SANS | GIAC CERTIFICATIONS

SANS Cyber Defense Initiative®

December 12–17, 2025
Washington, D.C.

Program Guide

#SANSCDI @SANSInstitute

SANS CYBER DEFENSE INITIATIVE 2025

Welcome Reception

Saturday, December 13 | 7:00–8:30 PM
International Terrace (TERRACE LEVEL)

Kick off your week of world-class cybersecurity training at the Welcome Reception! This is your chance to connect face to face with fellow practitioners, industry experts, and SANS Faculty in a relaxed, open-air setting. Enjoy delicious bites and a selection of beverages—adult and otherwise—as you ease into an exciting week of learning and networking.

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

CORE NETWARS

Mon, Dec 15 & Tue, Dec 16 | 6:30–9:30 PM
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.

All In-Person students who registered to attend a course at SANS CDI 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

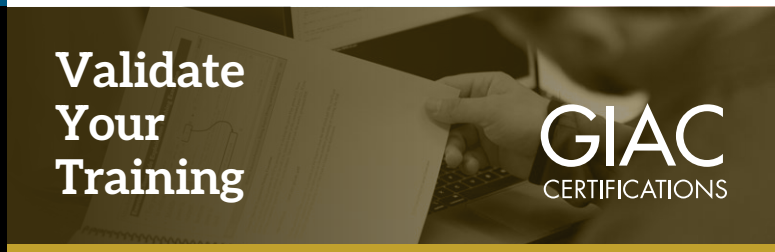
Add OnDemand Extended Access to your course.

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 Extended Access price: $999

sans.org/ondemand/extendedaccess



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 Ave. | NW Washington, D.C. 20009
Phone: 1-202-483-3000

Event Check-In | Badge & Courseware Distribution

Location: Terrace Foyer (TERRACE LEVEL)

Thursday, December 11 . . . . . 4:00–6:00 PM

Friday, December 12 . . . . . 7:00–8:30 AM

(SEC535 & Run #2 of SEC545)
Location: Columbia Ballroom Foyer (TERRACE LEVEL)

Monday, December 15 . . . . . 7:00–8:30 AM

Registration Support

Location: Columbia Ballroom Foyer (TERRACE LEVEL)

Fri, December 12 . . . . . 8:00 AM–5:30 PM

Sat, December 13 . . . . . 8:00 AM–3:30 PM

Location: Albright Room (TERRACE LEVEL)

Sun, December 14–Tue, December 16 . . . . . 8:00 AM–5:30 PM

Wed, December 17 . . . . . 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. SANS Cyber Defense Initiative 2025 attendees grant SANS all rights for such use without compensation, unless prohibited by law.

Parking*

- Self-Parking: $56.00 daily (includes in-and-out privileges for overnight guests staying at the hotel)
- Valet Parking: Unavailable
- Available self-parking is covered and secured with a maximum vehicle height of 6'2"

*Parking rates are subject to change.

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)

LDR414: SANS Training Program for CISSP® Certification

SEC401: Security Essentials: Network, Endpoint, and Cloud

SEC503: Network Monitoring and Threat Detection In-Depth

SEC511: Cybersecurity Engineering: Advanced Threat Detection and Monitoring

SEC540: Cloud Native Security and DevSecOps Automation

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

Extended Hours:

SEC501: Advanced Security Essentials – Enterprise Defender

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

Classes starting Friday, December 12

FOR500 Windows Forensic Analysis (6-DAY COURSE)
Ovie Carroll . . . . . Fairchild East (TERRACE)

FOR508 Advanced Incident Response, Threat Hunting, and Digital Forensics (6-DAY COURSE)
Carlos Cajigas . . . . . Columbia Hall 9 (TERRACE)

FOR578 Cyber Threat Intelligence (6-DAY COURSE)
Peter Szczepankiewicz . . . . . Cabinet (CONCOURSE)

FOR589 Cybercrime Investigations (5-DAY COURSE)
Kevin Ripa . . . . . Oak Lawn (LOBBY)

FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques (6-DAY COURSE)
Lenny Zeltser . . . . . Gunston West (TERRACE)

ICS410 ICS/SCADA Security Essentials (6-DAY COURSE)
Monta Elkins & Joel Cox . . . . . Georgetown East (CONCOURSE)

ICS515 ICS Visibility, Detection, and Response (6-DAY COURSE)
Mark Bristow . . . . . Piscataway (LOBBY)

