SANS | GIAC CERTIFICATIONS

SANS Cyber Defense Initiative® 2023

Washington, DC | December 11–16

PROGRAM GUIDE

#SANSCDI @SANSInstitute

TABLE OF CONTENTS

CYBER DEFENSE INITIATIVE 2023

Welcome Reception

Monday, December 11 | 7:00–8:30 PM
Location: International Terrace Foyer (TERRACE LEVEL)

Kick off your Cyber Defense Initiative 2023 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.

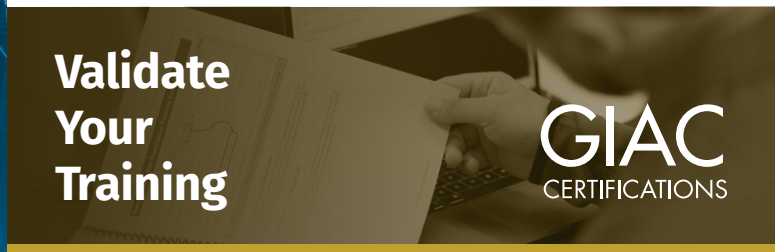
Add an OnDemand Bundle to your course.

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: $949

sans.org/ondemand/bundles



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: $949

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, December 10 . . . . . 4:00–6:00 PM
Monday, December 11 . . . . . 7:00–8:30 AM

Registration Support

Location: International Terrace (TERRACE LEVEL)

Mon, December 11 . . . . . 8:00 AM–5:30 PM

Location: Albright Room (TERRACE LEVEL)

Tue, December 12–Fri, December 15 . . . . . 8:00 AM–5:30 PM
Sat, December 16 . . . . . 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.

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 2023 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 8 (TERRACE LEVEL)

FOR508: Advanced Incident Response, Threat Hunting & Digital Forensics (6-DAY COURSE)
Chad Tilbury . . . . . Lincoln West (CONCOURSE LEVEL)

FOR509: Enterprise Cloud Forensics & Incident Response (6-DAY COURSE)
Terrence Williams. . . . . .Columbia Hall 12 (TERRACE LEVEL)

FOR578: Cyber Threat Intelligence (6-DAY COURSE)
Robert M. Lee &
Andreas Sfakianakis. . . . . .Columbia Hall 7 (TERRACE LEVEL)

FOR585: Smartphone Forensic Analysis In-Depth (6-DAY COURSE)
Heather Mahalik. . . . . Georgetown East (CONCOURSE LEVEL)

FOR608: Enterprise-Class Incident Response & Threat Hunting (6-DAY COURSE)
Tarot Wake. . . . . Piscataway (LOBBY LEVEL)

FOR610: Reverse-Engineering Malware: Malware Analysis Tools & Techniques (6-DAY COURSE)
Lenny Zeltser. . . . . Gunston East (TERRACE LEVEL)

ICS410: ICS/SCADA Security Essentials (6-DAY COURSE)
Justin Searle &
Paul Piotrowski. . . . . Int'l Ballroom West (CONCOURSE LEVEL)

ICS515: ICS Visibility, Detection, and Response (6-DAY COURSE)
Mark Bristow. . . . . Fairchild West (TERRACE LEVEL)

LDR414: SANS Training Program for CISSP® Certification (6-DAY COURSE)
Seth Misenar. . . . . .Morgan (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)

MGT512: Security Leadership Essentials for Managers (5-DAY COURSE)
My-Ngoc Nguyen . . . . . Int'l Ballroom East (CONCOURSE LEVEL)

MGT514: Security Strategic Planning, Policy & Leadership (5-DAY COURSE)
Frank Kim. . . . . .Lincoln East (CONCOURSE LEVEL)

SEC301: Introduction to Cyber Security (5-DAY COURSE)
Doc Blackburn. . . . . Gunston West (TERRACE LEVEL)

