SANS

CDI

CYBER DEFENSE INITIATIVE 2016

Washington, DC | December 10-17

PROGRAM GUIDE

@SANSInstitute  #SANSCDI

Bundle GIAC certification with SANS training and SAVE $340!

In the information security industry, certification matters. The Global Information Assurance Certification (GIAC) program offers skills-based certifications that go beyond high-level theory and test true hands-on and pragmatic skill sets that are highly regarded in the InfoSec industry.

Save $340 when you bundle your certification attempt with your SANS training course. Simply stop by Registration and add your certification option before the last day of class.

Find out more about GIAC at www.giac.org or call 301-654-7267.

SANS OnDemand Bundle

Add an OnDemand Bundle to your course to get an additional four months of intense training! OnDemand Bundles are just $689 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

Visit the Information Desk
located in the Constitution Foyer (HYATT)
Call (301) 654-SANS
Or email to ondemand@sans.org

TABLE OF CONTENTS

CORE NETWARS EXPERIENCE

Hosted by Jeff McJunkin
Thursday, December 15 and Friday, December 16
6:30-9:30pm | Independence A

DFIR NETWARS TOURNAMENT

Hosted by Philip Hagen & Chad Tilbury
Thursday, December 15 and Friday, December 16
6:30-9:30pm | Constitution A

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-2016/schedule

GENERAL INFORMATION

Registration Check-In Schedule

Location: Registration Desk (CONSTITUTION LEVEL – HYATT)

Saturday, December 10 (Short Courses Only) 8:00-9:00am
Sunday, December 11 (MGT305 Only) 8:00-9:00am

Location: Grand Foyer (DECLARATION LEVEL – HYATT)

Sunday, December 11 . . . . . 5:00-7:00pm
Monday, December 12 . . . . . 7:00-9:00am

Location: Registration Desk (CONSTITUTION LEVEL – HYATT)

Monday, December 12 . . . . . 9:00am - 5:00pm
Tuesday, December 13 - Saturday, December 17 . . . . . 8:00am - 5:00pm

Courseware Pick-up Location

Location: Latrobe (CONSTITUTION LEVEL – HYATT)

Saturday, December 10 (Short Courses Only) 8:00-9:00am
Sunday, December 11 (MGT305 Only) 8:00-9:00am
Sunday, December 11 (Welcome Reception) 5:00-7:00pm
Monday, December 12 . . . . . 7:00-9:00am

Internet Café *(WIRELESS)*

Location: Constitution Foyer (CONSTITUTION LEVEL – HYATT)
Open from noon on Monday, December 12
and closes Saturday, December 17 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 **8:00-8:30am** on **Monday, December 12** at the **General Session** in ***Independence A***

GENERAL INFORMATION

Photography Notice

SANS may take photos of classroom activities for marketing purposes. SANS Cyber Defense Initiative 2016 attendees grant SANS all rights for such use without compensation, unless prohibited by law. Those who wish not to be photographed onsite should notify the photographer.

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 day and evening session and drop it in the evaluation box.

Wear Your Badge

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

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

SEC511: Continuous Monitoring and Security Operations

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

SEC760: Advanced Exploit Development for Penetration Testers

MGT414: SANS Training Program for CISSP® Certification

Extended Hours:

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

SEC560: Network Penetration Testing and Ethical Hacking

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

COURSE SCHEDULE

START DATE: **Saturday, December 10**
Time: 9:00am-5:00pm (Unless otherwise noted)
All courses are located in the Hyatt (unless otherwise noted)

SEC440: Critical Security Controls: Planning, Implementing, and Auditing
Instructor: Randy Marchany . . . . . .Location: Tiber Creek A/B

SEC567: Social Engineering for Penetration Testers
Instructor: Dave Shackleford . . . . . Location: Farragut Square

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

MGT415: A Practical Introduction to Cyber Security Risk Management
Instructor: James Tarala. . . . . .Location: Penn Quarter B

MGT433: Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program
Instructor: Lance Spitzner . . . . . .Location: Declaration A/B

MGT535: Incident Response Team Management
Instructor: Christopher Crowley. . . .Location: Wilson/Roosevelt

DEV534: Secure DevOps: A Practical Introduction
Instructors: Frank Kim, Ben Allen Location: Cabin John/Arlington

HOSTED: Health Care Security Essentials
Instructor: Greg Porter . . .Location: McPherson/Franklin Square

HOSTED: Physical Access Control Systems: Elements of Design, Offense, and Defense
Instructor: The CORE Group . . . . . .Location: Shaw

START DATE: **Sunday, December 11**
Time: 9:00am-5:00pm (Unless otherwise noted)
All courses are located in the Hyatt (unless otherwise noted)

MGT305: Technical Communication and Presentation Skills for Security Professionals
Instructor: Bryan Simon . . . . . Location: Lafayette Park

START DATE: **Monday, December 14**
Time: 9:00am-5:00pm (Unless otherwise noted)
All courses are located in the Hyatt (unless otherwise noted)

SEC301: Intro to Information Security
Instructor: Keith Palmgren. . . . . .Location: Wilson/Roosevelt

