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.

Welcome Reception

Kick off your SANSFIRE 2022 experience at our Welcome Reception

Monday, July 11 | 6:30–8:00 PM
Location: McClellan’s Sports Bar and Lobby Patio (LOBBY LEVEL)

Be part of this premier 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 colleagues for a fun, relaxing evening. Beverages and refreshments will be served.
**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 10** .................. 4:00–6:00 PM  
**Monday, July 11** .................. 7:00–8:30 AM

---

**Registration Support**

Location: Albright Room (TERRACE LEVEL)

**Monday, July 11–Friday, July 15** .... 8:30 AM–5:00 PM  
**Saturday, July 16** .................. 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 subject to change

---

**Photography Notice**

SANS may take photos of classroom activities for marketing purposes. SANSFIRE 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)**

**SEC401:** Security Essentials: Network, Endpoint, and Cloud  
**SEC510:** Public Cloud Security: AWS, Azure, and GCP  
**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
<table>
<thead>
<tr>
<th>COURSE SCHEDULE</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIME: 9:00 AM–5:00 PM (UNLESS OTHERWISE NOTED)</td>
</tr>
<tr>
<td>NOTE: ALL CLASSES BEGIN AT 8:30 AM ON DAY 1 (MONDAY, JULY 11)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>COURSE CODE</th>
<th>COURSE TITLE</th>
<th>INSTRUCTOR(S)</th>
<th>LOCATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOR500</td>
<td>Windows Forensic Analysis</td>
<td>Lodrina Cherne</td>
<td>Columbia 7 (TERRACE LEVEL)</td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Incident Response, Threat Hunting, and Digital Forensics</td>
<td>Eric Zimmerman</td>
<td>Columbia 9/10 (TERRACE LEVEL)</td>
</tr>
<tr>
<td>FOR572</td>
<td>Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response</td>
<td>Philip Hagen</td>
<td>Morgan (LOBBY LEVEL)</td>
</tr>
<tr>
<td>FOR578</td>
<td>Cyber Threat Intelligence</td>
<td>Katie Nickels</td>
<td>Columbia 3/4 (TERRACE LEVEL)</td>
</tr>
<tr>
<td>FOR585</td>
<td>Smartphone Forensic Analysis In-Depth</td>
<td>Heather Mahalik</td>
<td>Columbia 12 (TERRACE LEVEL)</td>
</tr>
<tr>
<td>FOR608</td>
<td>Enterprise-Class Incident Response &amp; Threat Hunting</td>
<td>Mike Pilkington</td>
<td>Columbia 6 (TERRACE LEVEL)</td>
</tr>
<tr>
<td>FOR610</td>
<td>Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td>
<td>Michael Murr</td>
<td>Jay (LOBBY LEVEL)</td>
</tr>
<tr>
<td>ICS410</td>
<td>ICS/SCADA Security Essentials</td>
<td>Justin Searle</td>
<td>International Ballroom West (CONCOURSE LEVEL)</td>
</tr>
<tr>
<td>ICS612</td>
<td>ICS Cybersecurity In-Depth</td>
<td>Jason Dely &amp; Michael Hoffman</td>
<td>Monroe (CONCOURSE LEVEL)</td>
</tr>
<tr>
<td>LEG523</td>
<td>Law of Data Security and Investigations</td>
<td>Benjamin Wright</td>
<td>Georgetown East (CONCOURSE LEVEL)</td>
</tr>
<tr>
<td>MGT414</td>
<td>SANS Training Program for CISSP® Certification</td>
<td>Brian Ventura</td>
<td>Holmead West (LOBBY LEVEL)</td>
</tr>
<tr>
<td>MGT512</td>
<td>Security Leadership Essentials for Managers</td>
<td>My-Ngoc Nguyen</td>
<td>Lincoln West (CONCOURSE LEVEL)</td>
</tr>
<tr>
<td>MGT514</td>
<td>Security Strategic Planning, Policy, and Leadership</td>
<td>Mark Williams</td>
<td>Lincoln East (CONCOURSE LEVEL)</td>
</tr>
<tr>
<td>MGT551</td>
<td>Building and Leading Security Operations Centers</td>
<td>John Hubbard</td>
<td>International Ballroom East (CONCOURSE LEVEL)</td>
</tr>
<tr>
<td>SEC301</td>
<td>Introduction to Cyber Security</td>
<td>Doc Blackburn</td>
<td>Georgetown West (CONCOURSE LEVEL)</td>
</tr>
<tr>
<td>SEC401</td>
<td>Security Essentials: Network, Endpoint, and Cloud</td>
<td>Bryan Simon</td>
<td>Columbia 8 (TERRACE LEVEL)</td>
</tr>
<tr>
<td>SEC488</td>
<td>Cloud Security Essentials</td>
<td>Kenneth G. Hartman</td>
<td>Columbia 11 (TERRACE LEVEL)</td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, and Incident Handling</td>
<td>Jon Gorenflo</td>
<td>International Ballroom Center (CONCOURSE LEVEL)</td>
</tr>
<tr>
<td>SEC510</td>
<td>Public Cloud Security: AWS, Azure, and GCP</td>
<td>Brandon Evans</td>
<td>Jefferson West (CONCOURSE LEVEL)</td>
</tr>
<tr>
<td>SEC522</td>
<td>Application Security: Securing Web Apps, APIs, and Microservices</td>
<td>Dr. Johannes Ullrich</td>
<td>Columbia 1/2 (TERRACE LEVEL)</td>
</tr>
<tr>
<td>SEC540</td>
<td>Cloud Security and DevOps Automation</td>
<td>Eric Johnson</td>
<td>Jefferson East (CONCOURSE LEVEL)</td>
</tr>
<tr>
<td>SEC542</td>
<td>Web App Penetration Testing and Ethical Hacking</td>
<td>Timothy Mackenzie</td>
<td>Holmead East (LOBBY LEVEL)</td>
</tr>
<tr>
<td>SEC551</td>
<td>Advanced Penetration Testing, Exploit Writing, and Ethical Hacking</td>
<td>Stephen Sims</td>
<td>Fairchild East (TERRACE LEVEL)</td>
</tr>
</tbody>
</table>
**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.