SEC401: Security Essentials: Network, Endpoint & Cloud (6-DAY COURSE)
Ross Bergman. . . . . .Georgetown West (CONCOURSE 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)
Ryan Nicholson. . . . . Jefferson East (CONCOURSE LEVEL)

SEC497: Practical Open-Source Intelligence (OSINT) (6-DAY COURSE)
Matt Edmondson . . . . . Kalorama (LOBBY LEVEL)

SEC503: Network Monitoring & Threat Detection In-Depth (6-DAY COURSE)
Andrew Laman. . . . . Columbia Hall 4 (TERRACE 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)
Mick Douglas . . . . . Columbia Hall 5 (TERRACE LEVEL)
Hours: 8:30 AM–7:15 PM (Day 1)

SEC510: Public Cloud Security: AWS, Azure, and GCP (5-DAY COURSE)
Brandon Evans . . . . . .Columbia Hall 11 (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 2 (TERRACE LEVEL)

SEC530: Defensible Security Architecture & Engineering: Implementing Zero Trust for the Hybrid Enterprise (6-DAY COURSE)
Eric Conrad. . . . . Columbia Hall 3 (TERRACE LEVEL)

SEC540: Cloud Security & DevSecOps Automation (5-DAY COURSE)
David Hazar . . . . . .Holmead East (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)
Shaun McCullough . . . . . .Fairchild East (TERRACE LEVEL)

SEC542: Web App Penetration Testing & Ethical Hacking (6-DAY COURSE)
Aaron Cure . . . . . Columbia Hall 6 (TERRACE LEVEL)

SEC549: Enterprise Cloud Security Architecture (5-DAY COURSE)
Eric Johnson. . . . . Jay (LOBBY LEVEL)

SEC560: Enterprise Penetration Testing (6-DAY COURSE)
Jeff McJunkin. . . . . Columbia Hall 1 (TERRACE LEVEL)

SEC565: Red Team Operations & Adversary Emulation (6-DAY COURSE)
Jean-Francois Maes . . . . . .Oak Lawn (LOBBY LEVEL)

SEC566: Implementing & Auditing CIS Controls (5-DAY COURSE)
Brian Ventura. . . . . Northwest (LOBBY LEVEL)

SEC573: Automating Information Security with Python (6-DAY COURSE)
Mark Baggett . . . . . Columbia Hall 9 (TERRACE LEVEL)

SEC588: Cloud Penetration Testing (6-DAY COURSE)
Moses Frost . . . . . Holmead West (LOBBY LEVEL)

