Welcome Reception

Monday, July 10 | 6:30–8:00 PM
Location: McClellan’s Sports Bar (LOBBY LEVEL)

Kick off your SANSFIRE 2023 experience at the Welcome Reception. Be part of this kickoff event and join the industry’s most powerful gathering of cybersecurity professionals. Share stories, enjoy some games, make connections, and learn how to make the most out of your training this week in Washington, DC. Beverages (adult and otherwise) and bites will be served. We hope to see you there!
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

Validate Your Training

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, July 9 ............................................. 5:00–7:00 PM
Monday, July 10 ........................................... 7:00–8:30 AM

Registration Support
Location: Albright (TERRACE LEVEL)
Monday, July 10 ........................................... 8:30 AM–5:30 PM
Tuesday, July 11–Friday, July 14 ................. 8:00 AM–5:30 PM
Saturday, July 15 ......................................... 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 at the prevailing rate of $56 per day at the Washington Hilton. SANS does not have a negotiated parking discount with this venue.*
*Parking rates are subject to change.
Photography Notice
SANS may take photos of classroom activities for marketing purposes. SANSFIRE 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)
MGT414: SANS Training Program for CISSP® Certification
SEC503: Intrusion 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, July 10)

FOR500: Windows Forensic Analysis
Ovie Carroll ................... Jefferson West (CONCOURSE LEVEL)

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics
Eric Zimmerman ........... Int’l Ballroom West (CONCOURSE LEVEL)

FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response
Brian Olson ..................... Columbia Hall 5 (TERRACE LEVEL)

FOR578: Cyber Threat Intelligence
Katie Nickels ..................... Columbia Hall 7 (TERRACE LEVEL)

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Xavier Mertens ................. Columbia Hall 4 (TERRACE LEVEL)

ICS410: ICS/SCADA Security Essentials
Justin Searle ................. Oaklawn (LOBBY LEVEL)

ICS612: ICS Cybersecurity In-Depth
Jason Dely ......................... Georgetown West (CONCOURSE LEVEL)

MGT414: SANS Training Program for CISSP® Certification
Eric Conrad ......................... Northwest (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
My-Ngoc Nguyen ................... Lincoln East (CONCOURSE LEVEL)

MGT514: Security Strategic Planning, Policy, and Leadership
Mark Williams ...................... Lincoln West (CONCOURSE LEVEL)

MGT551: Building and Leading Security Operations Centers
John Hubbard ....................... Jay (LOBBY LEVEL)

SEC301: Introduction to Cyber Security
Doc Blackburn ..................... Jefferson East (CONCOURSE LEVEL)

Bryan Simon ..................... Columbia Hall 6 (TERRACE 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
Seth Misenar ...................... Holmead West (LOBBY LEVEL)

SEC488: Cloud Security Essentials
Simon Vernon ..................... Columbia Hall 9 (TERRACE LEVEL)

SEC497: Practical Open-Source Intelligence (OSINT)
Matt Edmondson .................. Gunston East (TERRACE LEVEL)

