SANS

CDI

CYBER DEFENSE INITIATIVE 2015

Washington, DC

December 12-19

PROGRAM GUIDE

POWERED BY

@SANSInstitute #SANSCDI

SANS OnDemand Bundle

Add an OnDemand Bundle to your course to get an additional four months of intense training! OnDemand Bundles are just $659 when added to your live course, and include:

- Four months of OnDemand access to our custom e-learning platform
- Quizzes
- MP3s and videos of lectures
- Labs
- Subject-matter expert support

OnDemand Bundle is available for these courses.

SEC301 – $659	AUD507 – $659
SEC401 – $659	DEV544 – $659
SEC501 – $659	FOR408 – $659
SEC503 – $659	FOR508 – $659
SEC504 – $659	FOR572 – $659
SEC505 – $659	FOR610 – $659
SEC511 – $659	ICS410 – $659
SEC560 – $659	LEG523 – $659
SEC566 – $659	MGT414 – $659
SEC575 – $659	MGT512 – $659
SEC579 – $659	MGT514 – $659
SEC660 – $659	

How to register!

Visit the
Grand Foyer Declaration Level (HYATT) or
the Staff Office – Meeting Room 15 (Renaissance),
Call (301) 654-SANS,
Or email to ondemand@sans.org

TABLE OF CONTENTS

CORE NETWARS TOURNAMENT

Hosted by Jeff McJunkin
Thursday, December 17 and Friday, December 18
6:30-9:30pm | Independence A

SANS DFIR NETWARS TOURNAMENT

Hosted by Jake Williams & Philip Hagen
Thursday, December 17 and Friday, December 18
6:30-9:30pm | Declaration A/B

All students who register for a 4-6 day course will be eligible to play NetWars for FREE.
Register Now!
sans.org/event/cyber-defense-initiative-2015/schedule

GENERAL INFORMATION

HYATT

Registration & Courseware Pick-up Information

Location: Constitution Foyer

Saturday, December 12 (Short Courses Only) 8:00-9:00am

Location: Grand Foyer (DECLARATION LEVEL)

Sunday, December 13 (Welcome Reception) 5:00-7:00pm

Monday, December 14 . . . . . 7:00am - 5:30pm

Tuesday, December 15 - Saturday, December 19 . . . . . 8:00am - 5:00pm

RENAISSANCE

Registration & Courseware Pick-up Information

Location: Foyer (MEETING ROOM LEVEL)

Sunday, December 13 (Welcome Reception) 5:00-7:00pm

Monday, December 14 . . . . . 7:00am - 5:30pm

Tuesday, December 15 - Saturday, December 19 . . . . . 8:00am - 5:00pm

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

Location:
Constitution Foyer (HYATT) *& Meeting Room Level Foyer* (RENAISSANCE)

Open 24 hours and closes Saturday, December 19 at 2:00pm

Course Times

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

Course Breaks

7:00-9:00am – Morning Coffee

10:30-10:50am – Morning Break

12:15-1:30pm – Lunch (On your own)

3:00-3:20pm – Afternoon Break

First Time at SANS?

Please attend the ***Welcome to SANS*** briefing designed to help you get the most from your SANS training experience. The talk is from **8:15-8:45am** on **Monday, December 14** at the **General Session** in ***Independence A*** (HYATT) or ***Meeting Room 10/11*** (RENAISSANCE)

GENERAL INFORMATION

Dining Options

We have assembled a short list of dining suggestions you may like to try during lunch breaks. See page 24 of this booklet.

Feedback Forms and Course Evaluations

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

Twitter

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

Wear Your Badge

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

Lead a BoF! (Birds of a Feather Session)

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

Bootcamp Sessions and Extended Hours

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

Bootcamps (Attendance Mandatory)

SEC401: Security Essentials Bootcamp Style

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

MGT414: SANS Training Program for CISSP® Certification

Extended Hours:

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

SEC560: Network Penetration Testing and Ethical Hacking

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

HOSTED: (ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Training Seminar

COURSE SCHEDULE

START DATE: **Saturday, December 12**

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

SEC440: Critical Security Controls: Planning, Implementing, and Auditing
Instructor: Jason Fossen
Location: Penn Quarter B (HYATT)

SEC524: Cloud Security Fundamentals
Instructor: Dave Shackleford
Location: Franklin Square (HYATT)

SEC580: Metasploit Kung Fu for Enterprise Pen Testing
Instructor: Bryce Galbraith
Location: Penn Quarter A (HYATT)

MGT415: A Practical Introduction to Cyber Security Risk Management
Instructor: James Tarala
Location: Cabin John/Arlington (HYATT)

MGT433: Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program
Instructor: Lance Spitzner
Location: Wilson/Roosevelt (HYATT)

MGT535: Incident Response Team Management
Instructor: Christopher Crowley
Location: Farragut Square (HYATT)

HOSTED: Physical Penetration Testing
Instructor: The CORE Group
Location: Lafayette Park (HYATT)

