Network Security 2022
September 7–12 | Las Vegas, NV

Program Guide

@SANSInstitute
#SANSNetworkSecurity
Keynote Welcome Reception

Thursday, September 8 | 5:30–6:30 PM
Location: Roman/Florentine Foyer

Kick off your SANS Network Security 2022 experience at the Keynote Welcome Reception before settling in for Justin Searle’s keynote. 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 Las Vegas, NV.

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: $849**
sans.org/ondemand/bundles

Validate Your Training

Add a GIAC Certification attempt to your course before September 8.

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
- Save over $1,100 when added to your SANS training

**GIAC Certifications Bundle price: $949**
giac.org
GENERAL INFORMATION

Venue
Caesars Palace
3570 Las Vegas Blvd South | Las Vegas, NV 89109
Phone: 1-866-227-5938

Event Check-In | Badge & Courseware Distribution
Location: Promenade Foyer
Tuesday, September 6 ......................... 4:00–6:00 PM
Wednesday, September 7 ................. 7:00–8:30 AM

Registration Support
Location: Office 3
Wednesday, September 7 ................. 8:30 AM–5:30 PM
Location: Siena
Thursday, Sept 8–Sunday, Sept 11 .......... 8:00 AM–5:30 PM
Monday, September 12 ...................... 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
*Snick and coffee to be provided during these break times.

Parking
Self-parking is available for $18 per day Monday–Thursday, and $23 per day Friday–Sunday. There are no in-and-out privileges.
Hotel guests receive a daily parking rate of $18 per day with in-and-out privileges.

Photography Notice
SANS may take photos of classroom activities for marketing purposes. Network Security 2022 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)
SEC503: Intrusion Detection In-Depth
SEC511: Continuous Monitoring and Security Operations
SEC540: Cloud Security and DevSecOps Automation
SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
MGT414: SANS Training Program for CISSP® Certification

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 (Wed, September 7)

**FOR500:** Windows Forensic Analysis  
Lodrina Cherne .............................................. Neopolitan I

**FOR508:** Advanced Incident Response, Threat Hunting, and Digital Forensics  
Chad Tilbury .................................................. Neopolitan II

**FOR509:** Enterprise Cloud Forensics and Incident Response  
Terrence Williams ....................................... Anzio

**FOR578:** Cyber Threat Intelligence  
Kevin Holvoet ............................................. Neopolitan III

**FOR585:** Smartphone Forensic Analysis In-Depth  
Mattia Epifani ............................................. Milano VI

**FOR608:** Enterprise-Class Incident Response & Threat Hunting  
Mike Pilkington ........................................... Milano II

**FOR610:** Reverse-Engineering Malware: Malware Analysis Tools and Techniques  
Michael Murr ............................................... Milano III

**ICS410:** ICS/SCADA Security Essentials  
Justin Searle ............................................... Milano IV

**ICS515:** ICS Visibility, Detection, and Response  
Dean Parsons ............................................... Sorrento

**ICS612:** ICS Cybersecurity In-Depth  
Jeffrey Shearer ............................................. Milano I

**LEG523:** Law of Data Security and Investigations  
Benjamin Wright ......... Florentine IV

**MGT414:** SANS Training Program for CISSP® Certification  
Seth Misenar ................................................. Milano VIII  
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  
My-Ngoc Nguyen ............................................ Florentine II

**MGT514:** Security Strategic Planning, Policy, and Leadership  
Mark Williams .............................................. Florentine III

**SEC301:** Introduction to Cyber Security  
Doc Blackburn ............................................... Roman I

**SEC401:** Security Essentials: Network, Endpoint, and Cloud  
Bryan Simon ................................................ Milano VII  
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–5)

**SEC487:** Open-Source Intelligence (OSINT) Gathering and Analysis  
Matt Edmondson ............................................. Milano V

**SEC503:** Intrusion Detection In-Depth  
Andrew Laman .............................................. Modena  
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–5)

**SEC504:** Hacker Tools, Techniques, and Incident Handling  
Kevin Fiscus ............................................... Roman II  
Hours: 8:30 AM–7:15 PM (Day 1)

**SEC511:** Continuous Monitoring and Security Operations  
Maxim Deweerdt .......................................... Salerno  
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  
Ismael Valenzuela ......................................... Roman III

**SEC540:** Cloud Security and DevOps Automation  
David Hazar ............................................... Capri  
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–4)

**SEC541:** Cloud Security Attacker Techniques, Monitoring, and Threat Detection  
Shaun McCullough ........................................ Florentine I

**SEC560:** Enterprise Penetration Testing  
Jeff McJunkin .............................................. Roman IV

**SEC573:** Automating Information Security with Python  
Mark Baggett ............................................... Livorno

**SEC595:** Applied Data Science and Machine Learning for Cybersecurity Professionals  
David Hoelzer ............................................. Messina

**SEC599:** Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses  
Erik Van Buggenhout ..................................... Neopolitan IV

**SEC660:** Advanced Penetration Testing, Exploit Writing, and Ethical Hacking  
Stephen Sims .............................................. Palermo  
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–5)
Enrich Your SANS Experience!

