

SANS 2025

Orlando, FL | April 13–18

#SANS2025  @SANSInstitute

PROGRAM GUIDE



Extend Your Training

SANS ▶ II
OnDemand

SANS 2025

Welcome Reception

Monday, April 14 | 6:30–8:00 PM | Terrace Pool (4TH LEVEL)

Come kick off your SANS 2025 experience at the Welcome Reception on the Upper Level Pool deck! This dynamic event invites you to forge valuable connections and build your cyber community, setting the perfect tone for a week of intense, immersive learning. Dive into discussions about cybersecurity trends, network with faculty and your fellow peers from the industry, gain the opportunity to align your training goals or just relax and have some fun. Beverages (adult and otherwise) and bites will be served.



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



Wednesday, April 16 & Thursday, April 17

6:30–9:30 PM | Windermere W (CONVENTION LEVEL)



Wednesday, April 16 & Thursday, April 17

6:30–9:30 PM | Windermere Y (CONVENTION LEVEL)

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

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

Hyatt Regency Orlando

9801 International Drive | Orlando, FL 32819

Phone: 407-284-1234

Event Check-In | Badge & Courseware Distribution

Location: Windermere X (CONVENTION LEVEL)

Saturday, April 12 4:00–6:00 PM

Sunday, April 13 7:00–8:30 AM

Registration Support

Location: Windermere Foyer (CONVENTION LEVEL)

Sunday, April 13–Monday, April 14 8:00 AM–5:30 PM

Location: Celebration 10 (CONVENTION LEVEL)

Tuesday, April 15–Thursday, April 17 8:00 AM–5:30 PM

Friday, April 18 8:00 AM–2:30 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.

Parking

Overnight self-parking is available for \$35 plus tax per night with in-and-out privileges.

Valet Parking is available for \$53.00 per day.

If you are an overnight hotel guest, this credit will be applied to your room. If you are driving in daily, please visit the Event Management Office to pick up your discount tickets.*

*Arrival ticket will still be required to depart the parking garage—the discount ticket needs to be placed into the machine after the arrival ticket to receive the discount.

Photography Notice

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

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 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:

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 (Sunday, April 13)

FOR498 Digital Acquisition and Rapid Triage™ (6-DAY COURSE)
Kevin Ripa Bayhill 26 (LOBBY LEVEL)

FOR500 Windows Forensic Analysis™ (6-DAY COURSE)
Ovie Carroll Celebration 2 (CONVENTION LEVEL)

FOR508 Advanced Incident Response, Threat Hunting & Digital Forensics™ (6-DAY COURSE)
Carlos Cajigas Windermere W (CONVENTION LEVEL)

FOR509 Enterprise Cloud Forensics & Incident Response™
(6-DAY COURSE)
Pierre Lidome Celebration 16 (CONVENTION LEVEL)

FOR577 Linux Incident Response and Threat Hunting™ (6-DAY COURSE)
Tarot Wake Celebration 15 (CONVENTION LEVEL)

FOR578 Cyber Threat Intelligence™ (6-DAY COURSE)
John Doyle Bayhill 21 (LOBBY LEVEL)

FOR585 Smartphone Forensic Analysis In-Depth™ (6-DAY COURSE)
Heather Barnhart Bayhill 18 (LOBBY LEVEL)

FOR608 Enterprise-Class Incident Response & Threat Hunting™ (6-DAY COURSE)
Mike Pilkington Challenger 39 (3RD LEVEL)

ICS410 ICS/SCADA Security Essentials™ (6-DAY COURSE)
Justin Searle Barrel Spring I (LOBBY LEVEL)

ICS515 ICS Visibility, Detection, and Response™ (6-DAY COURSE)
Dean Parsons Windermere Z (CONVENTION LEVEL)

LDR414 SANS Training Program for CISSP® Certification™
(6-DAY COURSE)
David R. Miller Bayhill 19 (LOBBY LEVEL)
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 Bayhill 22 (LOBBY LEVEL)

