SANS | GIAC CERTIFICATIONS

SANS Cyber Defense Initiative® 2024

Washington, DC | December 13–18

PROGRAM GUIDE

#SANSCDI @SANSInstitute

SANS CYBER DEFENSE INITIATIVE® 2024

Welcome Reception

Saturday, December 14 | 6:30–8:00 PM

LOCATION: **International Terrace** (TERRACE LEVEL)

Kick off your Cyber Defense Initiative® 2024 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 of your week in Washington, DC. Come join your instructors and fellow students for a fun, relaxed evening. Beverages (adult and otherwise) and small bites will be included.

SANS CYBER RANGES

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

NETWARS CORE

Monday, December 16 & Tuesday, December 17
6:30–9:30 PM
International Ballroom Center (CONCOURSE LEVEL)

All In-Person students who registered to attend a course at CDI 2024 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)

Thursday, December 12	4:00–6:00 PM
Friday, December 13	7:00–8:30 AM

Registration Support

Location: International Terrace (TERRACE LEVEL)

Fri, December 13 & Sat, December 14	8:30 AM–5:30 PM

Location: Albright Room (TERRACE LEVEL)

Sun, December 15–Tue, December 17	8:30 AM–5:30 PM
Wed, December 18	8:30 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.

Parking

Self-parking is available for $54 per day at the Washington Hilton.*

*Parking rates are subject to change.

Photography Notice

SANS may take photos of classroom activities for marketing purposes. SANS Cyber Defense Initiative® 2024 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 4–5.

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™

SEC510:™ Public Cloud Security: AWS, Azure, and GCP™

SEC540:™ Cloud Security and DevSecOps Automation™

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

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 (Monday, December 11)

FOR500™ Windows Forensic Analysis™ (6-DAY COURSE)
Ovie Carroll ...... Columbia Hall 4 (TERRACE LEVEL)

FOR508™ Advanced Incident Response, Threat Hunting & Digital Forensics™ (6-DAY COURSE)
Eric Zimmerman ...... Int'l Ballroom East (CONCOURSE LEVEL)

FOR509™ Enterprise Cloud Forensics & Incident Response™ (6-DAY COURSE)
Megan Roddie ...... Gunston West (TERRACE LEVEL)

FOR578™ Cyber Threat Intelligence™ (6-DAY COURSE)
Rebekah Brown ...... Columbia Hall 12 (TERRACE LEVEL)

FOR585™ Smartphone Forensic Analysis In-Depth™ (6-DAY COURSE)
Heather Barnhart ...... Holmead West (LOBBY LEVEL)

FOR610™ Reverse-Engineering Malware: Malware Analysis Tools & Techniques™ (6-DAY COURSE)
Lenny Zeltser ...... Columbia Hall 3 (TERRACE LEVEL)

ICS410™ ICS/SCADA Security Essentials™ (6-DAY COURSE)
Don C. Weber ...... Jefferson East (CONCOURSE LEVEL)

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

LDR414™ SANS Training Program for CISSP® Certification™ (6-DAY COURSE)
Seth Misenar ...... Cabinet (CONCOURSE 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 ...... Monroe (CONCOURSE LEVEL)

LDR514™ Security Strategic Planning, Policy & Leadership™ (5-DAY COURSE)
Frank Kim ...... Lincoln West (CONCOURSE LEVEL)

LDR516™ Building and Leading Vulnerability Management Programs™ (5-DAY COURSE)
Jonathan Risto ...... Columbia Hall 10 (TERRACE LEVEL)

LDR551™ Building and Leading Security Operations Centers™ (5-DAY COURSE)
Mark Orlando ...... Lincoln East (CONCOURSE LEVEL)

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

SEC301™ Introduction to Cyber Security™ (5-DAY COURSE)
Rich Greene ...... Jefferson West (CONCOURSE LEVEL)

SEC401™ Security Essentials: Network, Endpoint & Cloud™ (6-DAY COURSE)
Ted Demopoulos ...... Georgetown West (CONCOURSE 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)
John Hubbard ...... Fairchild West (TERRACE LEVEL)