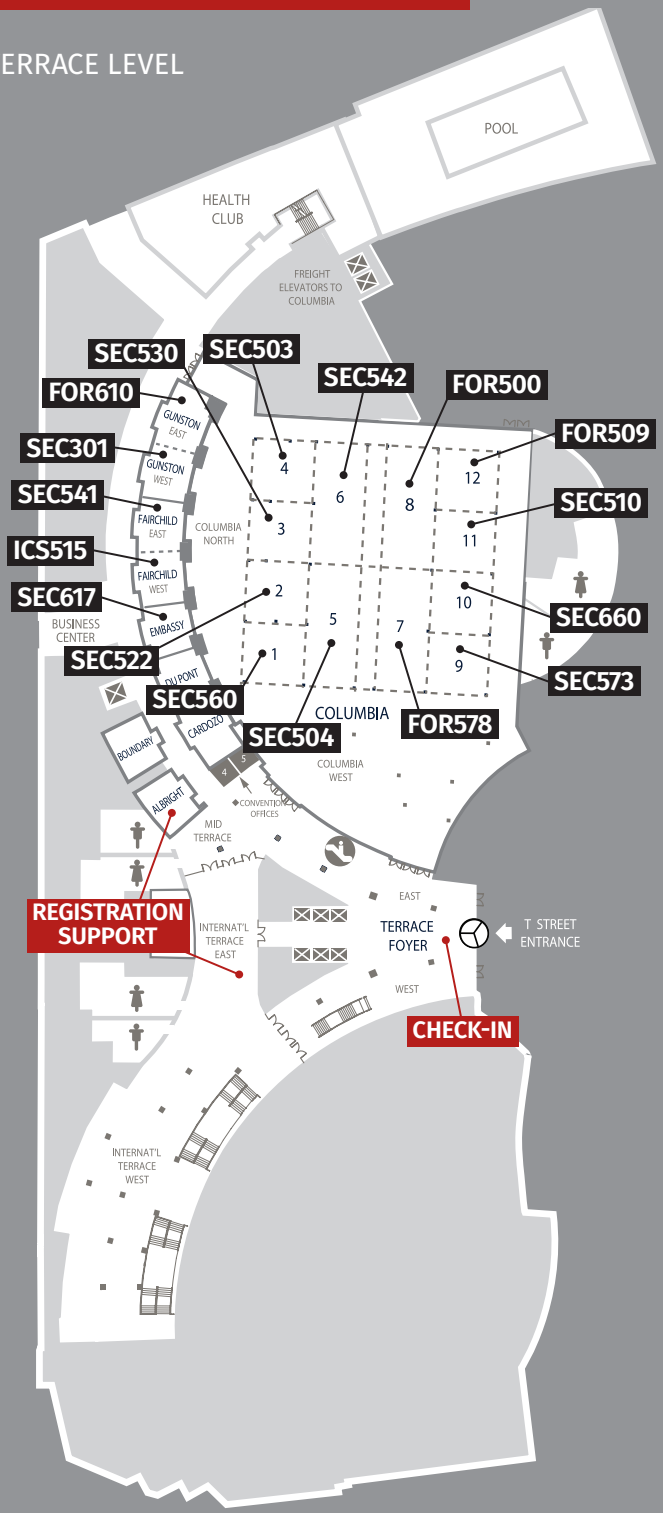
SEC595: Applied Data Science & AI/Machine Learning for Cybersecurity Professionals (6-DAY COURSE)
David Hoelzer . . . . . .Jefferson West (CONCOURSE LEVEL)

SEC617: Wireless Penetration Testing & Ethical Hacking (6-DAY COURSE)
Larry Pesce. . . . . Embassy (TERRACE LEVEL)