LDR514 Security Strategic Planning, Policy & Leadership™
(5-DAY COURSE)
Mark Williams Bayhill 20 (LOBBY LEVEL)

LDR516 Building and Leading Vulnerability Management Programs™ (5-DAY COURSE)
Jonathan Risto Peacock Spring (LOBBY LEVEL)

LDR521 Security Culture for Leaders™ (5-DAY COURSE)
Lance Spitzner Challenger 38 (3RD LEVEL)

LDR551 Building and Leading Security Operations Centers™
(5-DAY COURSE)
Mark Orlando Barrel Spring II (LOBBY LEVEL)

LDR553 Cyber Incident Management™ (5-DAY COURSE)
Steve Armstrong-Godwin Bayhill 24 (LOBBY LEVEL)

SEC301 Introduction to Cyber Security™ (5-DAY COURSE)
Doc Blackburn Bayhill 30 (LOBBY LEVEL)

SEC401 Security Essentials: Network, Endpoint & Cloud™
(6-DAY COURSE)
Bryan Simon Celebration 3 (CONVENTION LEVEL)
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–5)

SEC450 Blue Team Fundamentals: Security Operations and Analysis™ (6-DAY COURSE)
Mark Jeanmougin Celebration 1 (CONVENTION LEVEL)

SEC488 Cloud Security Essentials™ (6-DAY COURSE)
Kenneth G. Hartman Bayhill 28 (LOBBY LEVEL)

SEC497 Practical Open-Source Intelligence (OSINT)™ (6-DAY COURSE)
Mick Douglas Manatee Spring II (LOBBY LEVEL)

SEC503 Network Monitoring & Threat Detection In-Depth™
(6-DAY COURSE)
Andrew Laman Coral Spring I (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)
Josh Wright & Jeroen Hoof Windermere Y (CONVENTION LEVEL)
Hours: 8:30 AM–7:15 PM (Day 1)

SEC511 Cybersecurity Engineering: Advanced Threat Detection and Monitoring™ (6-DAY COURSE)
Seth Misenaar Bayhill 29 (LOBBY LEVEL)
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–5)

SEC522 Application Security: Securing Web Applications, APIs, and Microservices™ (6-DAY COURSE)
Dr. Johannes Ullrich Celebration 4 (CONVENTION LEVEL)

SEC530 Defensible Security Architecture & Engineering: Implementing Zero Trust for the Hybrid Enterprise™
(6-DAY COURSE)
Don Murdoch Bayhill 32 (LOBBY LEVEL)

COURSE SCHEDULE

- SEC540 Cloud Security & DevSecOps Automation™** (5-DAY COURSE)
Jon Zeolla Bayhill 33 (LOBBY LEVEL)
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–4)
- SEC542 Web App Penetration Testing & Ethical Hacking™**
(6-DAY COURSE)
Bojan Zdrnja Bayhill 31 (LOBBY LEVEL)
- SEC549 Cloud Security Architecture™** (5-DAY COURSE)
David Hazar Bayhill 17 (LOBBY LEVEL)
- SEC560 Enterprise Penetration Testing™** (6-DAY COURSE)
Jeff McJunkin Bayhill 23 (LOBBY LEVEL)
- SEC565 Red Team Operations & Adversary Emulation™** (6-DAY COURSE)
David Mayer Rock Spring (LOBBY LEVEL)
- SEC573 Automating Information Security with Python™**
(6-DAY COURSE)
Mark Baggett Coral Spring II (LOBBY LEVEL)
- SEC575 iOS and Android Application Security Analysis and Penetration Testing™** (6-DAY COURSE)
Jeroen Beckers Bayhill 27 (LOBBY LEVEL)
- SEC587 Advanced Open-Source Intelligence (OSINT) Gathering and Analysis™** (6-DAY COURSE)
Matt Edmondson Celebration 12 (CONVENTION LEVEL)
- SEC595 Applied Data Science & AI/Machine Learning for Cybersecurity Professionals™** (6-DAY COURSE)
Christopher Crowley Manatee Spring I (LOBBY LEVEL)
- SEC617 Wireless Penetration Testing and Ethical Hacking™**
(6-DAY COURSE)
Larry Pesce Celebration 14 (CONVENTION LEVEL)
- SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking™** (6-DAY COURSE)
Stephen Sims & Douglas McKee Bayhill 25 (LOBBY LEVEL)
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–5)