SEC488™ Cloud Security Essentials™ (6-DAY COURSE)
Simon Vernon ...... Morgan (LOBBY LEVEL)

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

SEC503™ Network Monitoring & Threat Detection In-Depth™ (6-DAY COURSE)
Andrew Laman ...... Oak Lawn (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)
Jon Gorenflo ...... Int'l Ballroom West (CONCOURSE LEVEL)
Hours: 8:30 AM–7:15 PM (Day 1)

SEC510™ Public Cloud Security: AWS, Azure, and GCP™ (5-DAY COURSE)
Kenneth G. Hartman ...... Embassy (TERRACE LEVEL)
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–4)

SEC522™ Application Security: Securing Web Apps, APIs, and Microservices™ (6-DAY COURSE)
Dr. Johannes Ullrich ...... Columbia Hall 9 (TERRACE LEVEL)

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

SEC540™ Cloud Security & DevSecOps Automation™ (5-DAY COURSE)
Eric Johnson ...... Northwest (LOBBY LEVEL)
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–4)

SEC541™ Cloud Security Attacker Techniques, Monitoring & Threat Detection™ (5-DAY COURSE)
Ryan Thompson ...... Columbia Hall 2 (TERRACE LEVEL)

SEC542™ Web App Penetration Testing & Ethical Hacking™ (6-DAY COURSE)
Timothy McKenzie ...... Fairchild East (TERRACE LEVEL)

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

SEC560™ Enterprise Penetration Testing™ (6-DAY COURSE)
Jeff McJunkin ...... Columbia Hall 7 (TERRACE LEVEL)

SEC565™ Red Team Operations & Adversary Emulation™ (6-DAY COURSE)
David Mayer ...... Columbia Hall 8 (TERRACE LEVEL)

SEC566™ Implementing & Auditing CIS Controls™ (5-DAY COURSE)
Randy Marchany,
Matthew Nappi ...... Columbia Hall 11 (TERRACE LEVEL)

SEC588™ Cloud Penetration Testing™ (6-DAY COURSE)
Christopher Elgee ...... Holmead East (LOBBY LEVEL)

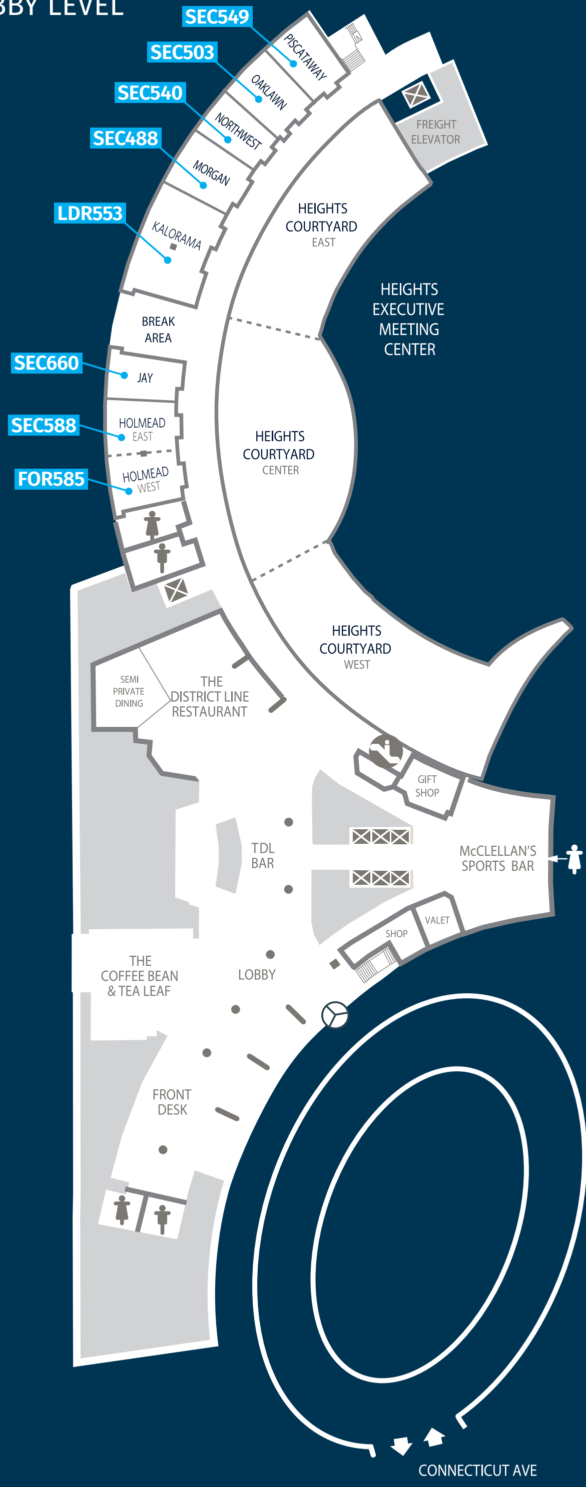
SEC595™ Applied Data Science & AI/Machine Learning for Cybersecurity Professionals™ (6-DAY COURSE)
David Hoelzer & Steve Sharman ...... Columbia Hall 5 (TERRACE LEVEL)

