SANS FIRE 2017

Washington, DC | July 22-29

PROGRAM GUIDE

@SANSInstitute #SANSFIRE

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

COURSES AVAILABLE:

SEC301	SEC573	FOR610
SEC401	SEC575	MGT414
SEC501	SEC579	MGT512
SEC503	SEC642	MGT514
SEC504	SEC660	DEV522
SEC505	FOR408/500	DEV541
SEC506	FOR508	DEV544
SEC511	FOR526	AUD507
SEC542	FOR572	LEG523
SEC560	FOR578	ICS410
SEC566	FOR585	

Three ways to register!

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

TABLE OF CONTENTS

Core NETWARS EXPERIENCE

Hosted by Jeff McJunkin & Tim Medin
Thursday, July 27 – Friday, July 28
6:30pm-9:30pm | Marriott Ballroom Salon 2

DFIR NETWARS TOURNAMENT

Hosted by Heather Mahalik & Philip Hagen
Thursday, July 27 – Friday, July 28
6:30pm-9:30pm | Marriott Ballroom Salon 1

CYBER DEFENSE NETWARS TOURNAMENT

Hosted by Eric Conrad & Seth Misenar
Thursday, July 27 – Friday, July 28
7:15pm-10:15pm | Washington 1

All students who register for a 4-6 day course will be eligible to play NetWars for FREE.
Space is limited. Please visit the Registration Support desk to register today.

GENERAL INFORMATION

Badge & Courseware Distribution

Location: Convention Registration Desk (Lobby Level)

Sat, July 22 – Sun, July 23 (SHORT COURSES ONLY) 8:00am-9:00am

Location: Exhibit Hall B (Exhibit Level)

Sun, July 23 (WELCOME RECEPTION) 5:00pm-7:00pm

Mon, July 24. . . . . 7:00am-9:00am

Registration Support

Location: Convention Registration Desk (Lobby Level)

Mon, July 24 – Fri, July 28 . . . . . .9:00am – 5:00pm

Sat, July 29. . . . . .9:00am - 2:00pm

Internet Café

Location: Marriott Ballroom Foyer (Lobby Level)

Mon, July 24 . . . . . Opens at noon

Tue, July 25 – Fri, July 28 . . . . . Open 24 hours

Sat, July 29 . . . . . Closes at 2:00pm

Course Times

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

Course Breaks

Morning Coffee. 7:00am-9:00am

Morning Break 10:30am-10:50am

Lunch (ON YOUR OWN) 12:15pm-1:30pm

Afternoon Break. 3:00pm-3:20pm

First Time at SANS?

Please attend our **Welcome to SANS** talk designed to help you get the most from your SANS training experience. The talk is from **8:00am-8:30am** on **Monday, July 24** in *Marriott Ballroom Salon 1.*

Photography Notice

SANS may take photos of classroom activities for marketing purposes. SANSFIRE 2017 attendees grant SANS all rights for such use without compensation, unless prohibited by law.

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 bonus 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

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, July 22**
Time: 9:00am - 5:00pm (Unless otherwise noted)

SEC440: Critical Security Controls: Planning, Implementing, and Auditing
Randy Marchany . . . . . Location: Virginia Suite A

SEC524: Cloud Security Fundamentals
Dave Shackleford. . . . . .Location: Roosevelt 4

SEC546: IPv6 Essentials
Dr. Johannes Ullrich. . . . . .Location: Maryland B

SEC567: Social Engineering for Penetration Testers
Micah Hoffman. . . . . Location: Maryland C

SEC580: Metasploit Kung Fu for Enterprise Pen Testing
Christopher Crowley . . . . . .Location: Roosevelt 1

MGT415: A Practical Introduction to Cyber Security Risk Management
James Tarala . . . . . Location: McKinley

MGT433: Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program
Lance Spitzner . . . . . .Location: Roosevelt 5

DEV531: Defending Mobile Applications Security Essentials
Gregory Leonard . . . . . .Location: Roosevelt 2

DEV534: Secure DevOps: A Practical Introduction
Frank Kim . . . . . .Location: Roosevelt 3

START DATE: **Sunday, June 23**
Time: 9:00am - 5:00pm (Unless otherwise noted)

MGT305: Technical Communication and Presentation Skills for Security Professionals
David Hoelzer. . . . . Location: Coolidge

START DATE: **Monday, July 24**
Time: 9:00am - 5:00pm (Unless otherwise noted)

SEC301: Intro to Information Security
Keith Palmgren. . . . . Location: Virginia Suite A

SEC401: Security Essentials Bootcamp Style
Bryan Simon . . . . . .Location: Washington 2
Bootcamp Hours: 5:00pm - 7:00pm (Course days 1-5)

SEC501: Advanced Security Essentials – Enterprise Defender
Paul A. Henry . . . . . .Location: Hoover

SEC503: Intrusion Detection In-Depth
David Hoelzer. . . . . .Location: Washington 6

SEC504: Hacker Tools, Techniques, Exploits & Incident Handling
John Strand . . . . . Location: Marriott Ballroom Salon 3
Extended Hours: 5:00pm - 7:15pm (Course Day 1 only)

SEC505: Securing Windows and PowerShell Automation
Jason Fossen. . . . . Location: Roosevelt 4

SEC506: Securing Linux/Unix
Hal Pomeranz. . . . . Location: Madison A

SEC511: Continuous Monitoring and Security Operations
Eric Conrad . . . . . Location: Washington 1
Bootcamp Hours: 5:15pm - 7:00pm (Course days 1-5)

SEC542: Web App Penetration Testing and Ethical Hacking
Seth Misenar . . . . . Location: Balcony A

SEC550: Active Defense, Offensive Countermeasures and Cyber Deception
Bryce Galbraith . . . . . Location: Wilson A

SEC560: Network Penetration Testing and Ethical Hacking
Ed Skoudis . . . . . Location: Marriott Ballroom Salon 2
Extended Hours: 5:00pm - 7:15pm (Course Day 1 only)
Extended hours will be led by John Strand in the SEC504 classroom located in Marriott Ballroom Salon 3

