Security East 2020
New Orleans | February 1-8
#SANSSECEast @SANSInstitute
Program Guide
Welcome Networking Reception

Sunday, February 2
6:00pm – 9:00pm
Fulton Alley
600 Fulton Street
New Orleans, LA 70130

Join your peers for a fun evening of bowling, shuffleboard, and darts while watching Super Bowl LIV. Food and beverages will be served.

*Pick up event badges during pre-registration: Sunday, Feb. 2 from 4:00pm - 6:00pm. Event badges are required for admission and the reception is for all registered Security East 2020 attendees.
Add an OnDemand Bundle to your course to get an additional four months of intense training! OnDemand Bundles are just $799 ($315 for short courses) when added to your live course, and include:

- Four months of OnDemand access to our custom e-learning platform
- Quizzes
- Labs
- MP3s and videos of lectures
- Subject-matter-expert support

**COURSES AVAILABLE:**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>FOR500</td>
<td>FOR572</td>
<td>FOR578</td>
<td>FOR585</td>
<td>MGT414</td>
<td>MGT514</td>
<td>ICS410</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Short course

To receive the discounted rate, you must sign up before Friday, February 14th at 8:00pm EDT

Add to your order via your Portal Account: [sans.org/account/login](http://sans.org/account/login)

Call or e-mail SANS Registration:

1-301-654-SANS (7267) | registration@sans.org
Event Check-In  |  Badge & Courseware Distribution

*Riverside Lobby* (RIVERSIDE)

**Sat, February 1** (2-Day Courses) 8:00am – 9:00am
**Sun, February 2** 4:00pm – 6:00pm
**Mon, February 3** 7:00am – 9:00am

Registration Support

*Bridge* (RIVERSIDE)

**Sat, February 1 – Sun, February 2** 9:00am – 5:00pm
**Mon, February 3** 7:00am – 5:00pm
**Tue, February 4 – Fri, February 7** 8:00am – 5:00pm
**Sat, February 8** 8:00am – 2:00pm

Internet Café

*Riverside Lobby* (RIVERSIDE)

**Mon, February 3**  Opens at Noon
**Tue, February 4 – Fri, February 7**  Open 24 hours
**Sat, February 8**  Closes at 2:00pm

Course Times

*All full-day courses will run from 9:00am – 5:00pm (unless noted)*

Course Breaks

**Morning Coffee** 7:00am – 9:00am
**Morning Break** 10:30am – 10:50am
**Lunch (ON YOUR OWN)** 12:15pm – 1:30pm
**Afternoon Break** 3:00pm – 3:20pm

Photography Notice

SANS may take photos of classroom activities for marketing purposes. Security East 2020 attendees grant SANS all rights for such use without compensation, unless prohibited by law.
Feedback Forms and Course Evaluations
The SANS planning committee wants to know what we should keep doing and what we need to improve – but we need your help! Please take a moment to fill out an evaluation form after each course day and bonus session and drop it in the evaluation box.

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 4-7.

Bootcamps (Attendance Mandatory)
- **SEC401**: Security Essentials Bootcamp Style
- **SEC503**: Intrusion Detection In-Depth
- **SEC540**: Cloud Security and DevOps Automation
- **SEC555**: SIEM with Tactical Analytics
- **MGT414**: SANS Training Program for CISSP® Certification

Extended Hours:
- **SEC504**: Hacker Tools, Techniques, Exploits & Incident Handling
- **SEC560**: Network Penetration Testing and Ethical Hacking
# COURSE SCHEDULE

## START DATE: Saturday, February 1

**Time:** 9:00am – 5:00pm (Unless otherwise noted)

**SEC440: Critical Security Controls: Planning, Implementing, and Auditing**  
Randy Marchany  
**Starboard (RIVERSIDE)**

**MGT415: A Practical Introduction to Cyber Security Risk Management**  
Russell Eubanks  
**Quarterdeck C (RIVERSIDE)**

## START DATE: Monday, February 3

**Time:** 9:00am – 5:00pm (Unless otherwise noted)

**SEC301: Introduction to Cyber Security**  
Keith Palmgren  
**Marlborough A (2ND LEVEL)**

**SEC401: Security Essentials Bootcamp Style**  
Bryan Simon  
Kabacoff  
**RIVERSIDE**

**SEC450: Blue Team Fundamentals: Security Operations and Analysis**  
John Hubbard, Mark Orlando  
Quarterdeck B  
**RIVERSIDE**

**SEC503: Intrusion Detection In-Depth**  
David Hoelzer  
Churchill C1  
**2ND LEVEL**

**SEC504: Hacker Tools, Techniques, Exploits & Incident Handling**  
Joshua Wright  
Chart B  
**RIVERSIDE**

**SEC530: Defensible Security Architecture and Engineering**  
Ismael Valenzuela  
Prince of Wales  
**2ND LEVEL**

**SEC540: Cloud Security and DevOps Automation**  
Eric Johnson  
Churchill C2  
**2ND LEVEL**

**SEC542: Web App Penetration Testing and Ethical Hacking**  
Eric Conrad, Timothy McKenzie  
Churchill B2  
**2ND LEVEL**

