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

Get more information on OnDemand Bundles at: sans.org/ondemand/bundles

“The course content and OnDemand delivery method have both exceeded my expectations.”

—Robert Jones, Team Jones, Inc.
GENERAL INFORMATION

Venue
Hyatt Regency Orlando
9801 International Drive | Orlando, FL 32819
Phone: 407-284-1234

Event Check-In | Badge & Courseware Distribution
Location: Regency Ballroom S (CONVENTION LEVEL)
Sat, April 9 ..................................................... 4:00–6:00 PM
Sun, April 10 ...................................................... 7:00–8:30 AM

Registration Support
Location: Silver Spring I (CONVENTION LEVEL)
Sun, April 10 – Thu, April 14 ............... 8:30 AM – 5:30 PM
Fri, April 15 ......................................................... 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
SANS attendees receive $5 off prevailing parking rates for daily self-parking or overnight parking.
Self-parking is available for $30 per day with no in-and-out privileges.
Overnight parking is available for $30 plus tax per night with in-and-out privileges.
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 chaser tickets.

Photography Notice
SANS may take photos of classroom activities for marketing purposes. SANS 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 4–6.

Bootcamps (Attendance Mandatory)
SEC511: Continuous Monitoring and Security Operations
SEC540: Cloud Security and DevSecOps Automation
SEC555: SIEM with Tactical Analytics
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 (Sunday, April 10)

FOR498: Battlefield Forensics & Data Acquisition
Kevin Ripa .................................. Bayhill 31/32 (LOBBY LEVEL)

FOR500: Windows Forensic Analysis
Ovie Carroll ............................. Windermere Y (CONVENTION LEVEL)

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics
Mike Pilkington .......................... Rainbow Springs (CONVENTION LEVEL)

FOR509: Enterprise Cloud Forensics and Incident Response
David Cowen ............................ Celebration 6 (CONVENTION LEVEL)

FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response
Philip Hagen ............................ Bayhill 27 (LOBBY LEVEL)

FOR578: Cyber Threat Intelligence
Katie Nickels ............................. Regency Ballroom U (CONVENTION LEVEL)

FOR585: Smartphone Forensic Analysis In-Depth
Heather Mahalik ........................ Celebration 12/13 (CONVENTION LEVEL)

ICS410: ICS/SCADA Security Essentials
Justin Searle ............................... Bayhill 25/26 (LOBBY LEVEL)

LEG523: Law of Data Security and Investigations
Benjamin Wright ........................ Bayhill 21 (LOBBY LEVEL)

MGT414: SANS Training Program for CISSP® Certification
David R. Miller ............................. Celebration 14/15 (CONVENTION 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
Brian Ventura ............................. Regency Ballroom T (CONVENTION LEVEL)

MGT514: Security Strategic Planning, Policy, and Leadership
Russell Eubanks .......................... Windermere W (CONVENTION LEVEL)

SEC301: Introduction to Cyber Security
Doc Blackburn ............................ Bayhill 29/30 (LOBBY LEVEL)

SEC401: Security Essentials Bootcamp Style
Bryan Simon ............................. Windermere X (CONVENTION LEVEL)
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 .......................... Bayhill 23/24 (LOBBY LEVEL)

SEC504: Hacker Tools, Techniques, and Incident Handling
Joshua Wright ............................ Regency Ballroom V (CONVENTION LEVEL)
Hours: 8:30 AM – 7:15 PM (Day 1)

SEC511: Continuous Monitoring and Security Operations
Seth Misenar ............................. Bayhill 17/18 (LOBBY LEVEL)
Hours: 8:30 AM – 7:00 PM (Day 1); 9:00 AM – 7:00 PM (Days 2–5)

SEC530: Defensible Security Architecture and Engineering
Ismael Valenzuela ........................ Celebration 2 (CONVENTION LEVEL)

SEC540: Cloud Security and DevOps Automation
Gregory Leonard & Jon Zeolla ........................ Windermere Z (CONVENTION 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, and Threat Detection
Shaun McCullough ........................ Celebration 3 (CONVENTION LEVEL)

SEC555: SIEM with Tactical Analytics
Mick Douglas ............................. Bayhill 28 (LOBBY LEVEL)
Hours: 8:30 AM – 7:00 PM (Day 1); 9:00 AM – 7:00 PM (Days 2–5)