Free Resources

Newsletters

NewsBites

Twice-weekly, high-level executive summaries of the most important news relevant to cybersecurity professionals.

OUCH!

The world's leading monthly free security awareness newsletter designed for the common computer user.

@RISK: The Consensus Security Alert

A reliable weekly summary of newly discovered attack vectors, vulnerabilities with active new exploits, how recent attacks worked, and other valuable data.

Virtual Events, Research & Webcasts

Analyst Program: Research & Content

Reports on emerging and mission-critical topics. Solution providers drive topic awareness to a qualified audience of decision-makers and influencers through insightful educational content and help security teams tackle today's threats.

Ask The Expert Webcasts

SANS Experts bring current and timely information on relevant topics in IT security. These are the go-to online format to obtain actionable information to help you in your security goals.

Solutions Forums & Summit Tracks

In partnership with a SANS subject-matter expert, invited speakers showcase their products and solutions to high-level security practitioners and cybersecurity decision-makers.

Many Other Free Resources

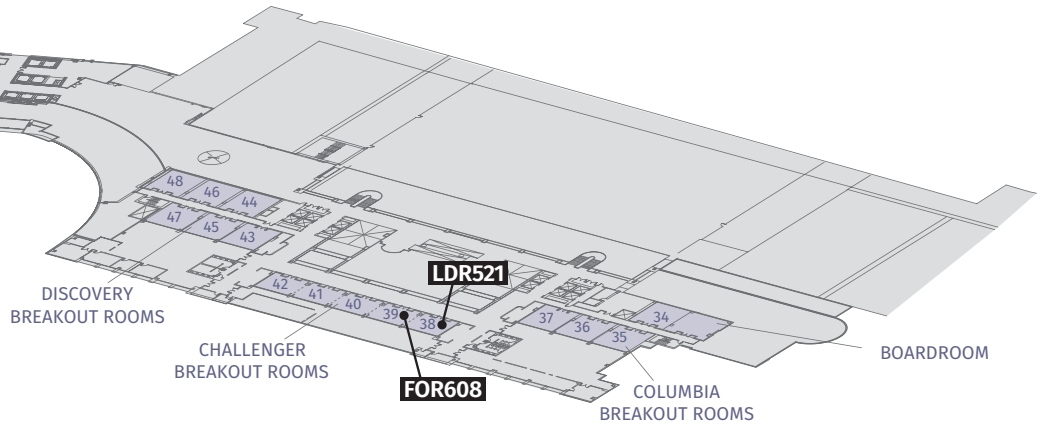
(SANS.org account not required)

- InfoSec Reading Room
- Top 25 Software Errors
- 20 Critical Controls
- Security Policies
- Intrusion Detection FAQs
- Tip of the Day
- Security Posters
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