START DATE: **Monday, December 14**

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

SEC301: Intro to Information Security
Instructor: Keith Palmgren
Location: Cabin John/Arlington (HYATT)

SEC401: Security Essentials Bootcamp Style
Instructor: Paul A. Henry
Location: Constitution Ballroom A (HYATT)
Bootcamp Hours: 5:00-7:00pm (Course days 1-5)

SEC501: Advanced Security Essentials – Enterprise Defender
Instructor: Bryan Simon
Location: Tiber Creek A/B (HYATT)

SEC503: Intrusion Detection In-Depth
Instructor: Mike Poor
Location: Independence D/E (HYATT)

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

COURSE SCHEDULE

SEC505: Securing Windows with PowerShell and the Critical Security Controls
Instructor: Jason Fossen
Location: Franklin Square (HYATT)

SEC511: Continuous Monitoring and Security Operations
Instructor: Seth Misenar
Location: Wilson/Roosevelt (HYATT)

SEC550: Active Defense, Offensive Countermeasures and Cyber Deception
Instructor: Bryce Galbraith
Location: Meeting Room 10/11 (RENAISSANCE)

SEC560: Network Penetration Testing and Ethical Hacking
Instructor: Ed Skoudis
Location: Declaration A/B (HYATT)
Extended Hours: 5:00-7:15pm (Course Day 1 only)

SEC566: Implementing and Auditing the Critical Security Controls – In-Depth
Instructor: James Tarala
Location: Meeting Room 13 (RENAISSANCE)

SEC575: Mobile Device Security and Ethical Hacking
Instructor: Christopher Crowley
Location: Constitution E (HYATT)

SEC579: Virtualization and Private Cloud Security
Instructor: Dave Shackleford
Location: Penn Quarter B (HYATT)

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
Instructors: James Lyne, Stephen Sims
Location: Lafayette Park (HYATT)
Bootcamp Hours: 5:15pm-7:00pm (Course days 1-5)

FOR408: Windows Forensic Analysis
Instructor: Ovie Carroll
Location: Farragut Square (HYATT)

FOR508: Advanced Digital Forensics and Incident Response
Instructor: Alissa Torres
Location: Independence H/I (HYATT)

FOR572: Advanced Network Forensics and Analysis
Instructors: Philip Hagen
Location: Independence B (HYATT)

FOR578: Cyber Threat Intelligence
Instructors: Jake Williams
Location: Independence Ballroom C (HYATT)

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Instructor: Lenny Zeltser
Location: Constitution B (HYATT)

COURSE SCHEDULE

MGT414: SANS Training Program for CISSP® Certification
Instructor: Eric Conrad
Location: Constitution D (HYATT)
Bootcamp Hours: 8:00-9:00am (Course days 2-6) &
5:00-7:00pm (Course days 1-5)

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

MGT514: IT Security Strategic Planning, Policy and Leadership
Instructor: Mark Williams
Location: Meeting Room 16 (RENAISSANCE)

AUD507: Auditing & Monitoring Networks, Perimeters, and Systems
Instructor: David Hoelzer
Location: Renwick/Bulfinch (HYATT)

DEV544: Secure Coding in .NET: Developing Defensible Apps
Instructor: Aaron Cure
Location: Meeting Room 12 (RENAISSANCE)

ICS410: ICS/SCADA Security Essentials
Instructor: Justin Searle
Location: Constitution C (HYATT)

ICS515: ICS Active Defense and Incident Response
Instructor: Robert M. Lee
Location: Meeting Room 14 (RENAISSANCE)

LEG523: Law of Data Security and Investigations
Instructor: Benjamin Wright
Location: Penn Quarter A (HYATT)

HOSTED: (ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Training Seminar
Instructor: Staff
Location: Shaw (HYATT)
Extended Hours: 5:00-6:00pm (Course Days 1-5)

START DATE: **Thursday, December 17**

CORE NetWars Tournament
Host: Jeff McJunkin . . . . . Location: Independence A (HYATT)
Hours: 6:30-9:30pm

DFIR NetWars Tournament
Hosts: Philip Hagen & Jake Williams . . . . . Location: Declaration A/B (HYATT)
Hours: 6:30-9:30pm

SPECIAL EVENTS

Enrich your SANS experience!

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

SUNDAY, DECEMBER 13

SPECIAL EVENT
Registration Welcome Reception
Sun, Dec 13 | 5:00-7:00pm
Location: Grand Foyer Declaration Level (HYATT)
Location: Meeting Room Level Foyer (RENAISSANCE)

Register early and network with your fellow students!

SANS@NIGHT
Securing The Kids
Speaker: Lance Spitzner
Sun, Dec 13 | 6:00-7:00pm | Location: Constitution A (HYATT)

Technology 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 today's world they have to know how to leverage these new tools. However, with all these capabilities come new risks, risks that as parents we may not understand or even be aware of. In this interactive talk we discuss the top three risks to kids online and the steps parents are taking to educate and protect them.