SEC401: Security Essentials Bootcamp Style
Instructor: Bryan Simon. . . . . .Location: Constitution B
Bootcamp Hours: 5:00-7:00pm (Course days 1-5)

COURSE SCHEDULE

SEC501: Advanced Security Essentials – Enterprise Defender
Instructor: Paul A. Henry . . . . . Location: Constitution C

SEC503: Intrusion Detection In-Depth
Instructor: Mike Poor. . . . . .Location: Cabin John/Arlington

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

SEC505: Securing Windows and PowerShell Automation
Instructor: Jason Fossen. . . . . .Location: Independence B

SEC511: Continuous Monitoring and Security Operations
Instructors: Seth Misenar, Ismael Valenzuela
Location: Constitution E
Bootcamp Hours: 5:00-7:00pm (Course days 1-5)

SEC542: Web App Penetration Testing and Ethical Hacking
Instructor: Eric Conrad . . . . . Location: Independence F/G

SEC550: Active Defense, Offensive Countermeasures, and Cyber Deception
Instructor: Bryce Galbraith . . . . . .Location: Tiber Creek A/B

SEC560: Network Penetration Testing and Ethical Hacking
Instructor: Michael Murr . . . . . Location: Independence D/E
Extended Hours: 5:00-7:15pm (Course Day 1 only)
**Extended hours will be led by John Strand in the SEC504 classroom located in Independence A*

SEC561: Immersive Hands-on Hacking Techniques
Instructor: Kevin Fiscus . . . . . .Location: Penn Quarter A

SEC566: Implementing and Auditing the Critical Security Controls – In-Depth
Instructor: James Tarala . . . . . Location: Independence H/I

SEC575: Mobile Device Security and Ethical Hacking
Instructor: Christopher Crowley
Location: Junior Ballroom 3 (MARRIOTT)

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

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
Instructor: Tim Medin. . . . . Location: Constitution D
Bootcamp Hours: 5:15pm-7:00pm (Course days 1-5)

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

FOR408: Windows Forensic Analysis
Instructor: Ovie Carroll . . . . . .Location: Constitution A

COURSE SCHEDULE

FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting
Instructor: Chad Tilbury . . .Location: McPherson/Franklin Square

FOR518: Mac Forensic Analysis
Instructor: Sarah Edwards . . . . . .Location: Shaw

FOR572: Advanced Network Forensics and Analysis
Instructors: Philip Hagen . . . . . Location: Farragut Square

FOR578: Cyber Threat Intelligence
Instructors: Jake Williams . . . . . .Location: London 1/II (MARRIOTT)

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Instructor: Lenny Zeltser . . . . . .Location: Declaration A/B

MGT414: SANS Training Program for CISSP® Certification
Instructor: David R. Miller . . . . . .Location: Capitol Hill (MARRIOTT)
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: Junior Ballroom 2 (MARRIOTT)
Extended Hours: 5:00-6:00pm (Course days 1-4)

MGT514: IT Security Strategic Planning, Policy, and Leadership
Instructor: Frank Kim. . . . .Location: Junior Ballroom 1 (MARRIOTT)

DEV522: Defending Web Applications Security Essentials
Instructor: Johannes Ullrich, PhD . . . . .Location: Penn Quarter B

AUD507: Auditing & Monitoring Networks, Perimeters, and Systems
Instructor: Clay Risenhoover . .Location: Penn Quarter (MARRIOTT)

ICS456: Essentials for NERC Critical Infrastructure Protection
Instructor: Tim Conway . . . . . Location: Lafayette Park

ICS515: ICS Active Defense and Incident Response
Instructor: Robert M. Lee. . . . . .Location: Renwick

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: Constitution A (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 11

SPECIAL EVENT

Registration Welcome Reception

Sun, Dec 11 | 5:00-7:00pm | Location: Constitution Foyer

Register early and network with your fellow students!

SANS@NIGHT

Securing Your Kids

Speaker: Lance Spitzner

Sun, Dec 11 | 7:00-8:00pm | Location: Mcpherson/Franklin

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 12

SPECIAL EVENT

General Session – Welcome to SANS

Mon, Dec 12 | 8:00-8:30am

Speaker: Bryan Simon | Location: Independence A

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 Microsoft Windows Server 2016 and Windows 10?

Speaker: Jason Fossen

Mon, Dec 12 | 7:15-9:15pm | Location: Independence A

Ubuntu Bash built into Windows? Microsoft open-source projects on GitHub? Free upgrades to Windows 10? It's a new Microsoft under CEO Satya Nadella, that's for sure. In this talk, Jason Fossen, a SANS Institute Fellow and author of the Securing Windows course (SEC505), will lay out what's new for security in Server 2016 and Windows 10. Come see how Docker containers, Credential Guard, Windows as a Service (WaaS), biometric facial scanning, Server Nano, PowerShell and Bash can all figure into your organization's IT security planning. Is it really a "New Microsoft" when it comes to security or just the same old thing wrapped in new buzzwords? Come to the event and see!