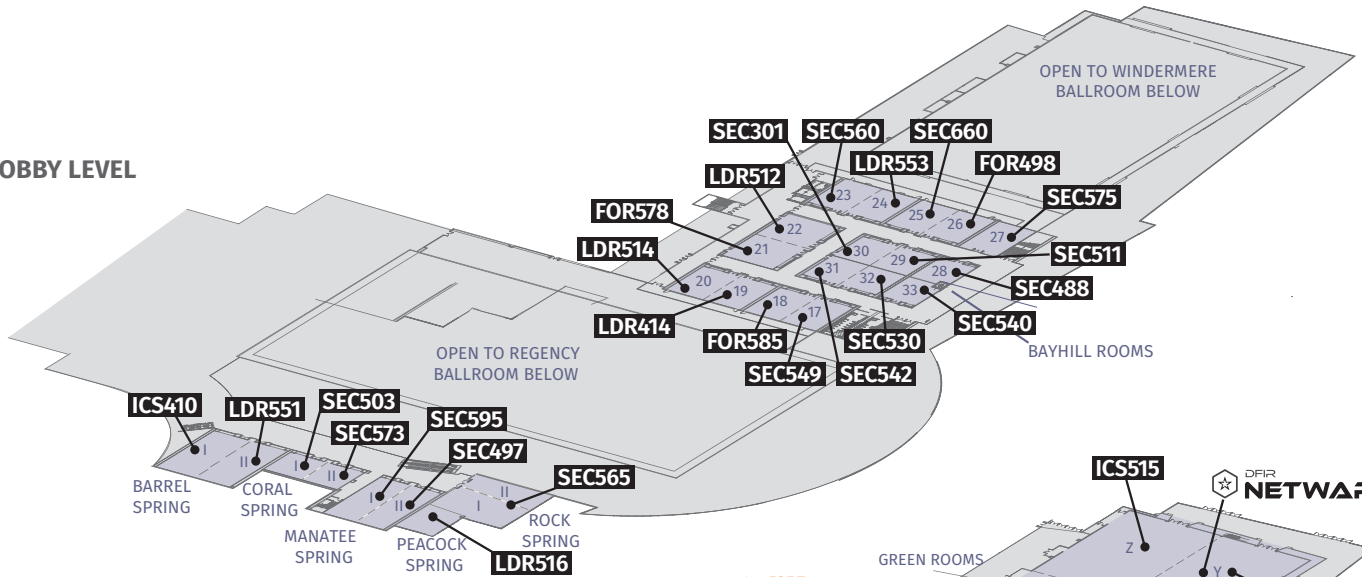
Sign into your SANS account to enjoy these free resources at www.sans.org/account