**KEYNOTE**

**The Internet Storm Center: How to Use and Contribute Data**

Speakers: Dr. Johannes Ullrich, ISC Director and Internet Storm Center Handlers  
Tuesday, July 12 | 7:15–9:15 PM | Int’l Ballroom Center (CONCOURSE LEVEL)

For about 20 years, the Internet Storm Center has offered terabytes of data to the community to help you understand attacks you are seeing and assist you in augmenting your logs or, as we often put it, “add color” to your network logs. In this keynote, we will introduce some of our volunteer handlers who contribute their insight in daily diaries (you will also learn why we call it a “diary” and not a “blog”). In addition, we will walk you through our site, our APIs, and the different reports and features we offer to help you make your job easier. We provide all the data we collect as soon as we receive it for free to the community. Are you interested in contributing? We will demonstrate the latest version of our honeypot. We will have a hands-on session showing how to install the honeypot in your home network and explaining how you and the whole family can enjoy the data. Packetnight with the family will never be the same!

**SANS@NIGHT**

**Who Said That Python was UNIX’s Best Friend Only?**

Speaker: Xavier Mertens, ISC Handler  
Wednesday, July 13 | 7:15–8:15 PM | Columbia 1/2 (TERRACE LEVEL)

Python is a wonderful language, easy to learn, powerful and integrates perfectly with any operating system. Yes, who said that Python was only popular in UNIX environments? (read: Linux, macOS, etc). Today, there are more and more malicious Python scripts in the wild that work on Windows. They can interact with the webcam, keyboard to steal your data, they are able to interact with all Microsoft API calls and, therefore, perform more low-level action like process injection. Even ransomware can be developed in Python. You feel safe because Python is not installed on your workstations? No problem, Python can be installed easily from stage 0! In this talk, I’ll present some findings that I have collected for a while around Python malicious code in the Windows ecosystem.

**SANS@NIGHT**

**Reviewing Pcaps from Emotet Infections**

Speaker: Brad Duncan, ISC Handler  
Wednesday, July 13 | 7:15–8:15 PM | Columbia 5 (TERRACE LEVEL)

After a complete takedown in January 2021, Emotet returned by November 2021, and its new infrastructure generates tens of thousands of emails each day in an attempt to infect vulnerable victims. In this presentation, Brad Duncan reviews recent infection activity from Emotet, focusing on packet captures (pcaps) of infections that include Cobalt Strike and spambot activity. Brad compares the malware binaries contained in the pcaps with malware binaries retrieved from the infected Windows’ host that generated the traffic. This presentation provides an up-to-date picture of the current Emotet threat landscape with a step-by-step walkthrough of a typical Emotet infection chain.