SEC561: Immersive Hands-on Hacking Techniques
Kevin Fiscus . . . . . Location: Jackson

SEC566: Implementing and Auditing the Critical Security Controls – In-Depth
James Tarala. . . . . Location: Roosevelt 5

SEC573: Automating Information Security with Python
Mark Baggett . . . . . Location: Roosevelt 1

SEC575: Mobile Device Security and Ethical Hacking
Peter Szczepankiewicz . . . . . Location: Wilson C

SEC579: Virtualization and Software-Defined Security
Dave Shackleford. . . . . Location: Virginia Suite B

SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques
Adrien de Beaupre . . . . . Location: Maryland Suite C

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

FOR500: Windows Forensic Analysis
Rob Lee . . . . . Location: Washington 5

FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting
Chad Tilbury. . . . . Location: Washington 3

COURSE SCHEDULE

FOR526: Memory Forensics In-Depth
Alissa Torres . . . . . Location: Tyler

FOR572: Advanced Network Forensics and Analysis
Philip Hagen . . . . . Location: Washington 4

FOR578: Cyber Threat Intelligence
Jake Williams . . . . . Location: Maryland Suite B

FOR585: Advanced Smartphone Forensics
Heather Mahalik . . . . . Location: Maryland Suite A

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Lenny Zeltser . . . . . Location: Marriott Ballroom Salon 1

MGT414: SANS Training Program for CISSP® Certification
David R. Miller . . . . . Location: Roosevelt 3
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™
Ted Demopoulos . . . . . Location: Balcony B
Extended Hours: 5:00pm - 6:00pm (Course days 1-4)

MGT514: IT Security Strategic Planning, Policy, and Leadership
Frank Kim . . . . . Location: Wilson B

MGT517: Managing Security Operations: Detection, Response, and Intelligence
Christopher Crowley . . . . . Location: Virginia Suite C

MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep
Jeff Frisk. . . . . Location: Delaware Suite A

DEV522: Defending Web Applications Security Essentials
Jason Lam . . . . . Location: Madison B

DEV541: Secure Coding in Java/JEE: Developing Defensible Applications
Gregory Leonard . . . . . Location: McKinley

DEV544: Secure Coding in .NET: Developing Defensible Applications
Eric Johnson . . . . . Location: Johnson

AUD507: Auditing & Monitoring Networks, Perimeters, and Systems
Clay Risenhoover. . . . . Location: Roosevelt 2

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

ICS410: ICS/SCADA Security Essentials
Eric Cornelius . . . . . Location: Coolidge

GIAC
CERTIFICATIONS

Add a GIAC Certification with your SANS training at SANSFIRE 2017 and

SAVE $360!

In the information security industry, certification matters. GIAC Certifications offer 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.

Pay just $689 when you bundle your certification attempt with your SANS training course during SANSFIRE 2017 for a savings of $360! After this event is over, the alumni bundle price goes to $1,049.

Stop by the Registration Support desk and add your GIAC-affiliated certification before the last day of class for the discount.

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

BONUS SESSIONS

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, JULY 23

Welcome Reception

Sunday, July 23 | 5:00pm-7:00pm
Location: Exhibit Hall B
Check in early and network with your fellow students!

MONDAY, JULY 24

SPECIAL EVENT

General Session – Welcome to SANS

Speaker: Dr. Johannes Ullrich
Monday, July 24 | 8:00am-8:30am | Location: Marriott Ballroom Salon 1

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.

KEYNOTE

State of the Internet Panel Discussion

Speakers: Internet Storm Center Handlers
Monday, July 24 | 7:15pm-9:15pm | Location: Marriott Ballroom Salon 1

SANSFIRE offers the greatest opportunity to meet Internet Storm Center handlers from around the world, and our most popular bonus session is their "State of the Internet" panel discussion. During this session, you will have the chance to hear from our handlers and ask their opinions and insights on current threats. This is a unique opportunity you will only have at SANSFIRE – a dozen of the industry's brightest minds at your disposal for two intriguing hours!

TUESDAY, JULY 25

SPECIAL EVENT

Coffee & Donuts with the Graduate School

Speaker: Shelley Moore
Tuesday, July 25 | 7:30am-9:00am
Location: Convention Registration Foyer

Join us for coffee, donuts, and conversation with graduate school staff and current students. Learn more about SANS's regionally accredited graduate program which combines SANS technical training and certifications, with leadership and management curriculum specifically designed for the unique needs of aspiring leaders. Find out how the class you're taking this week may be applied towards a master's degree or graduate certificate program. Visit www.sans.edu for complete information on curriculum, admissions, and funding options.

SPECIAL EVENT

GIAC Program Presentation

Speaker: Jeff Frisk
Tuesday, July 25 | 6:15pm-7:15pm | Location: Virginia Suite A

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 and 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.

SANS@NIGHT

The Three C's to Building a Mature Awareness Program

Speaker: Lance Spitzner
Tuesday, July 25 | 7:15pm-8:15pm | Location: Roosevelt 4

After working with hundreds of organizations we have found three common obstacles to a successful awareness program, which we call the three Cs: Communication, Collaboration and Culture. Learn how the most effective organizations are overcoming these three challenges and how you can apply their lessons learned to your own security awareness program.

BONUS SESSIONS

SANS@NIGHT

So, You Wanna be a Pentester?

Speaker: Adrien de Beaupre

Tuesday, July 25 | 7:15pm-8:15pm | Location: Roosevelt 5

This presentation will discuss the things that you will actually need to become a penetration tester, be prepared for a no-fluff honest discussion. So do you really want to be a penetration tester? We get these questions all the time, such as:

- **What is penetration testing?**
- **What are the top 10 coolest most important hacking tools for penetration testers?**
- **What are the top 10 skills that are important to become the worlds greatest hacker? Answer? Make up lots of lies, plagiarize, and write a book!**
- **How do I become the "bestest" cyber hacker?**
- **Can you hack my buddies hotmail for me?**
- **Do I need a cool hacker handle?**
- **Do I really need to learn all that stuff to be a cool hacker?**
- **Do I really have to work hard for many years to be a pentester?**
- **I have a $CERT or degree in so that makes me an expert!**

You will need the attitude, aptitude, initiative, desire, dedication, discipline, integrity, ethics, experience, knowledge, and tools.