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

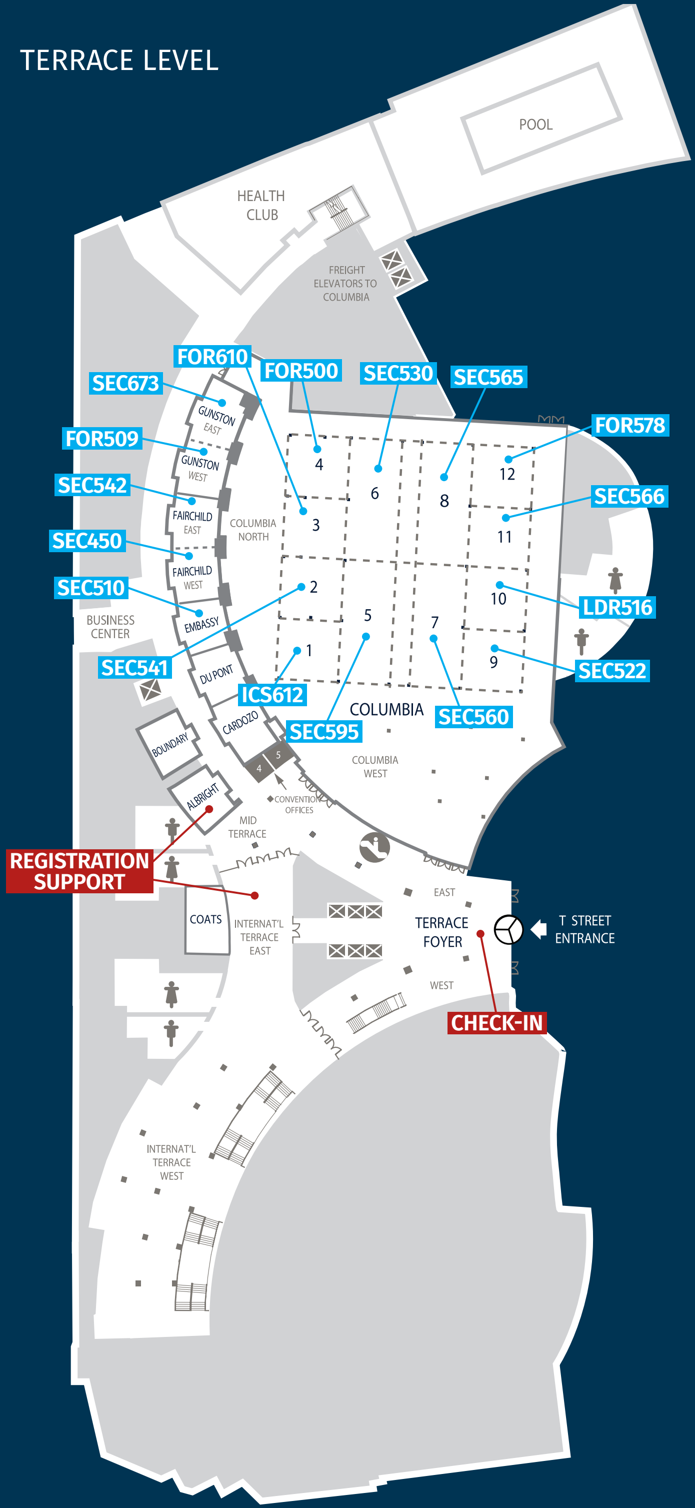
SEC673™ Advanced Information Security Automation with Python™ (6-DAY COURSE)
Mark Baggett ...... Gunston East (TERRACE LEVEL)