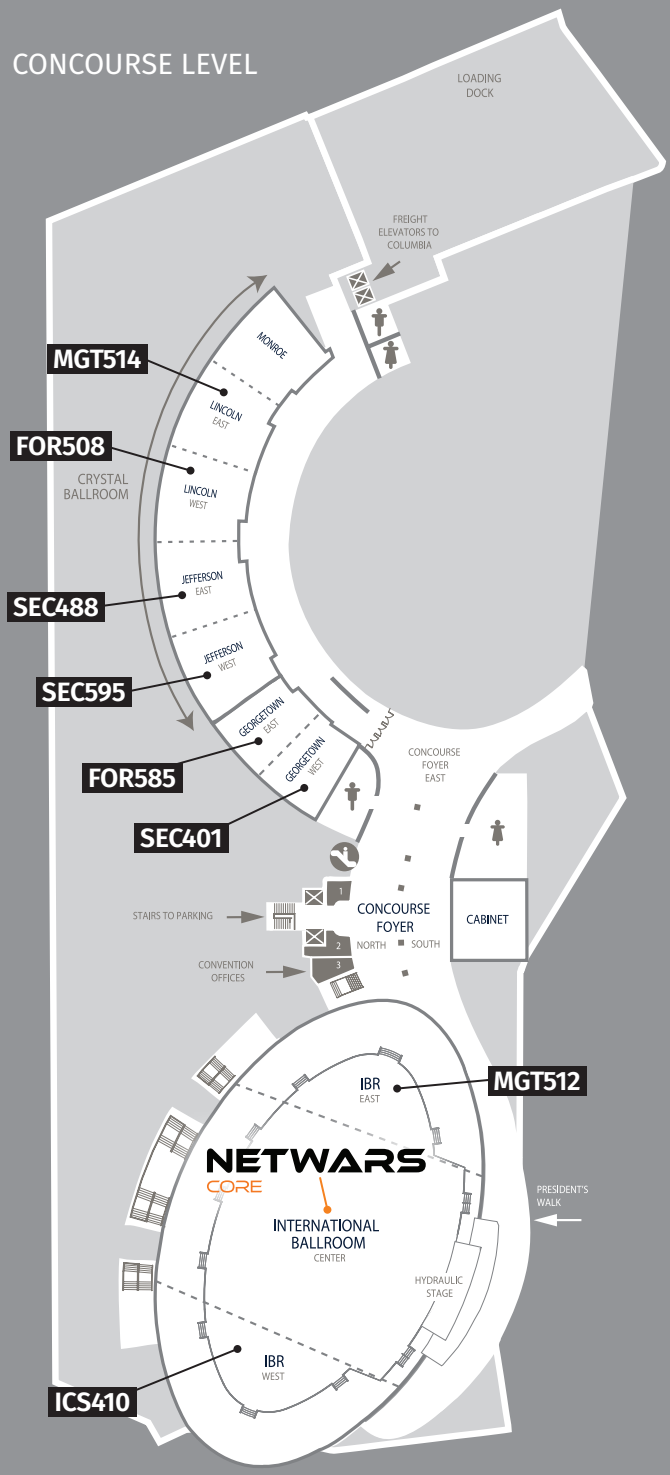
SEC660: Advanced Penetration Testing, Exploit Writing & Ethical Hacking (6-DAY COURSE)
Stephen Sims. . . . . Columbia Hall 10 (TERRACE LEVEL)
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–5)