ICS613 ICS/OT Penetration Testing & Assessments (5-DAY COURSE)
Don C. Weber & Tyler Webb . . . . . Columbia Hall 6 (TERRACE)

LDR414 SANS Training Program for CISSP® Certification (6-DAY COURSE)
Seth Misenar . . . . . Columbia Hall 1 (TERRACE)
Hours: 8:30 AM–7:00 PM (Day 1); 8:00 AM–7:00 PM (Days 2–5); 8:00 AM–5:00 PM (Day 6)

LDR512 Security Leadership Essentials for Managers (5-DAY COURSE)
My-Ngoc Nguyen . . . . . Columbia Hall 2 (TERRACE)

LDR514 Security Strategic Planning, Policy, and Leadership (5-DAY COURSE)
Russell Eubanks . . . . . Int'l Ballroom East (CONCOURSE)

LDR516 Strategic Vulnerability and Threat Management (5-DAY COURSE)
Jonathan Risto . . . . . Columbia Hall 8 (TERRACE)

LDR519 Cybersecurity Risk Management and Compliance (5-DAY COURSE)
James Tarala . . . . . Holmead West (LOBBY)

LDR551 Building and Leading Security Operations Centers (5-DAY COURSE)
John Hubbard . . . . . Fairchild West (TERRACE)

LDR553 Cyber Incident Management (5-DAY COURSE)
Matt Bromiley . . . . . Monroe (CONCOURSE)

SEC301 Introduction to Cyber Security (5-DAY COURSE)
Rich Greene . . . . . Gunston East (TERRACE)

SEC401 Security Essentials: Network, Endpoint and Cloud (6-DAY COURSE)
Bryan Simon . . . . . Columbia Hall 3 (TERRACE)
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–5)

SEC501 Advanced Security Essentials – Enterprise Defender (6-DAY COURSE)
Ross Bergman . . . . . Jay (LOBBY)
Hours: 8:30 AM–7:00 PM (Day 1)

SEC502 Cloud Security Tactical Defense (5-DAY COURSE)
Kenneth G. Hartman . . . . . Lincoln East (CONCOURSE)

SEC503 Network Monitoring and Threat Detection In-Depth (6-DAY COURSE)
Andrew Laman . . . . . Jefferson East (CONCOURSE)
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)
Chris Pizor . . . . . Georgetown West (CONCOURSE)
Hours: 8:30 AM–7:15 PM (Day 1)

SEC511 Cybersecurity Engineering: Advanced Threat Detection and Monitoring (6-DAY COURSE)
Eric Conrad . . . . . Morgan (LOBBY)
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–5)

SEC530 Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise (6-DAY COURSE)
Ismael Valenzuela . . . . . Columbia Hall 4 (TERRACE)

SEC540 Cloud Native Security and DevSecOps Automation (5-DAY COURSE)
David Hazar . . . . . Columbia Hall 11 (TERRACE)
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–4)

COURSE SCHEDULE

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

Classes starting Friday, December 12

SEC545 GenAI and LLM Application Security (3-DAY COURSE)
Jon Zeolla & Viswanath Chirravuri . . . . . Columbia Hall 5 (TERRACE)

SEC549 Cloud Security Architecture (5-DAY COURSE)
Eric Johnson . . . . . Columbia Hall 12 (TERRACE)

SEC560 Enterprise Penetration Testing (6-DAY COURSE)
Jon Gorenflo . . . . . Embassy (TERRACE)

SEC566 Implementing and Auditing CIS Controls (5-DAY COURSE)
Brian Ventura . . . . . Lincoln West (CONCOURSE)

SEC573 Automating Information Security with Python (6-DAY COURSE)
Mark Baggett . . . . . Holmead East (LOBBY)

SEC587 Advanced Open-Source Intelligence (OSINT) Gathering and Analysis (6-DAY COURSE)
Matt Edmondson . . . . . Columbia Hall 10 (TERRACE)

SEC588 Cloud Penetration Testing (6-DAY COURSE)
Moses Frost . . . . . Columbia Hall 7 (TERRACE)

SEC595 Applied Data Science and AI/Machine Learning for Cybersecurity Professionals (6-DAY COURSE)
David Hoelzer . . . . . Jefferson West (CONCOURSE)

SEC599 Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses (6-DAY COURSE)
Bryce Galbraith . . . . . Northwest (LOBBY)