HOTEL FLOOR PLAN

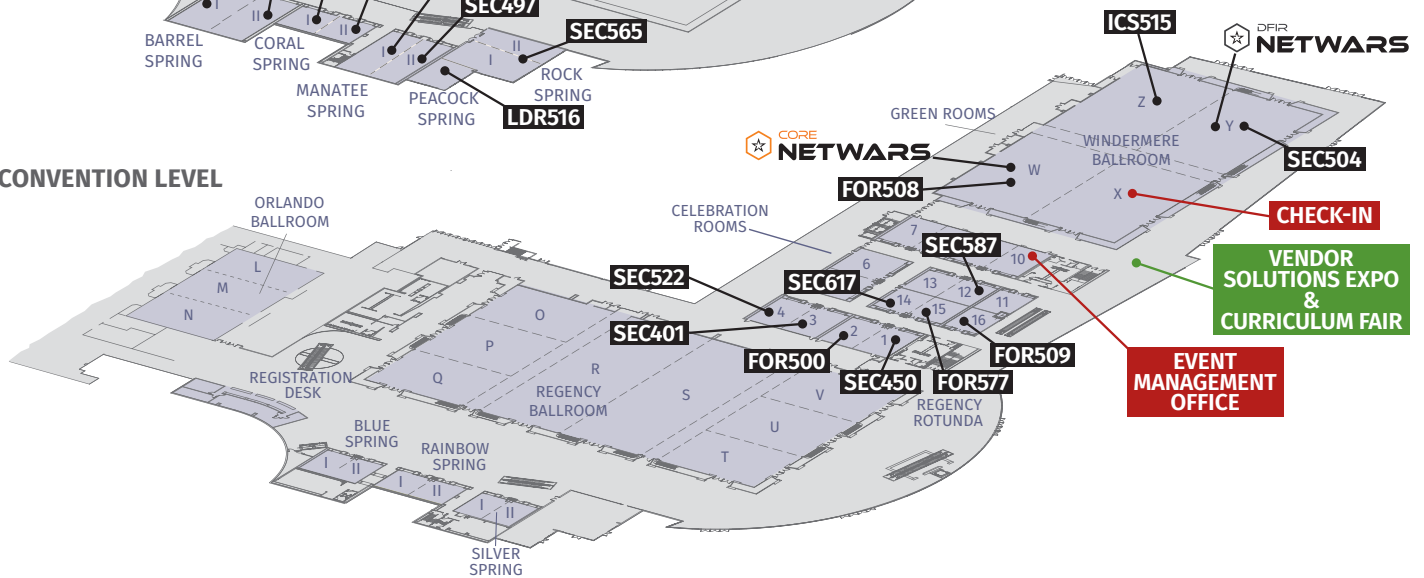
THIRD LEVEL



LOBBY LEVEL



CONVENTION 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.

LUNCH & LEARN

GIAC Exam Preparation Tips & Tricks

Sunday, April 13 | 12:30–1:15 PM

LOCATION: **Manatee Spring I** (LOBBY LEVEL)

SPEAKERS: **Farah Al Aina & Emily Sturnick, SANS Senior Client Success Managers**

GIAC Certifications is a leading provider of information security certifications, testing and validating expertise in cyber defense, penetration testing, forensics, software security, management, and industrial control systems (ICS). This session will focus on the benefits of certification and provide practical exam preparation tips to help candidates succeed.

SPONSORED EVENT

Silent Push Lunch & Learn

Monday, April 14 | 12:30–1:15 PM

LOCATION: **Windermere Y** (CONVENTION LEVEL)

SPEAKER: **João Ferreira, Threat Analyst**



SPONSORED EVENT

Level Blue Lunch & Learn

Monday, April 14 | 12:30–1:15 PM

LOCATION: **Manatee Spring I** (LOBBY LEVEL)



SPONSORED EVENT

Malwarebytes Lunch & Learn

Monday, April 14 | 12:30–1:15 PM

LOCATION: **Manatee Spring II** (LOBBY LEVEL)



FEATURED KEYNOTE

Russia and the Cyber Battlefield:

Geopolitical Motivations Behind State-Sponsored Hacking



Sunday, April 13 | 6:30–8:00 PM

LOCATION: **Windermere X** (CONVENTION LEVEL)

SPEAKER: **Dr. Bilyana Lilly, CISSP**

The 2025 Global Cybersecurity Outlook by the World Economic Forum identified geopolitical tensions as a key driver shaping cybersecurity strategies worldwide. Recent revelations of Chinese, Russian, and Iranian hackers positioning malware on U.S. infrastructure to enable disruptive attacks underscore the Forum's findings and serve as urgent reminders of the critical need to protect U.S. organizations against ever-evolving cyber threats. These advanced cyber operations are rarely isolated incidents; they are deeply embedded within broader national strategies, aligning with geopolitical objectives. This keynote will explore the intricate relationship between the foreign and domestic policies of Russia, China, and Iran and their cyber operations targeting U.S. organizations. The discussion will provide insights into how political agendas influence cyber tactics and will illuminate the shifting landscape of cybersecurity challenges in an increasingly interconnected and contested world.

BONUS SESSIONS

SPECIAL EVENT

Fireside Chat: How Certifications Can Help My Career

Monday, April 14 | 5:30–6:30 PM

LOCATION: **Windermere X** (CONVENTION LEVEL)

MODERATOR: **Ed Skoudis, SANS Fellow**

PANELISTS: **Dr. TJ O'Connor & Jeremiah Hainly**

Looking to advance your cybersecurity career? Wondering if certification is worth the investment?