HOTEL FLOOR PLAN

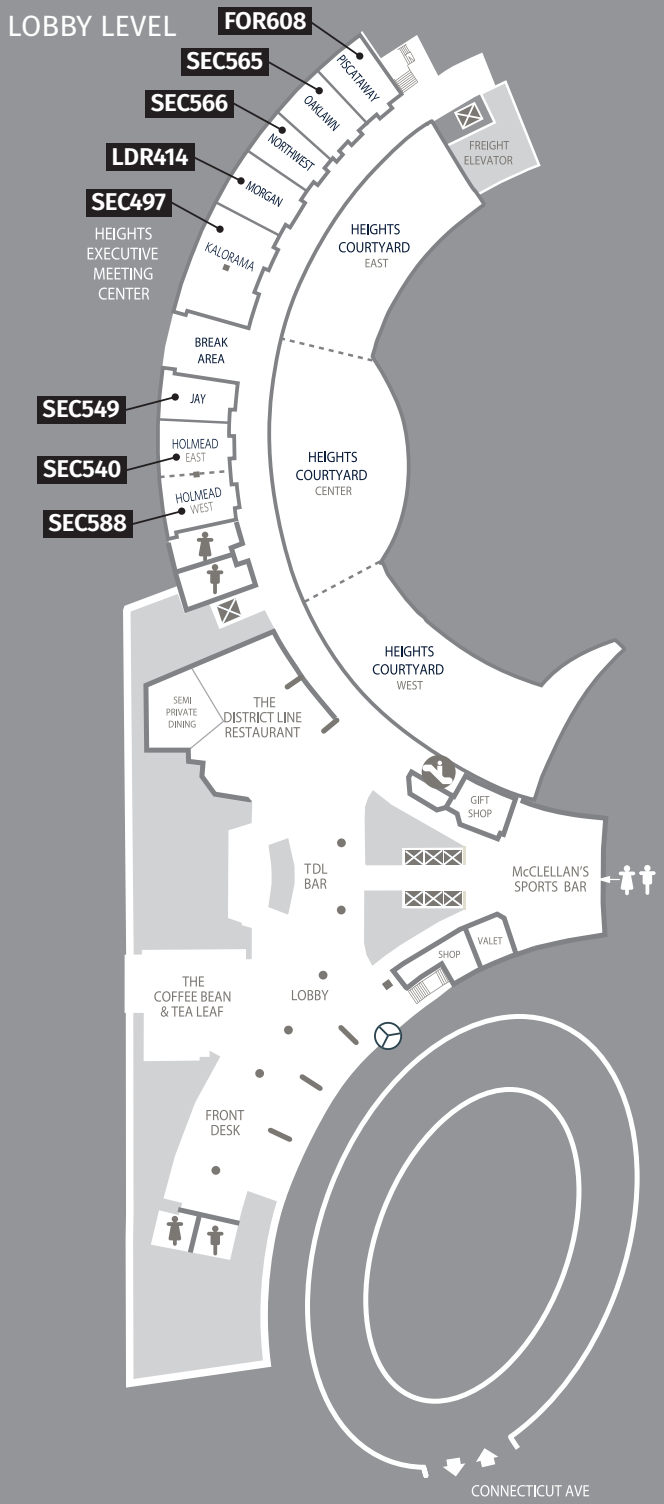
TERRACE LEVEL



CONCOURSE LEVEL



HOTEL FLOOR PLAN



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.

CYBER DEFENSE INITIATIVE 2023

Welcome Reception

Monday, December 11 | 7:00–8:30 PM
Location: International Terrace Foyer (TERRACE LEVEL)

Kick off your Cyber Defense Initiative 2023 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.

SANS@NIGHT

Security for Generative AI 101

Speaker: Frank Kim, SANS Faculty Fellow
Tuesday, December 12 | 6:00–7:00 PM
Location: International Ballroom East (CONCOURSE LEVEL)

Artificial Intelligence, Large Language Models (LLMs), Generative AI (GenAI), and transformers have made headlines since ChatGPT was released at the end of 2022. Now every security organization is considering how GenAI will impact their customers and business. As a result, security professionals have to understand how these technologies work and, importantly, how to use them securely. Come learn what is being done to secure the 1) usage of GenAI; 2) development of AI models; and 3) integration of GenAI functionality into business applications.

SANS@NIGHT

Leveraging AI: A Tutorial

Speaker: David Hoelzer, SANS Faculty Fellow
Tuesday, December 12 | 7:15–8:45 PM
Location: International Ballroom East (CONCOURSE LEVEL)

ChatGPT, GPT-4, Llama 2, Bard, Minerva, Megatron, Claude, Chinchilla... What exactly are these "Large Language Models" that are in the news? What are they really good for? How do they work? What are the risks when we incorporate these into our business process?

This 90-minute presentation and tutorial will explain how these models work, what transformers are, how embeddings work, and how to build a question answering AI—the easy way and the hard way—in addition to discussing the very real risks that come into play when we try to integrate these systems into a business process!

BONUS SESSIONS

SANS@NIGHT

Cracking the Code: The Role of Programming in Information Security

Speaker: Mark Baggett, SANS Senior Instructor
Wednesday, December 13 | 6:00–7:00 PM
Location: Jefferson West (TERRACE LEVEL)

In this presentation, we'll explore an unpatched vulnerability within Windows, one that attackers can likely exploit to bypass your defenses. Through the lens of this attack, we'll address a significant question: "Are programming skills a requisite for excelling in the field of information security?"

Recent research indicates that approximately 20% of entry-level positions in information security demand proficiency in programming. Yet, the ongoing debate in online forums highlights the uncertainty surrounding the necessity of coding skills. Join me as we navigate through this discussion, examining the intricate relationship between coding expertise and achieving success in the realm of information security.