MONDAY, DECEMBER 14

SPECIAL EVENT
General Session – Welcome to SANS
Mon, Dec 14 | 8:15-8:45am
Speaker: Jason Fossen
Location: Independence A (HYATT)
and
Speaker: Bryce Galbraith
Location: Meeting Room 10/11 (RENAISSANCE)

Join us for a 30-minute overview to help you get the most out of your SANS training experience. You will receive event information and learn about programs and resources offered by SANS. This brief session will answer many questions and get your training experience off to a great start. This session will be valuable to all attendees but is highly recommended for first time attendees.

SPECIAL EVENTS

KEYNOTE

What's New for Security in Windows 10 and Server 2016?

Speaker: Jason Fossen

Mon, Dec 14 | 7:15-9:15pm | Location: Independence A (HYATT)

Windows 8 was a flop, worse than Vista, so will Windows 10 be successful? The return of the Start Menu, touch screen integration, the faster Edge browser, and Cortana should make Windows 10 popular with users. Windows 10 also includes significant changes for security and manageability in large organizations, such as "Windows as a Service" rolling updates and deeper integration with Azure Active Directory. In this lively talk, Jason Fossen, author of the Securing Windows (SEC505) course at SANS, will lay out what to love and fear in Windows 10 and Windows Server 2016. We will also talk about some of the epic changes going on at Microsoft, now that CEO Steve Ballmer is gone. Is it really a new era for Microsoft? Come join the presentation and see what Microsoft is betting its future on!

TUESDAY, DECEMBER 15

SPECIAL EVENT

SANS Online Training Reception

Tue, Dec 15 | 6:00-7:00pm | Location: Latrobe Room (HYATT)

Transport yourself to the Latrobe Room on the Constitution level for a quick and fun Star Wars themed reception with the SANS Online Training team. Learn about our 2016 online course schedule, mingle with your fellow CDI classmates, and grab a bite while also vying for a few movie-inspired prizes.

SPECIAL EVENT

Women's CONNECT Event in Partnership with ISSA International Women In Security Special Interest Group (WIS SIG)

Speaker: Deanna Boyden

Tue, Dec 15 | 6:15-7:15pm | Location: Grand Foyer/Banneker (HYATT)

This reception is free of charge, but space is limited.
Join SANS and ISSA International Women In Security Special Interest Group (WIS SIG) as we partner with local DC metro area chapters and groups to foster an evening of connections. 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 attendees as well as the various groups who will be featured at the event. **Register at www.sans.org/bonus-sessions/register/8677/38942**

SPECIAL EVENTS

SANS@NIGHT

Offensive Countermeasures, Active Defenses, and Internet Tough Guys

Speaker: John Strand

Tue, Dec 15 | 7:15-8:15pm | Location: Independence A (HYATT)

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

SANS@NIGHT

The Crazy New World of Cyber Investigations: Law, Ethics, and Evidence

Speaker: Benjamin Wright

Tue, Dec 15 | 7:15-8:15pm | Location: Constitution A (HYATT)

Increasingly, employers and enterprises are engaged in cyber investigations. The explosion of cyber evidence (email, text, meta data, social media, etc.) about every little thing that anyone does or says creates a massive need for HR departments, IT departments, internal audit departments and other investigators to find and sift through this evidence. These cyber investigations are guided, motivated and restricted by a blizzard of new laws and court cases. Increasingly enterprises need professionals with backgrounds in cyber forensics, cyber law and computer privacy.

SANS@NIGHT

Automating Post-Exploitation with PowerShell

Speaker: James Tarala

Tue, Dec 15 | 7:15-8:15pm | Location: Constitution B (HYATT)

As organizations assess the security of their information systems, the need for automation has become more and more apparent. Not only are organizations attempting to automate their assessments, the need is becoming more pressing to perform assessments centrally against large numbers of enterprise systems. Penetration testers can use this automation to make their post-exploitation efforts more thorough, repeatable, and efficient. Defenders need to understand the techniques attackers are using once an initial compromise has occurred so they can build defenses to stop the attacks. Microsoft's PowerShell scripting language has become the defacto standard for many organizations looking to perform this level of distributed automation. In this presentation James Tarala, of Enclave Security, will describe to students the enterprise capabilities PowerShell offers and show practical examples of how PowerShell can be used to perform large scale penetration tests of Microsoft Windows systems.

SANS@NIGHT

The Effectiveness of Microsoft's EMET

Speaker: Stephen Sims

Tue, Dec 15 | 8:15-9:15pm | Location: Independence A (HYATT)

In this talk we will take a look at Microsoft's Enhanced Mitigation Experience Toolkit (EMET) and how it stops exploits from working. This free tool has a low adoption rate inside of companies, but has the ability to stop 0-day attacks from being successful. We will cover the effectiveness of the various controls, how they work, as well as techniques used to bypass the tool in targeted attacks.

