SANS

CYBER DEFENSE INITIATIVE

POWERED BY NETWARS

Program Guide

December 10-19, 2014 | Washington, DC

@SANSInstitute | #SANSCDI

Table of Contents

General Information

Registration Information

Location: Constitution Foyer

Wednesday, December 10 (Short Classes only) 8:00am-9:00am
Thursday, December 11(Short Classes only) 8:00am-9:00am

Location: Independence Foyer

Thursday, December 11 (Welcome Reception) 5:00pm-7:00pm
Friday, December 12 . . . . . .7:00am-5:30pm
Saturday, December 13-Thursday, December 18 . . . . . .8:00am-5:30pm
Friday, December 19 . . . . . .8:00am-9:00am (Closes)

Courseware Pick-up Information

Location: Constitution Foyer

Wednesday, December 10 (Short Classes only) 8:00am-9:00am
Thursday, December 11(Short Classes only) 8:00am-9:00am

Location: Independence Foyer

Thursday, December 11 . . . . . 5:00pm-7:00pm
Friday, December 12 . . . . . .7:00am-9:00am
Thursday, December 18 . . . . . .8:00am-9:00am

Internet Café *(WIRED & WIRELESS)*

Location: Constitution Foyer

Friday, December 12 . . . . . .Opens at noon – 24 hours
Saturday, December 13-Tuesday, December 16 . . . . . .Open 24 hours
Wednesday, December 17 . . . . . .Closes at 2:00pm

Course Times

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

Course Breaks

7:00am - 9:00am – Morning Coffee
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 Friday, December 12 at the General Session in Independence Ballroom A.

General Information

Dining Options

We have assembled a short list of dining suggestions you may like to try during lunch breaks. See page 19 of this booklet.

Feedback Forms and Course Evaluations

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

Social Board and Twitter

You can post open invites to lunch, dinner or other outings. Located on the Bulletin Board near the Registration Desk. Join the conversation on Twitter and use the hashtag **#SANSCDI** for up-to-date information from fellow attendees!

Wear Your Badge Daily

To make sure you are in the right place, the SANS door monitors will be checking your badge for each course you enter. For your convenience, please wear your badge 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 Independence Foyer.

Bootcamp Sessions and Extended Hours

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

Bootcamps (Attendance Mandatory)

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

SEC401: Security Essentials Bootcamp Style

SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking

Extended Hours:

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

SEC504: Hacker Tools, Techniques, Exploits and Incident Handling

Course Schedule

START DATE: **Wednesday, December 10**
Time: 9:00am-5:00pm (Unless otherwise noted)

SEC524: Cloud Security Fundamentals
Instructor: Dave Shackleford . . . . . Location: Conference Theatre

MGT433: Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program
Instructor: Lance Spitzner . . . . . Location: Constitution Ballroom D

HOSTED: Embedded Device Security Assessments For The Rest Of Us
Instructor: Paul Asadoorian . . . . . Location: Constitution Ballroom E

HOSTED: Physical Penetration Testing – Introduction
Instructor: Deviant Ollam . . . . . Location: Constitution Ballroom C

START DATE: **Thursday, December 11**
Time: 9:00am-5:00pm (Unless otherwise noted)

MGT305: Technical Communication and Presentation Skills for Security Professionals
Instructor: David Hoelzer. . . . . Location: Penn Quarter B

MGT415: A Practical Introduction to Risk Assessment
Instructor: James Tarala . . . . . Location: Penn Quarter A

MGT535: Incident Response Team Management
Instructor: Christopher Crowley . . . . . Location: Bulfinch/Latrobe

START DATE: **Friday, December 12**
Time: 9:00am-5:00pm (Unless otherwise noted)

SEC301: Intro to Information Security
Instructors: Fred Kerby, Keith Palmgren . . . . . Location: Layfayette Park

SEC401: Security Essentials Bootcamp Style
Instructor: Dr. Eric Cole . . . . . Location: Conference Theatre
BOOTCAMP HOURS: 5:00pm-7:00pm (Course days 1-5)

SEC501: Advanced Security Essentials – Enterprise Defender
Instructor: Bryce Galbraith . . . . . Location: Independence Ballroom E

SEC503: Intrusion Detection In-Depth
Instructor: Mike Poor . . . . . Location: Constitution Ballroom B