SANS@NIGHT

Actionable Detects: Blue Team Cyber Defense Tactics

Speaker: Seth Misenar

Tuesday, July 25 | 7:15pm-8:15pm | Location: Roosevelt 2

Organizations relying on third parties to detect breaches can go almost a full year before finding out they have been compromised. Detect the breach yourself, and on average you will find it within about a month of the initial occurrence. Considering detection and defense against modern adversaries too costly to perform yourself can be a very expensive miscalculation considering the substantially increased price of response and recovery with breach duration. This continually evolving presentation provides you thoughts, tactics, techniques, and procedures to once again take pride in your Blue Team Cyber capabilities. Not applying these lessons learned could prove costly in the face of adapting threat actors. Dig in and learn to hold your head high when talking about your defensive cyber operations capabilities.

SANS@NIGHT

The Cider Press: Extracting Forensic Artifacts from Apple Continuity

Speakers: Heather Mahalik, Sarah Edwards & Philip Hagen
Tuesday, July 25 | 7:15pm-8:15pm | Location: Washington 5

Apple Continuity allows us to move between our devices without disruption in activity. Just think of the ultimate handoff where you can start browsing the Internet on your iPhone, continue on your Mac without the hassle of having to type a search a second time. Essentially, your devices work together enabling you to do less. Imagine how this looks on a Mac, iPhone, or Apple Watch. Will you be able to tell which device the user conducted an activity on? What will the on-device forensic artifacts look like? Continuity requires inter-device communications, so what artifacts will be present on the WiFi and Bluetooth fronts? What if this feature would make or break your investigation?

STI MASTER'S PRESENTATION

Auto-Nuke it from Orbit: A Framework for Critical Security Control Automation

Speaker: Jeremiah Hanley, Master's Degree Candidate
Tuesday, July 25 | 8:15pm-8:55pm | Location: Washington 6

Over 83% of security teams report that the use of automation in security needs to increase within the next three years (Algosec, 2016). With automation becoming a reality for a growing number of companies, there will also be an increased demand for open-sourced scripts to get started. This presentation will provide a framework for prioritizing and developing security automation and will demonstrate this process by creating a script to automate a common information security response procedure - the reimaging of an infected endpoint. The primary function of the script will be to access the application program interface (API) of various enterprise software solutions to speed up the manual tasks involved in performing a reimage.

SANS@NIGHT

Securing Your Kids

Speaker: Lance Spitzner
Tuesday, July 25 | 8:15pm-9:15pm | Location: Roosevelt 4

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 steps you can take to protect them.

BONUS SESSIONS

SANS@NIGHT

Espionage, Influence Operations and Political Breaches: What Do the High Profile Attacks Teach Us About Enterprise Security

Speaker: John Bambenek, ISC Handler

Tuesday, July 25 | 8:15pm-9:15pm | Location: Roosevelt 5

The last 12 months have been filled with news of high-profile political targets being subjected to nation-state attacks. Stolen data are being used by non-friendly adversaries to manipulate and influence public opinion. It is easy to assume that skilled attackers are only interested in high-value targets, but the reality is that this is very much not the case. In a world of high-profile espionage attacks there are important lessons for enterprises to learn about their own security and what they should be doing. This talk will cover the tactics adversarial actors have used to establish their foothold in their victims and the similarity those same tactics have to more traditional cybercriminal actors. The surprising reality is that most of the techniques involve social engineering where, had the victims known what to look for, they would have been able to protect themselves. This talk will also cover how data was exfiltrated and detection strategies for enterprises to determine if they have data leakage occurring that requires response. Lastly, adversaries can and do engage in deception where strategies exist to detect that automatically to protect uses from breach. The advent of defensive deception has also provided promising possibilities to protect enterprises (and high-value targets).

SANS@NIGHT

Offensive Digital Forensics

Speaker: Alissa Torres

Tuesday, July 25 | 8:15pm-9:15pm | Location: Washington 5

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

SANS@NIGHT

Five Key Steps for Building an AppSec Program

Speaker: Frank Kim & Eric Johnson

Tuesday, July 25 | 8:15pm-9:15pm | Location: Roosevelt 2

How do organizations take control of their application security? Chances are, at any given moment, your organization's applications are under attack. The bad guys see your applications as the front door, and a single bad line of code allows them entry. Through a mobile app, web application, or REST API, attackers can pivot to a backend database, your business partner's workstation, or even a payment processing vendor. As development teams continue to push new applications to web, mobile, and cloud environments, the need for an application security program is at an all-time high. Here's the problem: the application security space has nearly twice as many job openings as candidates. For every 100 developers, there are roughly 10 operations team members and only one security professional. Explore the real-world impact of application security breaches, discuss some alarming statistics and trends, and walk through a series of practical steps for building security into applications from the beginning. Attendees will walk away with actionable ideas and recommended practical tools to help improve their application security program.

WEDNESDAY, JULY 26

STI MASTER'S PRESENTATION

Defense Against the Dark Arts 12b: Defending Linux/Unix Against the Ransomware Threat

Speaker: David Kennel, Master's Degree Candidate

Wednesday, July 26 | 7:15pm-7:55pm | Location: Washington 6

Most Security Operations Centers are built for compliance, not security. One well-known retail firm suffered the theft of over a million credit cards. Some 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. We will also provide an overview of DeepBlueCLI, a PowerShell framework for automatically detecting the deadliest events.

BONUS SESSIONS

SANS@NIGHT

A Hunting We Will Go...

Speaker: John Strand

Wednesday, July 26 | 7:15pm-8:15pm | Location: Roosevelt 2

In this talk we will discuss the RITA framework for detecting advanced beacons. It is free, it runs on top of Bro, and it rocks. We will walk through how it works and how you can set it up in your environment. Right now. In under 15 minutes.

SANS@NIGHT

Prioritizing Your Security Program

Speaker: Keith Palmgren

Wednesday, July 26 | 7:15pm-8:15pm | Location: Roosevelt 5

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 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. 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.