TUESDAY, DECEMBER 13

SPECIAL EVENT

Women's CONNECT Event

Hosted by SANS COINS Program and ISSA WIS SIG

Tue, Dec 13 | 6:15-9:15pm | Location: Grand Foyer

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/10345/27544**

SPECIAL EVENT

GIAC Program Presentation

Speaker: Scott Cassity

Tue, Dec 13 | 6:15-7:15pm | Location: Cabin John/Arlington

Global Information Assurance Certification (GIAC) develops and administers the premier certifications for information security professionals. More than 30 GIAC certifications align with SANS training and ensure mastery in critical, specialized InfoSec domains. GIAC certifications provide the highest and most rigorous assurance of cybersecurity knowledge and skill available to industry, government, and military clients across the world. Join us for an informational presentation along with a Q&A session. We'll cover everything from why you should get certified, what testing looks like, how to keep certifications current and more. GIAC staff will be present to answer your questions before and after the presentation.

SPECIAL EVENTS

SANS@NIGHT

Security Awareness: Understanding and Managing Your Top Seven Human Risks

Speaker: Lance Spitzner

Tue, Dec 13 | 7:15-8:15pm | Location: Independence H/I

A key step to managing your human risk is first identifying and then prioritizing those risks and then focusing on the top ones. After working with hundreds of organizations, Lance Spitzner will discuss what are the seven most common human risks he finds in organizations and what you can do to effectively manage and measure those specific risks.

SPECAL EVENT

(CS)²AI Special Event: Control System Cyber Security Association International

Speakers: Derek Harp and Mike Assante

Tue, Dec 13 | 7:15-8:15pm | Location: Tiber Creek A/B & Foyer

Highlight your CDI experience with Derek Harp, Mike Assante and other ICS security leaders at the (CS)²AI special event. Network with your peers as you learn more about this growing new control and automation system security-focused organization.

STI MASTER'S PRESENTATION

Using Splunk to Detect DNS Tunneling

Speaker: Steve Jaworski

Tue, Dec 13 | 7:15-7:55pm | Location: Independence D/E

DNS tunneling is a method to bypass security controls and exfiltrate data from a targeted organization. Choose any endpoint on your organization's network and perform a lookup to a public site, if it resolves with the site's IP address, that endpoint is susceptible to DNS Tunneling. It is not possible to block all DNS tunnels. Logging all DNS transactions is necessary to detect the occurrence of DNS Tunnels. Using Splunk can help ingest the large volume of log data and mine the information to determine what malicious actors may be using DNS tunneling techniques on target organizations networks.

SANS@NIGHT

Analysis of the Cyber Attack on the Ukrainian Power Grid

Speaker: Robert M. Lee

Tue, Dec 13 | 8:15-9:15pm | Location: Independence H/I

On Dec 23, 2016, the Ukrainian power grid suffered outages to roughly 230,000 customers due to a cyber attack. This was the first ever public cyber attack on a power grid that led to outages and holds lessons for a wide variety of communities. Robert M. Lee and the SANS ICS team broke the news on the malware uncovered and later confirmed the cyber attack. In this presentation learn about the investigation, the analysis, and the lessons learned for the larger security community.

SPECIAL EVENTS

SANS@NIGHT

Current and Future Trends in Digital Investigative Analysis

Speaker: Ovie Carroll

Tue, Dec 13 | 8:15-9:15pm | Location: Constitution A

In this fun and fast-paced presentation, Ovie Carroll will discuss current and future trends in digital investigative analysis. Ovie will cover critical challenges digital investigative analyst (computer forensic examiners) face and cover some of the most interesting digital artifacts.

STI MASTER'S PRESENTATION

Gh0st in the Dshell: Decoding Undocumented Protocol

Speaker: David Martin

Tue, Dec 13 | 8:15-8:55pm | Location: Independence D/E

While many types of malware use well-documented protocols, such as HTTP, HTTPS, or IRC for command and control, any network traffic analyst will eventually encounter malware that uses an undocumented, custom protocol. This traffic is sometimes encrypted but often relies on simple obfuscation techniques or security through obscurity to avoid detection. These protocols must be decoded to understand what an attacker is doing on a victim system and develop signatures to detect it. The art of reverse-engineering undocumented network protocols can be a difficult and time-consuming process, but can be greatly simplified by using Dshell, a network traffic analysis framework developed by the U.S. Army Research Lab and recently released open source to the information security community. Dshell comes with a number of powerful built-in decoders, but also allows analysts to write custom decoder and parser modules for new network protocols. This case study will demonstrate the process of reverse engineering a command and control protocol and writing a Dshell decoder for it, using the Gh0st remote access Trojan (RAT)'s proprietary network communication protocol as an example.

WEDNESDAY, DECEMBER 14

SANS@NIGHT

The iOS of Sauron: How iOS Tracks Everything You Do

Speaker: Sarah Edwards

Wed, Dec 14 | 7:15-8:15pm | Location: Independence H/I

iOS devices have the ability to track everything the user does – how many steps the user takes, where the user has been – and keeps track of how they use their devices. This presentation will dive into some of the protected files that keep track of every detail of a user's life that iOS tracks. These databases and files can be used to correlate user activity down to the smallest detail. Methods of analysis as well as some scripts will be shown to help analyze these files.