SANS@NIGHT

How to Bring Some Advanced Persistent Trickery to Your Fight Against Advanced Persistent Threats

Speaker: Bryce Galbraith

Tue, Dec 15 | 8:15-9:15pm | Location: Constitution A (HYATT)

You know you have intruders in your house. But this is your house and no one knows it better than you. Don't sit back and wait. It's game on. This presentation will explore ways that you can frustrate, annoy, and potentially reveal Advanced Persistent Threats (APTs) with active defense, offensive countermeasures and cyber deception (legally and ethically).

WEDNESDAY, DECEMBER 16

SANS@NIGHT

Malware Analysis for Incident Responders: Getting Started

Speaker: Lenny Zeltser

Wed, Dec 16 | 7:15-8:15pm | Location: Independence A (HYATT)

Knowing how to analyze malware has become a critical skill for incident responders and forensic investigators. A good way to get started with such efforts involves examining how malicious software behaves in a controlled laboratory environment. In this two-hour seminar briefing, Lenny Zeltser demonstrates key aspects of this process, walking you through behavioral analysis of a malware specimen by using several free tools and even peeking into the world of code analysis. You will see practical techniques in action and understand how malware analysis will help you to triage the incident to assess key capabilities of the malicious software. You will also learn how to determine ways of identifying this malware on systems in your environment by establishing indicators of compromise (IOCs). This seminar will help you start learning how to turn malware inside out.

SPECIAL EVENTS

SANS@NIGHT

ICS/SCADA Cyber Attacks: Fact vs. Fiction

Speaker: Robert M. Lee

Wed, Dec 16 | 7:15-8:15pm | Location: Constitution B (HYATT)

Industrial Control Systems (ICS) play a huge role in almost every aspect of modern day life. Supervisory control and data acquisition (SCADA) as an example play a large role in monitoring and controlling the power grid, oil pipelines, and more. It's understandable then that they gain attention in national headlines when they come under attack. Due to this ability to grab attention and the complexity behind getting the technical details right though there have been cases where the stories have just been down right wrong. These inaccurate case-studies push hype and confusion which drives the investment of resources into trying to solve the wrong problem. The threat is real, but plenty of the stories are not. In this presentation, Robert M. Lee, the ICS515 author and FOR578 co-author will break down a number of high-profile stories that are fiction and then deconstruct real threats to show the actual issues in the community and what can be learned towards defense.

SANS@NIGHT

The Tap House

Speaker: Phil Hagen

Wed, Dec 16 | 7:15-8:15pm | Location: Constitution A (HYATT)

Packets move pretty fast. The field of Network Forensics needs to move fast, too. Whether you are investigating a known incident, hunting unidentified adversaries in your environment, or enriching forensic findings from disk- and memory-based examinations, it's critical to stay abreast of the latest developments in the discipline. In this @Night series, Phil Hagen will discuss some of the latest technologies, techniques, and tools that you will want to know in pursuit of forensication nirvana. Phil is also an avid craft beer fan, so there's a good chance you will learn something about a new notable national or interesting local beer in the process. This presentation will be helpful for those that wish to keep up-to-date on the most cutting-edge facets of Network Forensics.

SPECIAL EVENT

GIAC Program Overview

Speaker: Courtney Imbert

Wed, Dec 16 | 8:15-9:15pm | Location: Cabin John/Arlington (HYATT)

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

The Plinko Board of Modern Persistence Techniques

Speaker: Alissa Torres

Wed, Dec 16 | 8:15-9:15pm | Location: Constitution A (HYATT)

No matter what techniques an attacker employs to hide and persist on compromised remote systems, we must be up for the challenge, to detect, analyze and remediate. This session focuses on the latest techniques modern malware is using to ensure continued presence in your network. As detailed in recently released industry threat intelligence reports, these methods are increasing in sophistication and are often times missed by forensics tools developed to only enumerate common autorun and service persistence methods. In this presentation, we will cover advanced detection techniques, pivoting from physical memory analysis to the examination of remnants found on the file system.

SANS@NIGHT

Debunking the Complex Password Myth

Speaker: Keith Palmgren

Wed, Dec 16 | 8:15-9:15pm | Location: Constitution B (HYATT)

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

THURSDAY, DECEMBER 17

LUNCH & LEARN

STI Lunch and Learn

Speaker: Bill Lockhart

Thu, Dec 17 | 12:30-1:15pm | Location: Banneker Room (HYATT)

Space is Limited – RSVP Required (rsvp@sans.edu)

Extend your training with a graduate degree from SANS. Join us for lunch to learn how the class you're taking this week may apply towards a master's degree or graduate certificate program. Find out more at **www.sans.edu**. Email us at **info@sans.edu**.