SANS@NIGHT

Malware Analysis for Incident Responders: Getting Started

Speaker: Lenny Zeltser

Wednesday, July 26 | 7:15pm-8:45pm | Location: Washington 3

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 and 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.

SANS@NIGHT

Quality Not Quantity: Continuous Monitoring's Deadliest Events

Speaker: Eric Conrad

Wednesday, July 26 | 7:15pm-8:15pm | Location: Roosevelt 4

Most Security Operations Centers are built for compliance, not security. One well-known retail firm suffered the theft of over a million credit cards. Some 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. We will also provide an overview of DeepBlueCLI, a PowerShell framework for automatically detecting the deadliest events.

SANS@NIGHT

Ten Tenets of CISO Success

Speaker: Frank Kim

Wednesday, July 26 | 7:15pm-8:15pm | Location: Washington 5

The era of CISO-as-dictator is at an end. The increased importance of cybersecurity as a vital component of business growth requires security leaders to find new ways to work with executive leaders, business partners, and their own team members. Learn 10 tenets that CISOs and security leaders can utilize to go beyond technical skills, successfully lead organizations through change, and ultimately get to "yes" with the business.

SANS@NIGHT

Using Security Onion to Review Suspicious Network Traffic

Speaker: Brad Duncan, ISC Handler

Wednesday, July 26 | 8:15pm-9:15pm | Location: Roosevelt 4

Malicious network traffic is often difficult for security professionals to recognize without the help of an intrusion detection system (IDS) or and other security tools. The Security Onion Linux distro is an outstanding resource that can help people analyze suspicious network traffic. In this presentation, ISC Handler Brad Duncan discusses how he first discovered Security Onion in 2013 and how he has used it since then. He covers how to use Security Onion in a lab environment to test traffic from exploit kits and links or attachments from malicious spam. Brad also covers how to set up Security Onion to monitor live traffic in a physical or virtual research environment. Such environments provide an excellent way to review network traffic or examine malware from infected Windows hosts.

BONUS SESSIONS

SANS@NIGHT

Three Keys to Mobile Security: Are You Doing Everything You Can to Protect Your Apps?

Speaker: Gregory Leonard

Wednesday, July 26 | 8:15pm-9:15pm | Location: Washington 5

The threat landscape against mobile applications continues to grow. Malicious apps are still being discovered in the Apple and Google Play app stores, and questions continue to grow about how well protected mobile users really are. To combat this increasing threat landscape, mobile devices are providing new hardware and software features to help protect users from exploitation. We will discuss how developers can use features such as fingerprint scanning, on-device cryptography, and MDM/MAM to provide a secure environment for users and their data.

SANS@NIGHT

DOS-No-More: An Automation Toolset for Upstream Mitigation of DOS and DDOS Attacks

Speaker: Rob Vandenbrink, ISC Handler

Wednesday, July 26 | 8:15pm-9:15pm | Location: Roosevelt 5

Recently we've been seeing DDOS attacks making a comeback. Or is it that they never left? In days gone by, when a DDOS attack involving hundreds or thousands of attackers occurred, we had to rely on a manual configuration on the upstream ISP to filter the attack traffic, usually by some mix of source and destination IP. More recently, we're now able to buy some really expensive hardware or upstream solutions that will automate some of this. In this presentation we will outline current methods of upstream mitigation of DDOS attacks, for zero or close to zero budget. DNM (Dos No More) uses a set of Python modules and ELK to query and interpret firewall and IPS logs to identify DOS and DDOS attacks, then characterizes "malicious traffic" using up to 12 different metrics. This is then used to update a table on the local router, which propagates that information to the ISP where the attack can be mitigated in any one of several ways, all dictated by the client to the ISP. The ruleset to identify attacks and specify how to deal with each attack type is held in a simple configuration file, so is easily customized. In the live demo, you will see attacks against production sites as well as amplification attacks. All attacks are identified in an automated fashion by the customer infrastructure, and then blocked, rate limited or otherwise mitigated at the ISP.

SANS@NIGHT

PowerLine: Updated

Speaker: Brian Fehrman

Wednesday, July 26 | 8:15pm-9:15pm | Location: Washington 1

Running into environments where the use of PowerShell is being monitored or is just flat-out disabled? Are wishing you could covertly use the scripts through your favorite C2 channel such as Meterpreter, Empire, or your own custom channel? Look no further! In this talk, we will discuss the newly-updated PowerLine framework. We will overview the tool, walk you through how to use it, show you how you can add additional PowerShell scripts with little effort, and demonstrate just how powerful (all pun intended) this little program can be!

SANS@NIGHT

Making Sense of the Critical Security Controls in the Cloud

Speaker: Eric Johnson

Wednesday, July 26 | 8:15pm-9:15pm | Location: Roosevelt 2

Is cloud security feeling a bit nebulous? A solid framework can help get you on stable footing. The CIS Critical Security Controls are publicly available (and free), and offer just such a framework. This talk will offer an in-depth examination of three of the Critical Security Controls and how they can be applied using Amazon Web Service (AWS) services and tools.

THURSDAY, JULY 27

LUNCH & LEARN

How to Become a SANS Instructor

Speaker: Eric Conrad

Thursday, July 27 | 12:30pm-1:15pm | Location: Washington 1

This presentation is free of charge, but space is limited to the first 40 registrations. Please register online at www.sans.org/sansfire

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. Eric Conrad, a SANS Certified Instructor, will share his experiences and show you how to become part of the SANS top-rated instructor team.

BONUS SESSIONS

Core NETWARS EXPERIENCE

Hosted by Jeff McJunkin & Tim Medin
Thursday, July 27 – Friday, July 28
6:30pm-9:30pm | Marriott Ballroom Salon 2

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

Hosted by Heather Mahalik & Philip Hagen
Thursday, July 27 – Friday, July 28
6:30pm-9:30pm | Marriott Ballroom Salon 1

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.

