SANS | GIAC CERTIFICATIONS

POWERED BY INTERNET STORM CENTER

SANSFIRE

July 14–19, 2025
Washington, DC

PROGRAM GUIDE

#SANSFIRE @SANSInstitute

SANSFIRE 2025

Welcome Reception

Monday, July 14 | 6:30–8:00 PM
McClellan's Sports Bar & Patio (LOBBY LEVEL)

Kick off your SANSFIRE 2025 experience at the Welcome Reception. Be part of this kickoff event and join the industry's most powerful gathering of cybersecurity professionals. Share stories, make connections, and learn how to make the most out of your training this week in Washington, DC. Beverages (adult and otherwise) and bites will be served. Hope to see you there!

Develop and practice real-world skills to be prepared to defend your environment.

CORE NETWARS

Thursday, July 17 & Friday, July 18 | 6:30–9:30 PM
Int'l Ballroom Center (CONCOURSE LEVEL)

CYBER DEFENSE NETWARS

Thursday, July 17 & Friday, July 18 | 7:15–10:15 PM
Int'l Ballroom East (CONCOURSE LEVEL)

All In-Person students who registered to attend a course at SANSFIRE 2025 are eligible to play NetWars for FREE. Space is limited. Please register for NetWars through your SANS Account Dashboard.

Extend Your Training

SANS OnDemand

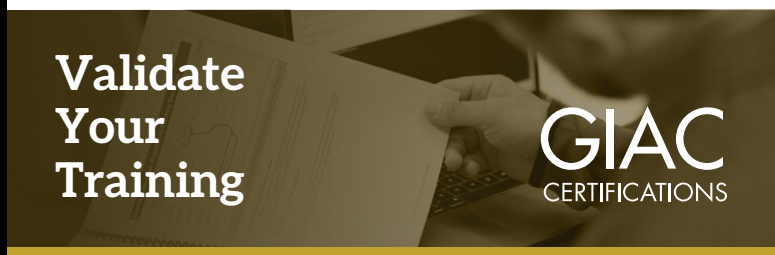
Add an OnDemand Bundle to your course.

Extend Your Training Experience with an OnDemand Bundle

- Four months of supplemental online review
- 24/7 online access to your course lectures, materials, quizzes, and labs
- Subject-matter-expert support to help you increase your retention of course material

OnDemand Bundle price: $999

sans.org/ondemand/bundles



Validate Your Training

GIAC CERTIFICATIONS

Add a GIAC Certification attempt to your course.

Get Certified with GIAC Certifications

- Distinguish yourself as an information security leader
- 30+ GIAC cybersecurity certifications available
- Two practice exams included
- Four months of access to complete the attempt

GIAC Certifications Bundle price: $999

giac.org

GENERAL INFORMATION

Venue

Washington Hilton
1919 Connecticut Avenue, N.W.
Washington D.C. 20009
Phone: 202-483-3000

Event Check-In | Badge & Courseware Distribution

Location: Terrace Foyer (TERRACE LEVEL)

Sunday, July 13 . . . . . 4:00–6:00 PM
Monday, July 14 . . . . . 7:00–8:30 AM

Registration Support

Location: International Terrace (TERRACE LEVEL)

Monday, July 14–Tuesday, July 15 . . . . . 8:30 AM–5:30 PM

Location: Albright Room (TERRACE LEVEL)

Wednesday, July 16–Friday, July 18 . . . . . 8:00 AM–5:30 PM
Saturday, July 19 . . . . . 8:00 AM–2:00 PM

Course Breaks

Morning Coffee . . . . . 7:00–9:00 AM
Morning Break* . . . . . 10:30–10:50 AM
Lunch (ON YOUR OWN) . . . . . 12:15–1:30 PM
Afternoon Break* . . . . . 3:00–3:20 PM

*Snack and coffee to be provided during these break times.

Photography Notice

SANS may take photos of classroom activities for marketing purposes. SANSFIRE 2025 attendees grant SANS all rights for such use without compensation, unless prohibited by law.

Parking*

Self-parking is available at the prevailing rate of $56/day at the Washington Hilton. SANS does not have a negotiated parking discount with this venue.

*Parking rates are subject to change.