**SEC545: Cloud Security Architecture and Operations**  
Dave Shackleford  
Compass  
**RIVERSIDE**
SEC555: SIEM with Tactical Analytics  
Mick Douglas ........................ Quarterdeck A (RIVERSIDE)  
*Bootcamp Hours: 5:00pm – 7:00pm (Course days 1-5)*

SEC560: Network Penetration Testing and Ethical Hacking  
Jeff McJunkin .......................... River (RIVERSIDE)  
*Hours: 9:00am – 7:15pm (Day 1)*

SEC573: Automating Information Security with Python  
Mark Baggett .......................... Churchill B1 (2ND LEVEL)

SEC599: Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses  
Alissa Torres .......................... Churchill A1 (2ND LEVEL)

SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques  
Adrien de Beaupre .......................... Starboard (RIVERSIDE)

FOR500: Windows Forensic Analysis  
Rob Lee .................................. Chart A (RIVERSIDE)

FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response  
Philip Hagen .......................... Eglinton Winton (2ND LEVEL)

FOR578: Cyber Threat Intelligence  
Peter Szczepankiewicz ........................ Cambridge (2ND LEVEL)

FOR585: Smartphone Forensic Analysis In-Depth  
Heather Mahalik, Mattia Epifani .... Quarterdeck C (RIVERSIDE)

MGT414: SANS Training Program for CISSP® Certification  
Seth Misenar .......................... Chart C (RIVERSIDE)  
*Hours: 9:00am – 7:00pm (Day 1)*  
8:00am – 7:00pm (Days 2-5)  
8:00am – 5:00pm (Day 6)*

MGT514: Security Strategic Planning, Policy, and Leadership  
Mark Williams .......................... Port (RIVERSIDE)

MGT516: Managing Security Vulnerabilities: Enterprise and Cloud  
David Hazar .......................... Marlborough B (2ND LEVEL)

ICS410: ICS/SCADA Security Essentials  
Monta Elkins .......................... Churchill A2 (2ND LEVEL)
Enrich Your SANS Experience!

Morning and 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.

SUNDAY, FEBRUARY 2

SPECIAL EVENT
Early Event Check-In | Badge & Courseware Distribution
Sun, Feb 2 | 4:00pm - 6:00pm | Riverside Foyer

Arriving early or planning to attend the Welcome Reception at Fulton Alley? Want to bypass the check-in line on the morning classes begin? The check-in desk will be open during this time to allow you to pick up your badge and courseware on Sunday evening.

SPECIAL EVENT
Security East 2020 Welcome Reception
Sun, Feb 2 | 6:00pm - 9:00pm | Fulton Alley – 600 Fulton Street (4-Minute Walk from the Hilton New Orleans Riverside)

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 New Orleans. Join your peers for a fun evening of bowling, shuffleboard, and darts while watching Super Bowl LIV.

*Event badges are required for admission.

MONDAY, FEBRUARY 3

SPECIAL EVENT
General Session – Welcome to SANS
Speaker: Bryan Simon
Mon, February 3 | 8:00am – 8:30am | River (RIVERSIDE)

Join SANS Principal Instructor Bryan Simon for a 30-minute overview to help you get the most out of your SANS training experience. You will receive event information and learn about programs and resources offered by SANS. This brief session will answer many questions and get your training experience off to a great start. This session will be valuable to all attendees but is highly recommended for first-time attendees.
KEYNOTE
Everything You Ever Learned About Passwords Is Wrong
Speaker: Keith Palmgren
Mon, February 3 | 7:15pm – 9:15pm | River (RIVERSIDE)

Perhaps the worst advice you can give a user is “choose a complex password.” The result is the impossible-to-remember password requiring the infamous sticky note on the monitor. In addition, that password gets used at a dozen sites at home, AND the very same password gets used at work. The final result ends up being the devastating password compromise. In this one-hour talk, we will look at the technical and non-technical (human nature) issues behind passwords. Attendees will gain a more complete understanding of passwords and receive solid advice on creating more easily remembered AND significantly stronger passwords at work and at home, for their users, for themselves and even for their children.

TUESDAY, FEBRUARY 4

SPECIAL EVENT
Coffee & Donuts with the College Students
Tue, February 4 | 7:30am – 9:00am | Riverside Foyer (RIVERSIDE)

Get the inside scoop on what it’s like to pursue a graduate or undergraduate program in cybersecurity from the SANS Technology Institute (SANS.edu) from admissions specialists and students currently enrolled in SANS.edu programs. Learn about SANS’ regionally accredited master’s degree and graduate certificate programs for InfoSec professionals and undergraduate certificate program for people seeking to launch a cybersecurity career. Find out if the class you’re taking this week or GIAC certifications you’ve earned may be applied towards a SANS.edu program. Visit www.sans.edu for information on curriculum, admissions, and funding options.