HOTEL FLOOR PLAN

LOBBY LEVEL

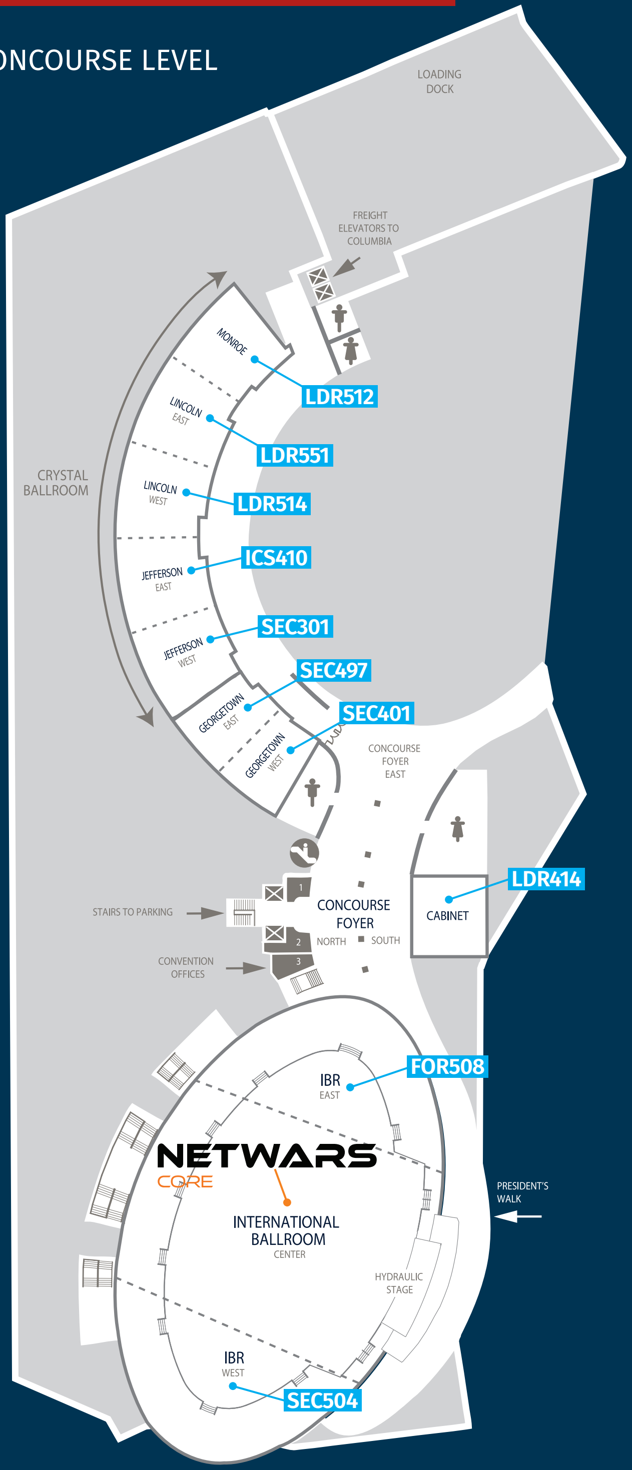


TERRACE LEVEL



HOTEL FLOOR PLAN

CONCOURSE LEVEL



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**

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 2024 Welcome Reception

Saturday, December 14 | 6:30–8:00 PM
LOCATION: **International Terrace** (TERRACE LEVEL)