SPECIAL EVENTS

SANS@NIGHT

CISSP®: How to Get the Certification that Matters the Most

Speaker: David R. Miller

Wed, Dec 14 | 7:15-8:15pm | Location: Independence F/G

See why the CISSP® certification is so important to your IT career. Companies are in great need of qualified security professionals. The positions are there. The budget is there. Many IT security positions remain available because there are too few certified IT security professionals. This means you can choose which position you want from many companies.

STI MASTER'S PRESENTATION

Collecting Windows Installed Software Details

Speaker: Jonathan Risto

Wed, Dec 14 | 7:15-7:55pm | Location: Independence D/E

The 20 Critical Controls provide a guideline for the controls that need to be placed in our networks to manage and secure our systems. The second control states there should be a software inventory that contains the names and versions of the products for all devices within the infrastructure. The challenge for a large number of organizations is the ability to have accurate information available with minimal impact on tight IT budgets. This presentation will discuss the Microsoft Windows command line tools that will gather this information, and demonstrate example scripts to collect this information.

SANS@NIGHT

DLP FAIL!!! Using Encoding, Steganography, and Covert Channels to Evade DLP and Other Critical Controls

Speaker: Kevin Fiscus

Wed, Dec 14 | 8:15-9:15pm | Location: Independence H/I

It's all about the information! Two decades after the movie Sneakers, the quote remains as relevant, if not more so. The fact that someone hacks into an environment is interesting but not that relevant. What is important is what happens after the compromise. If the data is destroyed or modified, organizations are negatively impacted but the benefits to an attacker for destruction or alteration are somewhat limited. Stealing information however, is highly profitable. Identity theft, espionage, and financial attacks involve the exfiltration of sensitive data. As a result, organizations deploy tools to detect and/or stop that data exfiltration. While these tools can be extremely valuable, many have serious weaknesses; attackers can encode, hide, or obfuscate the data, or can use secret communication channels. This session will talk about and demonstrate a range of these methods.

SPECIAL EVENTS

SANS@NIGHT

The Tap House

Speaker: Philip Hagen

Wed, Dec 14 | 8:15-9:15pm | Location: Independence F/G

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.

STI MASTER'S PRESENTATION

Using Vagrant to Create Repeatable and Sharable Research Environments

Speaker: Shaun McCullough

Wed, Dec 14 | 8:15-8:55pm | Location: Independence D/E

This presentation will introduce the Vagrant software application and will discuss how it can be used by Information Security (InfoSec) professionals to provide their audience with an infrastructure environment to accompany their research. InfoSec professionals conducting research or publishing write-ups can provide opportunities for their audience to replicate and walk through the research themselves in their own environment. Vagrant is a popular DevOps tool for providing portable and repeatable production environments for application developers, and can be used to provide richer research environments for InfoSec professionals. The presentation will investigate how Vagrant works, the pros and cons of the technology and how it is typically used. The presentation will demonstrate how it can be used to create repeatable environments highlighting different features of Vagrant.

THURSDAY, DECEMBER 15

LUNCH & LEARN

How to Become a SANS Instructor

Speaker: Eric Conrad

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

This presentation is free, but space is limited to the first 40 registrations.

Have you ever wondered what it takes to become a SANS instructor? How does your SANS instructor rise to the top and demonstrate the talents to become part of the SANS faculty? Attend this session and learn how to become part of the faculty and learn the steps to make that goal a reality. SANS Principal instructor Eric Conrad will share his experiences and show you how to become part of the SANS top-rated instructor team.

SPECIAL EVENTS

SPECIAL EVENT

Maintaining a Digital Evidence Program in an Ever-Changing Environment

Speaker: Charles Mallery

Thu, Dec 15 | 5:30-6:30pm | Location: Lafayette Park

Digital Evidence is critical to many criminal investigations. Advancements in technology are presenting tremendous challenges to law enforcement, who must rapidly adopt new procedures and implement new techniques to access and analyze digital evidence. The need for adaptability is leading to shifts in hiring practices and redesign of digital evidence programs. These challenges make it more critical than ever for companies to maintain relationships with their local FBI offices, and to have a plan that preserves evidence required by law enforcement.

CORE NETWARS EXPERIENCE

Host: Jeff McJunkin

Thu, Dec 15 & Fri, Dec 16 | 6:30-9:30pm | Location: Independence A

SANS Core NetWars Experience 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: Philip Hagen & Chad Tilbury

Thu, Dec 15 & Fri, Dec 16 | 6:30-9:30pm | Location: Constitution A

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.

SPECIAL EVENTS

SANS@NIGHT

Quality Not Quantity: Continuous Monitoring's Deadliest Events

Speaker: Eric Conrad

Thu, Dec 15 | 7:15-8:15pm | Location: Independence F/G

Most Security Operations Centers are built for compliance, not security. One well-known retail firm suffered the theft of over a million credit cards. 60,000 true positive events were reported to their SOC during that breach... and missed: lost in the noise of millions. If you are bragging about how many events your SOC "handles" each day: you are doing it wrong. During this talk we will show you how to focus on quality instead of quantity, and provide an actionable list of the deadliest events that occur during virtually every successful breach.