SEC560: Enterprise Penetration Testing
Jeff McJunkin ............................ Bayhill 19/20 (LOBBY LEVEL)

SEC566: Implementing and Auditing CIS Critical Controls
James Tarala ............................. Celebration 4 (CONVENTION LEVEL)

SEC573: Automating Information Security with Python
Mark Baggett ............................. Bayhill 22 (LOBBY LEVEL)

SEC575: Mobile Device Security and Ethical Hacking
Jeroen Beckers ........................... Celebration 16 (CONVENTION LEVEL)

SEC587: Advanced Open-Source Intelligence (OSINT) Gathering and Analysis
David Mashburn ........................... Celebration 1 (CONVENTION LEVEL)

SEC588: Cloud Penetration Testing
Moses Frost & Karim Lalji ........................ Celebration 5 (CONVENTION LEVEL)

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
Stephen Sims ............................ Celebration 11 (CONVENTION LEVEL)
Hours: 8:30 AM – 7:00 PM (Day 1); 9:00 AM – 7:00 PM (Days 2–5)
Add a GIAC Certification attempt to your course before April 11.

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: $849
Get more information on GIAC Certifications at: giac.org

“GIAC is the only certification that proves you have hands-on technical skills.”
—Christina Ford, Department of Commerce

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

Validate Your Training

Add a GIAC Certification attempt to your course before April 11.

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: $849
Get more information on GIAC Certifications at: giac.org

“GIAC is the only certification that proves you have hands-on technical skills.”
—Christina Ford, Department of Commerce
**BONUS SESSIONS**

*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.

**SPECIAL EVENT**

**SANS 2022 Welcome Reception**

*Sunday, April 10 | 6:30–9:30 PM*
*Location: Main Event – Pointe Orlando*
*9101 International Drive (0.3 mile walk from Hyatt)*

Kick off your SANS 2022 experience at the Welcome Reception taking place at Main Event located in Pointe Orlando just 0.3 miles from the Hyatt Regency. Be part of this kickoff event and join the industry’s most powerful gathering of cybersecurity professionals. Share stories, make connections, and enjoy the arcade and game offerings of Main Event. Beverages (adult and otherwise) and bites will be served.

All-you-can-play activities including arcade games, bowling, billiards, and more: 6:30–9:30 PM (3 hours).

Beer, wine, and non-alcoholic beverage bar: 6:30–8:30 PM (2 hours)*

*Cash bar available following the bar hours listed above.

**KEYNOTE**

**RSA – Years in Review and What is Still Lingering. Threats Don’t Just Go Away.**

speakers: Heather Mahalik and Katie Nickels

*Monday, April 11 | 6:30–8:00 PM | Regency Ballroom S (CONVENTION LEVEL)*

Together, Heather Mahalik and Katie Nickels will look back at the top threats discussed at RSA and what is still lingering. What can you do to be more secure? How can these threats impact not only your organizations, but you personally?

**SANS @NIGHT**

**Real Serverless Use Cases in AWS**

Speaker: David Hazar

*Tuesday, April 12 | 7:15–8:15 PM | Regency Ballroom U (CONVENTION LEVEL)*

In this talk, SANS Certified Instructor David Hazar will walk you through some of the Serverless functions he has developed and implemented to support a variety of real-world use cases and demonstrate how these Serverless functions are used to support specific product functionality at Next Level3. See how to configure API Gateway to proxy requests to Lambda, how to perform delayed actions after X minutes with SQS and Lambda, and how to use Amazon Eventbridge rules and Lambda to lock and unlock AWS users and their associated access keys based on certain events. We will also briefly look at how to customize a SignIn flow with Azure AD B2C and Azure Functions.

**NETWARS**

**CORE**

*Wednesday, April 13 & Thursday, April 14*

**6:30–9:30 PM**

**Regency Ballroom T (CONVENTION LEVEL)**

**NETWARS**

**CYBER DEFENSE**

*Wednesday, April 13 & Thursday, April 14*

**7:15–10:15 PM**

**Regency Ballroom V (CONVENTION LEVEL)**

“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 for a SANS course at SANS 2022 are eligible to play NetWars for FREE.

Space is limited. Please register for NetWars through your SANS Account Dashboard.
LUNCH & LEARNS: Lunch is provided and registration is required.
Sign up in advance at the Check-In Desk (REGENCY BALLROOM S) or email forums@sans.org.