SPECIAL EVENT

Hands-On Workshop: Phishing and App Consent

Hosted by: Moses Frost, SANS Senior Instructor
Wednesday, December 13 | 6:45–8:45 PM
Location: Columbia Hall 6 (TERRACE LEVEL)

Phishing is a common attack path for attackers. Phishing users is one of the predominant attacks that are still highly effective today. It relies on the ability of end users to make quick and rash decisions. It also relies on users being unable to determine a real email from a legitimate source from one that is illegitimate. Understanding how to mount a phishing campaign is a key item many penetration testers should learn how to do.

In this workshop, we will cover how you can model what an App Consent attack looks like, how it operates, and how you, as the attacker, can abuse it. Are you a manager, director, or nontechnical people manager? This workshop is still for you!

This workshop will also help guide you with building preventative measures to protect your users. This is *THE* workshop to take if you want to simulate App Consent attacks. This is a sneak preview directly from the updated SEC588: Cloud Penetration Testing, so even if you have taken the course and want to see some additional material in the new versions, you'll want to attend.

SPECIAL EVENT

Hands-On Workshop: Cyber42 – Operational Leader

Hosted by: Brian Ventura, SANS Certified Instructor
Wednesday, December 13 | 6:45–8:45 PM
Location: Columbia Hall 5 (TERRACE LEVEL)

Practice your skills in an engaging, team-based environment to improve your operational cybersecurity decision-making proficiency. Cyber42 is a realistic leadership simulation with applicable and discussion-based outcomes. Continue to develop key skills needed in all operational security leaders: nimble decision making and information synthesis.

As cyber-attacks become more common and more expensive, many organizations are making a foundational shift to view operations from the point of view of an adversary in order to protect their most sensitive information. Despite vulnerability tools and programs being available for several decades, breaches still happen regularly from known vulnerabilities. Complicating the matter more are a wide range of modern technologies requiring more time and knowledge to manage, more known vulnerabilities than ever before, an unprecedented migration to cloud, and ever-increasing legal and regulatory compliance standards. Information assurance engineers, auditors, SOC analysts, and cybersecurity managers need more to better defend an organization's data systems.

Cyber42 is a leadership simulation game that puts you in the driver's seat of making tough executive calls on behalf a fictitious organization that needs your expertise. Each outcome will be followed by thoughtfully crafted group discussion. The winning team will be decided by who makes the strongest security cultural impact to the fictitious organization.

This version of the game supports concepts from the following three cybersecurity leadership training courses that comprise the Operational Cybersecurity Executive Triad:

- **LDR516: Building and Leading Vulnerability Management Programs**
- **LDR551: Building and Leading Security Operations Centers**
- **SEC566: Implementing and Auditing Security Frameworks and Controls**

BONUS SESSIONS

SANS@NIGHT

The Industrial (ICS/OT) Cyber Threat Landscape

Speaker: Robert M. Lee, SANS Faculty Fellow
Thursday, December 14 | 7:15–8:45 PM
Location: Columbia Hall 5 (TERRACE LEVEL)

This talk will give an introduction to ICS/OT followed by an in-depth discussion on the changes that are taking place in the industrial world such as digital transformation as a precursor to an in-depth discussion on the threats. The talk will cover new adversary groups targeting industrial networks, the trends to watch, and make recommendations with a walkthrough of the SANS ICS five critical controls.

This talk is accessible to everyone of any background.

LUNCH AND LEARN

DoD CIO Cyber Workforce Session

Speaker: Mark S. Gorak, Principal Director for Resources & Analysis, DoD Office of the Chief Information Officer
Friday, December 15 | 12:30–1:15 PM
Location: International Ballroom East (CONCOURSE LEVEL)

This event, open to active U.S. Military and Federal Contractors, will be presented by Mark S. Gorak, Principal Director for Resources & Analysis of the DoD Office of the Chief Information Officer. The Office of the DoD CIO recently published two critical initiatives: the 2023-2027 DoD Cyber Workforce Strategy and DoD Manual 8140.03. The strategy establishes the direction for unified management of the cyber workforce and outlines a roadmap for its advancement while DoDM 8140 changes the way that we qualify our workforce. Through the DoD 8140 Cyber Workforce Qualification Program, DoD is expanding the qualification program to roughly 225,000 military, civilian, and contractor positions by establishing foundational and residential qualification criteria for each DoD Cyber Workforce Framework work role. Together, the strategy and program will enable the DoD to develop and deploy an agile, capable, and ready cyber workforce.