CYBER DEFENSE NETWARS TOURNAMENT

Hosted by Eric Conrad & Seth Misenar
Thursday, July 27 – Friday, July 28
7:15pm-10:15pm | Washington 1

The all-new NetWars Defense Competition is a defense-focused challenge aimed at testing your ability to solve problems and secure your systems from compromise. With so much focus on offense, NetWars Defense is a truly unique experience and opportunity to test your skills in architecture, operations, threat hunting, log analysis, packet analysis, cryptography, and much more!

SPECIAL EVENT

Women's CONNECT Event

Hosted by the SANS COINS Program and ISSA WIS SIG
Thursday, July 27 | Location: Exhibit Hall A
6:00pm-7:00pm – Networking Reception
7:15pm-9:15pm – SANS@Night Bonus Sessions

Joins SANS and the ISSA International Women In Security Special Interest Group (WIS SIG) as we partner with local association chapters and groups to foster an evening of connections. Association members and group representatives will be on hand to discuss their activities and the benefits of membership. 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. Enjoy the connection building and camaraderie of your peers, while discussing the recent successes relating to local luminaries such as Joann Maguire, Sandra Rothenberg, Pam Shockley-Zalabak, and Judith Wagner, among MANY others.

SANS@NIGHT

Pwning NoSQL Applications for Fun and Profit

Speaker: Bojan Zdrnja, ISC Handler
Thursday, July 27 | 7:15pm-8:15pm | Location: Roosevelt 5

In the last couple of years, NoSQL databases have become the main database used by many web developers. Together with popular stacks, such as the MEAN stack (MongoDB, Express.js, Angular.js and Node.js), NoSQL databases are increasingly popular, since such stacks support both client- and server-side programs written in JavaScript, allowing easy development. The core database used by the MEAN stack, MongoDB, is a NoSQL database program that uses JSON-like documents with dynamic schemas allowing huge flexibility. Although NoSQL databases are not vulnerable to standard SQL injection attacks, they can be exploited with various injection vulnerabilities depending on the creation of queries, which can even include user-defined JavaScript functions. This presentation will demonstrate how applications that use NoSQL databases can be exploited through NoSQL injection in order to retrieve data from the database and do even more.

BONUS SESSIONS

SANS@NIGHT

You've Got Ransomware! Managing the Legal Risk of Cyber Fraud

Speaker: Benjamin Wright

Thursday, July 27 | 7:15pm-8:15pm | Location: Roosevelt 2

Today most fraud has a cyber component, and most fraud investigations involve digital evidence. Cyber fraud like ransomware can trigger a legal crisis for your firm or your client. Mr. Wright will share insights on how to manage the legal risk. He will examine legal measures such as disclaimers, cyber insurance and invocation of attorney confidentiality rules.

SANS@NIGHT

Evolving Threats

Speaker: Paul A. Henry

Thursday, July 27 | 7:15pm-8:15pm | Location: Roosevelt 4

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 attackers' 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.

SANS@NIGHT

Fun With NetFlow: What Are You Missing?

Speaker: Lorna Hutcheson, ISC Handler

Thursday, July 27 | 7:15pm-8:15pm | Location: Washington 5

NetFlow is one of the most overlooked tools available to analysts, incident responders, network admins, etc. It provides a view of your network that is difficult, if not impossible, to obtain any other way. Still, I am amazed at the number of analysts who have no experience with it or they are using it in a very limited capacity. This presentation is going to focus on the value of NetFlow to the intrusion analyst and ways to incorporate it into your daily activities. Whether you have never used it or you have been using it for years, stop by for some fun with NetFlow!

SANS@NIGHT

IR Awakens

Speaker: Tom Webb, ISC Handler

Thursday, July 27 | 8:15pm-9:15pm | Location: Roosevelt 5

Incident response at EDUs is a target rich environment; this allows for lots of opportunities to test tools and techniques. By analyzing your incidents statistics and your IR team's metrics, you can start to pinpoint gaps. We will review historical stats, incident details, and tools deployed. We will discuss how we reduced discovery time and investigation time at the University of South Carolina and what change was the most effective. These lessons can be applied to your environment to improve your IR program.

SANS@NIGHT

Performing Cyber Threat Intelligence in Power Infrastructure

Speaker: Manuel Humberto Santander Palaez, ISC Handler

Thursday, July 27 | 8:15pm-9:15pm | Location: Roosevelt 4

Effective cybersecurity requires companies to be one step ahead of hackers so their movements in the network can be effectively tracked before the cyberattack completely materializes. But in Operation Technology, how can this be done without any kind of affectation to the process? In this presentation we will review a practical case on implementation of cyber threat intelligence process for power generation, transmission and distribution, including tools used for Modbus, IEC 6087-5-104 and IEC 61850.

SANS@NIGHT

Infosec Rock Star: Geek Will Only Get You So Far

Speaker: Ted Demopoulos

Thursday, July 27 | 8:15pm-9:15pm | Location: Roosevelt 2

Some of us are so effective, and well known, that the term "Rock Stars" is entirely accurate. What kind of skills do Rock Stars have and wannabe Rock Stars need to develop? Although we personally may never be swamped by groupies, we can learn the skills to be more effective, well respected, and well paid. Obviously it's not just about technology; in fact most of us are very good at the technology part. The fact is that increasing our skills more on the social and business side will make most of us more effective at what we do than learning how to read hex better while standing on our heads, becoming "One with Metasploit," or understanding the latest hot technologies.

VENDOR EVENTS

Vendor Solutions Expo

Wednesday, July 26 | 12:00pm-1:30pm | 5:30pm-7:30pm
Location: Exhibit Hall B

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-Sponsored Lunch Session

Wednesday, July 26 | 12:00pm-1:30pm | Location: Exhibit Hall B

Sign up at the SANS vendor table 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 contact 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 expo floor and get introduced to providers and their solutions that align with the security challenges being discussed in class.

Luncheon sponsors are:

Anomali
Bricata
LogRhythm
MobileIron
Netbrain
Risk IQ
Sophos
Terbium Labs
ThreatQuotient

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.