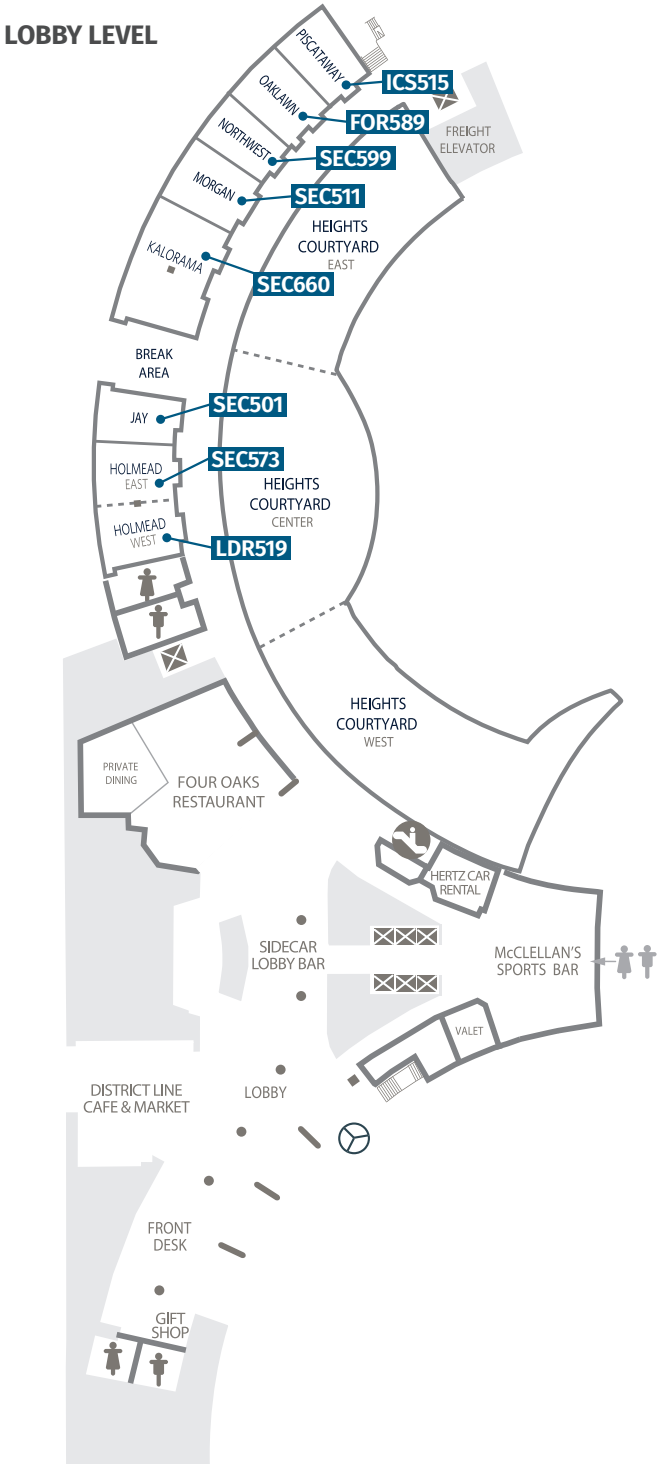
SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking (6-DAY COURSE)
Stephen Sims . . . . . Kalorama (LOBBY)
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–5)

Classes starting Monday, December 15

SEC535 Offensive AI – Attack Tools and Techniques (3-DAY COURSE)
Foster Nethercott . . . . . Int'l Ballroom West (CONCOURSE)