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

SEC505: Securing Windows with the Critical Security Controls
Instructor: Jason Fossen . . . . . Location: Independence Ballroom D

SEC542: Web App Penetration Testing & Ethical Hacking
Instructor: Eric Conrad . . . . . Location: Cabin John/Arlington

SEC562: CyberCity Hands-on Kinetic Cyber Range Exercise
Instructor: Tim Medin . . . . . Location: Independence Ballroom C

Course Schedule

SEC566: Implementing and Auditing the Critical Security Controls – In-Depth
Instructor: James Tarala . . . . . Location: Farragut Square

SEC575: Mobile Device Security and Ethical Hacking
Instructor: Christopher Crowley . . . . . Location: Constitution Ballroom D

SEC579: Virtualization and Private Cloud Security
Instructor: Dave Shackleford. . . . . Location: Wilson/Roosevelt

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
Instructor: Stephen Sims. . . . . Location: Independence Ballroom B
BOOTCAMP HOURS: 5:15pm-7:00pm (Course days 1-5)

FOR408: Windows Forensic Analysis
Instructor: Mike Pilkington . . . . . Location: Constitution Ballroom C

FOR508: Advanced Computer Forensic Analysis and Incident Response
Instructor: Chad Tilbury. . . . . Location: Independence Ballroom H/I

FOR526: Memory Forensics In-Depth
Instructor: Alissa Torres . . . . . Location: Constitution Ballroom E

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Instructor: Jake Williams . . . . . Location: Bulfinch/Latrobe

MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam
Instructor: Paul A. Henry. . . . . Location: Penn Quarter A
BOOTCAMP HOURS: 8:00am-9:00am (Course days 2-6) &
5:00pm-7:00pm (Course days 1-5)

MGT512: SANS Security Leadership Essentials for Managers with Knowledge Compression™
Instructor: G. Mark Hardy . . . . . Location: Constitution Ballroom A
EXTENDED HOURS: 5:00pm-6:00pm (Course days 1-4)

AUD507: Auditing & Monitoring Networks, Perimeters, and Systems
Instructor: David Hoelzer. . . . . Location: Penn Quarter B

ICS410: ICS/SCADA Security Essentials
Instructor: Matthew Luallen . . . . . Location: Independence Ballroom F/G

HOSTED: (ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program
Instructor: Frank Shirmo . . . . . Location: Franklin Square

START DATE: **Thursday, December 18**
Time: 9:00am-5:00pm (Unless otherwise noted)

SEC580: Metasploit Kung Fu for Enterprise Pen Testing
Instructor: Eric Conrad . . . . . Location: Independence Ballroom F/G

HOSTED: Offensive Countermeasures: The Art of Active Defenses
Instructor: Mick Douglas . . . . . Location: Independence Ballroom H/I

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.

THURSDAY, DECEMBER 11

Registration Welcome Reception

Thu, Dec 11 | 5:00pm-7:00pm | Location: Independence Foyer

Register early and network with your fellow students!

FRIDAY, DECEMBER 12

Welcome to SANS General Session

Speaker: Dr. Eric Cole

Fri, Dec 12 | 8:15am-8:45am | Location: Independence Ballroom A

Women in Technology Reception

Fri, Dec 12 | 6:15pm-7:15pm | Location: Independence Ballroom E

SANS will be hosting a Women in Technology Meet and Greet at SANS CDI. From Jean Jennings Bartik to Diane Greene, women have always been a driving force in the field of information technology. Their experiences have been filled not only with stories of overcoming challenges but also ones of innovation and inspiration. Join us to hear some of these stories and come share your own. After the discussions, stay and network with other conference attendees.

KEYNOTE

Continuous Ownage: Why you Need Continuous Monitoring

Speaker: Eric Conrad

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

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: SEC511: Continuous Monitoring and Security Operations.