SANS@NIGHT

Prioritizing Your Security Program

Speaker: Keith Palmgren

Thu, Dec 15 | 7:15-8:15pm | Location: Declaration A/B

Building a cybersecurity program is easy. Building a cybersecurity program that is effective is seriously hard! When faced with a seemingly insurmountable task, prioritization is vital. Investing time and money in the right place at the right time is the difference between success and being the next cyberbreach headline. Whether you are new to cybersecurity or an old hand, you may feel lost in the storm. If so, this talk is for you. Cybersecurity's five (5) historic and current pitfalls that prevent organizations from building an effective IT Security platform will be discussed: Poor Passwords, Vulnerabilities, Malware/Crimeware, Insider Threat, and Mismanagement. To build that effective cybersecurity platform in today's ever-changing information technology environment, organizations must prioritize and focus on five key principles that address those pitfalls. We must look at those critical security principles in new and different ways. 'The Principle of Least Privilege'; Authentication, Authorization, & Accountability (AAA); Confidentiality, Integrity, & Availability (CIA); Policy, Procedure, & Training (PPT); Hardening, Patching, & Monitoring (HPM); and Protect, Detect, & Respond (PDR). Every organization needs a cybersecurity strategy. An effective strategy requires that you understand the problems as well as the solutions to those problems. Only then can you prioritize your limited cybersecurity resources. Managers and technicians alike will gain valuable insight in this non-technical talk.

SPECIAL EVENTS

STI MASTER'S PRESENTATION

Portable NFAT Tools, Techniques, and System Build

Speaker: Don Murdoch

Thu, Dec 15 | 7:15-7:55pm | Location: Independence D/E

With today's malicious software and myriad of network aware client-side software, one of the tools that should be in the forensic analysts' toolbox is a portable response system for data collection and analysis. This presentation will provide a cookbook approach to build a portable forensic workstation that provides several virtual environments installed together with supplemental hardware, such as multiple NICs and modern managed switch in order to provide a network forensic tool.

SANS@NIGHT

Open-Source Intelligence (OSINT) Tips for Malware Investigations

Speaker: Lenny Zeltser

Thu, Dec 15 | 8:15-9:15pm | Location: Independence D/E

Alf you're responding to a malware incident, you need to quickly derive relevant and actionable information about the malicious program and the context within which it was employed. This involves not only examining the specimen in your lab, but also benefiting from relevant publicly-available details. Accomplishing this requires the right skills to locate and makes sense of the data. This engaging presentation will show several real-world examples, tools, and data sources for gathering such open-source intelligence (OSINT).

FRIDAY, DECEMBER 16

SPECIAL EVENT

Trustworthiness with Cyber-Physical Systems

Speaker: Paul Shaw & Chris Newborn

Fri, Dec 16 | 5:30-6:30pm | Location: Lafayette Park

Traditional cybersecurity efforts required knowledge of the cyber threat and an ability to detect their presence for a proper response. Emerging cybersecurity concepts and technologies for cybersecurity are more dependent upon a combination of robustness and resilience. Emerging resilience concepts and technologies are doing more with trustworthiness. When a defender uses emerging resilience concepts, the adversary has a more difficult time maintaining control of their attack chain. The concept of trustworthiness will be explored with Cyber-Physical Systems (CPS). The urgency and consequence for CPS to a cybersecurity portfolio approach for robustness and resilience will be explained. This presentation explores going beyond traditional cybersecurity constructs of vulnerability elimination and focus more on adaptive, dynamic defense.

VENDOR EVENTS

Vendor Solutions Expo

Wed, Dec 14 | 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 14 | 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 14 | 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	InfoArmor	Recorded Future
Anomali	Javelin Networks	Sophos
Circadence	LogRhythm	Syncurity
Cloudera	MetricStream	Terbium Labs
Crossmatch	Mobileiron	ThreatConnect
Farsight Security	NetBrain	ThreatQuotient
Guardicore	Qualys	

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.

ANOMALI™

LUNCH AND LEARN

Manual Threat Intelligence Management: Doing it the Hard Way

Speaker: Chris Black, Sr. Sales Engineer
Tue, Dec 13 | 12:30-1:15pm | Location: Independence H/I

Threat Intelligence is a popular topic in security circles these days. Many organizations are now utilizing a threat feed that comes bundled with some other security product. This presentation will explore the steps required to set up a manual threat intelligence life cycle management program for those who prefer the in-house approach.

NetBrain®

LUNCH AND LEARN

Adaptive Network Automation Framework in Support of Cyber Defense

Speaker: Richard Larkin, Sr. Network Engineer
Tue, Dec 13 | 12:30-1:15pm | Location: Constitution A

Network Automation improves efficiency of NetOps by providing real-time and historic network visibility and facilitates collaboration with CyberOps. It can have a dramatic impact before, during and after cyber-attacks. Network Automation allows for compliance verification and validation, on-demand monitoring though visual troubleshooting and remediation. With the increasing pace and complexity of cyber-attacks in a resource strained environment, network automation is important for maintaining a solid cyber defense.