SEC503: Network Monitoring and Threat Detection In-Depth
Andrew Laman
Benjamin Barnes .................. Columbia Hall 10 (TERRACE LEVEL)
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–5)
<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Instructor</th>
<th>Room</th>
<th>Level</th>
<th>Days</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, and Incident Handling</td>
<td>Jon Gorenflo</td>
<td>Int'l Ballroom Center</td>
<td>CONCOURSE</td>
<td>Day 1</td>
<td>8:30 AM–7:15 PM</td>
</tr>
<tr>
<td>SEC510</td>
<td>Public Cloud Security: AWS, Azure, and GCP</td>
<td>Kenneth G. Hartman</td>
<td>Piscataway</td>
<td>LOBBY</td>
<td>Days 1–4</td>
<td>8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–4)</td>
</tr>
<tr>
<td>SEC522</td>
<td>Application Security: Securing Web Apps, APIs, and Microservices</td>
<td>Dr. Johannes Ullrich</td>
<td>Int'l Ballroom East</td>
<td>LOBBY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC530</td>
<td>Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise</td>
<td>Ismael Valenzuela</td>
<td>Int'l Ballroom East</td>
<td>LOBBY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC540</td>
<td>Cloud Security and DevSecOps Automation</td>
<td>Jon Zeolla</td>
<td>Monroe</td>
<td>CONCOURSE</td>
<td>Day 1</td>
<td>8:30 AM–7:00 PM</td>
</tr>
<tr>
<td>SEC541</td>
<td>Cloud Security Attacker Techniques, Monitoring, and Threat Detection</td>
<td>Shaun McCullough</td>
<td>Columbia Hall 11</td>
<td>TERRACE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC542</td>
<td>Web App Penetration Testing and Ethical Hacking</td>
<td>Bojan Zdrnja</td>
<td>Columbia Hall 12</td>
<td>TERRACE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC560</td>
<td>Enterprise Penetration Testing</td>
<td>Jeff McJunkin</td>
<td>Georgetown East</td>
<td>CONCOURSE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC565</td>
<td>Red Team Operations and Adversary Emulation</td>
<td>Greg Bailey</td>
<td>Morgan</td>
<td>LOBBY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC573</td>
<td>Automating Information Security with Python</td>
<td>Mark Baggett</td>
<td>Kalorama</td>
<td>LOBBY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC575</td>
<td>iOS and Android Application Security Analysis and Penetration Testing</td>
<td>Jeroen Beckers</td>
<td>Fairchild West</td>
<td>TERRACE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC588</td>
<td>Cloud Penetration Testing</td>
<td>Christopher Elgee</td>
<td>Columbia Hall 1</td>
<td>TERRACE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC595</td>
<td>Applied Data Science and AI/Machine Learning for Cybersecurity Professionals</td>
<td>David Hoelzer</td>
<td>Columbia Hall 8</td>
<td>TERRACE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC599</td>
<td>Defeating Advanced Adversaries – Purple Team Tactics &amp; Kill Chain Defenses</td>
<td>Erik Van Buggenhout</td>
<td>Columbia Hall 3</td>
<td>TERRACE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC617</td>
<td>Wireless Penetration Testing and Ethical Hacking</td>
<td>James Leyte-Vidal</td>
<td>Fairchild East</td>
<td>TERRACE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC660</td>
<td>Advanced Penetration Testing, Exploit Writing, and Ethical Hacking</td>
<td>Stephen Sims</td>
<td>Columbia Hall 2</td>
<td>TERRACE</td>
<td>Days 2–5</td>
<td>8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–5)</td>
</tr>
</tbody>
</table>
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.

SPECIAL EVENT
SANSFIRE 2023 Welcome Reception
Monday, July 10 | 6:30–8:00 PM
Location: McClellan’s Sports Bar (LOBBY LEVEL)
Kick off your SANSFIRE 2023 experience at the Welcome Reception. Be part of this kickoff event and join the industry’s most powerful gathering of cybersecurity professionals. Share stories, enjoy some games, make connections, and learn how to make the most out of your training this week in Washington, DC. Beverages (adult and otherwise) and bites will be served. We hope to see you there!

FEATURED KEYNOTE
Internet Storm Center: What’s New and Current Threat Brief
Speaker: Dr. Johannes Ullrich
Tuesday, July 11 | 6:30–8:00 PM
International Ballroom East (CONCOURSE LEVEL)

The Internet Storm Center is all about “coloring your logs”—finding out what matters and doesn’t matter by adding context to otherwise abstract datapoints like IP addresses and domain names. This free data is made available via our website and easy to use APIs. During this session, we will talk about some of the changes we have made to make the data more useful and more available. We will also illustrate how you can learn about ongoing trends and improve your skills via our amazing collaborative community.
SPECIAL EVENT
SANSFIRE 2023 5k Walk/Run and Reception
Wednesday, July 12 | 6:30–8:00 AM | Meet in Hotel Lobby
Seize the day and get your steps in before class! SANS invites you to join some faculty members and fellow attendees for a morning walk or run in Washington, DC! We will meet at 6:30am in the hotel lobby at the Washington Hilton and head down Connecticut Avenue towards the Smithsonian’s National Zoo! You are welcome to stay with a group or move at your own pace. Refreshments and light energizing bites will be provided afterwards.

WORKSHOP
Beyond Firewalls: Techniques for Protecting Cloud-Based Assets
Speaker: Simon Vernon, SANS Certified Instructor
Wednesday, July 12 | 6:45–8:45 PM | Columbia Hall 1 (TERRACE LEVEL)
When a system designed for on-premises operation is migrated to a public cloud, it is exposed to additional vulnerabilities and risks of exploitation. This workshop will delve into the realm of cloud native security solutions and techniques, to demonstrate how it is possible to protect such systems that are otherwise considered indefensible particularly in the case of “Lift and Shift.”
Prerequisites: This workshop will require participants to have an Azure account with full administrative rights.