Special Events

SATURDAY, DECEMBER 13

SANS Technology Institute Graduation

Speaker: Alan Paller

Sat, Dec 13 | 7:00pm-8:00pm | Location: Independence Ballroom E

Congratulations to the Class of 2014

CANDIDATES FOR M.S. IN INFORMATION SECURITY ENGINEERING

Trenton Bond
Michael Hoehl
Robert Sorensen
Sally Vandeven

CANDIDATES FOR M.S. IN INFORMATION SECURITY MANAGEMENT

Robert Comella
Mason Pokladnik

SANS@NIGHT

An Introduction to PowerShell for Security Assessments

Speaker: James Tarala

Sat, Dec 13 | 7:15pm-8:15pm | Location: Constitution Ballroom A

With the increased need for automation in operating systems, every platform now provides a native environment for automating repetitive tasks via scripts. Since 2007, Microsoft has gone "all in" with their PowerShell scripting environment, providing access to every facet of the Microsoft Windows operating system and services via a scriptable interface. Administrators can completely administer and audit not only an operating system from this shell, but most all Microsoft services, such as Exchange, SQL Server, and SharePoint services as well. In this presentation James Tarala of Enclave Security will introduce students to using PowerShell scripts for assessing the security of these Microsoft services. Auditors, system administrators, penetration testers, and others will all learn practical techniques for using PowerShell to assess and secure these vital Windows services.

SANS@NIGHT

Security Awareness Metrics: Measuring Human Behavior

Speaker: Lance Spitzner

Sat, Dec 13 | 7:15pm-8:15pm | Location: Constitution Ballroom B

Security awareness is nothing more than another control designed to reduce risk, specifically human risk. This session will discuss the different ways organizations are effectively measuring human risk, which methods are proving to be the most successful, and steps you can take to have successful metrics for your awareness program.

SANS@NIGHT

Attacking and Defending Building Automation Systems at Scale: A Case Study

Speaker: Billy Rios

Sat, Dec 13 | 7:15pm-8:15pm | Location: Independence Ballroom A

Modern facilities (such as corporate headquarters) are marvels of engineering. These buildings employ numerous embedded and software systems to help ensure convenience, business efficiency, and even security. The door that unlocks after you swipe your badge is managed by an access control system. The lights and energy flowing to your building are managed by an energy management system. The HVAC systems that keep your data center cool are controlled by an environmental control system. These invisible embedded and software systems make modern life in the corporate facility efficient, convenient, and comfortable. Given the importance and of these systems, how do we secure a modern smart building? What about a corporate campus full of thousands of automation systems? Let's take a look how building automation systems are hacked and explore approaches to secure building automation systems at scale.

SANS@NIGHT

Everything They Told Me About Security Was Wrong

Speaker: John Strand

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

If you were to believe the vendors and the trade shows, you would think everything was OK with IT security. You would think AV works. You would think plug and play IDS was effective. You would think that Data Loss Prevention would prevent data loss. Why then is it that very large organizations are still getting compromised? Organizations with very large budgets and staff, still get compromised in advanced and persistent ways. Let's find out what is wrong and how we can fix it.

SANS@NIGHT

Securing The Kids

Speaker: Lance Spitzner

Sat, Dec 13 | 8:15pm-9:15pm | Location: Constitution Ballroom B

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.

SUNDAY, DECEMBER 14

SANS Technology Institute Information Session

Speaker: Bill Lockhart

Sun, Dec 14 | 5:45pm-7:15pm | Location: Constitution Ballroom A

Join us starting at 5:45 pm for light refreshments. This informal reception will be a chance for current students, prospective students, and graduates to connect with each other as well as members of the SANS Technology Institute faculty and staff. At 6:15 pm, Bill Lockhart, Executive Director of the SANS Technology Institute, will provide an overview of the master's degree and graduate certificate programs, including a description of the courses, faculty, relationship to SANS & GIAC, and the admissions process. After the presentation, we will take and answer questions from participants.

The SANS Technology Institute takes the best of SANS and transforms it into an integrated, graduate-level program. Our students gain a unique combination of technical, leadership, and management skills that enable them to become precisely the "new kind" of InfoSec leader now sought by senior executives globally.

MASTERS PRESENTATION

The Threat Landscape of PKI: System and Cryptographic Security of X.509, Algorithms and their Implementaions

Speaker: Blain Hein

Sun, Dec 14 | 7:15pm-7:55pm | Location: Penn Quarter B

With the unavoidable reliance on public key cryptography in modern communications and information systems (CIS) it is critical to maintain visibility into the threat landscape which can adversely impact the trust in public key infrastructure (PKI) implementations. This knowledge is useful as an input to a risk analysis process to determine whether current PKI practices are sufficient, and to determine when to migrate to new algorithms, key lengths, or procedures. This presentation provides a discussion of the main attacks against PKI systems, both system and cryptographic in origin. This presentation suggests appropriate methods to strengthen PKI systems against these attacks and provides references for additional reading on these attacks.

