it takes you to watch the Avengers, the DFIR hero team will take you through an end-to-end investigation starting with core steps in digital forensics, incident response, memory analysis, and RE Malware. Instructors Chad Tilbury (FOR408: Digital Forensics), Rob Lee (FOR508: Incident Response), Alissa Torres (FOR526: Windows Memory Forensics), and Lenny Zeltser (FOR610: REM) will step through how key skills are used to solve a single case. The tag team approach will detail how teams can be leveraged in your environment to effectively respond to incidents on a single system and the enterprise. Four forensicators, one million hackers – the odds are just about even.

STI MASTER'S PRESENTATION

### *Discovering Security Events of Interest Using Splunk*

Speaker: Carrie Roberts
Fri, Dec 13 | 8:15pm - 8:55pm | Location: Columbia Hall 12

Security events of interest can be discovered by analyzing several different sources of machine data, including logs. Applications and the servers they run on contain many valuable logs which detail the events that have occurred on them. By analyzing and correlating this data, important information about the attacks against these systems can be discovered. Splunk is a powerful tool for analyzing such data. It provides a high performance solution for analyzing large amounts of unstructured data from multiple sources. This presentation includes a description of Splunk software features and architecture. Methods for setting up a Splunk server and forwarding data to it from multiple sources are included. Example searches and use of pre-built add on functionality is given. It is a concise, comprehensive guide for deploying and using a centralized system for intelligence gathering, with a focus on detecting security events of interest.

## SATURDAY, DECEMBER 14

SANS@NIGHT

### *Continuous Ownage: Why you Need Continuous Monitoring*

Speakers: Eric Conrad and Seth Misenar
Sat, Dec 14 | 7:15pm-8:15pm | Location: Jefferson

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

## Special Events

SANS@NIGHT

### *Security Onion: Installed and Now What?*

Speaker: Chris Mohan
Sat, Dec 14 | 7:15pm-8:15pm | Location: Georgetown East

Security Onion is one the easiest and most effective way to deploy a free Network Security Monitoring (NSM) solution. Download it from SourceForge.net, boot the ISO image, follow the super quick setup guide, then Security Onion is up and running. See, it's easy. But what do you do after that?

We'll go through the steps to make sure everything is tested, alerting, and working as expected before you run into a real attack. By going through these steps now, you'll avoid that steep learning curve of learning how to do real incident response with Security Onion. Throw in a couple of today's current attacks, just to see what they look like, and you'll be ready to go out and build out your own working, pre-tested NSM environments.

STI MASTER'S PRESENTATION

### *A Predictive Security Model Using Bayesian Networks*

Speaker: Dan Lyon
Sat, Dec 14 | 7:15pm-7:55pm | Location: Columbia Hall 12

Designing systems with security at the front of the product development cycle is the only way to ensure a secure system, but how do you measure security on a system under design? The information security industry lacks a concrete method to collect meaningful metrics on existing systems, primarily because a security breach that has not been detected cannot be measured. In development, this lack of detection problem is amplified by not having the system available for penetration testing. Therefore the current approach from the information security community is inadequate, and a new model must be created that enables appropriate business and design decisions. This presentation will show a model using Design for Six Sigma techniques to measure a system's level of security.

SANS@NIGHT

### *An Introduction to PowerShell for Security Assessments*

Speaker: James Tarala
Sat, Dec 14 | 8:15pm-9:15pm | Location: Jefferson

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 the Microsoft services. Auditors, system administrators, penetration testers, and others will all learn practical techniques for using PowerShell to assess and secure these vital Windows services.

## Special Events

SANS@NIGHT

### *Closing the Door on Web Shells*

Speaker: Anuj Soni

Sat, Dec 14 | 8:15pm-9:15pm | Location: Georgetown East

While many attackers install malware on end-user workstations to accomplish their goals, external-facing servers continue to be prime targets of attack. In many of these cases, web shell backdoors are utilized by the adversary to download/upload files, execute arbitrary commands, and access back-end databases and other resources. Web shells are often heavily customized and obfuscated to evade detection. They may be only several lines of code, and they can be deployed on a variety of platforms. Every incident responder should be familiar with this dangerous category of malware. This talk will discuss how web shells work, dive deep into several specimens, discuss approaches to detect related activity, and touch on some best practices to reduce the likelihood of ever seeing them on your systems.