WORKSHOP
Deep Dive into SSRF and Insecure Deserialization Vulnerabilities
Speaker: Bojan Zdrnja, Internet Storm Center Handler
Wednesday, July 12 | 6:45–8:45 PM | Int’l Ballroom West (CONCOURSE LEVEL)
In this workshop we will quickly go through the OWASP Top 10 list of vulnerabilities and then we’ll dive into two labs where we will hack web applications by identifying a few simpler vulnerabilities that, when chained together, will lead to us compromising the application completely. Specifically, we will cover Server-side Request Forgery (SSRF) vulnerabilities as well as Insecure Deserialization vulnerabilities—both of these categories of vulnerabilities will be exploited during the workshop by chaining them with some low hanging fruit (without which, it would be maybe even impossible to identify them).
Prerequisites: Familiarity with Burp suite

SPECIAL EVENT
Birds of a Feather: Open Mic Night
Wednesday, July 12 | 7:00–9:00 PM | Cabinet (CONCOURSE LEVEL)
Join us for a bit of fun and music! Let’s gather in the 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. Join us and sing along to classics like American Pie and Country Roads. If you are so inclined, bring your own instrument!
**BONUS SESSIONS**

**SANS@NIGHT**  
**Malware Analysis for the Poor**  
**Speaker:** Xavier Mertens, Internet Storm Center Handler  
**Wednesday, July 12 | 7:15–8:15 PM | Columbia Hall 7 (TERRACE LEVEL)**

When you think about malware analysis, many people immediately see big screens full of ASM code in debuggers and disassemblers. But most of the malware you see daily remains simple and can be analyzed using generic tools. In this presentation, Xavier takes a sample he collected through his honeypot and takes the audience by the hand to explain how to address this kind of document using simple tools and quickly spotting the malicious activity.

**SANS@NIGHT**  
**Lessons Learned from Interrupting a Double Extortion Attack – An Incident Responder Perspective**  
**Speaker:** Renato Marino, Internet Storm Center Handler  
**Wednesday, July 12 | 7:15–8:15 PM | Columbia Hall 5 (TERRACE LEVEL)**

From the input vector to the data exfiltration, this presentation details the path taken by the double-extortion attacker on the network in the search for the most sensitive data while trying to circumvent the protections. Along this path, Renato will focus on the detection and defense opportunities missed by the defense team and how we act to reverse data exfiltration and break the chain of attack. The lessons learned include technical implementations that could have given visibility to malicious steps and the decision processes on how to act when the possibility to revert the data exfiltrated was presented to the war room.

**SANS@NIGHT**  
**Using APIs and Free Tools for Reconnaissance**  
**Speaker:** Rob Vandenbrink, Internet Storm Center Handler  
**Wednesday, July 12 | 8:15–9:15 PM | Columbia Hall 7 (TERRACE LEVEL)**

The conventional wisdom is that the Reconnaissance phase should be a significant portion of any security assessment or penetration test—because after all—you can’t assess or attack what you don’t know is there, right?

In this session, we’ll explore various methods of finding hosts or subnets that might not be in your original scope, and often will be a surprise to your client! Using these recon approaches, you’ll find that phrases like “No we don’t patch that, we were told it was shut down three years ago” or “who’s paying the AWS bill for that?” tend to come up in conversations during customer meetings. Also, “and they were using PROD data for that DEV instance nobody told us about.” It’s a rare gig where you can’t find at least a few hosts that the client forgot about or never knew were there. As you can tell, the possibilities are endless—for the attacker that is!

We’ll use both commercial and open-source intelligence API’s and data sources, and everything from simple one-liner queries to some full OSINT distro’s to get the job done. Cool tools aside, you’ll be surprised to find how much you can find with a one-line curl statement and an API key (and sometimes not even the API key).
SPECIAL EVENT

SANSFIRE 2023 Puppy Cuddle Break
Thursday, July 13 | 12:00–2:00 PM | Columbia Foyer (TERRACE LEVEL)
Join the Lucky Dog Animal Rescue for a fun, stress busting, cuddle with some cute, adoptable, pups. Take a break from the firehose that is SANS training to rejuvenate before returning to class, and maybe take home a new life-long best friend.

SANSFIRE 2023 Puppy Cuddle Break
Thursday, July 13 | 12:00–2:00 PM | Columbia Foyer (TERRACE LEVEL)

Join the Lucky Dog Animal Rescue for a fun, stress busting, cuddle with some cute, adoptable, pups. Take a break from the firehose that is SANS training to rejuvenate before returning to class, and maybe take home a new life-long best friend.

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

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 register for a 4–6 day In-Person course will be eligible to play NetWars for FREE.

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

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

Lunch & Learn (& Earn)
Receive one 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!