Evening 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 Tips & Tricks
Wednesday, September 7 | 12:30–1:15 PM | Roman IV
GIAC Certifications is the leading provider and developer of Information Security Certifications. GIAC tests and validates the ability of practitioners in cyber defense, pen testing, forensics, software security, management, and ICS. GIAC certification holders are recognized as experts in the IT industry and are sought after globally by government, military, and industry to protect the cyber environment. Join us for an informational presentation along with a Q and A session. We’ll cover everything from why you should get certified, what testing looks like, how to keep certifications current and more. GIAC Certifications staff will be present to answer your questions before and after the presentation.

SPECIAL EVENT
Keynote Welcome Reception
Thursday, September 8 | 5:30–6:30 PM | Roman/Florentine Foyer
Kick off your SANS Network Security 2022 experience at the Keynote Welcome Reception before settling in for Justin Searle’s keynote. 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 Las Vegas, NV.

KEYNOTE
Scanning Highly Sensitive Networks
Justin Searle, SANS Senior Instructor
Thursday, September 8
6:30–8:00 PM | Roman III
Regardless of the industry you work in, all large companies have at least a few network segments that are highly sensitive to network probes and scans. Most of the time these are due to legacy systems, especially when those legacy systems are embedded devices not running Windows or Linux. This keynote session will explore the most common issues that cause legacy systems to crash/hang and provide a range of recommendations to configure your scanning tools to match the risks of each network you need to scan. These techniques have been developed in production SCADA/ICS networks where potential risks could include loss of employee life and limb, and where the utmost care must be taken.

SANS@NIGHT
Birds of a Feather: Open Mic Night
Friday, September 9 | 7:00–9:00 PM | Pisa
Join us for a bit of fun and music! Let’s gather Friday evening for some instrument playing and karaoke style singalongs! It will be a laid back, no pressure get-together with fellow students and some SANS faculty and staff. Be prepared to join us and sing along to classics like American Pie and Country Roads! If you are so inclined, bring your own instrument!

SANS@NIGHT
Active ICS Cyber Defense: Colonel Mustard...
Candlestick...Kitchen
Speaker: Dean Parsons, Certified Instructor
Friday, September 9 | 7:15–8:15 PM | Roman III
The presentation draws attention to practical threat detection and incident response from dissecting advanced ICS adversary threat capabilities, tactics techniques and procedures. Dean will illustrate why the cyber weapons and the techniques may be more important than adversary attribution for tactical ICS incident response. And why ICS-aware Network Security Monitoring can be applied as a focus in ICS/OT environments for the win!

SANS@NIGHT
The Architecture of Security in AWS
Speaker: Shaun McCullough, Certified Instructor Candidate
Friday, September 9 | 8:15–9:15 PM | Roman III
Come join Shaun McCullough as we all play the role of a security architect hired to design (from the ground up), a new platform in AWS. Using the AWS Well-Architected Framework & the AWS Security Maturity Model as a guide, we will look at the most critical security controls we will implement, and how that will drive the new architecture. Some slides, more discussion and as many poorly drawn architecture diagrams as we can fit in an hour.
Develop and practice real-world skills to be prepared to defend your environment.

**SPONSORED EVENTS**

**LUNCH & LEARN (& EARN)**

Receive 1 CPE for each lunchtime bonus session you attend! These lightning-talk lunch sessions provide attendees lunch and feature the leading options in information security. Secure your spot during event check-in!

**PENTERA**

**Changing the Game of Offensive Security**

Janet Rae, Sales Engineer, Pentera  
Wednesday, September 7 | 12:30–1:15 PM | Florentine I

This session will take a deep dive through automated security validation. Organizations over the years have been following a defense in depth model to protect their critical assets. While this strategy makes sense; the tools, processes, and procedures surrounding this initiative have grown significantly. How confident can organizations be that each layer and the enormous effort undertaken is working effectively? We will take the time to walk through how Pentera can validate which risks are present, which mitigative efforts are working efficiently, and how security practitioners of all expertise can leverage Pentera both internally and externally to know with certainty how strong the security posture actually is.

**corelight**

**Network Forensics & Incident Response with Open Source Tools**

Ed Smith, Head of Alliance Partner Marketing, Corelight  
Wednesday, September 7 | 12:30–1:15 PM | Roman III

Open source security technologies such as Zeek, Suricata, and Elastic can deliver powerful network detection and response capabilities and the global communities behind these tools can also serve as a force multiplier for security teams, such as accelerating their response times to zero-day exploits via community-driven detection engineering and intel sharing. This presentation will review popular open source technologies used in network DFIR and cover use cases, integrations, and open source design patterns.