Alternative Parking Options:
SANS recommends researching nearby parking facilities for more affordable options. Below are some popular parking apps that can help you locate and reserve space during your training:

SpotHero | ParkMobile | ParkWhiz

Feedback Forms and Course Evaluations

SANS is committed to offering the best information security training, and that means continuous course improvement. Your student feedback is a critical input to our course development and improvement efforts. Please take a moment to complete the electronic evaluation posted in your class Slack channel each day.

Wear Your Badge

To confirm you are in the right place, SANS Work-Study participants 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: Network, Endpoint, and Cloud™

SEC503: Network Monitoring and Threat Detection In-Depth™

SEC540: Cloud Native Security and DevSecOps Automation™

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

SEC670: Red Teaming Tools – Developing Windows Implants, Shellcode, Command and Control™

Extended Hours:

ICS456: Essentials for NERC Critical Infrastructure Protection™

SEC504: Hacker Tools, Techniques, and Incident Handling™

COURSE SCHEDULE

Time: 9:00 AM–5:00 PM (Unless otherwise noted)
NOTE: All classes begin at 8:30 AM on Day 1 (Monday, July 14)

FOR500 Windows Forensic Analysis™ (6-DAY COURSE)
Ovie Carroll . . . . . Piscataway (LOBBY LEVEL)

FOR508 Advanced Incident Response, Threat Hunting & Digital Forensics™ (6-DAY COURSE)
Carlos Cajigas . . . . . Columbia Hall 11 (TERRACE LEVEL)

FOR509 Enterprise Cloud Forensics & Incident Response™ (6-DAY COURSE)
Terrence Williams . . . . . Columbia Hall 9 (TERRACE LEVEL)

FOR578 Cyber Threat Intelligence™ (6-DAY COURSE)
Peter Szczepankiewicz . . . . . Lincoln West (CONCOURSE LEVEL)

FOR585 Smartphone Forensic Analysis In-Depth™ (6-DAY COURSE)
Dominica Crognale & Josh Hickman . . . . . Oak Lawn (LOBBY LEVEL)

FOR608 Enterprise-Class Incident Response & Threat Hunting™ (6-DAY COURSE)
Marcus Guevara . . . . . Columbia Hall 2 (TERRACE LEVEL)

FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques™ (6-DAY COURSE)
Lenny Zeltser . . . . . Int'l Ballroom East (CONCOURSE LEVEL)

ICS410 ICS/SCADA Security Essentials™ (6-DAY COURSE)
Monta Elkins . . . . . Int'l Ballroom West (CONCOURSE LEVEL)

ICS456 Essentials for NERC Critical Infrastructure Protection™ (5-DAY COURSE)
Jason Christopher . . . . . Columbia Hall 4 (TERRACE LEVEL)
Hours: 8:30 AM–6:30 PM (Day 1)

ICS515 ICS Visibility, Detection, and Response™ (6-DAY COURSE)
Dean Parsons . . . . . Jefferson West (CONCOURSE LEVEL)

ICS612 ICS Cybersecurity In-Depth™ (5-DAY COURSE)
Jason Dely . . . . . Columbia Hall 1 (TERRACE LEVEL)

LDR512 Security Leadership Essentials for Managers™ (5-DAY COURSE)
Frank Kim . . . . . Monroe (CONCOURSE LEVEL)

LDR514 Security Strategic Planning, Policy, and Leadership™ (5-DAY COURSE)
Russell Eubanks . . . . . Lincoln East (CONCOURSE LEVEL)

LDR516 Building and Leading Vulnerability Management Programs™ (5-DAY COURSE)
Jonathan Risto . . . . . Holmead West (LOBBY LEVEL)

LDR520 Cloud Security for Leaders™ (5-DAY COURSE)
Jason Lam . . . . . Columbia Hall 3 (TERRACE LEVEL)

LDR553 Cyber Incident Management™ (5-DAY COURSE)
Steve Armstrong-Godwin . . . . . Fairchild East (TERRACE LEVEL)

SEC301 Introduction to Cyber Security™ (5-DAY COURSE)
Rich Greene . . . . . Jay (LOBBY LEVEL)

SEC401 Security Essentials: Network, Endpoint & Cloud™ (6-DAY COURSE)
Bryan Simon . . . . . Columbia Hall 6 (TERRACE LEVEL)
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–5)

SEC488 Cloud Security Essentials™ (6-DAY COURSE)
Serge Borso . . . . . Columbia Hall 12 (TERRACE LEVEL)