CORE NETWARS TOURNAMENT

Host: Jeff McJunkin

Thu, Dec 17 & Friday, Dec 18 | 6:30-9:30pm

Location: Independence A (HYATT)

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

DFIR NETWARS TOURNAMENT

Hosts: Jake Williams and Phil Hagen

Thu, Dec 17 & Friday, Dec 18 | 6:30-9:30pm

Location: Declaration A/B (HYATT)

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

Evolving Threats

Speaker: Paul Henry

Thu, Dec 17 | 7:15-8:15pm | Location: Constitution A (HYATT)

For nearly two decades defenders have fallen into the "Crowd Mentality Trap." They have simply settled on doing the same thing everyone else was doing, while at the same time attackers have clearly evolved both in terms of malware delivery vectors and attack methodology. Today our defenses focus primarily on the gateway and upon attempting to outwit attacker's delivery methods. This leaves us woefully exposed and according to a recent Data Breach Report has resulted in 3,765 incidents, 806 million records exposed, and $157 billion in data breach costs in only the past six years. This presentation will highlight recent/current developments in the evolution of both attacks and defenses.

SANS@NIGHT

Card Fraud 101

Speaker: G. Mark Hardy

Thu, Dec 17 | 7:15-8:15pm | Location: Constitution B (HYATT)

Ever get a call from your bank saying your credit card was stolen, but it was still in your wallet? What's going on here? Card fraud costs $16 billion annually, and it's not getting better. Target, PF Changs, Michaels, Home Depot, who's next? Find out how these big card heists are pulled off, why chip-and-pin won't solve the fraud problem, and how crooks compromised Apple Pay. See if your bank even bothers to use the security protections it could – we'll have a mag stripe card reader so you can really see what's in your wallet. Certified SANS Instructor G. Mark Hardy is the CEO and founder of CardKill Inc., a start-up that helps banks preemptively kill stolen cards BEFORE they are used in fraud.

STI MASTER'S PRESENTATION

Building a Web Application Vulnerability Management Program

Speaker: Jason Pubal

Thu, Dec 17 | 7:15-8:15pm | Location: Constitution E (HYATT)

SANS@NIGHT

The 14 Absolute Truths of Security

Speaker: Keith Palmgren

Thu, Dec 17 | 8:15-9:15pm | Location: Constitution A (HYATT)

Keith Palmgren has identified fourteen "Absolute Truths" of security – things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these fourteen absolute truths and how they affect a security program can lead to the success of that program. Failing to recognize these truths will spell almost certain doom. Here we will take a non-technical look at each of the fourteen absolute truths in turn, examine what they mean to the security manager, what they mean to the security posture, and how understanding them will lead to a successful security program.

SANS@NIGHT

Information Security Risk Management – No Exceptions!

Speaker: Mark Williams

Thu, Dec 17 | 8:15-9:15pm | Location: Constitution B (HYATT)

As a risk analyst or manager, it is likely that your days are filled with requests for exceptions to policy to permit people to do things wrong. I believe there is a better way. Permitting exceptions can be a valuable tool in developing a process life cycle. It can also become an easy way to avoid making decisions to upgrade or improve systems. We are all faced daily with decisions on whether to permit exceptions. Let me show you how I think that continuous risk assessment and risk management can actually avoid the need for exceptions. By using a logical approach to risk identification, categorization and decision making, you too can do the "impossible" and say: NO EXCEPTIONS!

VENDOR EVENTS

Vendor Solutions Expo

Wed, Dec 16 | 12:00-1:30pm | 5:30-7:30pm
Location: Independence Foyer (HYATT)

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, Dec 16 | 5:30-7:30pm | Location: Independence Foyer (HYATT)

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, Dec 16 | 12:00-1:30pm | Location: Independence Foyer (HYATT)

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:

A10 Networks	ExaBeam	Pwnie Express
Cybereason	Forescout	Qualys
Datacom Systems	Keeper Security	ThreatConnect
Domain Tools	LightCyber	ThreatQuotient
ESVA	LogRhythm	ThreatSTOP
EventTracker	Malware Bytes	ThreatStream
	Palo Alto Networks	

VENDOR EVENTS

Vendor-Sponsored Lunch & Learns

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

LUNCH AND LEARN

Busting The Rebel Scum - QRadar and Box

Speakers: Peter Szczepankiewicz, IBM Product Manager
Sonny Hashmi, Managing Director, Box
Mon, Dec 14 | 12:30-1:15pm | Location: Latrobe

Cyber threats have become too common – compromising government agencies big and small. As a result, a multi-billion dollar cybersecurity industry has risen using innovations in technology to tackle increasingly sophisticated hacking threats. This lunch and learn will discuss the advanced defense techniques available inside IBM QRadar. The demo and discussion will cover many of the real-world cloud deployments and experiences in finding evil insiders using QFlow and advanced analytics. Updates from the latest release will be discussed, including IBM App Exchange, integration with your chosen IOC's through STIX TAXI, and other APIs, and how to handle MSSP events and flows for separate customers through a shared infrastructure.