Join Ed Skoudis, SANS Fellow as he moderates an insightful fireside chat with two accomplished GIAC-certified experts:

- **Dr. TJ O'Connor**—A retired U.S. Army Lieutenant Colonel with a 20-year military career, Dr. O'Connor has deep experience in cyber operations, Special Forces support, and academia. He currently leads Florida Tech's cybersecurity program, coaching students to national and international victories in cyber competitions.
- **Jeremiah Hainly**—A security solutions manager at the Hershey Company and a SANS online training subject-matter expert, Hainly is a GIAC Security Expert (GSE) and NetWars champion with a wealth of experience in offensive and defensive security.

Expect a lively and candid discussion on:

- What employers really look for in candidates
- The tangible and intangible benefits of certification
- Future trends in cybersecurity hiring and skills
- Balancing career growth with personal life
- How to choose the right certification for your goals

Don't miss this opportunity to gain expert insights, ask questions, and network with industry leaders. Whether you're just starting out or looking to level up, this session will be insightful.

RECEPTION

SANS 2025 Welcome Reception

Monday, April 14 | 6:30–8:00 PM | LOCATION: **Terrace Pool** (4TH LEVEL)

Come kick off your SANS 2025 experience at the Welcome Reception on the Upper Level Pool deck! This dynamic event invites you to forge valuable connections and build your cyber community, setting the perfect tone for a week of intense, immersive learning. Dive into discussions about cybersecurity trends, network with faculty and your fellow peers from the industry, gain the opportunity to align your training goals or just relax and have some fun. Beverages (adult and otherwise) and bites will be served.

SPONSORED EVENT

Vendor Solutions Expo – Breakfast

Tuesday, April 15 | 7:30–9:00 AM

LOCATION: **Windermere Foyer** (CONVENTION LEVEL)

SPECIAL EVENT

Professional Headshot Lounge

Tuesday, April 15 | 8:00 AM–6:00 PM

LOCATION: **Windermere Foyer** (CONVENTION LEVEL)

Take a break from training and step into the spotlight with a fresh new headshot at SANS 2025! Whether you're updating your LinkedIn profile, refreshing your company bio, or just want a polished new look, Inbound Video Pros have you covered. Their team of expert photographers and editors will be on-site all day, capturing high-quality, studio-lit headshots that bring out your best. Plus, with instant access and delivery, you'll walk away with a new headshot in no time—no registration or sign-ups required. Stop by, give your best smile, and leave with a headshot that makes a lasting impression!

SPONSORED EVENT

Vendor Solutions Expo – Lunch

Tuesday, April 15 | 12:15–1:30 PM

LOCATION: **Windermere Foyer** (CONVENTION LEVEL)

RECEPTION

SANS 2025 AlumNight: Powered by Cloud Security + DFIR

Tuesday, April 15 | 5:30–6:30 PM

LOCATION: **Regency Lounge** (CONVENTION LEVEL)

Dive into a night of celebration and connection at the SANS 2025 AlumNight! Whether this marks your debut or your return, you're in for the industry's premier cybersecurity gathering. Join us for an unforgettable evening of networking, bites, beverages, and exclusive giveaways.

Revel in dynamic discussions led by seasoned experts and connect with a community of SANS alumni and instructors. Set in a lively and engaging atmosphere, this event bridges the gap between in-person participants and local cybersecurity professionals, creating a rich tapestry of experiences.

SANS 2025 AlumNight isn't just an event—it's a powerhouse experience designed to ignite your passion for cybersecurity and cultivate connections that last a lifetime.

"Once a SANS Alumni, Always a SANS Alumni."

RECEPTION

LATAM Community Night

Tuesday, April 15 | 6:30–7:30 PM

LOCATION: **Celebration 1** (CONVENTION LEVEL)

We invite you to our LATAM Community Night where Latin American SANS enthusiasts get together. Our Latin American SANS instructors and staff will be there.

ALUMNIGHT CLOUD SECURITY WORKSHOP

Prevent Remote Code Execution with Private Endpoints

Tuesday, April 15 | 6:45–8:45 PM

LOCATION: **Manatee Spring I** (LOBBY LEVEL)

SPEAKER: **Kenneth Hartman, Certified Instructor**

As demonstrated in the Aviata Cloud series, public cloud resources pose a major risk. One mitigation, Private Endpoints, allows users and workloads to connect to cloud services without internet access. This allows cloud administrators to isolate workloads from the world while enabling them to continue using the cloud services they need. They can also be used to prevent access to sensitive data in cloud services if the request did not originate from the private network.