SEC497 Practical Open-Source Intelligence (OSINT)™ (6-DAY COURSE)
Mick Douglas . . . . . Holmead East (LOBBY LEVEL)

SEC503 Network Monitoring and Threat Detection In-Depth™ (6-DAY COURSE)
Andrew Laman . . . . . Morgan (LOBBY LEVEL)
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–5)

SEC504 Hacker Tools, Techniques & Incident Handling™ (6-DAY COURSE)
Joshua Wright . . . . . Int'l Ballroom Center (CONCOURSE LEVEL)
Hours: 8:30 AM–7:15 PM (Day 1)

SEC522 Application Security: Securing Web Applications, APIs, and Microservices™ (6-DAY COURSE)
Dr. Johannes Ullrich . . . . . Cabinet (CONCOURSE LEVEL)

SEC530 Defensible Security Architecture & Engineering: Implementing Zero Trust for the Hybrid Enterprise™ (6-DAY COURSE)
Ismael Valenzuela . . . . . Jefferson East (CONCOURSE LEVEL)

SEC540 Cloud Native Security and DevSecOps Automation™ (5-DAY COURSE)
Eric Johnson, Dakota Riley . . . . . Columbia Hall 8 (TERRACE LEVEL)
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–4)

COURSE SCHEDULE

SEC542 Web App Penetration Testing and Ethical Hacking™ (6-DAY COURSE)
Bojan Zdrnja . . . . . Georgetown East (CONCOURSE LEVEL)

SEC549 Cloud Security Architecture™ (5-DAY COURSE)
David Hazar . . . . . Kalorama (LOBBY LEVEL)

SEC560 Enterprise Penetration Testing™ (6-DAY COURSE)
Jon Gorenflo . . . . . Columbia Hall 10 (TERRACE LEVEL)

SEC565 Red Team Operations and Adversary Emulation™ (6-DAY COURSE)
Jean-Francois Maes . . . . . Columbia Hall 7 (TERRACE LEVEL)

SEC573 Automating Information Security with Python™ (6-DAY COURSE)
Mark Baggett . . . . . Northwest (LOBBY LEVEL)

SEC587 Advanced Open-Source Intelligence (OSINT) Gathering and Analysis™ (6-DAY COURSE)
Matt Edmondson . . . . . Fairchild West (TERRACE LEVEL)

SEC595 Applied Data Science and AI/Machine Learning for Cybersecurity Professionals™ (6-DAY COURSE)
Christopher Crowley . . . . . Columbia Hall 5 (TERRACE LEVEL)

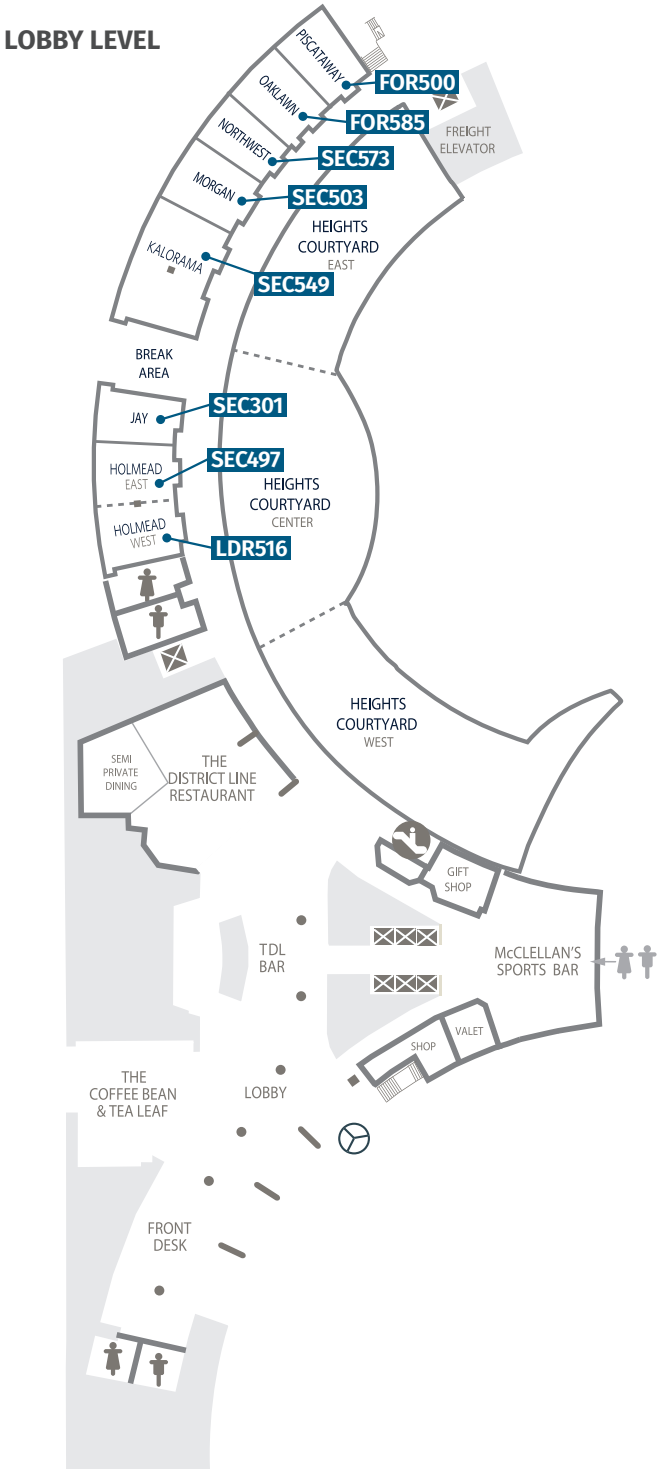
SEC598 Security Automation for Offense, Defense, and Cloud™ (6-DAY COURSE)
Jason Ostrom . . . . . Embassy (TERRACE LEVEL)