Special Events

SANS@NIGHT

Gone in 60 Minutes: Have You Patched Your System Today?

Speaker: David Hoelzer

Sun, Dec 14 | 7:15pm-8:15pm | Location: Constitution Ballroom B

In our industry we hear about new vulnerabilities every day, but there can be a perception that moving from the discovery of a flaw to a workable exploit is very difficult. The result is that most organizations are perfectly happy operating with a 30-day patch rollout cycle. Is this really fast enough? How hard is it really to exploit a vulnerability? How hard is it to scale a proof of concept into a working tool that can compromise thousands of hosts? This presentation demonstrates the entire process, walking through the process that a security researcher or hacker follows from research through proof of concept and working exploit... all in less than 60 minutes. While aspects of this presentation can be somewhat technical, the emphasis isn't on the technical but on the process and speed with which a working exploit can be developed. There's something for everyone to take away from this presentation!

SANS@NIGHT

Windows Exploratory Surgery with Process Hacker

Speaker: Jason Fossen

Sun, Dec 14 | 7:15pm-8:45pm | Location: Constitution Ballroom A

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. http://processhacker.sourceforge.net

SANS@NIGHT

The 13 Absolute Truths of Security

Speaker: Keith Palmgren

Sun, Dec 14 | 8:15pm-9:15pm | Location: Constitution Ballroom B

Keith Palmgren has identified thirteen absolute truths of security – things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these thirteen 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 thirteen 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.

Special Events

MASTERS PRESENTATION

Home-Field Advantage: Hunting the Advanced Persistent Threat by Interdicting their Tactics with Network Traps and Snares

Speaker: Matthew Toussain

Sun, Dec 14 | 8:15pm-8:55pm | Location: Penn Quarter B

Within the information security community it is almost universally agreed that the adversary has the edge when they attack our networks. This premise stems from the idea that the attacker only needs to succeed once in order to get access to an organization's sensitive information while the defender must succeed every time. This principle is a fallacy. An attacker must succeed in some way at each stage of the hacker's methodology in order to penetrate their targets. As defenders we only need to stop them at one point. Furthermore, defensive cyber operators know their environment better than any antagonist can ever hope to. There are ways for the defender to take the initiative and hunt down the adversary as attacks occur. Organizations should leverage their home-field advantage by seeding their network with traps, snares, and pitfalls that will generate alerts early in the intrusion kill chain.

SANS@NIGHT

Introduction to IDA Pro and Debugging

Speaker: Stephen Sims

Sun, Dec 14 | 8:15pm-9:15pm | Location: Conference Theatre

In this presentation, Stephen will discuss the most commonly used features and plugins for IDA Pro and WinDbg from an exploitation perspective. You will learn about IDA navigation, IDAPython and IDC scripting, remote debugging, and Kernel debugging. The presentation will be 50% lecture and 50% demonstration.

MONDAY, DECEMBER 15

Vendor Solutions Expo

Mon, Dec 15 | 12:00pm-1:30pm & 5:30pm-7:30pm | Location: Independence 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

Mon, Dec 15 | 5:30pm-7:30pm | Location: Independence 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.

Special Events

There will be three simultaneous NetWars Tournament events held at SANS CDI 2014:

CORE NETWARS TOURNAMENT

Hosts: Ed Skoudis, Tim Medin & Jeff McJunkin
Dec 15 & 16 | 6:30-9:30pm | Location: Independence Ballroom A

CORE 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

SANS DFIR NETWARS TOURNAMENT

Hosts: Alissa Torres & Jake Williams
Dec 15 & 16 | 6:30-9:30pm | Location: Independence Ballroom H/I

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

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

NETWARS TOURNAMENT of CHAMPIONS

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

Special Events

SANS@NIGHT

A Night of Crypto

Speaker: G. Mark Hardy
Mon, Dec 15 | 7:15pm-9:15pm | Location: Constitution Ballroom A

Want to learn a bit more about cryptography but not get wrapped up in the math? G. Mark Hardy has been writing crypto contests for major hacker conferences for years (DEFCON, Toorcon, Shmoocon, THOTCON, SkyDogCon, etc.), and is going to share insights into the reasons behind cryptography, why some algorithms work and some fail, and take a look at what's in use in business today. We'll even cover the cryptographic principles behind Bitcoin. Plus, you'll get a chance to see how crypto puzzles are designed, which might give you some ideas for your own.