Kick off your Cyber Defense Initiative 2024 experience at the Welcome Reception. Be part of this kickoff event and join us for a community gathering you cannot miss. Share stories, make connections, and learn how to make the most of your week in Washington, DC. Come join your fellow students for a fun, relaxed evening and enjoy the arcade and table game offerings. Beverages (adult and otherwise) and bites will be served.

RECEPTION

SANS CDI 2024 AlumNight: Powered by Cyber Defense & Cloud Security

Sunday, December 15
RECEPTION: **5:30–6:30 PM** | TALKS: **6:45–8:45 PM**
LOCATION: **Columbia Ballroom** (TERRACE LEVEL)

Embark on your cybersecurity journey and make it unforgettable! Whether it's your first SANS event or you're returning, join the industry's premier gathering of cybersecurity professionals! Experience an electrifying celebration where networking, food, drinks, giveaways, and dynamic expert discussions converge. Connect with fellow SANS Alumni and Instructors in a vibrant atmosphere. This is more than an event; it's an immersive experience that fuels your passion for cybersecurity and fosters invaluable connections.

FEATURED KEYNOTE

Cybersecurity Insights: *An Interactive Fireside Chat with USCYBERCOM's Morgan M. Adamski and Rob Lee*

Friday, December 13 | 6:30–7:30 PM
LOCATION: **Int'l Ballroom Center** (CONCOURSE LEVEL)
SPEAKERS: **Morgan M. Adamski, Executive Director, U.S. Cyber Command and Rob Lee, SANS Fellow and Chief of Research**

Morgan Adamski will share USCYBERCOM's strategic priorities, upcoming initiatives, and the evolving cyber threat landscape. Topics will include enhancing defensive capabilities, leveraging emerging technologies like AI and quantum computing, and strengthening public-private partnerships.

Attendees will have the opportunity to participate in live polls, offering their perspectives on key cybersecurity challenges and priorities. We will gather questions from all participants and facilitate an upvoting process to highlight the most pressing topics. This ensures that the discussion addresses the areas you care about most, from workforce development and diversity in cybersecurity teams to international cooperation and cyber resilience strategies.

Rob Lee will provide his expertise on integrating cutting-edge research and curriculum development to support the cybersecurity workforce, complementing Morgan Adamski's operational insights.

BONUS SESSIONS

SANS@NIGHT

Breaking the Kubernetes Kill Chain: Host Path Mount

Sunday, December 15 | 6:45–7:45 PM

LOCATION: **Columbia 5** (TERRACE LEVEL)

SPEAKERS: **Eric Johnson, SANS Senior Instructor and Ryan Thompson, SANS Certified Instructor**

Microsoft's Threat Matrix for Kubernetes helps organizations understand the attack surface a Kubernetes deployment introduces to their environments. This ensures that adequate detections and mitigations are in place. By covering over 40 different attacker techniques, defenders can learn about Kubernetes-specific mitigations and controls to deploy to their environments.

In this session, we will explore the MS-TA9013 Host Path Mount technique, which is commonly used by attackers to perform privilege escalation in a Kubernetes cluster. Attendees will learn how attackers and defenders can:

- Escape the container's host volume mount to gain persistence on an underlying node
- Move laterally from the underlying node into the customer's cloud environment
- Analyze Kubernetes audit logs to detect pods deployed with a hostPath mount
- Deploy an admission controller that prevents new pods from using a hostPath mount

SANS@NIGHT

AI & Cybersecurity: 2024 Review and Strategic Insights for 2025

Sunday, December 15 | 7:45–8:45 PM

LOCATION: **Columbia 6** (TERRACE LEVEL)

SPEAKER: **Seth Misenar, SANS Fellow**

As 2024 draws to a close, join SANS Fellow Seth Misenar for an in-depth review of the year's pivotal milestones and challenges in AI and cybersecurity. From groundbreaking advancements to significant setbacks, this session will explore the rapid evolution of AI technologies since the debut of OpenAI's ChatGPT barely two years ago. How have these technologies already reshaped the cybersecurity landscape? What unexpected vulnerabilities have emerged, and what lessons can we draw as we prepare for 2025?