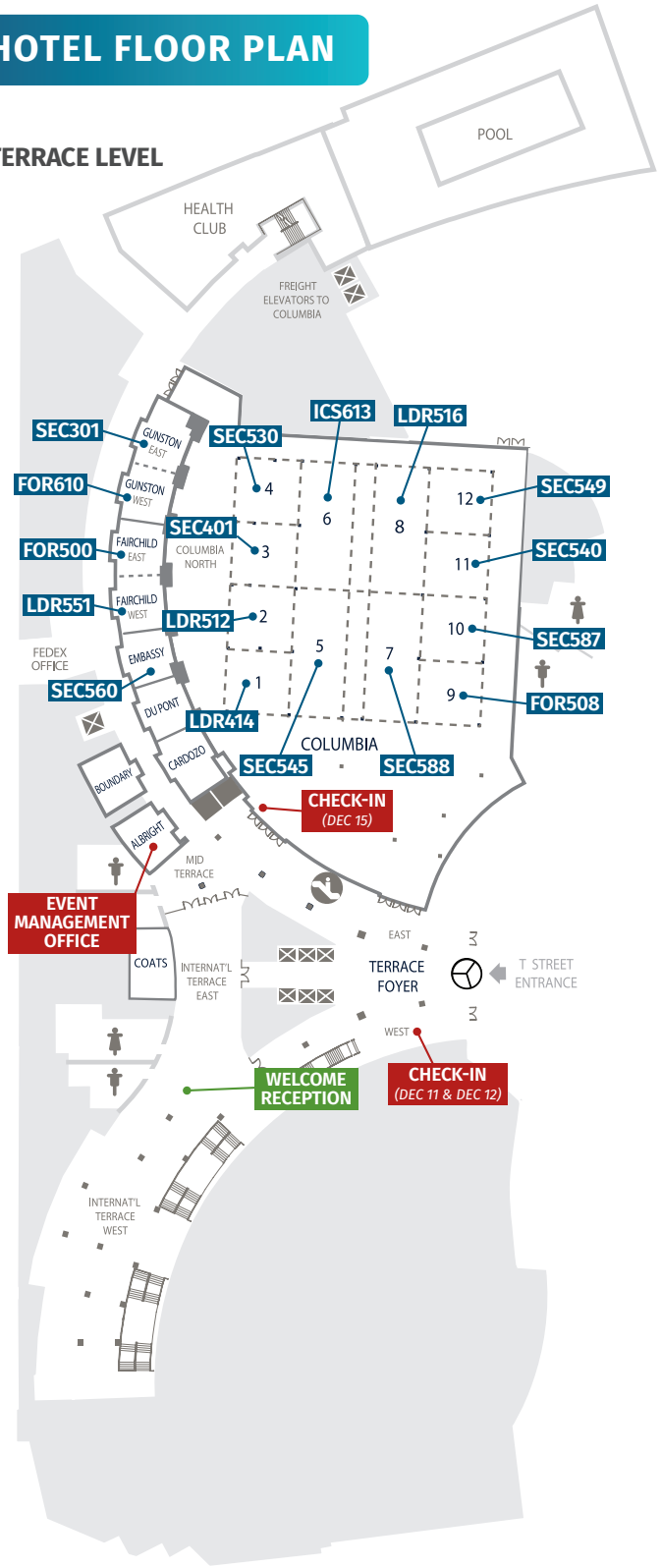
SEC545 GenAI and LLM Application Security (3-DAY COURSE)
Jon Zeolla & Viswanath Chirravuri . . . . . Columbia Hall 5 (TERRACE)