STI MASTER'S PRESENTATION

### *Active Deception to Augment Intrusion Detection*

Speaker: Josh Johnson

Sat, Dec 14 | 8:15pm-8:55pm | Location: Columbia Hall 12

## SUNDAY, DECEMBER 15

### GIAC Program Overview

Speaker: Jeff Frisk

Sun, Dec 15 | 7:15pm-8:15pm | Location: Georgetown East

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@NIGHT

### *Booting a Write-blocked Drive to a VM Using Linux (Ubuntu)*

Speaker: Carlos Cajigas

Sun, Dec 15 | 7:15pm-8:15pm | Location: Columbia 12

SANS@NIGHT

### *Who's Watching the Watchers?*

Speaker: Mike Poor

Sun, Dec 15 | 7:15pm-8:15pm | Location: Columbia 5

We have instrumented our networks to the Nth degree. We have firewalls, IDS, IPS, Next Gen Firewalls, Log correlation and aggregation...but do we know if we have it right? Will we detect the NextGen™ attackers? In this talk we will explore ways that we improve the signal/noise ratio in our favor, and help identify the needle in the needlestack.

## Special Events

SANS@NIGHT

### *Sharing Without Borders: Attacking and Testing SharePoint*

Speaker: Kevin Johnson

Sun, Dec 15 | 8:15pm-9:15pm | Location: Columbia 5

SharePoint has become one of the most common platforms in organizations today. Originally designed for simple content management, it has grown into a workflow, CMS, and communication powerhouse that runs on the Internet and intranets all over the world. While it is powerful, most organizations do not realize the risks it exposes within their organization. Kevin Johnson will be walking attendees through the systems available under the SharePoint name, as well as showing ways that penetration testers are able to assess and exploit them. He will also be releasing a series of tools and guidelines to help organizations assess their SharePoint systems.

NETWARS

***There will be three simultaneous NetWars Tournament events held at SANS CDI 2013:***

### Pen Testing NetWars Tournament

Host: Yori Kvitchko

Dec 15 & 16 | 6:30-9:30pm | Location: Lincoln/Monroe

*Pen Testing NetWars Tournament is designed to help participants develop skills in several critical pen testing areas:*

- *Vulnerability Assessments*
- *System Hardening*
- *Malware Analysis*
- *Incident Response*
- *Packet Analysis*
- *Penetration Testing*

### DFIR NetWars Tournament

Host: Rob Lee

Dec 15 & 16 | 6:30-9:30pm | Location: Jefferson

*DFIR NetWars Tournament is designed' to help participants develop skills in several critical DFIR areas:*

- *Host forensics*
- *Malware analysis*
- *Network forensics*
- *Memory analysis*

### SANS NETWARS TOURNAMENT of CHAMPIONS

*An invite-only Tournament where the best-of-the-best from past competitions have been invited to face off.*

SANS@NIGHT

### *Hacking Back, Active Defense, and Internet Tough Guys*

Speaker: John Strand

Sun, Dec 15 | 8:15pm-9:15pm | Location: Georgetown West

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.

## MONDAY, DECEMBER 16

SANS@NIGHT

### *Effective Phishing that Employees Like*

Speaker: Lance Spitzner

Mon, Dec 16 | 7:15pm-8:15pm | Location: Columbia 5

One of the toughest challenges in establishing a high-impact security awareness program is measuring the impact. Are you changing behavior and reducing risk? Phishing assessments are a powerful way to measure such change, while addressing one of the most common human risks. As more organizations use phishing assessments, many of them are doing it wrong, not only negatively impacting their metrics but generating resentment among employees. In this short presentation, learn how to create a fun, engaging phishing program that not only effectively measures and reinforces key behaviors, but is also truly enjoyed by employees.

SANS@NIGHT

### *New School Forensics: Latest Tools and Techniques in Memory Analysis*

Speaker: Chad Tilbury

Mon, Dec 16 | 7:15pm-8:15pm | Location: Georgetown East

Whether you are just getting started with memory forensics, or you have been at it since the early days, the last year produced a wealth of new memory analysis capabilities. Notably, nearly all of the progress has been accomplished in free and open source tools. Learn about the latest and greatest additions to the memory forensics arsenal: in-memory registry forensics; building and analyzing memory object timelines; Mac and Linux memory analysis; and the advantages of live memory analysis.