LUNCH AND LEARN

Launch, Detect, Evolve: The Mutation of Malware

Speaker: Andres Ortiz, Malware Intelligence Analyst
Tue, Dec 15 | 12:30-1:15pm | Location: Independence H/I

In order to hit their targets, malware developers need to constantly evolve their tactics. This evolution is frequently done in very small incremental changes to known malware attacks. Today, malicious developers know their malware has a short half-life before detection. In order to optimize their efforts, cyber criminals now modify their "products" just enough to evade detection a little bit longer.

ForeScout
Access ability.

LUNCH AND LEARN

An Architecture for Continuous Monitoring and Mitigation

Tue, Dec 15 | 12:30-1:15pm | Location: Independence F/G

This session examines a reference architecture for continuous monitoring and mitigation, based on next-generation network access control, and a standards-based architecture to share information between and among legacy security systems. It will also examine a reference architecture for continuous monitoring and mitigation, based on next-generation network access control, and a standards-based architecture to share information between and among legacy security systems.

ThreatSTOP™

LUNCH AND LEARN

Defining Your First Line of Defense

Speaker: John Thompson, Director, Systems Engineering
Tue, Dec 15 | 12:30-1:15pm | Location: Independence D/E

Most people think of the perimeter as the initial enforcement point for security defenses. Prioritizing your strategy around managing inbound attacks will leave your organization exposed. A strategy for both inbound attacks and outbound malicious traffic prepares you for a broad range of attacks: DDoS, scanners, malware, data exfiltration, and data corruption (think ransomeware). Your security defense strategy should be bi-directional, with a first line of defense in place for all attack types. This talk will discuss the various types of attacks, and the best placement for your first line of defense, for both inbound and outbound traffic.

LIGHTCYBER

LUNCH AND LEARN

Think Like an Attacker: What You Must Know About Targeted Attack Techniques

Speaker: Michael Mumcuoglu, Co-Founder, and Chief Technology Officer, LightCyber
Tue, Dec 15 | 12:30-1:15pm | Location: Farragut Square

Attend the session and learn practical insight and detail on:

- How intruders move from a single compromised host or account to multiple points of control and gain full access to data and other resources completely undetected
- How attackers can be pinpointed through their operational activities
- How to detect only anomalies indicative of an active attack
- How to spot risky or improper internal behavior or the workings of a malicious insider

SOPHOS Infogressive, Inc.
Aggressive Information Security

LUNCH AND LEARN

Prevent – Detect – Respond

Speaker: Derrick Masters, Security Analyst
Tue, Dec 15 | 12:30-1:15pm | Location: Independence A

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

DOMAINTOOLS

LUNCH AND LEARN

See Threats Coming with DomainTools

Speaker: Mark Kendrick, Director of Solution Engineering
Thu, Dec 17 | 12:30-1:15pm | Location: Constitution A

The best incident responders know attribution can be a proxy for risk. Even when you don't know who's behind an attack, simply knowing what's linked to it can give you tremendous insight. This session will explore specific techniques for enumerating an attacker's online infrastructure and revealing patterns in the history of their domain names and IP addresses. You'll see firsthand the value of a domain-focused, actor-centric investigative model.

paloalto networks

LUNCH AND LEARN

Crack the Code: Defeat the Advanced Adversary

Speaker: Robert Clark, Systems Engineer
Thu, Dec 17 | 12:30-1:15pm | Location: Constitution B

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

QUALYS® CONTINUOUS SECURITY

LUNCH AND LEARN

Foundational Cybersecurity Hygiene: Getting Back to Basics

Speaker: Hariom Singh, CISSP, Director of Policy Compliance
Thu, Dec 17 | 12:30-1:15pm | Location: Wilson/Roosevelt

With cybersecurity taking the front seat in the boardroom, IT security and audit teams now have more visibility than ever before, and the stakes have never been higher. The challenge is that many teams are struggling to gain the visibility they need to be effective considering the consequences of Shadow IT, the disappearing perimeter, and the explosion of assets across a typical distributed enterprise. While it may be tempting to jump onto the next advanced technology bandwagon to address these risks, it's actually more effective to return to the basics of foundational cybersecurity hygiene. In this session, we'll share pragmatic lessons learned on how you can reduce risk and gain visibility and control – simply by returning to the basics: foundational cybersecurity hygiene.