**SANS@NIGHT**

**Blueprint Podcast Live! A Q&A Panel Discussion**

Speakers: John Hubbard and Guests  
Wednesday, July 13 | 7:15–8:15 PM  
International Ballroom Center (TERRACE LEVEL)

Those attending SANSFIRE 2022 won’t want to miss this special SANS@Night event coinciding with the season 3 launch of the Blueprint podcast. John Hubbard, Blueprint host and SANS Cyber Defense Curriculum Lead, will be joined by a panel of cybersecurity experts for this powerful discussion. John and guests will share their wisdom on trends they are seeing in the cyber industry and offer advice as to how we should be looking at cyber defense in 2022 and beyond.
SANS@NIGHT

Security Research Is Not Just For Experts – You Can Do It Too!

Speaker: Jan Kopriva, ISC Handler

Wednesday, July 13 | 8:15–9:15 PM | Columbia 7 (TERRACE LEVEL)

Cybersecurity research is slightly unusual in that unlike in many other fields, the ability to discover something “new” is still firmly within the grasp of experienced professionals, not just academic teams, or specialized research organizations. Furthermore, security research doesn’t necessarily have to be limited to professionals with wide-ranging experience – given the availability of open data sets, number of vulnerabilities in modern applications, and the frequency with which new versions of malware are being developed, there is enough easily-accessible material for research that almost anyone can engage in it, regardless of their technical knowledge. In this presentation, we will demonstrate that the bar for meaningful security research truly doesn’t have to be too high and show the attendees how they can engage in it as well. We will introduce a simple research methodology suitable to arbitrary security research topics, go over some of the freely available data sets and resources that aspiring researchers may take advantage of, and show real-world examples of simple research ideas, that lead to interesting results – discovery of sensitive data published online, identification of new malware capabilities and discovery of new vulnerabilities, just to name a few.

SPECIAL EVENT

SANS Women Connect Reception

Thursday, July 14 | 5:30–7:00 PM | International Terrace (TERRACE LEVEL)

From Jean Jennings Bartik to Diane Greene, women have always been a driving force in the field of information technology. Their experiences have been filled not only with stories of overcoming challenges but also ones of innovation and inspiration. Join SANS to foster an evening of connections among our strong community of women leaders including students, faculty and membership-based organizational partners.
Add a GIAC Certification attempt to your course before July 12.

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

**Breakfast Solutions Expo**
Wednesday, July 13 | 7:30–9:00 AM
International Terrace (TERRACE LEVEL)

**Lunch Solutions Expo & Raffle Drawing**
Wednesday, July 13 | 12:15–1:30 PM
International Terrace (TERRACE LEVEL)
Raffle Drawing at 1:30 PM

Solution Providers Available:

- AXONIUS
- corelight
- DEVO
- Delinea
- DISPEL
- DOMAINTOOLS®
- GREYNOISE
- paloalto®
- SOPHOS

**ENTER TO WIN!**

*Raffle Drawing at the Lunch Solutions Expo*
Wednesday, July 13 | 1:30 PM
International Terrace (TERRACE LEVEL)

Join us for breakfast and lunch on Wednesday, July 13 in the International Terrace 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
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
SAVE THE Date!

SANSFIRE 2023
Returning to the Washington Hilton

→ July 10–15, 2023

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 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>
<tr>
<td>SANS Cloud &amp; DevOps (San Francisco, CA)</td>
<td>VIRTUAL &amp; IN-PERSON</td>
<td>Aug 15–20</td>
</tr>
<tr>
<td>DFIR Summit &amp; Training (Austin, TX)</td>
<td>VIRTUAL &amp; IN-PERSON</td>
<td>Aug 15–22</td>
</tr>
<tr>
<td>SANS Virginia Beach (Virginia Beach, VA)</td>
<td>VIRTUAL &amp; IN-PERSON</td>
<td>Aug 22–27</td>
</tr>
<tr>
<td>SANS Stay Sharp: August</td>
<td>VIRTUAL</td>
<td>Aug 29–Sep 2</td>
</tr>
<tr>
<td>SANS Puerto Rico (San Juan, PR)</td>
<td>IN-PERSON</td>
<td>Aug 29–Sep 3</td>
</tr>
<tr>
<td>Blockchain Security Summit</td>
<td>VIRTUAL</td>
<td>Aug 31–Sep 1</td>
</tr>
<tr>
<td>SANS Network Security (Washington, DC)</td>
<td>VIRTUAL &amp; IN-PERSON</td>
<td>Sep 7–12</td>
</tr>
<tr>
<td>SANS Cybersecurity Leadership Summit &amp; Training (Arlington, VA)</td>
<td>VIRTUAL &amp; IN-PERSON</td>
<td>Sep 14–24</td>
</tr>
<tr>
<td>SANS Cyber Security Central: September</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>
</tbody>
</table>