SANS@NIGHT

### *Using RE to Turn the Tables!*

Speaker: David Hoelzer

Mon, Dec 16 | 8:15pm-9:15pm | Location: Georgetown East

In this 60 minute presentation we will examine the discovery of a piece of targeted malware, discover hidden features and use the malware's own libraries to turn the tables on the attacker to recover the passwords used to safeguard the "hidden features" and administrative interfaces that the malware contains! While the presentation will demonstrate reverse engineering, including binary disassembly, the discussion is always at a level that anyone attending can walk away with useful information, whether you are deeply technical or a C level executive! Come and help us turn the tables on this attacker!

SANS@NIGHT

### *Securing The Kids*

Speaker: Lance Spitzner

Mon, Dec 16 | 8:15pm-9:15pm | Location: Columbia 5

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 takeaways 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

# 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**

**FOR408 – $449**

**FOR508 – $449**

**FOR610 – $449**

**MGT414 – $449**

**MGT512 – $449**

**SEC301 – $449**

**SEC401 – $449**

**SEC501 – $449**

**SEC503 – $449**

**SEC504 – $449**

**SEC505 – $449**

**SEC542 – $449**

**SEC566 –$449**

**SEC575 – $449**

**SEC579 – $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 Solutions Expo

Friday, December 13
12:00pm-1:30pm & 5:00pm-7:00pm
Location: Columbia Hall 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

Friday, December 13 | 5:00pm-7:00pm
Location: Columbia Hall 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

Friday, December 13 | 12:00pm - 1:30pm
Location: Columbia Hall 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:*

**LogRhythm**

**BEW Global**

**Emulex**

**BeyondTrust**

**General Dynamics Fidelis Cybersecurity**

## 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**

LUNCH & LEARN

BEWGLOBAL
DATA PROTECTION EXPERTS

### *Building a Security Program that Protects an Organization's Most Critical Assets – A Different Approach*

Speaker: Robert Eggebrecht, President and CEO, BEW Global
Thu, Dec 12 | 12:30pm – 1:15pm | Location: Monroe

Join BEW Global as we discuss the step-by-step process to building a risk-based, cost-effective critical asset protection program.

Topics covered:

- Obtaining executive level management buy-in / involvement
- Defining assets based on revenue, income, reputation, core operational impact
- Building / optimizing the program and creating a milestone program for business leaders

LUNCH & LEARN

FORTINET®

### *Fortinet Next Generation Firewalls*

Speaker: Justin Kallhoff, CEO Infogressive
Thu, Dec 12 | 12:30pm – 1:15pm | Location: Lincoln

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.

LUNCH & LEARN

EMULEX®

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

Speaker: Ron Leibfreid – Senior Sales Engineer, Emulex
Sat, Dec 14 | 12:30pm – 1:15pm | Location: Lincoln

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 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.