SEC617 Wireless Penetration Testing and Ethical Hacking™ (6-DAY COURSE)
James Leyte-Vidal . . . . . Georgetown West (CONCOURSE LEVEL)

SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking™ (6-DAY COURSE)
Stephen Sims . . . . . Gunston East (TERRACE LEVEL)
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–5)

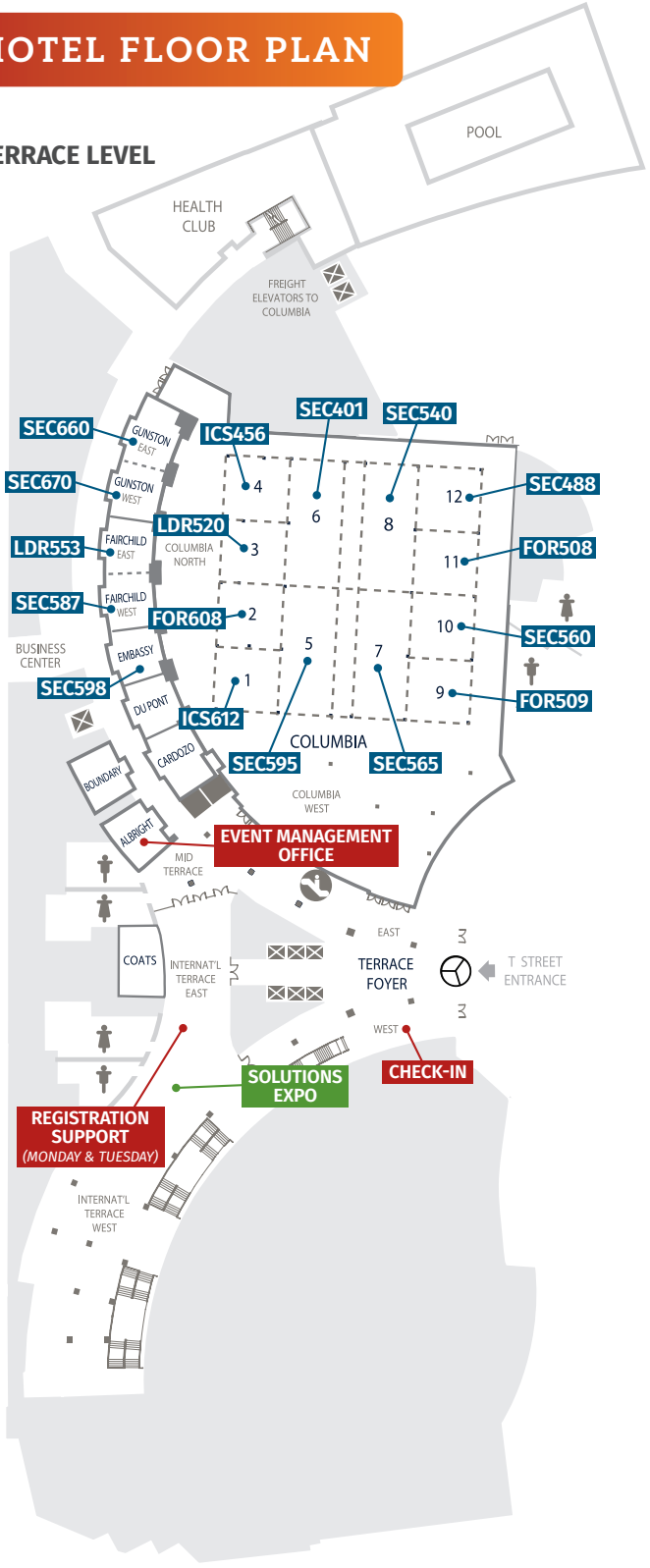
SEC670 Red Teaming Tools – Developing Windows Implants, Shellcode, Command and Control™ (6-DAY COURSE)
Jonathan Reiter . . . . . Gunston West (TERRACE LEVEL)
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–5)