SOPHOS

LUNCH AND LEARN

Stop the Exploits. Stop the Attacks. Keep Threats Off Your Devices, Before They Can Run

Speaker: David Gurganious, Enterprise Sales Engineer

Tuesday, July 25 | 12:30pm-1:15pm | Location: Washington 2

Ransomware is one of the biggest threats facing organizations today. The security industry has traditionally struggled to keep up with this sophisticated, ever-changing attack. Until now. Sophos Intercept X is a brand new solution that stops ransomware in its tracks. Deploying a range of innovative next-gen technologies to block all kinds of advanced attacks. It gives you comprehensive protection from ransomware, rootkits, zero-day vulnerabilities, malicious traffic, and everything in-between.

ANOMALI™

LUNCH AND LEARN

Cyber Threat Intelligence: Big Data Simplified. Operationalizing Threat Intelligence

Speaker: Brian Roy, Sr. Security Engineer

Tuesday, July 25 | 12:30pm-1:15pm | Location: Washington 3

There are hundreds of OSINT feeds available today. This can make the topic of Cyber Threat Intelligence confusing. With no established standard (Cybox, STIX\TAXII, OpenIOC, etc.,) it makes it even more difficult for organizations today. We are going to discuss how we can turn a big data issue into a solution to enable organizations in being proactive in identifying threats to their organization.

TERBIUM LABS

Data Intelligence

LUNCH AND LEARN

Data Breaches on the Dark Web: Between Defense and Response

Speaker: Alex Viana, VP of Engineering

Tuesday, July 25 | 12:30pm-1:15pm | Location: Roosevelt 4

There are hundreds of OSINT feeds available today. This can make the topic of Cyber Threat Intelligence confusing. With no established standard (Cybox, STIX\TAXII, OpenIOC, etc.,) it makes it even more difficult for organizations today. We are going to discuss how we can turn a big data issue into a solution to enable organizations in being proactive in identifying threats to their organization.

VENDOR EVENTS

MobileIron

LUNCH AND LEARN

Beyond Usernames and Passwords: Securing Cloud Services in a Mobile World

Speaker: James Plouffe, Lead Solutions Architect

Tuesday, July 25 | 12:30pm-1:15pm | Location: Roosevelt 5

Mobile app-to-cloud security requires a solution that enforces conditional access policies based on user identity, the security posture of the mobile device, and the state of the mobile app. Traditional cloud security solutions that rely primarily on user ID and password can't sufficiently protect cloud data from falling into the wrong hands through unsecured mobile apps and devices. IT must adopt solutions that are specifically designed to manage mobile app-to-cloud security risks. Join MobileIron' s James Plouffe, Lead Solutions Architect, to discuss how to improve the cloud app to mobile user experience with a secure single sign on.

LUNCH AND LEARN

Adaptive Network Automation in Support of Cyber Defense

Speaker: Richard Larkin, Senior Network Engineer

Tuesday, July 25 | 12:30pm-1:15pm | Location: Roosevelt 2

Adaptive Network Automation can improve data visualization, automate playbooks and integrate with other security applications and systems, providing a holistic understanding of the Cyber landscape. It also improves efficiency of both Network and Security teams by providing real-time and historic network visibility and facilitates collaboration within an organization. With the increasing pace and complexity of cyber-attacks in a resource strained environment, network automation is important for maintaining a solid cyber defense.

Future Training Events

San Antonio
San Antonio, TX | Aug 6-11 | #SANSSanAntonio

Boston
Boston, MA | Aug 7-12 | #SANSBoston

New York City
New York City, NY | Aug 14-19 | #SANSNYC

Salt Lake City
Salt Lake City, UT | Aug 14-19 | #SANSSLC

Network Security
Las Vegas, NV | Sep 10-17 | #SANSNetworkSecurity

Baltimore Fall
Baltimore, MD | Sep 25-30 | #SANSBaltimore

Rocky Mountain Fall
Denver, CO | Sep 25-30 | #SANSRocky

Phoenix – Mesa
Mesa, AZ | Oct 9-14 | #SANSMesa

Tysons Corner Fall
McLean, VA | Oct 14-21 | #SANSTysons

San Diego
San Diego, CA | Oct 30 - Nov 4 | #SANSSanDiego

Seattle
Seattle, WA | Oct 30 - Nov 4 | #SANSSeattle

Miami
Miami, FL | Nov 6-11 | #SANSMiami

San Francisco Winter
San Francisco, CA | Nov 27 - Dec 2 | #SANSSanFrancisco

Austin Winter
Austin, TX | Dec 4-9 | #SANSAustin

Cyber Defense Initiative
Washington, DC | Dec 12-19 | #SANSCDI

Future Summit Events

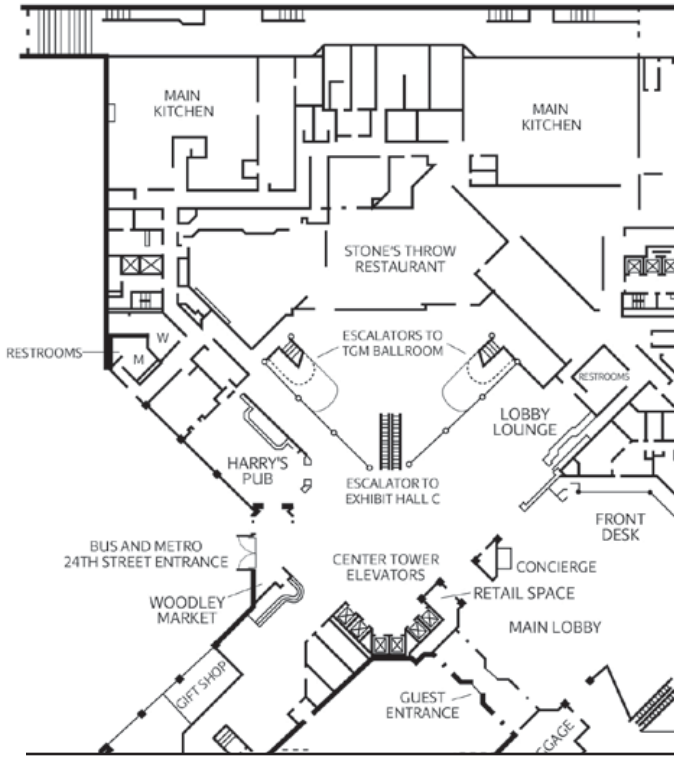
Security Awareness
Nashville, TN | July 31 - Aug 9 | #SecAwareSummit