VENDOR EVENTS

LUNCH AND LEARN

Modern Mobility Ushers in a New Age of Security

Speaker: Sean Frazier, Chief Technical Evangelist
Tue, Dec 13 | 12:30-1:15pm | Location: Independence D/E

The shift of the modern enterprise to mobile and cloud has forced a rethink of enterprise security fundamentals. It can feel like a complicated puzzle of new approaches and technologies. MobileIron will walk you through best practices when it comes to securing modern mobility.

SOPHOS

LUNCH AND LEARN

Exploit Prevention: Stop Ransomware, Zero-Day and Modern Attacks Before They Get In

Speaker: Matt Hickey, Director, Sales Engineering
Tue, Dec 13 | 12:30-1:15pm | Location: Independence F/G

While old school anti-virus protection focuses examining files to detect malware, cyber criminals have persisted and can now polymorph malware so that no signature-based detection method has a chance. By leveraging zero-day vulnerabilities, hackers can easily bypass even the most advanced file analysis detection products.

MetricStream

LUNCH AND LEARN

Building the Business Case for IT Vendor Risk Management

Speaker: French Caldwell, Chief Evangelist
Tue, Dec 13 | 12:30-1:15pm | Location: Declaration A/B

As IT Organizations increase their exposure and dependency on vendors to manage an increasingly digital enterprise, organizations need a definitive strategy backed by intelligent technology to manage the risks. Today, Organizations need to simplify and strengthen their IT vendor on-boarding, ongoing risk assessment and remediation workflows to mitigate the risks while managing the relationships effectively. Join us, as we discuss the tenets of an effective and robust IT vendor risk management program and provide some tips on building a business case for the top management as a key part of the overall IT Risk and Compliance program within the organization.

VENDOR EVENTS

SPECIAL VENDOR EVENT

Test Your Cybersecurity Skills Through Gaming

Tue, Dec 13 | 6:30-8:30pm | Location: Constitution C

Bring your laptop and test your skills at cybersecurity defense or offense through our online gamification platform. We are looking for players to be broken into teams on offensive and defensive missions. Don't be shy – Athena (A.I.) will guide you along the way. Cyber ninjas will be rewarded. ***Sign up at vendor registration.***

LUNCH AND LEARN

Lets Plan an APT

Speaker: Guy Franco, CTO Javelin Networks

Thu, Dec 15 | 12:30-1:15pm | Location: Independence H/I

Once breached at the endpoint, what does an attacker do? Where is he going? What does he want? Since 1999, Microsoft has made the Windows Domain the 'heart' of the network. Once accessed, it permits the attacker to control the organization – undetected and indefinitely. This presentation will discuss all moves an attacker can make to go from a compromised machine to achieve his goal from a statistical point of view; we will present the probability of detection and evidence-gathering for any move made along the way.

LUNCH AND LEARN

Keep Calm and Prioritize: Five Requirements for Streamlining Vulnerability Remediation

Speaker: Jimmy Graham, Director of Product Management

Thu, Dec 15 | 12:30-1:15pm | Location: Constitution B

IT organizations face an abundance of vulnerabilities, some of which are trivial and some of which pose a significant risk. Without knowledge of what to tackle first, organizations become overwhelmed, and high-risk vulnerabilities can easily remain unaddressed. In this presentation, you'll learn the five key elements for successfully prioritizing vulnerability remediation. Then learn best practices for using tools that allow you to take full control of evolving threats by correlating active threats against your vulnerabilities, so you know which vulnerabilities to remediate first.

VENDOR EVENTS

cloudera®

LUNCH AND LEARN

Moving Cybersecurity Forward: Introducing Apache Spot

Speaker: Rocky DeStefano, SME
Thu, Dec 15 | 12:30-1:15pm | Location: Declaration A/B

Rocky DeStefano outlines a more scalable and future-proof platform for detecting security threats based on Apache Hadoop and Apache Spot (incubating), exploring real-world examples of how to accomplish a more scalable, flexible, and complete approach to finding advanced threats than the traditional SIEM-based approached in use today.

LUNCH AND LEARN

All Your Base64 are Belong to Us: A Case Study

Speaker: Allan Liska, Senior Solutions Architect, Recorded Future
Thu, Dec 15 | 12:30-1:15pm | Location: Independence D/E

For some organizations, threat intelligence is lists of malicious IP, domains, and file hashes. Indicators are a key tool for every analyst, but technical threat intel is even more valuable when it's linked to other forms of external intel and context. This session presents a specific threat intelligence use case, in which attackers evaded detection by traditional security measures using PowerShell and a Base64 encoded RAT. Learn how threat intelligence enables analysts to move from flash intel about adversary tactics to specific security and threat intel actions.

TERBIUM LABS

Data Intelligence

LUNCH AND LEARN

It'll Be Easy, They Said: Building a Dark Web Crawler

Speaker: Alex Viana, VP of Engineering, Terbium Labs
Thu, Dec 15 | 12:30-1:15pm | Location: Constitution A

While building a conventional web crawler is an increasingly common and well-understood problem, crawling the so-called Dark Web is a significantly more difficult problem. Unlike the clear web, sites are both more difficult to find, and not as keen to be indexed. We will discuss these challenges as they pertain to building Matchlight, our dark web data intelligence platform.