THREATSTREAM®

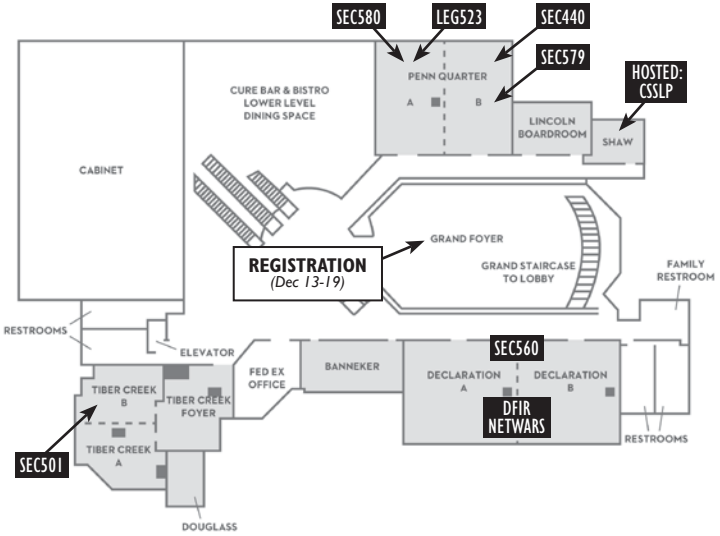
LUNCH AND LEARN

CISA: How Do We Get Past Walking and Actually Start Running with Information Sharing?

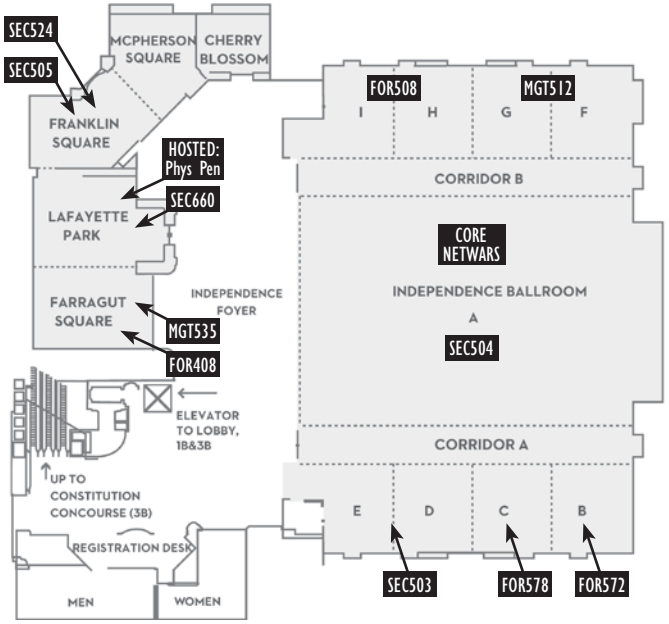
Speaker: Trish Cagliostro, Principal Security Architect
Thu, Dec 17 | 12:30-1:15pm | Location: Cabin John/Arlington

The road to the Cybersecurity Information Sharing Act (CISA) passing the Senate on October 27th was long and complicated. After years of discussion on information sharing, a recent string of high profile breaches provided the momentum to finally bring CISA to the Senate floor. There is consensus that we need to improve the overall security posture of the U.S., but many in industry are divided on the impact that CISA will have. Join ThreatStream to learn about the key points of CISA and the power of information sharing so you can be be the expert in your organization.

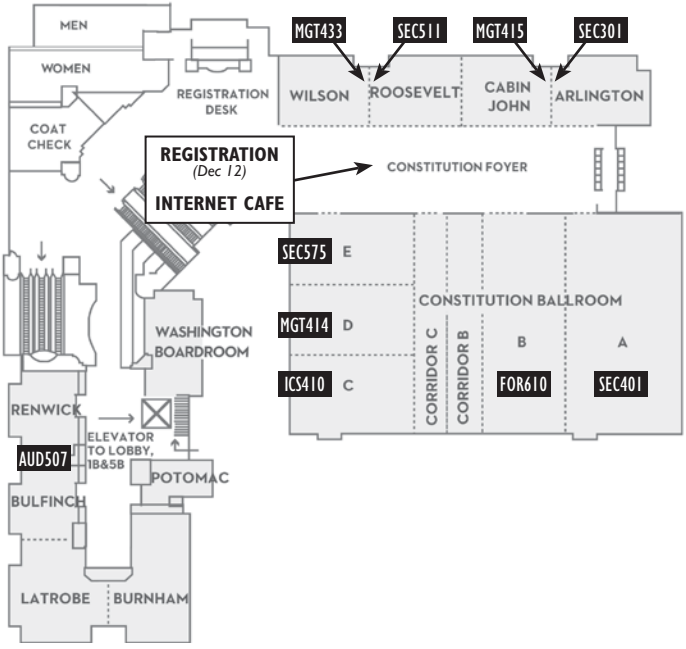
HYATT
DECLARATION LEVEL (1B)