HOTEL FLOOR PLAN

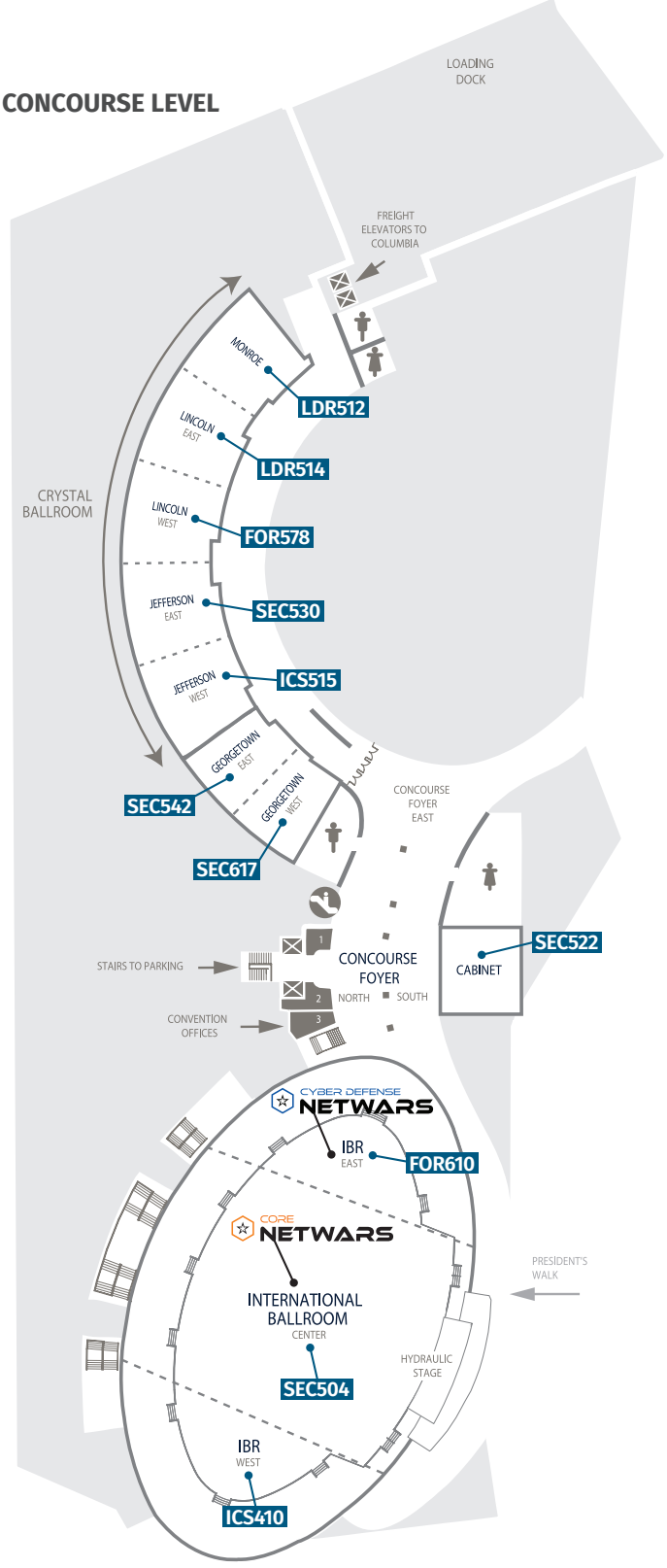


HOTEL FLOOR PLAN

TERRACE LEVEL



CONCOURSE LEVEL



BONUS SESSIONS

Enrich Your SANS Experience!