SPONSORED LUNCH & LEARN

Dodge the Sliver Bullet and Find the Smoking Gun
Tuesday, July 11 | 12:30–1:15 PM | Columbia Hall 5 (TERRACE LEVEL)
Sliver is rising in popularity and is thought to be taking significant market share off other well known C2 frameworks. Corelight Content can better power your Sliver detections highlighting what’s on your network to build a strategic data reserve when you need to investigate an incident. Come learn about Corelight Content, insightful community developed detections, and an open NDR that puts the power in your hands.

ATTEND VIRTUALLY

SPONSORED LUNCH & LEARN

Applying Moving Target Defense to Data Streams
Thursday, July 13 | 12:30–1:15 PM | Columbia Hall 7 (TERRACE LEVEL)
If you want to protect the content of a transmission, you use encryption. If you want to protect the context or connected parties to a transmission, you use a Moving Target Defense network. We will cover four stories from the field: an energy system; a force protection problem; a biotech team collaborating on pre-patented data; and a manufacturer that needed real-time visibility across its plants. Relevant topics: basic theory and relevant standards, stream stability, scale factors, reliability, cost forecasting, implementation considerations, and how to get this done through the Board level.

ATTEND VIRTUALLY

D I S P E L
SANSFIRE 2023 students and faculty are invited to join our featured solution providers for a FREE BREAKFAST & LUNCH!

**Breakfast**

**Solutions Expo**

Wednesday, July 12 | 7:30–9:00 AM
International Terrace (CONCOURSE LEVEL)

**Lunch**

**Solutions Expo & Raffle Drawing**

Wednesday, July 12 | 12:15–1:30 PM
International Terrace (CONCOURSE LEVEL)

*Raffle Drawing at 1:30 PM
You do NOT have to be present to win!*

**Prizes:**

Amazon Gift Cards
## Upcoming SANS Training Events

<table>
<thead>
<tr>
<th>EVENT</th>
<th>TRAINING FORMAT</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cloud Security – San Francisco</strong> San Francisco, CA</td>
<td>HYBRID</td>
<td>Jul 17–22</td>
</tr>
<tr>
<td><strong>New York City</strong> New York, NY</td>
<td>HYBRID</td>
<td>Jul 24–29</td>
</tr>
<tr>
<td><strong>Nashville</strong> Nashville, TN</td>
<td>HYBRID</td>
<td>Aug 7–12</td>
</tr>
<tr>
<td><strong>Chicago</strong> Chicago, IL</td>
<td>HYBRID</td>
<td>Aug 14–19</td>
</tr>
<tr>
<td><strong>Virginia Beach</strong> Virginia Beach, VA</td>
<td>HYBRID</td>
<td>Aug 21–Sep 1</td>
</tr>
<tr>
<td><strong>Network Security</strong> (Las Vegas, NV)</td>
<td>HYBRID</td>
<td>Sep 6–11</td>
</tr>
<tr>
<td><strong>Stay Sharp: September</strong></td>
<td>VIRTUAL (ET)</td>
<td>Sep 11–15</td>
</tr>
<tr>
<td><strong>Maryland – Rockville</strong> Rockville, MD</td>
<td>HYBRID</td>
<td>Sep 18–23</td>
</tr>
<tr>
<td><strong>Seattle</strong> Seattle, WA</td>
<td>HYBRID</td>
<td>Sep 25–30</td>
</tr>
<tr>
<td><strong>Managing Security Risk</strong></td>
<td>VIRTUAL (CT)</td>
<td>Sep 25–30</td>
</tr>
<tr>
<td><strong>Executive Leadership Training</strong> Dulles, VA</td>
<td>IN-PERSON</td>
<td>Oct 2–6</td>
</tr>
<tr>
<td><strong>Stay Sharp: October</strong></td>
<td>VIRTUAL (ET)</td>
<td>Oct 2–4</td>
</tr>
<tr>
<td><strong>Baltimore Fall</strong> Baltimore, MD</td>
<td>HYBRID</td>
<td>Oct 9–14</td>
</tr>
<tr>
<td><strong>San Francisco Fall</strong> San Francisco, CA</td>
<td>HYBRID</td>
<td>Oct 9–14</td>
</tr>
<tr>
<td><strong>Rocky Mountain Fall</strong> Denver, CO</td>
<td>HYBRID</td>
<td>Oct 23–28</td>
</tr>
<tr>
<td><strong>Orlando Fall</strong> Orlando, FL</td>
<td>HYBRID</td>
<td>Oct 30–Nov 4</td>
</tr>
<tr>
<td><strong>San Diego Fall</strong> San Diego, CA</td>
<td>HYBRID</td>
<td>Nov 6–11</td>
</tr>
</tbody>
</table>