HOTEL FLOOR PLAN

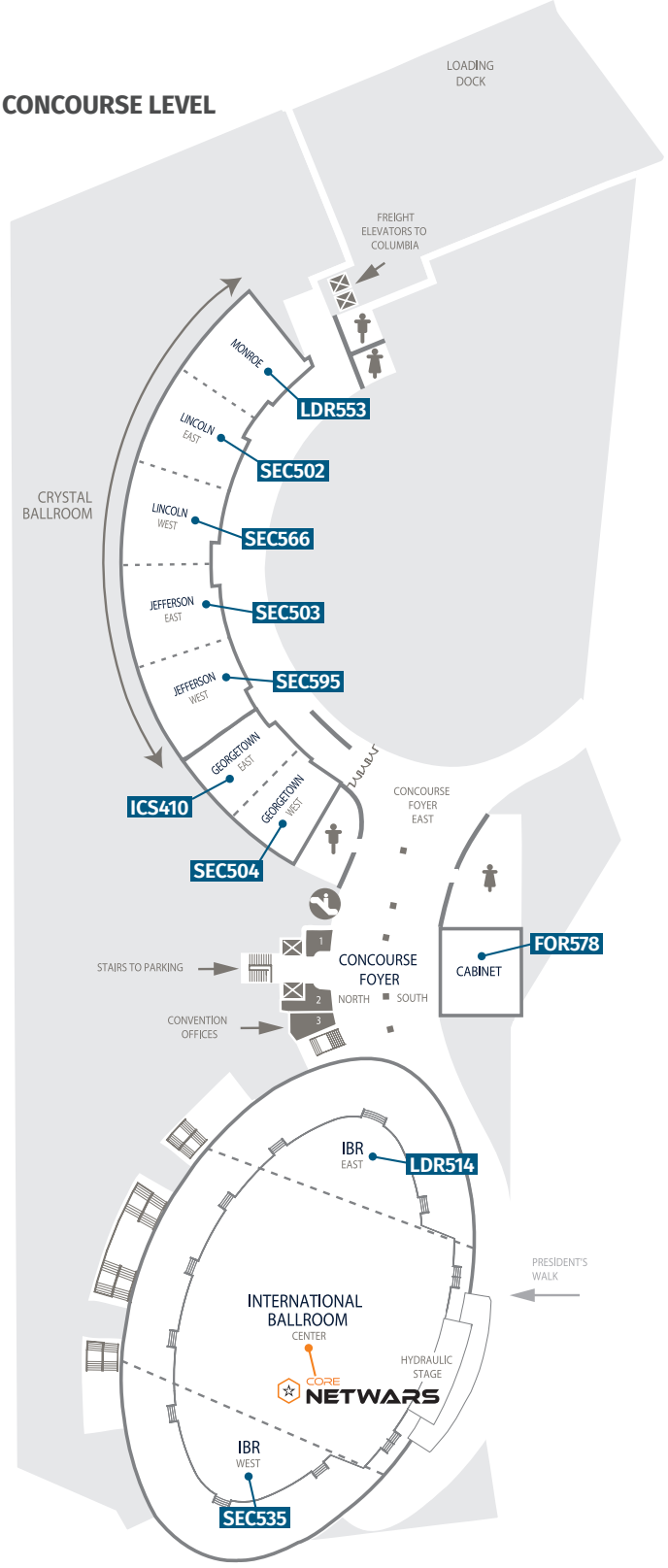


HOTEL FLOOR PLAN

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

SANS CDI 2025 Welcome Reception

DATE/TIME: **Saturday, December 13 | 7:00–8:30 PM**
LOCATION: **International Terrace** (TERRACE LEVEL)

Kick off your SANS Cyber Defense Initiative 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 D.C. Beverages (adult and otherwise) and appetizers will be served. Hope to see you there!

RECEPTION

SANS Community Night: Strengthening Connections in Cybersecurity

DATE/TIME: **Sunday, December 14 | 5:30–6:30 PM**
LOCATION: **International Terrace** (TERRACE LEVEL)

Join us for a special "Community Night" at SANS Cyber Defense Initiative 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. Join SANS staff, faculty, and peers in the field for an inspiring night filled with bites, beverages, and connections.

Plus, stay for two SANS@Night talks or a featured workshop to follow in Columbia 5 or Columbia 7 (Terrace Level) starting at 6:45 PM.

FEATURED KEYNOTE

Cybersecurity Insights:

An Interactive Fireside Chat with U.S. Department of State's Gharun Lacy

DATE: **Friday, December 12**

TIME: **5:00–6:00 PM** (RECEPTION)
6:00–7:00 PM (KEYNOTE)

LOCATION: **Int'l Ballroom Center** (CONCOURSE LEVEL)

SPEAKER: **Gharun S. Lacy, Deputy Assistant Secretary**

As a known hub for the direction of geopolitics, sanctions, and trade, the Department of State is an attractive target for advanced nation-state threat actors motivated more by a desire for information than by greed, and as public-facing representatives of the U.S. overseas, diplomatic staff and buildings don't have the benefit of anonymity.

Deputy Assistant Secretary Gharun Lacy will share Diplomatic Security's cybersecurity strategies for navigating the evolving cyber threat landscape and leveraging emerging technologies as a uniquely positioned law enforcement entity in the U.S. government's most global agency.

BONUS SESSIONS

SANS@NIGHT

How I've Changed the Way I Use AI in 2025

DATE/TIME: **Sunday, December 14 | 6:45–7:45 PM**
LOCATION: **Columbia 5** (TERRACE LEVEL)
SPEAKER: **Matt Edmondson, SANS Senior Instructor**
Founder at Argelius Labs

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 in 2025 and into 2026.

WORKSHOP

USB Trust Issues: Program a $4 Microcontroller to Own Your Systems

DATE/TIME: **Sunday, December 14 | 6:45–8:15 PM**
LOCATION: **Columbia 7** (TERRACE LEVEL)
SPEAKER: **Monta Elkins, SANS Principal Instructor**
Hacker-in-Chief at FoxGuard Solutions

This hands-on workshop provides both practical experience and free hardware. Participants will receive a microcontroller and learn how to program it for USB Human Interface Device (HID) attacks. These attacks bypass standard security controls by impersonating trusted peripherals such as keyboards or mice. We'll explore how inexpensive microcontrollers—available for as little as $4—have dramatically lowered the barrier to entry for such attacks. By the end of the session, you'll know how to configure the provided device to function as a malicious keyboard or as a simple "mouse jiggler."