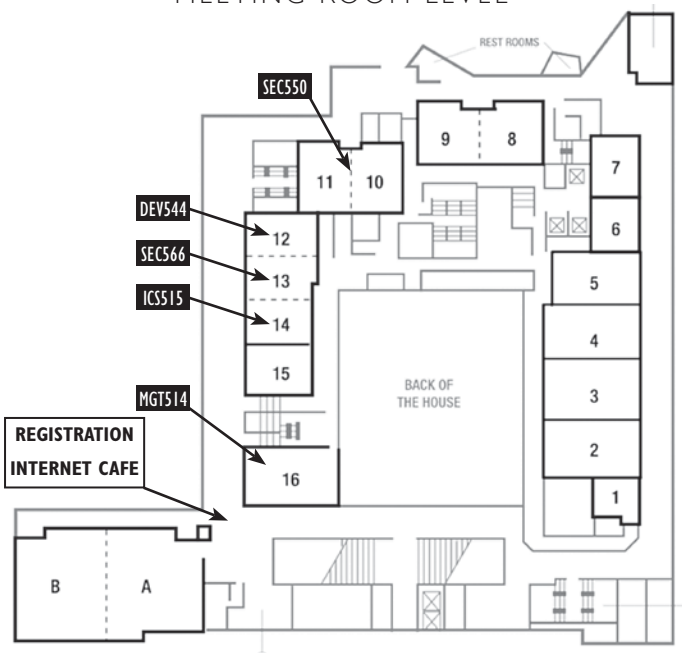
HYATT
INDEPENDENCE LEVEL (5B)



HYATT
CONSTITUTION LEVEL (3B)



RENAISSANCE
MEETING ROOM LEVEL



HOTEL FLOORPLAN

DINING OPTIONS

Cure Bar & Bistro

Cure Bar & Bistro in the Penn Quarter near Chinatown is a unique DC restaurant inspired by the culinary tradition of curing foods and pairing beverages to create a taste profile. The process first entails spicing, drying, salting and smoking foods to then match them with beverages that enhance their flavor. The seasonal menu of this delicious restaurant at Grand Hyatt Washington includes the finest sustainable ingredients for a mouthwatering, farm-to-table dining experience. The wine, beer and spirit selections are extensive, earning Cure Bar & Bistro top ranks among Washington, DC bars. Happy Hour specials are available.

Cure Bar & Bistro is ideal for socializing with friends while sharing light dishes and drinks, or enjoying a relaxing four-course meal. The welcoming ambiance of Cure Bar & Bistro is complemented by high ceilings, an open fireplace and walls clad in stone and red oak.

The Grand Cafe

Dining in the park.... with no threat of rain! The atmosphere is always charming at The Grand Cafe, our informal, atrium restaurant. Start your day off with a delicious breakfast from our tempting buffet, accompanied by a cup of freshly brewed Starbucks coffee. Take a break from a busy round of meetings with a relaxing lunch alongside the lagoon. Serving breakfast and lunch daily, The Grand Cafe offers a wide variety of menu choices.

Zephyr Deli

Need to grab a bite and head to a meeting? Taking lunch with you as you spend the day touring this fascinating city? Stop by Zephyr Deli for delicious and satisfying breakfast and lunch options, just right for eating on the run. Choose from an ever-changing selection of freshly baked pastries, seasonal fruit, gourmet sandwiches, salads and paninis. Satisfy your sweet tooth with a scrumptious treat from our bakery section, featuring tempting pies, cakes and cookies.

Starbucks®

Starbucks is a one stop for your favorite coffee, tea and treats. Conveniently located on the lobby level, Starbucks offers a wide selection of coffee, cappuccino, lattes, Frappuccinos, flavored teas and seasonal creations, as well as light snacks and pastries.

Room Service

Whether you prefer a Continental breakfast served in your Washington, DC hotel room as your wake-up call, a working lunch as you complete a report or a romantic dinner for two, our professional in-room dining staff is at your service. Choose from a complete dining menu, including a full selection of wine and beer.

Several of our welcoming rooms and suites provide the perfect place to host a small gathering of family or business associates. Contact in-room dining or the concierge for more information and menu option.

Future SANS Training Events

Las Vegas 2016
Las Vegas, NV | Jan 9-14

Security East 2016
New Orleans, LA | Jan 25-30

Cyber Threat Intelligence SUMMIT & TRAINING 2016
Alexandria, VA | Feb 3-10

Scottsdale 2016
Scottsdale, AZ | Feb 8-13

McLean 2016
McLean, VA | Feb 15-20

ICS Security SUMMIT & TRAINING 2016
Orlando, FL | Feb 16-23

Anaheim 2016
Anaheim, CA | Feb 22-27

Philadelphia 2016
Philadelphia, PA | Feb 29 - Mar 5

SANS 2016
Orlando, FL | Mar 12-21

Reston 2016
Reston, VA | Apr 4-9

Atlanta 2016
Atlanta, GA | Apr 4-9

Threat Hunting and Incident Response
SUMMIT & TRAINING 2016
New Orleans, LA | Apr 12-19

Pen Test Ausitin 2016
Austin, TX | Apr 18-23

Security West 2016
San Diego, CA | April 29 - May 6

Baltimore Spring 2016
Baltimore, MD | May 9-14

Houston 2016
Houston, TX | May 9-14

Security Operations Center SUMMIT & TRAINING 2016
Crystal City, VA | May 19-26

SANSFIRE 2016
Washington, DC | Jun 11-18

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