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.

CABINET

Whether you prefer made-to-order omelets, smoked salmon, or bagels with whipped cream cheese, you'll find all of these breakfast staples and more served from CABINET's sumptuous buffet line. You're also welcome to try the savory, such as Chesapeake Bay Blue Crab Hash, or the sweet, including Pumpkin-Buttermilk Griddle Cakes, and anything in between from the breakfast menu. CABINET is host to a warm and welcoming atmosphere, perfect for casual dining in the heart of Washington D.C. Indulge in the restaurant's many offerings for breakfast every day of the week, with a special lunch menu available on weekends.

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.

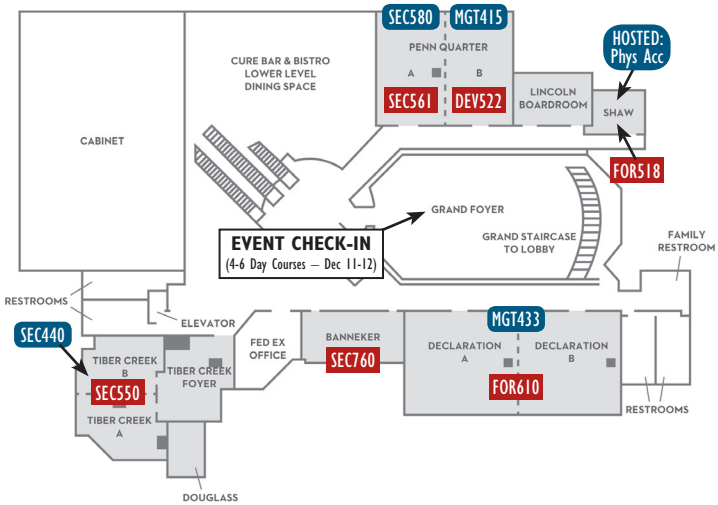
Room Service

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.

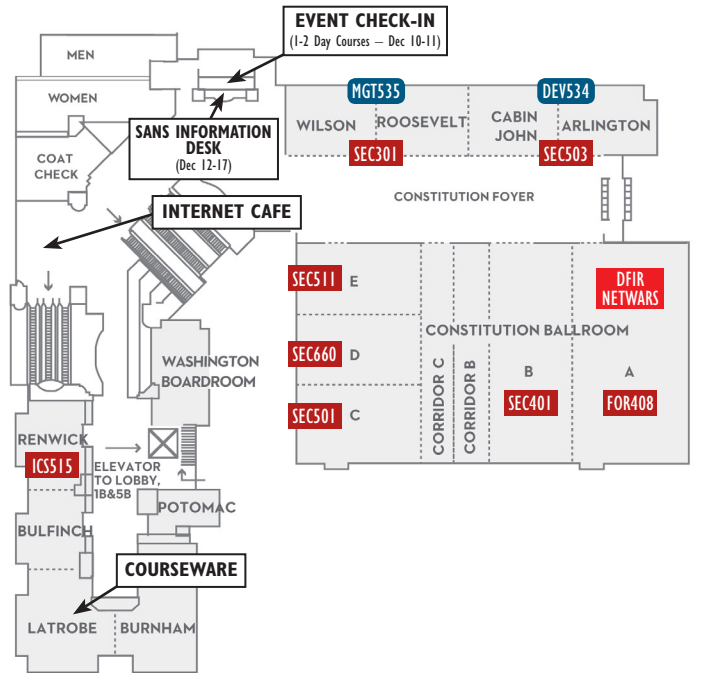
Several of our welcoming rooms and suites provide the perfect place to host a small gathering of family or business associates. Contact in-room dining or the concierge for more information and menu option.

HOTEL FLOORPLAN

GRAND HYATT
DECLARATION LEVEL (1B)



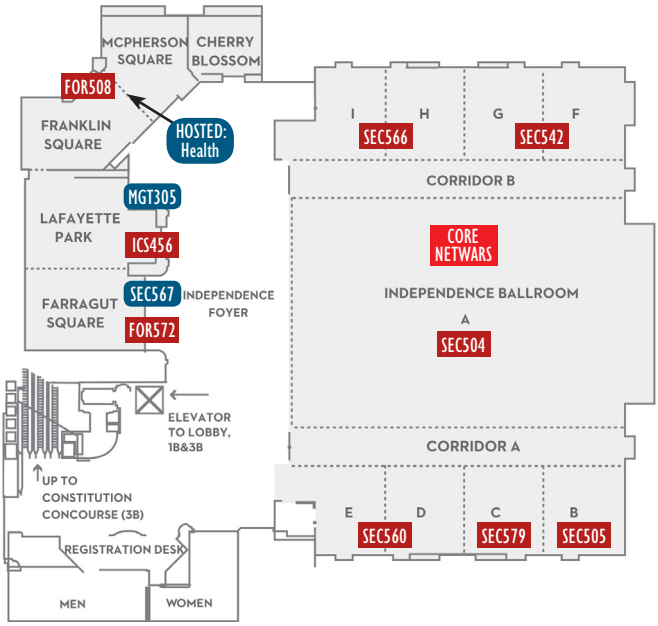
GRAND HYATT
CONSTITUTION LEVEL (3B)