We will dive into key areas such as the integration of AI-driven automation in cyber defense, the challenges of ethical and responsible AI practices, and the evolving threat landscape of AI-enabled adversaries. Beyond overzealous hype and entrenched skepticism, this presentation will critically assess where AI is headed and what it means for cybersecurity professionals. Expect to leave with strategic insights that will help you navigate the complex and rapidly changing intersection of AI and cybersecurity in the coming year.

SPECIAL EVENT

SANS CDI 2024 Relaxation Lounge

Monday, December 16 | 7:00 AM–1:00 PM

LOCATION: **Coats – International Terrace** (TERRACE LEVEL)

7:00–8:00 AM	Rise and shine—All levels flow
8:00–9:00 AM	Scents and sounds lounge—Sound bath and aromatherapy (please stop in at any time during this segment)
10:35–10:45 AM	Mid-morning inscape—Meditational yoga nidra practice
12:15–12:30 PM	Cyber-strong plank-off
12:40–1:10 PM	Seated serenity chair yoga

NOTE: Please stop by our Relaxation Lounge at any time between sessions to enjoy some peace and quiet or to just escape from the day.

BONUS SESSIONS

RECEPTION

Women's Connect Reception

Monday, December 16 | 5:30–7:00 PM

LOCATION: **Columbia Foyer** (TERRACE LEVEL)

SANS Institute's Women's Connect community is happy to host a networking reception at SANS CDI 2024 to foster interaction and career advancement for women throughout cybersecurity and beyond. Please join us to build your network of women in the industry and celebrate the mission of SANS to foster diversity in cybersecurity.

CYBER RANGES

Core NetWars Tournament

Monday, December 16 | 6:30–9:30 PM

LOCATION: **Int'l 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 Core NetWars tournament throughout the year are offered a chance to compete in the annual SANS Core NetWars Tournament of Champions.

SANS@NIGHT

Cybersecurity at the Crossroads: Trends, Challenges, and Leadership Solutions

Monday, December 16 | 7:15–8:15 PM

LOCATION: **Columbia 5** (TERRACE LEVEL)

SPEAKER: **My-Ngoc Nguyen, SANS Principal Instructor**

In an era where digital transformation drives business success, cybersecurity has emerged as a critical aspect for organizational leadership. As cyber threats grow in sophistication, understanding the latest trends and challenges is no longer optional—it's essential. This presentation offers a deep dive into the latest and evolving cybersecurity landscape, uncovering the most pressing areas that leaders must address today. We'll explore cutting-edge trends, from the rise of AI-driven attacks to the complexities of securing remote workforces, and present actionable strategies for mitigating and managing risks. Join us to learn how effective leadership can address cybersecurity challenges.

CYBER RANGES

Core NetWars Tournament

Tuesday, December 17 | 6:30–9:30 PM

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

SANS@NIGHT

Back to Basics: The Indispensable Role of Cybersecurity Fundamentals in a Complex World

Tuesday, December 17 | 7:15–8:15 PM

LOCATION: **Columbia 5** (TERRACE LEVEL)

SPEAKER: **Rich Greene, SANS Certified Instructor Candidate**

In today's fast-paced digital landscape, it's easy to be swept up in the allure of cutting-edge technologies and advanced security measures. However, amidst the rush towards innovation, the core principles of cybersecurity—the fundamentals—often get overlooked. In this engaging talk, Rich Greene, will explore why these foundational elements are more critical than ever. Drawing on real-world examples and personal experiences, Rich will illustrate how neglecting the basics can lead to significant vulnerabilities and how a solid grasp of these principles can fortify an organization's defense strategy. Attendees will leave with a renewed appreciation for the essential building blocks of cybersecurity and practical insights on how to integrate these fundamentals into their security practices.