Without internet access, it should not be possible to exfiltrate private data or perform Remote Code Execution (RCE). Unfortunately, attackers can leverage improperly configured private endpoints to do both. By creating their own publicly accessible cloud resources, attackers can trick workloads into downloading malicious code and exfiltrate data without a single packet leaving the cloud network.

In this workshop, we will analyze a real cloud application powered by AWS Lambda, exfiltrate data with an RCE executed through a supply-chain attack and escalate privileges using AWS IAM credentials. We will then lock down the Lambda to a private network with private endpoints and prevent these IAM credentials from being used externally. Next, we will then demonstrate that this configuration is still vulnerable to this attack. Finally, we will lock down the private endpoint policy to block the attack altogether.

This workshop was inspired by “Exfiltration Paths in Isolated Environments using VPC Endpoints” by Jonathan Adler.

ALUMNIGHT DFIR WORKSHOP

Threat Hunting and Criminal Infrastructure Analysis

Tuesday, April 15 | 6:45–8:45 PM

LOCATION: **Manatee Spring II** (LOBBY LEVEL)

SPEAKER: **Conan Beach**

This hands-on workshop will take you through a detailed FOR589: Cybercrime Investigations course lab focusing on the complexities of cybercrime infrastructure. You will delve into the critical types of infrastructure indicators—atomic, behavioral, and computed—and their roles in detecting and understanding cybercrime activities.

Learn about the pivotal role that domains, IP addresses, and email accounts play as atomic indicators, and understand how Infrastructure-as-a-Service (IaaS) helps in identifying the ownership of these indicators. The workshop includes practical exercises where you will use advanced fingerprinting techniques not only to identify but also to predict cybercrime behaviors. This approach will enhance your skills in analyzing and countering cyber threats.

LUNCH & LEARN

GIAC CyberLive Demo Lunch & Learn

Wednesday, April 16 | 12:30–1:15 PM

LOCATION: **Manatee Spring I** (LOBBY LEVEL)

SPEAKERS: **GIAC Security Engineers Jonathan Baeckel & Brian O'Hara**

CyberLive is a hands-on, real-world testing experience designed to validate cybersecurity skills through practical, real-world tasks. This 100% virtual machine environment simulates operating systems and requires the application of technical capabilities and skills. CyberLive exams allow for creative thinking, with multiple ways to solve problems, reflecting the dynamic nature of cybersecurity roles. Most new GIAC certifications will incorporate CyberLive, providing an authentic assessment of candidates' abilities in a realistic setting.

What you will see:

- How CyberLive mirrors real-world job tasks in a virtual machine environment.
- The application of technical skills and creative problem-solving in a dynamic test format.
- A fully virtual machine environment and operating systems used during the exam.
- How to approach and solve problems creatively with multiple solutions.

BONUS SESSIONS

SPECIAL EVENT

SANS Curriculum Fair and Evening Reception

Wednesday, April 16 | 8:00 AM–6:00 PM

LOCATION: **Windermere Foyer** (CONVENTION LEVEL)

Prepare for an unparalleled preview of the latest SANS curriculum and product innovations. This exclusive event presents a unique opportunity in 2025 to experience the newest SANS developments firsthand—before anyone else! Be the first and ONLY to explore game-changing updates, enhancements, and launches within each curriculum here at SANS that could redefine your cybersecurity career.