Talks 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.

RECEPTION

SANSFIRE 2025 Welcome Reception

DATE/TIME: **Monday, July 14 | 6:30–8:00 PM**
LOCATION: **McClellan's Sports Bar & Patio** (LOBBY LEVEL)

Kick off your SANSFIRE 2025 experience at the Welcome Reception. Be part of this kickoff event and join the industry's most powerful gathering of cybersecurity professionals. Share stories, make connections, and learn how to make the most out of your training this week in Washington, DC. Beverages (adult and otherwise) and bites will be served. Hope to see you there!

SPONSORED EVENT

Lookout Lunch & Learn:

DATE/TIME: **Tuesday, July 15 | 12:30–1:15 PM**
LOCATION: **Columbia Hall 5** (TERRACE LEVEL)

SPONSORED EVENT

Feedly Lunch & Learn:

DATE/TIME: **Tuesday, July 15 | 12:30–1:15 PM**
LOCATION: **Columbia Hall 7** (TERRACE LEVEL)

SANS@NIGHT

How I Changed the Way I Use AI in 2025

DATE/TIME: **Tuesday, July 15 | 6:00–7:00 PM**
LOCATION: **International Ballroom East** (CONCOURSE LEVEL)
SPEAKER: **Matt Edmondson, Senior Instructor**

I've been a heavy user of AI since the beginning, but the way that I use AI has recently shifted. In this fast-paced, fun talk, we'll cover the top ways that I've improved my efficiency and productivity by changing the way I interact with AI so far in 2025.

INTERNET STORM CENTER KEYNOTE

Squirrels:

Taming AI Distractions for Smarted Security Operations

DATE: **Wednesday, July 16**
TIME: **6:45–7:45 PM**
LOCATION: **Int'l Ballroom Center** (CONCOURSE LEVEL)

SPEAKER: **Dr. Johannes Ullrich**, SANS Fellow

For security operations, distractions can be dangerous. A "denial of service" against a defender often leads to missed alerts and compromise. The tool must never be the focus but the results the tool provides should determine the value of the tool. AI tools are currently in the "new and cool" phase of the hype cycle. There is no week without a major new AI development. As a result, defenders tend to spend a lot of time trialing new tools and little time properly integrating them into security operations. During this presentation, we interview several defenders to learn what turned out to be just a distraction, or what tools turned out to be a game changer for operations once properly integrated.

BONUS SESSIONS

SANS@NIGHT

How to Use AI to Design a C2 Framework

DATE/TIME: **Tuesday, July 15 | 7:00–8:00 PM**
LOCATION: **Jefferson East** (CONCOURSE LEVEL)
SPEAKER: **Jonathan Reiter, Certified Instructor**

Like it or not, AI is here to stay, so why not embrace it and the capabilities offered. This talk will showcase how to use two different models to design a custom C2 framework from scratch. Privacy concerns will also be addressed during the talk and will highlight how to maintain control of sensitive company information, or just information you don't want a model to have. Attendees will understand how to feed a model various prompts to get what is desired as well as how to begin the implementation of what's given back to you from your prompt's response. Those in a dev-like role should attend this talk, but it is also open to anyone who might be curious about the process.

SPONSORED EVENT

Vendor Solutions Expo – Breakfast

DATE/TIME: **Wednesday, July 16 | 7:30–9:00 AM**
LOCATION: **International Terrace** (TERRACE LEVEL)

SPONSORED EVENT

Vendor Solutions Expo – Lunch

DATE/TIME: **Wednesday, July 16 | 12:15–1:30 PM**
LOCATION: **International Terrace** (TERRACE LEVEL)

RECEPTION

SANSFIRE 2025 Community Night

DATE/TIME: **Wednesday, July 16 | 5:30–6:30 PM**
LOCATION: **International Terrace** (TERRACE LEVEL)

Join us for a special "Community Night" at SANSFIRE 2025. This gathering is open to all cybersecurity professionals and designed to foster connections across the entire spectrum of our community—from newcomers to seasoned experts. Whether you are a new student, a long-time alum, or a cybersecurity professional passionate about the latest advancements, this evening offers an exceptional opportunity to network, share insights, and discuss the evolving challenges and solutions in cybersecurity. This is your chance to blend past experiences with new insights, building lasting relationships and strengthening our collective efforts in the cybersecurity landscape.