Requirements: Attendees must bring a laptop (with a USB-A port or a USB-C to USB-A adapter).

SANS@NIGHT

A Current Look at the Threat Landscape, and How AI Plays a Role

DATE/TIME: **Sunday, December 14 | 7:45–8:45 PM**
LOCATION: **Columbia 5** (TERRACE LEVEL)
SPEAKER: **Stephen Sims, SANS Research Fellow**

In this talk we will take a look at the most recent attack techniques, targets, and trends. This includes understanding what kind of malware and illicit access items are available on the dark web for sale and how it can be the first sign of a breach, social engineering attacks, and the latest on 0-day and n-day vulnerability research.

CYBER RANGES

Core NetWars Tournament

DATE/TIME: **Mon, Dec 15 & Tue, Dec 16 | 6:30–9:30 PM**
LOCATION: **Int'l Ballroom Center** (CONCOURSE LEVEL)

Core NetWars is the most comprehensive of the NetWars ranges, this ultimate multi-disciplinary cyber range powers up the most diverse cyber skills. 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.

SANS@NIGHT

From Servant to Surrogate: The Misenar 4A Model for Agentic Security

DATE/TIME: **Monday, December 15 | 7:15–8:15 PM**
LOCATION: **Columbia 5** (TERRACE LEVEL)
SPEAKER: **Seth Misenar, SANS Fellow**
Founder at Context Security Consulting

Organizations keep deploying AI "agents" without understanding what autonomy level they're getting or what governance it warrants. The Misenar 4A Model maps AI autonomy across four levels: Assistant, Adjuvant, Augmentor, and Agent. Each has specific capabilities, boundaries, and control expectations. The framework identifies "DANGER CLOSE," where AI shifts from advisor to executor, and establishes readiness criteria for crossing it. The model includes vendor evaluation tools that cut through marketing, controls that scale with capabilities, and phased implementation strategies.

SANS@NIGHT

Pay to Play: Surviving and Winning Ransomware Negotiations in 2025

DATE/TIME: **Tuesday, December 16 | 7:15–8:15 PM**
LOCATION: **Columbia 7** (TERRACE LEVEL)
SPEAKER: **Matt Bromiley, SANS Certified Instructor**
Security R&D at Prophet Security

When cybercriminals hold your data hostage, do you pay the ransom or call their bluff? In 2024, only 25% of organizations paid ransoms—an all-time low—yet those who did pay still only achieved 46% full data recovery. In this talk, we'll dissect the high-stakes world of ransomware negotiations, where million-dollar decisions happen under extreme pressure. Drawing from real-world negotiation transcripts and the groundbreaking Coinbase case—where a $20M ransom demand was flipped into a $20M bounty for attacker arrests—we'll expose how RaaS platforms have professionalized extortion with customer service portals and triple extortion tactics.

SAVE THE DATE

SANS CDI 2026 is returning to Washington DC
December 14–19, 2026

Upcoming SANS Training Events

Nashville Winter	Nashville, TN	Hybrid	Jan 12–17
Stay Sharp: Jan		Virtual (ET)	Jan 20–22
Rockville	Rockville, MD	Hybrid	Feb 2–7
SANS Surge	La Jolla, CA	Hybrid	Feb 23–28
DC Metro March	Arlington, VA	Hybrid	Mar 2–7
SANS 2026	Orlando, FL	Hybrid	Mar 29–Apr 3
Rocky Mountain	Denver, CO	Hybrid	April 20–25
Security Central	New Orleans, LA	Hybrid	May 11–16
Security West	San Diego, CA	Hybrid	May 11–16
DC Metro June	Arlington, VA	Hybrid	Jun 1–6
Chicago	Chicago, IL	Hybrid	Jun 8–13
Austin	Austin, TX	Hybrid	Jun 22–27
SANSFIRE	Washington, DC	Hybrid	Jul 13–18
Nashville Summer	Nashville, TN	Hybrid	Jul 27–Aug 1
New York	New York, NY	Hybrid	Aug 10–15
Virginia Beach	Virginia Beach, VA	Hybrid	Aug 24–Sep 4
Network Security	Las Vegas, NV	Hybrid	Sep 21–26
DC Metro September	Bethesda, MD	Hybrid	Sep 28–Oct 3
Miami	Coral Gables, FL	Hybrid	Oct 26–31
San Francisco	San Francisco, CA	Hybrid	Nov 2–7
Dallas	Dallas, TX	Hybrid	Dec 7–12
Cyber Defense Initiative®	Washington, DC	Hybrid	Dec 14–19