LUNCH & LEARN
Automating Internal and External Security Intelligence
Speaker: Andrew Senko
Monday, April 11  |  12:30–1:15 PM
Regency Ballroom V (CONVENTION LEVEL)

The amount of context that cybersecurity analysts and engineers require for assessing security alerts is overwhelming. But here’s the good news: Intelligence can help. Intelligence is the process of collecting, processing, and analyzing data to help teams understand the motives, targets, and behaviors of threat actors. Investing in a strategy to collect and curate intelligence should be a necessity for every cybersecurity team. And automation is the tactic that teams employ to scale their efforts and reduce team burnout. This is done by translating team tradecraft into logic that a machine can perform on the team’s behalf. Join this session to learn more about:

• How to define security intelligence use cases
• Collecting and curating asset information to create asset intelligence
• Automating the collection of external data sources to create threat intelligence
• Five essential steps for automating security use cases

LUNCH & LEARN
Evolve Your SOC with Richer Data, Guided Analytics, and Scalable Expertise
Speaker: Michael Lyons
Monday, April 11  |  12:30–1:15 PM
Regency Ballroom T (CONVENTION LEVEL)

Are you straining to scale your security analysts and defenses to stop attackers? If so, you’re not alone. Combating today’s threats requires new approaches to how your SOC manages its data, analytics and expertise. Join Devo as we explore innovative ways your security team can thrive in the era of massive data growth, talent shortage, and constantly evolving threats with:

• Analytics that leverage automation and ML to uplift your team’s performance
• Community expertise and curated content for faster threat resolution
• Innovative adversary simulation tools to test attacks and practice defenses

Solutions Expo – Breakfast & Lunch
Tuesday, April 12  |  7:30–9:00 AM  |  12:15–1:30 PM
Regency Rotunda Foyer (CONVENTION LEVEL)

Join our sponsoring exhibitors and fellow attendees for free breakfast and lunch while you become familiar with solutions and services that showcase the leading options in information security. Take time to browse the expo floor and get introduced to providers and their solutions that align with the security challenges being discussed in class.
LUNCH & LEARNS:
Lunch is provided and registration is required.
Sign up in advance at the Check-In Desk (REGENCY BALLROOM S) or email forums@sans.org.

LUNCH & LEARN
Leveraging MITRE and ML to Focus Your SOC Operations
Speaker: Inbar Raz
Wednesday, April 13 | 12:30–1:15 PM
Regency Ballroom U (CONVENTION LEVEL)

When it comes to detecting and prioritizing security events from multiple data sources across numerous domains, security teams face several challenges: unfavorable signal-to-noise ratio, false alerts, lack of visibility, and shortage of both domain-specific and broad-based security knowledge. “Mean Time to Know” - the ability to not just detect an incident, but to actually know if it is real and to understand its impact - has become a leading indicator for the ability of the SOC effectively respond and mitigate to threats.

When incidents are identified, it is critical to provide SOC analysts with clear understanding of the activity. Since security vendors named actors and threats with a variety of different names and descriptors, the MITRE frameworks should be the common language to enable security practitioners from different industries and with diverse data sources to understand the story behind the incident.

Join this session to learn:
• How ML is being used to detect suspicious events
• The challenges in scoring alerts, events and stories
• How the built-in integration of the MITRE ATT&CK framework enables better event scoring and prioritization
• Why Hunters chose to become a Founding Affiliate of the Center for Threat-Informed Defense, by MITRE Engenuity

LUNCH & LEARN
What Does XDR Mean for Your Organization?
Speaker: Alex Kirk
Wed, April 13 | 12:30–1:15 PM
Regency Ballroom V (CONVENTION LEVEL)

As one of the hottest new buzzwords in the InfoSec space, XDR means many things to many people. This talk will discuss all of the possible components of an XDR solution through the lens of SOC operations, laying out the pros and cons of various approaches such as SaaS versus on-premise, specialized versus general tooling, etc. for organizations of different sizes, funding, and maturity levels.

Best practice suggestions will be provided throughout, from general principles to specific integration code.