---

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

All students who registered to attend an In-Person course at SANS Network Security 2022 are eligible to play NetWars for FREE.

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

LUNCH & LEARNS (CONTINUED)

THREATLOCKER

Zero Trust for Applications
Danny Jenkins, CEO and Co-Founder, ThreatLocker
Wednesday, September 7 | 12:30–1:15 PM | Florentine III
The Zero Trust framework is based on the principle of “never trust, always verify.” Join us to learn about Zero Trust, how to adopt it for applications, and the technologies you need to take control of your environment in the fight against ransomware.

AXONIUS

Optimizing Security Operations Programs with Asset Intelligence
Sean Blenkhorn, VP of Sales Engineering, Axonius
Friday, September 9 | 12:30–1:15 PM | Roman III
The goal of SecOps teams is to monitor, detect, investigate, and respond to suspicious activity and events. Often, this leaves these teams in a reactive state, with minimal opportunity to reduce false-positives and innovate. One key aspect of innovative, mature SecOps programs? Their ability to gather context from data sources to inform investigations.

Network Security students and faculty are invited to join our featured solution providers for FREE BREAKFAST & LUNCH!

Breakfast Solutions Expo
Thursday, September 8 | 7:30–9:00 AM
Promenade Foyer

Lunch Solutions Expo
& Raffle Drawing
Thursday, September 8 | 12:15–1:30 PM
Promenade Foyer
Raffle Drawing at 1:30 PM
You do NOT have to be present to win!

ENTER TO WIN!

Raffle Drawing at the Lunch Solutions Expo
Thursday, September 8 | 1:30 PM
Promenade Foyer
You do NOT have to be present to win!

Join us for breakfast and lunch on Thursday, September 8 in the Promenade Foyer to pick up and submit your entry form! All entry forms must be submitted by 1:30 PM.

Prizes include:

Five $20 Amazon Gift Cards
Nintendo Switch

Solution Providers Available:
### Upcoming SANS Training Events

<table>
<thead>
<tr>
<th>EVENT</th>
<th>TRAINING FORMAT</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Cybersecurity Leadership Summit &amp; Training</td>
<td>VIRTUAL</td>
<td>Sep 14–24</td>
</tr>
<tr>
<td>SANS Cyber Security Central: Sept</td>
<td>VIRTUAL</td>
<td>Sep 19–24</td>
</tr>
<tr>
<td>SANS Baltimore Fall (Baltimore, MD)</td>
<td>VIRTUAL &amp; IN-PERSON</td>
<td>Sep 26–Oct 1</td>
</tr>
<tr>
<td>SANS Cyber Security Central: Oct</td>
<td>VIRTUAL</td>
<td>Oct 3–8</td>
</tr>
<tr>
<td>Blue Team Summit &amp; Training (Scottsdale, AZ)</td>
<td>VIRTUAL &amp; IN-PERSON</td>
<td>Oct 3–10</td>
</tr>
<tr>
<td>SANS Rocky Mountain Fall (Denver, CO)</td>
<td>VIRTUAL &amp; IN-PERSON</td>
<td>Oct 10–15</td>
</tr>
<tr>
<td>SANS NoVA (McLean, VA)</td>
<td>VIRTUAL &amp; IN-PERSON</td>
<td>Oct 24–29</td>
</tr>
<tr>
<td>SANS Leadership and Cloud Security (Allen, TX)</td>
<td>VIRTUAL &amp; IN-PERSON</td>
<td>Oct 24–29</td>
</tr>
<tr>
<td>SANS Cyber Security East: Nov</td>
<td>VIRTUAL</td>
<td>Nov 7–12</td>
</tr>
<tr>
<td>SANS DFIRCON (Charlotte, NC)</td>
<td>VIRTUAL &amp; IN-PERSON</td>
<td>Nov 14–19</td>
</tr>
<tr>
<td>Pen Test HackFest Summit &amp; Training (Arlington, VA)</td>
<td>VIRTUAL &amp; IN-PERSON</td>
<td>Nov 14–21</td>
</tr>
<tr>
<td>SANS Cyber Security Central: Nov</td>
<td>VIRTUAL</td>
<td>Nov 28–Dec 3</td>
</tr>
<tr>
<td>SANS Stay Sharp: Nov</td>
<td>VIRTUAL</td>
<td>Nov 29–Dec 1</td>
</tr>
<tr>
<td>SANS San Francisco Winter (San Francisco, CA)</td>
<td>VIRTUAL &amp; IN-PERSON</td>
<td>Dec 5–10</td>
</tr>
<tr>
<td><strong>SANS Cyber Defense Initiative®</strong> (Washington, DC)</td>
<td>VIRTUAL &amp; IN-PERSON</td>
<td>Dec 12–17</td>
</tr>
</tbody>
</table>