SANS@NIGHT

Debunking the Complex Password Myth

Speaker: Keith Palmgren
Mon, Dec 15 | 7:15pm-8:15pm | Location: Constitution Ballroom B

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.

TUESDAY, DECEMBER 16

SANS@NIGHT

IT Security meets Research: Lessons from NASA's Science Labs

Speaker: Joel Offenberg
Tue, Dec 16 | 7:15pm-8:15pm | Location: Constitution Ballroom B

With a complicated web of partnerships, customized equipment, always-changing configurations, and arbitrary deadlines, securing a science lab's computer systems can seem to be a daunting task. The solutions to securing the lab can be elegant or expensive, complicated or cheap, or anywhere in-between...and can be used in other challenging environments. The author discusses solutions for research lab cybersecurity based on his experiences working with scientists and engineers as a NASA contractor.

Vendor Events

Vendor Solutions Expo

Monday, December 15 | 12:00pm-1:30pm & 5:30pm-7:30pm
Location: Independence 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

Monday, December 15 | 5:30pm-7:30pm
Location: Independence 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: Independence 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:

BeyondTrust
Bromium
Click Security
Domain Tools
Forescout Technologies
General Dynamics Fidelis Cybersecurity
Pwnie Express
Qualys
Splunk
Threatstream

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 & LEARN

GENERAL DYNAMICS
Fidelis Cybersecurity Solutions

Stay Ahead of the Adversary with Network Security Analytics

Speaker: Mike Nichols, Senior Manager, Sales Engineering
Fri, Dec 12 | 12:30pm – 1:15pm | Location: Independence Ballroom A

Threat actors often modify their tactics, or the tools they use to attack, but their techniques, or methods, have a much longer lifecycle. Much like the way the antivirus industry learned signature-based detection of malware was a perfect method of detection, the network security community is learning that detecting threats by looking at a single event in time does not provide total protection. If network defenses are to evolve and defeat new attacks, we must look for the attackers' ingrained behavior, not their constantly changing tactics. Network security analytics allows us to track attacks over time, alerting when a series of events is determined to be a method of attack, and empowering us with the ability to stay one step ahead of the adversary.

LUNCH & LEARN

Br Bromium®

Sat, Dec 13 | 12:30pm – 1:15pm | Location: Constitution Ballroom B

Vendor Events

LUNCH & LEARN

DOMAINTOOLS

Connect the Dots with Domain Name Intelligence from DomainTools

Speaker: Mark Kendrick, Director of Business Development

Sun, Dec 14 | 12:30pm – 1:15pm | Location: Independence Ballroom F/G

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. We'll dig deep into published reports on various advanced persistent threats (APTs) and recreate the analysis which lead to their conclusions with resources you can put to immediate use.

LUNCH & LEARN

QUALYS® CONTINUOUS SECURITY

Defending Your Global Perimeter

Speaker: Jonathan Trull, Chief Information Security Officer, Qualys, Inc.

Sun, Dec 14 | 12:30pm – 1:15pm | Location: Independence Ballroom H/I

Hackers probe your perimeter constantly, using automated tools to exploit the vulnerabilities they find. Yet enterprises, burdened with inflexible systems, outdated processes and limited resources, are forced to treat perimeter security as a monthly or quarterly project. This session will lay out a blueprint for creating a continuous security practice spanning the entire lifecycle, from discovering assets to prioritizing issues and mitigating exploits. In particular, it will demonstrate the use of Qualys' new Continuous Monitoring cloud-based solution to perpetually audit your perimeter so you can baseline your environment, set appropriate rules, receive exception-based alerts and act quickly.

Vendor Events

LUNCH & LEARN

ForeScout
Access ability.