Curriculum Fair Schedule:

AM Break	8:00–9:00 AM
Mid-Morning Break	10:30–10:50 AM
Lunch Break (LUNCH NOT PROVIDED)	12:15–1:30 PM
Afternoon Break	3:00–3:20 PM
Evening Reception (LIGHT BITES & BEVERAGES PROVIDED)	5:00–6:00 PM

SANS@NIGHT

SBOMs the Hard Way: Hacking Bob the Minion

Wednesday, April 16 | 6:00–7:00 PM | LOCATION: Manatee I (LOBBY LEVEL)

SPEAKER: **Larry Pesce, Principal Instructor**

This presentation delves into the intricate process of generating a Software Bill of Materials (SBOM) for the Bob the Minions WiFi router by Davolink—a device whose firmware isn't publicly available. Traditional SBOM creation methods rely on readily accessible firmware, but Davolink's restricted release policies necessitated an unconventional approach. This talk covers the step-by-step journey of hardware disassembly, firmware extraction via SPI flash and JTAG/SWD interfaces, and the tools and techniques employed.

Finally, we'll demonstrate how the recovered firmware is used to generate a comprehensive SBOM, highlighting any security vulnerabilities discovered and reported to the vendor. This session aims to provide attendees with practical insights into overcoming SBOM generation challenges in the IoT domain through hands-on hardware hacking, and leveraging the firmware and SBOMs for vulnerability discovery, as well as security improvement.

SANS@NIGHT

There is No Spoon!

Thursday, April 17 | 6:00–7:00 PM | LOCATION: Manatee I (LOBBY LEVEL)

SPEAKER: **Steve Armstrong-Godwin, Principal Instructor**

Dive into the captivating world of cybersecurity with a twist as we unravel the matrix within your Incident Response plans. Drawing inspiration from "The Matrix," this talk challenges the conventional belief that you're in control. Imagine your IR plans as the blue pill, offering a false sense of security. Choose the red pill, and Steve will guide you through Wonderland, exposing the intricacies missing from your strategies.

Beginning with a wake-up call, we'll explore the illusions surrounding your readiness for black swan incidents. This matrix-themed journey scrutinizes challenges at both SOC and Exec levels, revealing the reality beneath the surface. Brace yourself for an engaging exploration that goes beyond the ordinary.

Join Steve to acquire Response Planning Kung-Fu and reshape your approach to incident response. This talk isn't just a presentation; it's an invitation to break free from the matrix of conventional thinking. Embrace the red pill, and let's together navigate the Wonderland of cybersecurity complexities, ensuring you're truly prepared for whatever the digital realm may throw your way.

CYBER RANGES

Core NetWars Tournament



Wednesday, April 16 & Thursday, April 17 | 6:30–9:30 PM

LOCATION: **Windermere W** (CONVENTION 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

DFIR NetWars Tournament



Wednesday, April 16 & Thursday, April 17 | 6:30–9:30 PM

LOCATION: **Windermere Y** (CONVENTION LEVEL)

Focused on digital forensics, incident response, threat hunting, and malware analysis, this tool-agnostic approach covers everything from low-level artifacts to high-level behavioral observations.

SAVE THE DATE

SANS 2026 is returning to the Hyatt Regency Orlando March 29–April 5, 2026

Upcoming SANS Training Events

Stay Sharp: April		Virtual (CT)	Apr 28–30
Chicago Spring	Chicago, IL	Hybrid	Apr 28–May 3
Security West™	San Diego, CA	Hybrid	May 5–10
SEC504: Part-Time Schedule		Virtual (ET)	May 13–Jun 12
SEC588: Part-Time Schedule		Virtual (ET)	May 13–Jun 12
Security Leadership Nashville	Nashville, TN	Hybrid	May 19–23
Baltimore Spring	Baltimore, MD	Hybrid	Jun 2–7
Cyber Defense Miami	Coral Gables, FL	Hybrid	Jun 2–7
Offensive Operations East	Baltimore, MD	Hybrid	Jun 8–14
Rocky Mountain	Denver, CO	Hybrid	Jun 23–28
SANSFIRE™	Washington, DC	Hybrid	Jul 14–19
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
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
Stay Sharp: Nov		Virtual (ET)	Nov 10–12