Pen Test Hackfest
Bethesda, MD | Nov 13-20

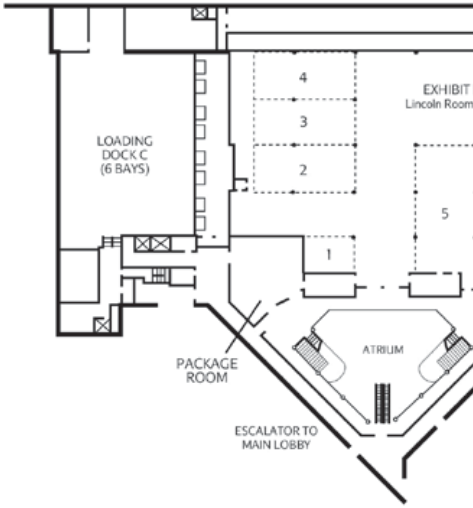
SIEM & Tactical Analytics
Scottsdale, AZ | Nov 28 - Dec 5

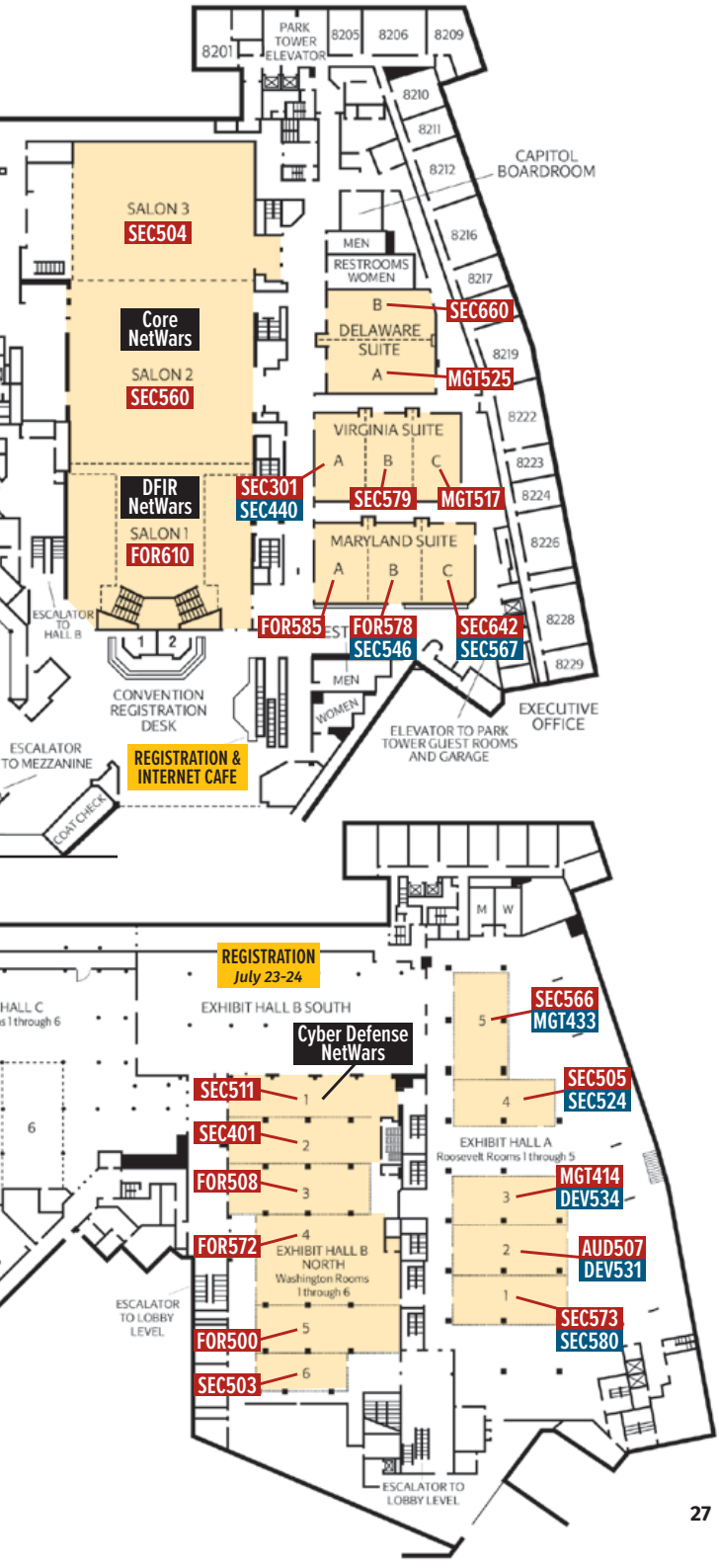
HOTEL FLOOR PLANS

LOBBY LEVEL



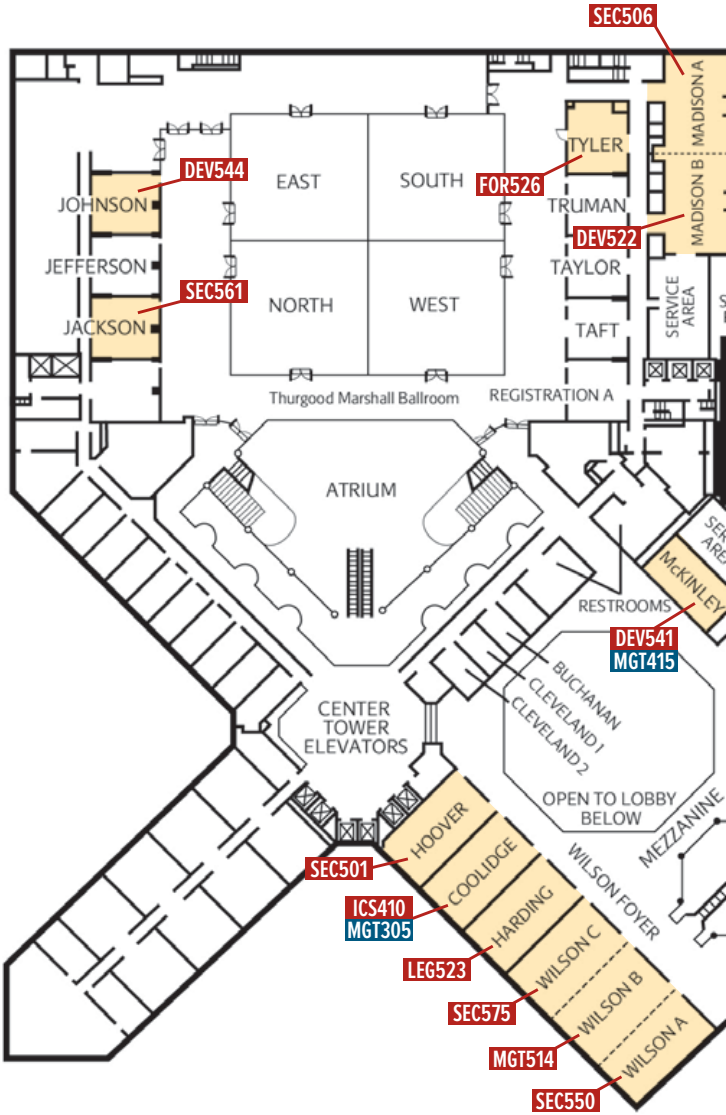
EXHIBITION LEVEL

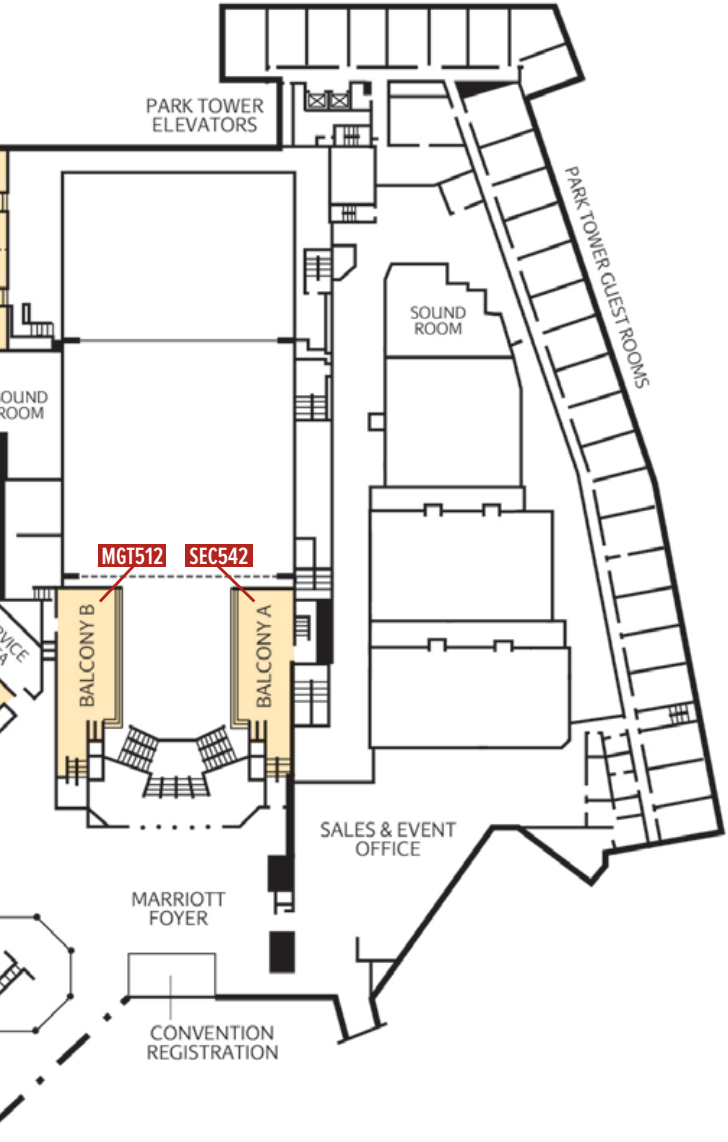



PARK TOWER ELEVATOR
8201
8205
8206
8209
8210
8211
8212
CAPITOL BOARDROOM
SALON 3
SEC504
MEN
RESTROOMS
WOMEN
8216
8217
B
SEC660
DELAWARE SUITE
A
MGT525
8219
Core NetWars
SALON 2
SEC560
VIRGINIA SUITE
A
B
C
8222
8223
8224
DFIR NetWars
SEC301
SEC440
SEC579
MGT517
SALON 1
FOR610
MARYLAND SUITE
A
B
C
8226
ESCALATOR TO HALL B
FOR585
FOR578
SEC546
SEC642
SEC567
8228
8229
1
2
CONVENTION REGISTRATION DESK
MEN
WOMEN
EXECUTIVE OFFICE