Continuous Monitoring & Mitigation

Speaker: Timothy Jones, Federal Systems Engineer

Sun, Dec 14 | 12:30pm – 1:15pm | Location: Constitution Ballroom A

You've already invested in multiple kinds of security systems, but are they working together effectively? Do they share intelligence? Do they coordinate their responses? Are all your remediations automated? This session examines a reference architecture for continuous monitoring and mitigation, based on next-generation network access control and open standards-based information sharing architecture.

LUNCH & LEARN

ThreatSTOP™

CyberCrime as a Business: How Criminal Networks use "Cloud Services" and "Involuntary Contribution Associates" to Make Money

Speaker: Tom Byrnes, CEO of ThreatSTOP

Sun, Dec 14 | 12:30pm – 1:15pm | Location: Bullfinch/Labrobe

Tom Byrnes is the CEO and Founder of ThreatSTOP, the creator of the ThreatSTOP Botnet Defense Cloud. ThreatSTOP is leading the way in providing collaborative network defense against botnets and criminal malware. Over the past 23 years Tom has held technical leadership positions in both civilian and military capacities in all areas of Information Technology, including: the US Army, Manufacturers, VARs and Distributors of equipment; as CTO of an ISP and e-commerce hosting company; and Sr. VP of Technology of a Mutual and Venture fund.

Vendor Events

LUNCH & LEARN

beyondtrust®
Beyond Traditional Security

Are Privileged Accounts a Vulnerability Risk? Absolutely.

Speaker: Rod Simmons, Director of Privilege Management at BeyondTrust

Tue, Dec 16 | 12:30pm – 1:15pm | Location: Cabin John/Arlington

It's no secret that when you have accounts with excessive privilege, you've got a breach waiting to happen - whether by malicious insiders or at the hands of external attackers. Organizations spend significant money on cyber security, but frequently they don't focus on the right areas. Very often we see advanced techniques to patch vulnerabilities and thwart external attacks, but a failure to build the proper foundation to manage and secure the privileged accounts that serve as the access gateway to the most sensitive business data.

LUNCH & LEARN

FORTINET® Infogressive, Inc.
Aggressive Information Security

Fortinet Next Generation Firewalls

Speaker: Will Tipton, Security Engineer

Tue, Dec 16 | 12:30pm – 1:15pm | Location: Constitution Ballroom A

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.

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.

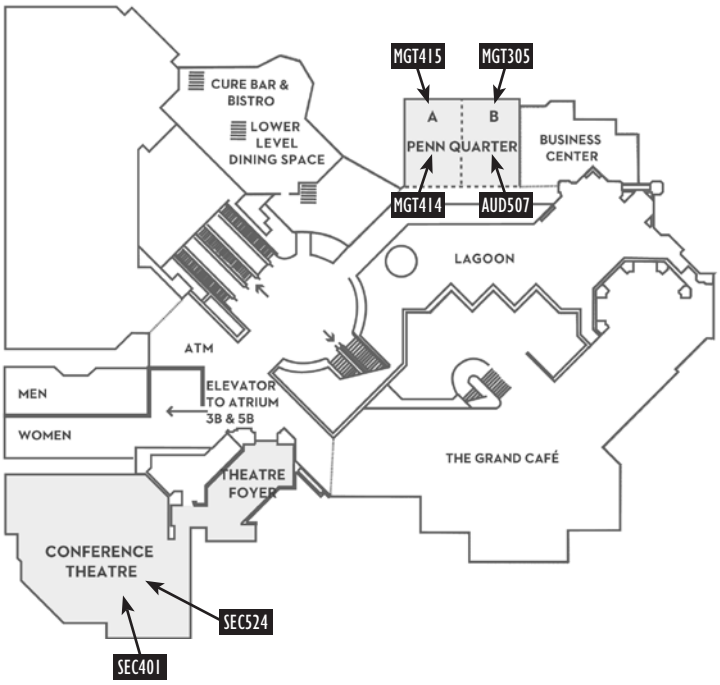
Room Service

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.