LUNCH & LEARN

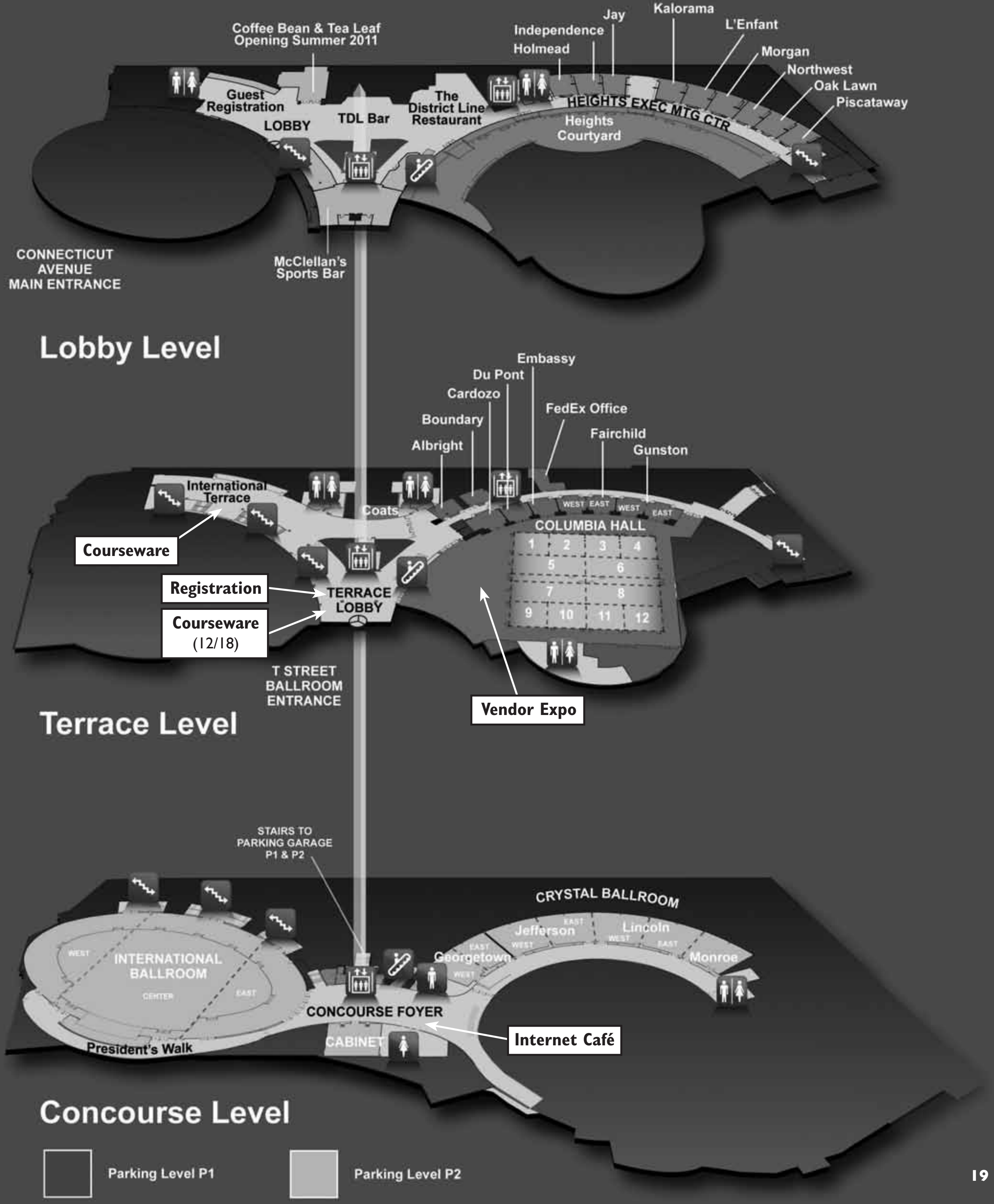
GENERAL DYNAMICS
Fidelis Cybersecurity Solutions

### *Targeted, Wire-speed Yara Analysis for Real-time Malware Prevention*

Speaker: Mike Nichols, Technical Product Manager
Mon, Dec 16 | 12:30pm – 1:15pm | Location: Lincoln

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.

# Hotel Floorplans



Courseware

Registration

Courseware (12/18)

Vendor Expo

Internet Café

## Dining Options

### 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. McClellan's offers 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 WiFi 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 WiFi 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.

# Future SANS Training Events

**FOR572 Advanced Network Forensics**
San Antonio, TX | Jan 5-10

**FOR585 Adv Smartphone and Mobile Device Forensics**
San Antonio, TX | Jan 13-18

**SANS Security East 2014**
New Orleans, LA | Jan 20-25

**AppSec 2014**
Austin, TX | Feb 3-8

**SANS Cyber Threat Intelligence Summit**
Washington, DC | Feb 4-11

**SANS CyberCon Spring 2014**
Online Training | Feb 10-15

**SANS Scottsdale 2014**
Scottsdale, AZ | Feb 17-22

**RSA Conference 2014**
San Francisco, CA | Feb 23-24

**SANS Cyber Guardian 2014**
Baltimore, MD | Mar 3-8

**SANS DFIRCON 2014**
Monterey, CA | Mar 5-10

**ICS Summit - Orlando**
Lake Buena Vista, FL | Mar 12-18

**SANS Northern Virginia 2014**
Reston, VA | Mar 17-22

**SANS 2014**
Orlando, FL | Apr 5-14

**SANS Austin 2014**
Austin, TX | Apr 28-May 3

**SANS Security West 2014**
San Diego, CA | May 10-15

For a full list of training events, please visit www.sans.org.

Dates and locations are subject to change.