ELEVATOR TO PARK TOWER GUEST ROOMS AND GARAGE
ESCALATOR TO MEZZANINE
REGISTRATION & INTERNET CAFE
COAT CHECK
M
W
REGISTRATION
July 23-24
HALL C
s 1 through 6
EXHIBIT HALL B SOUTH
Cyber Defense NetWars
5
SEC566
MGT433
SEC511
1
SEC505
SEC524
4
6
SEC401
2
EXHIBIT HALL A
Roosevelt Rooms 1 through 5
FOR508
3
MGT414
DEV534
FOR572
4
EXHIBIT HALL B NORTH
Washington Rooms 1 through 6
2
AUD507
DEV531
ESCALATOR TO LOBBY LEVEL
1
SEC573
SEC580
FOR500
5
SEC503
6
ESCALATOR TO LOBBY LEVEL

HOTEL FLOOR PLANS

MEZZANINE LEVEL




PARK TOWER ELEVATORS
PARK TOWER GUEST ROOMS
SOUND ROOM
MGT512
SEC542
BALCONY B
BALCONY A
SALES & EVENT OFFICE
MARRIOTT FOYER
CONVENTION REGISTRATION

Join us again next year!

SANS FIRE 2018

Washington, DC

July 14-21, 2018

Save the Date!