RECEPTION

SANSFIRE 2025 Women's CONNECT

DATE/TIME: **Thursday, July 17 | 5:30–6:30 PM**
LOCATION: **International Terrace** (TERRACE LEVEL)

Join us for an exclusive evening of connection and inspiration at SANSFIRE 2025 Women's Connect, hosted in partnership with Women in CyberSecurity (WiCyS). This special gathering is open to SANS students and members of the local cybersecurity community—from CISOs to early-career practitioners. Enjoy complimentary light bites and beverages while networking with fellow professionals, thought leaders, and advocates committed to advancing gender diversity in cybersecurity. Don't miss the chance to visit the WiCyS booth for exclusive swag and to learn about opportunities with the DC-MD-VA local chapter. Immediately following the reception, join us for an insightful WiCyS @Night Talk, where women leaders will share their journeys, lessons learned, and strategies for thriving in a rapidly evolving threat landscape.

Whether you're a seasoned expert or just starting out, Women's Connect at SANSFIRE 2025 offers a meaningful opportunity to build lasting connections and celebrate the collective strength of women in cybersecurity.

SANS@NIGHT

Back to Basics (and Having a Blast): Why Cybersecurity Fundamentals Still Rule in a High-Tech World

DATE/TIME: **Thursday, July 17 | 6:00–7:00 PM**
LOCATION: **Columbia Hall 5** (TERRACE LEVEL)
SPEAKER: **Rich Greene, Certified Instructor**

Buckle up for a lively ride through the wild world of cybersecurity! Sure, today's tech landscape is all about AI, quantum computing, and other fancy buzzwords that make your head spin but guess what? None of that cutting-edge stuff means squat if you're ignoring the good old basics. In this upbeat, interactive session, we'll dive into why the tried-and-true fundamentals (think password hygiene, patch management, and access controls) are the secret sauce to surviving and thriving in the age of ever-evolving cyber threats. Prepare for real-life "oops" moments, plenty of laughs, and hands-on tips you can actually use. This is not your buttoned-up, corporate snooze-fest: you'll leave inspired, empowered, and ready to fortify your digital defenses with good vibes and rock-solid basics. Let's have some fun getting back to what really matters!

BONUS SESSIONS

WORKSHOP

SANSFIRE 2025 Honeypot Workshop

DATE/TIME: **Thursday, July 17 | 6:00–7:00 PM**
LOCATION: **International Ballroom West** (CONCOURSE LEVEL)
SPEAKERS: **Internet Storm Center Handlers, Guy Bruneau and Jesse La Grew**

Become part of the largest, oldest, and most open sensor network on the internet. Learn how to build, configure, and operate your very own honeypot. We will provide up to twenty honeypots free on a first-come basis. You are also welcome to bring your own Raspberry Pi, n100, or similar system (or cloud account).

This is a hands-on session and requires some familiarity with Linux. Once deployed, the three honeypots submitting data most consistently for the first three months will have a yet-to-be-announced prize.

CYBER RANGES

Core NetWars Tournament

DATE/TIME: **Thursday, July 17 & Friday, July 18 | 6:30–9:30 PM**
LOCATION: **International Ballroom Center** (CONCOURSE LEVEL)

The most comprehensive of the NetWars ranges, this ultimate multi-disciplinary cyber range powers up the most diverse cyber skills. This range is ideal for advancing your cybersecurity prowess in today's dynamic threat landscape. The winning team and the top five solo players from every NetWars tournament throughout the year are offered a chance to compete in the annual SANS NetWars Tournament of Champions.

CYBER RANGES

Cyber Defense NetWars Tournament

DATE/TIME: **Thursday, July 17 & Friday, July 18 | 7:15–10:15 PM**
LOCATION: **International Ballroom East** (CONCOURSE LEVEL)

Focused on preventing, analyzing, and defending against complex real-world attack scenarios, including brute-force attacks and ransomware campaigns.