HOTEL FLOORPLAN

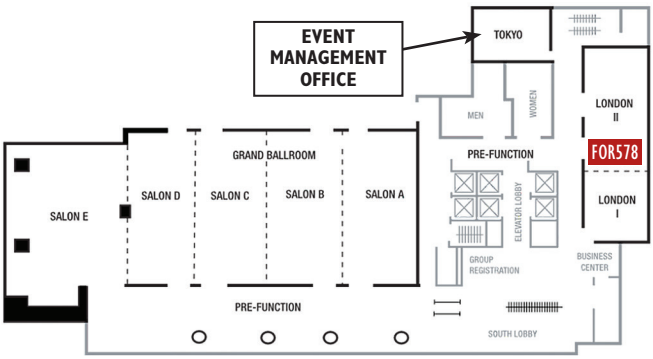
GRAND HYATT

INDEPENDENCE LEVEL (5B)

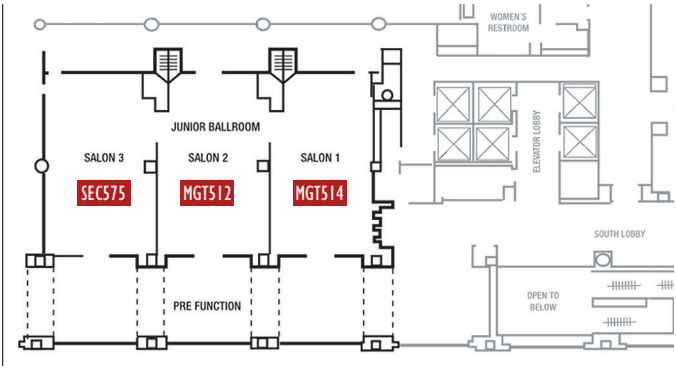


HOTEL FLOORPLAN

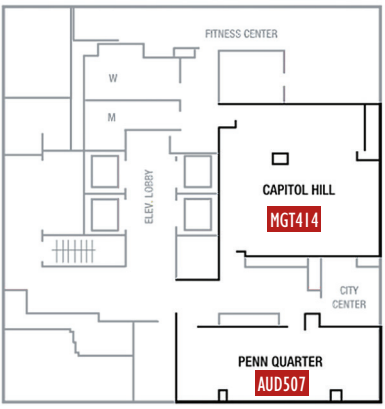
MARRIOTT
BALLROOM LEVEL



MARRIOTT
SECOND FLOOR



MARRIOTT
THIRD FLOOR



Future SANS Training Events

SANS **Security East** 2017
New Orleans, LA | Jan 9-14 | #SANSSecurityEast

SANS **Cloud Security** SUMMIT 2017
San Francisco, CA | Jan 17-19 | #CloudSummit

SANS **Las Vegas** 2017
Las Vegas, NV | Jan 23-30 | #SANSLasVegas

SANS **Cyber Threat Intelligence** SUMMIT & TRAINING 2017
Arlington, VA | Jan 25 - Feb 1 | #CTISummit

SANS Southern California – **Anaheim** 2017
Anaheim, CA | Feb 6-11 | #SANSAnaheim

SANS **Scottsdale** 2017
Scottsdale, AZ | Feb 20-25 | #SANSScottsdale

SANS **Dallas** 2017
Dallas, TX | Feb 27 - Mar 4 | #SANSDallas

SANS **San Jose** 2017
San Jose, CA | Mar 6-11 | #SANSSanJose

SANS **Tysons Corner Spring** 2017
McLean, VA | Mar 20-25 | #SANSTysons

SANS **ICS Security** SUMMIT & TRAINING 2017
Orlando, FL | Mar 20-27 | #ICSSummit

SANS **Pen Test Austin** 2017
Austin, TX | Mar 27 - Apr 1 | #SANSPenTest

SANS 2017
Orlando, FL | Apr 7-14 | #SANS2017

SANS **Threat Hunting and IR** SUMMIT & TRAINING 2017
New Orleans, LA | Apr 18-25 | #ThreatHuntingSummit

SANS **Baltimore Spring** 2017
Baltimore, MD | April 24-29 | #SANSBaltimore

SANS **Automotive Cybersecurity** SUMMIT & TRAINING 2017
Detroit, MI | May 1-8 | #SANSAutoSummit

SANS **Security West** 2017
San Diego, CA | May 9-18 | #SANSSecurityWest

SANS **Northern Virginia - Reston** 2017
Reston, VA | May 21-26 | #SANSReston

SANS **Atlanta** 2017
Atlanta, GA | May 30 - June 4 | #SANSAtlanta

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

Join us again next year!

SANS CDI

CYBER DEFENSE INITIATIVE 2017

Dec 12-19, 2017

Save the Date!

At The Washington Hilton