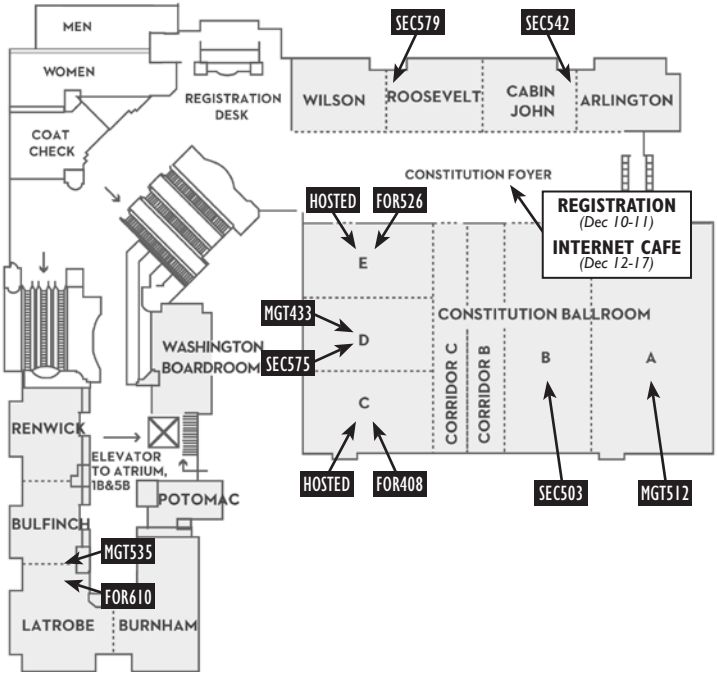
Several of our welcoming rooms and suites provide the perfect place to host a small gathering of family or business associates. Contact in-room dining or the concierge for more information and menu option.

Hotel Floorplans

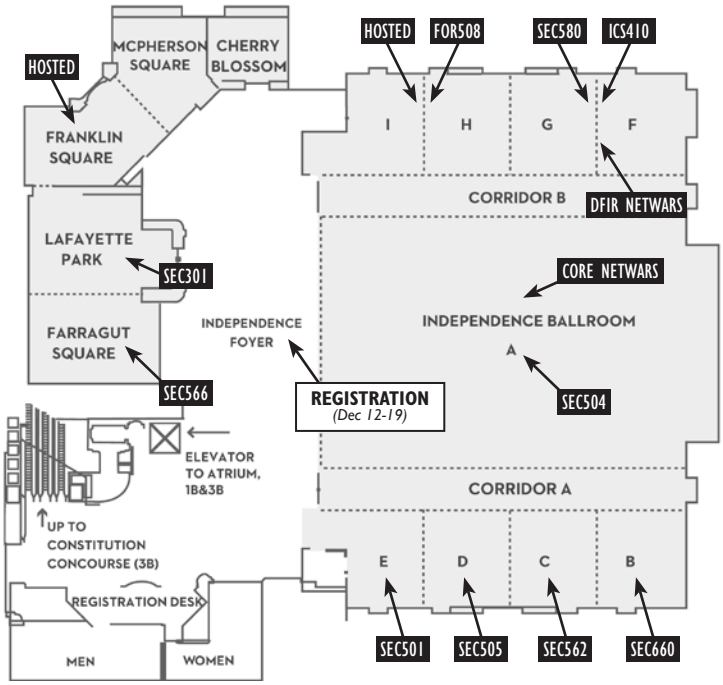
LAGOON LEVEL (1B)



CONSTITUTION LEVEL (3B)



INDEPENDENCE LEVEL (5B)



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.

SEC301 – $599
SEC401 – $599
SEC501 – $599
SEC503 – $599
SEC504 – $599
SEC505 – $599
SEC542 – $599
SEC566 –$599
SEC575 – $599
SEC579 – $599
SEC660 – $599
AUD507 – $599
FOR408 – $599
FOR508 – $599
FOR526 – $599
FOR610 – $599
ICS410 – $599
MGT414 – $599
MGT512 – $599

Three ways to register!

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

Bundle GIAC certification with SANS training and SAVE $300!

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.

You can save $300 on certification when you bundle your certification attempt with your SANS training course. Click on the GIAC certification option during registration or add the certification on-site before the last day of class.

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

"GIAC is the only certification that proves you have hands-on technical skills."