LUNCH & LEARN
How to Build Continuous Education Programs for Your Cybersecurity Team
Speaker: Marco Garcia
Wednesday, April 13 | 12:30–1:15 PM
Regency Ballroom T (CONVENTION LEVEL)

With a crippling cybersecurity skills shortage, it's never been more vital to invest in continuous cybersecurity education and training. Whether it's keeping ahead of emerging new technologies or ensuring that junior team members have clearly defined growth paths – investment in education and training helps cybersecurity teams respond faster, improve defensive posture, and increase retention of valuable employees. But building an effective education program can be time-consuming, and divert focus from priority one – keeping the organization safe.

In this talk, Marco Garcia, Field CTO at Torq, will discuss how to right-size training and education opportunities for your team, and how to use real-world attacks and threats as opportunities to help junior team members enrich skills. He’ll focus on three areas:
1. How to keep teams current on new threats, attack vectors, and technology trends
2. Establishing effective mentorship programs to help junior team members quickly acquire new skills
3. How to balance training and learning opportunities against mission-critical work that demands focus
Launch or Advance Your Career from the Best College in Cybersecurity.

- Bachelor’s Degrees
- Undergraduate Certificates
- Master’s Degrees
- Graduate Certificates

sans.edu

Create a Cyber Resilient Workforce.

Security awareness training for maximum engagement and comprehension to recognize and prevent current cyber threats.

- End User Training
- Phishing Platform
- Assessment Suite
- Developer Training

sans.org/security-awareness
## Upcoming SANS Training Events

<table>
<thead>
<tr>
<th>EVENT</th>
<th>TRAINING FORMAT</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Cyber Security Central: April</td>
<td>VIRTUAL</td>
<td>Apr 25–30</td>
</tr>
<tr>
<td>SANS Security West (San Diego, CA)</td>
<td>VIRTUAL &amp; IN-PERSON</td>
<td>May 5–10</td>
</tr>
<tr>
<td>Neurodiversity in Cybersecurity Summit</td>
<td>VIRTUAL</td>
<td>May 17–22</td>
</tr>
<tr>
<td>SANS Cyber Security East: May</td>
<td>VIRTUAL</td>
<td>May 16–21</td>
</tr>
<tr>
<td>SANS Leadership &amp; Cloud Security</td>
<td>VIRTUAL</td>
<td>May 23–28</td>
</tr>
<tr>
<td>ICS Security Summit &amp; Training (Lake Buena Vista, FL)</td>
<td>VIRTUAL &amp; IN-PERSON</td>
<td>Jun 1–9</td>
</tr>
<tr>
<td>SANS Dallas (Dallas, TX)</td>
<td>VIRTUAL &amp; IN-PERSON</td>
<td>Jun 6–11</td>
</tr>
<tr>
<td>SANS Rocky Mountain Summer (Denver, CO)</td>
<td>VIRTUAL &amp; IN-PERSON</td>
<td>Jun 13–18</td>
</tr>
<tr>
<td>SANS Cloud Defender Summer</td>
<td>VIRTUAL</td>
<td>Jun 13–18</td>
</tr>
<tr>
<td>Ransomware Summit</td>
<td>VIRTUAL</td>
<td>Jun 16–17</td>
</tr>
<tr>
<td>SANS Cyber Security Central: June</td>
<td>VIRTUAL</td>
<td>Jun 20–25</td>
</tr>
<tr>
<td>SANS Stay Sharp: June</td>
<td>VIRTUAL</td>
<td>Jun 20–25</td>
</tr>
<tr>
<td>SANSFIRE (Washington, DC)</td>
<td>VIRTUAL &amp; IN-PERSON</td>
<td>Jul 11–16</td>
</tr>
<tr>
<td>SANS Cyber Security Mountain: July</td>
<td>VIRTUAL</td>
<td>Jul 18–23</td>
</tr>
<tr>
<td>SANS Cyber Security East: July</td>
<td>VIRTUAL</td>
<td>Jul 25–30</td>
</tr>
<tr>
<td>Security Awareness Summit &amp; Training (Austin, TX)</td>
<td>VIRTUAL &amp; IN-PERSON</td>
<td>Aug 1–13</td>
</tr>
<tr>
<td>SANS Cyber Security East: August</td>
<td>VIRTUAL</td>
<td>Aug 1–6</td>
</tr>
<tr>
<td>SANS Boston Summer (Boston, MA)</td>
<td>VIRTUAL &amp; IN-PERSON</td>
<td>Aug 8–13</td>
</tr>
</tbody>
</table>