This presentation is only for Federal Military and Federal Contractors working for the U.S. Military.

SANS@NIGHT

Developers, Developers, Developers: Three Ways (and More) How Developers are Being Targeted by Attackers

Speaker: Dr. Johannes Ullrich, SANS Faculty Fellow
Friday, December 15 | 7:15–8:15 PM
Location: Columbia Hall 5 (TERRACE LEVEL)

Everybody is talking about supply chain security. But supply chains are more than parts, libraries, and APIs. They include people, and developers, to duct tape the parts into something that vaguely resembles functioning software. While developers often hide in their cubicles or home offices to seek safety in the shadows of large monitors, attackers have found them. They found them in IDA plugin stores, software package repositories, Stackoverflow, and in online gaming communities (even during work hours). Network defenders on the other hand have often ignored developers, not just because they are "weird", but because standard security solutions often interfere with their work and cause them to complain loudly. In this talk, you will learn about some of these attacks, and how to defend against them, and you will also learn some bad jokes about developers.

SANS

CYBER RANGES

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

NETWARS CORE

Thursday, December 14 & Friday, December 15
6:30–9:30 PM
International Ballroom Center (CONCOURSE LEVEL)

> **NetWars takes the concepts in the class and gives you an opportunity to put them into action. Highly recommended!**
>
> —Kyle McDaniel, **Lenovo**

All In-Person students who registered to attend a course at SANS Cyber Defense Initiative 2023 are eligible to play CORE NetWars for FREE.

Space is limited. Please register for NetWars through your SANS Account Dashboard.

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
Network Security 2024

September 4–9 | Las Vegas, NV or Virtual

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

LIMITED TIME EARLY BIRD OFFER:
SAVE $750!

Use code "**EarlyBird23**" when registering for any 4–6 day course by **December 9, 2023**.

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

www.sans.org/ns24

SAVE THE DATE

SANS Cyber Defense Initiative® 2024

Returning to Washington Hilton

December 13–18, 2024

Upcoming SANS Training Events

Cloud Defender	VIRTUAL (ET)	Jan 8–13
SANS Classic	VIRTUAL (ET)	Jan 15–20
Cyber Security Mountain: January	VIRTUAL (MT)	Jan 22–27
Tysons Corner – NOVA Tysons Corner, VA	HYBRID	Feb 5–10
San Diego San Diego, CA	HYBRID	Feb 12–17
Security East New Orleans, LA	HYBRID	Feb 19–24
Las Vegas Las Vegas, NV	HYBRID	Mar 4–9
Dallas Dallas, TX	HYBRID	Mar 11–16
Stay Sharp: March	VIRTUAL (ET)	Mar 18–20
SANS 2024 Orlando, FL	HYBRID	Mar 24–29
New York City Spring New York, NY	HYBRID	Apr 8–13
Santa Clara Santa Clara, CA	HYBRID	Apr 8–13
Pen Test Austin Austin, TX	HYBRID	Apr 22–27
Baltimore Spring Baltimore, MD	HYBRID	Apr 28–May 3
Security West San Diego, CA	HYBRID	May 9–14
Leadership & Cloud Security Arlington, VA	HYBRID	May 20–24
Stay Sharp: May	VIRTUAL (ET)	May 29–31
Rocky Mountain Summer Denver, CO	HYBRID	Jun 17–22
SANSFIRE Washington, DC,	HYBRID	Jul 15–20