-Christina Ford, U.S. Department of Commerce

10TH ANNUAL

ICS SECURITY

SUMMIT & TRAINING

Orlando, FL

SUMMIT: Feb 23-24, 2015 | TRAINING: Feb 25 - Mar 2, 2015

For SCADA, Industrial Automation, and Control System Security

Choose from these popular courses

CyberCity Hands-on Kinetic Cyber Range Exercise

ICS/SCADA Security Essentials

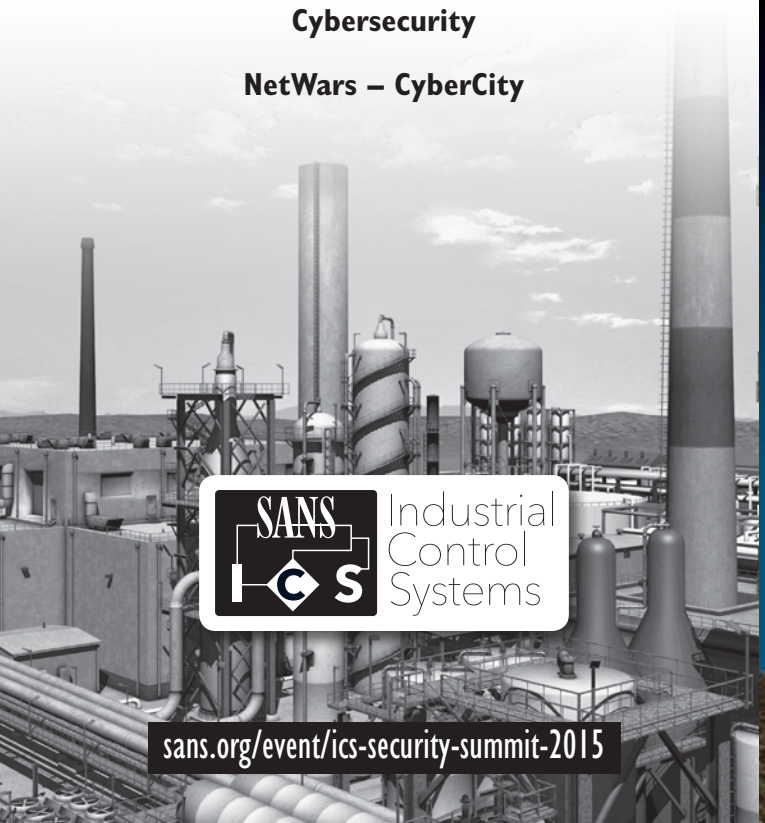
Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program

Critical Infrastructure Protection

Assessing and Exploiting Control Systems

Critical Infrastructure and Control System Cybersecurity

NetWars – CyberCity



SANS Industrial Control Systems

sans.org/event/ics-security-summit-2015

FUTURE SANS TRAINING EVENT

SANS 2015

Orlando, FL

April 11-18, 2015

Our most comprehensive information security training event of the year... something for everyone!

SANS 2015 will be held at the

Walt Disney World Swan and Dolphin Resort

Future SANS Training Events

SANS **Security East** 2015
New Orleans, LA | January 16-21 | #SecurityEast

SANS **Cyber Threat Intelligence** SUMMIT & TRAINING 2015
Washington, DC | February 2-9 | #CTISummit

SANS **Scottsdale** 2015
Scottsdale, AZ | February 16-21 | #SANSScottsdale

10TH ANNUAL **ICS Security** SUMMIT – ORLANDO 2015
Orlando, FL | February 23 - March 2 | #SANSICS

SANS **DFIR Monterey** 2015
Monterey, CA | February 23-28 | #DFIRMonterey

SANS **Cyber Guardian** 2015
Baltimore, MD | March 2-7 | #CyberGuardian

SANS **Northern Virginia** 2015
Reston, VA | March 9-14 | #SANSNoVA

SANS **Houston** 2015
Reston, VA | March 23-28 | #SANSHouston

SANS 2015
Orlando, FL | April 11-18 | #SANS2015

SANS **Security West** 2015
San Diego, CA | May 3-12 | #SecurityWest

SANS **Leadership** SUMMIT & TRAINING 2015
Dallas, TX | May 13-20 | #SANSLeadershipSummit

SANS **Pen Test Austin** 2015
Austin, TX | May 18-23 | #PenTestAustin

SANSFIRE 2015
Baltimore, MD | June 11-22 | #SANSFIRE

SANS **Rocky Mountain** 2015
Denver, CO | June 22-27 | #SANSRockyMtn

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