Share Your Experience with SANS Social Reporter, Rich Greene

What are you most looking forward to from your experience at SANS Cyber Defense Initiative 2024?

We want to hear about it. Share your story and inspire others! By recounting your journey, you encourage fellow cybersecurity professionals to embark on their own learning paths. Don't miss this chance to shine a spotlight on your success and make your voice heard in the cybersecurity community. Stop by the SANS Social Reporter step and repeat location on the Terrace Level to share and make an impact!

SANS Refer-A-Friend – Your Exclusive Alumni Opportunity!

Unlock the power of networking with ***SANS Refer-A-Friend!*** As a valued SANS Alumni, we're offering SANS Cyber Defense Initiative 2024 In-Person students the exclusive opportunity to pass education savings onto a fellow colleague and join us at **SANS Security East™ Baltimore 2025**.

When you refer a friend, ***they will receive $2,500 off their course fee***, and you will too! SANS Faculty will distribute these vouchers in class on Day 4 of the event, so get ready to help your friends and colleagues take a step forward in their cybersecurity career.

Prepare Your Executive Team

SANS Executive Cyber Exercises guide your leadership team through a simulated crisis.

Industry experts test the security of your plan while coaching your stakeholders on best practices for crisis response.

- Assess organizational readiness at the Board level for response
- Pressure-test your documented crisis management plan
- Apply industry-best practices in cybersecurity, organizational structure, and crisis communications
- Understand and plan for emerging trends in cybercrime

sans.org/ece

SANS | EXECUTIVE CYBER EXERCISES
PREPARE | PRACTICE | PREVAIL

Elevate Your Defense Strategies at

SANS 2025™

April 13–18 | Orlando, FL or Virtual

Enhance your skillsets with serious cybersecurity training. Register now and fortify your defenses against tomorrow's threats – today!

SAVE $500
WHEN YOU REGISTER BY JANUARY 13

Seize this exclusive opportunity to save while securing your spot at this premier event.

www.sans.org/sans-2025

SAVE THE DATE

SANS Cyber Defense Initiative™ 2025 is returning to Washington Hilton
December 12–17, 2025

Upcoming SANS Training Events

Nashville Winter	Nashville, TN	Hybrid	Jan 13–18
Stay Sharp: Jan		Virtual (ET)	Jan 21–23
Cyber Security East: Jan		Virtual (ET)	Jan 27–Feb 1
San Francisco Winter	San Francisco, CA	Hybrid	Jan 27–Feb 1
Cyber Security Central: Feb		Virtual (CT)	Feb 3–8
Security Leadership DC Metro	Tysons Corner, VA	Hybrid	Feb 10–15
New Orleans	New Orleans, LA	Hybrid	Feb 17–22
San Diego Winter	San Diego, CA	Hybrid	Feb 24–Mar 1
Security East™ Baltimore	Baltimore, MD	Hybrid	Mar 3–8
San Antonio Spring	San Antonio, TX	Hybrid	Mar 17–22
DFIR Dallas	Dallas, TX	Hybrid	Mar 24–29
Cyber Security Mountain: Mar		Virtual (MT)	Mar 31–Apr 5
SANS 2025™	Orlando, FL	Hybrid	Apr 13–18
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
Security Leadership Nashville	Nashville, TN	Hybrid	May 19–23
Cyber Defense Miami	Coral Gables, FL	Hybrid	Jun 9–14
Rocky Mountain	Denver, CO	Hybrid	Jun 23–28
SANSFIRE™	Washington, DC	Hybrid	Jul 14–19
San Antonio	San Antonio, TX	Hybrid	Aug 4–9