SANS@NIGHT

Rethinking the Weakest Link: Human Roles in AI-Driven Cybersecurity

DATE/TIME: **Thursday, July 17 | 6:45–7:45 PM**
LOCATION: **Jefferson East** (CONCOURSE LEVEL)
SPEAKER: **Deborah Kariuki, Graduate Program Director, MAE-UMBC**

The persistent framing of users as the "weakest link" in cybersecurity has long shaped how risks and responsibilities are distributed in digital systems. However, in the age of artificial intelligence (AI), this narrative demands reexamination. As AI increasingly mediates critical decisions, from authentication to threat detection, the question of "who or what" constitutes the weakest link becomes more complex. This presentation interrogates the validity and implications of this label in contemporary AI-enabled systems. Drawing from human-centered computing, cybersecurity, and AI ethics literature, we explore how system design, algorithmic opacity, and socio-technical contexts contribute to security failures often misattributed to users.

SANS@NIGHT

Unlocking Secrets: Keypad Safe Attack Using Side-Channel Timing and Pulseview

DATE/TIME: **Friday, July 18 | 6:00–7:00 PM**
LOCATION: **Columbia Hall 5** (TERRACE LEVEL)
SPEAKER: **Monta Elkins, Principal Instructor**

In this demo of hardware hacking, we'll introduce PulseView—the "Wireshark of hardware hacking"—and demonstrate a technique to unlock a keypad safe. Our method? A Side-Channel Timing Attack, which relies on the timing discrepancies in the user interface. Using an affordable logic analyzer (priced under $15), we'll capture microsecond changes in response times tied to incorrect passcodes. By leveraging this side-channel data, we will carefully decipher the true passcode of the safe.

Unique Approach: Traditional hacking often focuses on software vulnerabilities to exfiltrate sensitive data. In this demonstration, we will show how the timing of system responses can leak data without any traditional vulnerabilities. This approach emphasizes the power and subtlety of side-channel attacks in extracting valuable information.

Insights for Attendees: Understand how a side-channel timing attack works to reveal sensitive data. Learn about the key functionality of logic analyzers and the PulseView software, often called the "Wireshark of hardware hacking." Gain practical knowledge on how to utilize changes in response time to recover the passcode of a keypad safe.

Join us for this insightful session to explore the intricacies of hardware hacking and enhance your cybersecurity skill set with real-world applications and techniques.

SAVE THE DATE

SANSFIRE 2026 is returning to the Grand Hyatt Washington **July 13–18, 2026**

Upcoming SANS Training Events

Anaheim	Anaheim, CA	Hybrid	Jul 21–26
Huntsville	Huntsville, AL	Hybrid	Jul 28–Aug 2
San Antonio	San Antonio, TX	Hybrid	Aug 4–9
Chicago	Chicago, IL	Hybrid	Aug 11–16
Boston	Boston, MA	Hybrid	Aug 11–16
Virginia Beach	Virginia Beach, VA	Hybrid	Aug 18–23
Emerging Threats: Leadership Response	Virginia Beach, VA	Hybrid	Aug 25–29
Stay Sharp: Sept		Virtual (ET)	Sep 8–10
Raleigh	Raleigh, NC	Hybrid	Sep 15–20
Network Security	Las Vegas, NV	Hybrid	Sep 22–27
DC Metro Fall	Rockville, MD	Hybrid	Sep 29–Oct 4
San Diego Fall	San Diego, CA	Hybrid	Oct 20–25
Orlando Fall	Orlando, FL	Hybrid	Oct 27–Nov 1
Houston: Mission Critical OT Training	Hoston, TX	Hybrid	Nov 3–8
Stay Sharp: Nov		Virtual (ET)	Nov 12–14
DFIRCON Miami	Coral Gables, FL	Hybrid	Nov 16–22
San Francisco Fall	San Francisco, CA	Hybrid	Nov 17–22
Dallas	Dallas, TX	Hybrid	Dec 1–6
Cyber Defense Inintiative®	Washington, DC	Hybrid	Dec 12–17
Nashville Winter 2026	Nashville, TN	Hybrid	Jan 12–17
Rockville	Rockville, MD	Hybrid	Feb 2–7
CyberCon San Diego	La Jolla, CA	Hybrid	Feb 23–28
SANS 2026	Orlando, FL	Hybrid	Mar 29–Apr 3
Security West	San Diego, CA	Hybrid	May 11–16