SPECIAL EVENT
Community Connect Informational Session
Tue, February 4 | 6:30pm – 7:30pm | Port (RIVERSIDE)

Come out and learn how you working with your favorite InfoSec organization and company can collaborate with Community SANS to positively give back to your local neighborhood. Community CONNECT is composed of two events which take place directly in your hometown. The first is an organized week-long training in which you, working with your company, choose from a plethora of SANS courses. The second part is an @night event in which Community SANS brings together your community leaders and InfoSec organizations to hear a riveting cyber talk as well as learn more about key Community SANS platforms beneficial for women, high school students, college students, vets, minorities, and senior cyber professionals.
Enterprise Security Architecture – It May Not Be What You Think!

Speaker: Mark Williams
Tue, February 4  |  7:15pm – 8:15pm  |  Compass (RIVERSIDE)

You have likely heard the term, unless you reside under a rock. But what is it? Is it the same as all these other “Architect” positions and ideas we hear about? How does it relate to engineering? Are engineers also architects? Why do we need this “Enterprise” model? Enterprise Security architecture is a unique specialty which straddles Enterprise Architecture and Security. There are both structural and practical aspects that make it different. Come and learn what some of these differences are, and how they play out in practical ideas, that are generated by EISA. Mark has an interesting presentation that includes real life examples of solutions to the questions of the day for many enterprises, like “how do we relate our goals to defined measurement criteria or KPIs?” We will show how an organizations’ goals can be translated into actionable steps by the Information Security team members.

Who’s in Your Wallet?
Capital One Debrief and Post Mortem

Speaker: Eric Johnson
Tue, February 4  |  7:15pm – 8:15pm  |  River (RIVERSIDE)

Join Eric Johnson for a walk-through of the Capital One breach. We will demonstrate how the attacker compromised Amazon Web Services virtual machine credentials, gained access to privileged resources, and exfiltrated data from the account. The conversation then shifts to a post mortem discussion about cloud security controls that could have prevented or limited the blast radius of the attack.

Virtuous Cycles: Rethinking the SOC for Long-Term Success

Speaker: John Hubbard
Tue, February 4  |  8:15pm – 9:15pm  |  Compass (RIVERSIDE)

Many Security Operations Centers (SOCs) have a burnout problem that leads to negativity and constant turnover. With the cybersecurity talent shortage, keeping the people we have will only become increasingly important. The problem is that “Tier 1” and other SOC roles historically seem to quickly burn people out. So what do we do? While the field of psychology understands the factors that cause burnout, many SOCs do not take the time to do the research and create an environment to fight it. Though meticulously defined process and analyst tiering may be the norm, does it lead to sacrificing quality and happiness in the long term? Using science-backed research on intrinsic motivation and studies on SOC burnout factors, this talk will make the case that it’s time to reconsider how we structure SOCs in order to create long-term success that benefits both the individual and the organization.
We have had tools and technology to help us identify vulnerabilities for over 20 years. The Nessus project began in 1998. Qualys and Rapid7 released products shortly thereafter. Tools for identifying vulnerabilities in code were made available around the same time with AppScan, Fortify, WebInspect, and Acunetix being just a handful of early options. The number of identification mechanisms and the maturity of tools has greatly increased over the years, yet we still struggle to eliminate vulnerabilities in our environments. Why can’t we solve this seemingly simple problem? Obviously, identification is not the key to effective vulnerability management. So, what should we be doing and what are some of the reasons we are failing? Join me as I share examples of the struggles many of my clients are facing and discuss the best practices that can help organizations avoid these failures.

**WEDNESDAY, FEBRUARY 5**

**SANS@NIGHT**

**Machine Learning and Network Monitoring: Welcome to the Machine**

**Speaker: David Hoelzer**

**Wed, February 5 | 7:15pm – 8:15pm | River (RIVERSIDE)**

Is machine learning all just snake oil today, or are there practical applications that can be made that make your life easier? In this presentation, David Hoelzer will talk about the current trends and then walk you through demonstrations of machine learning methods applied to real network monitoring problems.

**SANS@NIGHT**

**What is New with Volatility 3.0: Memory Forensics on the Rails**

**Speaker: Alissa Torres**

**Wed, February 5 | 7:15pm – 8:15pm | Compass (RIVERSIDE)**

Memory analysis is critical in incident investigations today, particularly those involving sophisticated malicious code. The Volatility Memory Forensics Framework has been a go-to tool for forensic examiners and incident responders for the last ten years. Join Alissa to learn what enhancements are introduced with this latest 3.0 version as well as tips on authoring your own custom plug-ins.

**SANS@NIGHT**

**Web Apps Dripping with Honey**

**Speaker: Mick Douglas**

**Wed, February 5 | 8:15pm – 9:15pm | River (RIVERSIDE)**

Web applications are under constant attack. To make matters worse, the defenses have been relatively static for years. Couple that in with known frameworks, and you have the relative dumpster fire that web app security has been. Attendees of this talk will learn various defenses that are low cost/low risk yet highly effective.
Hands-On Information Security Challenges

“NetWars takes the concepts in the class and gives you an opportunity to put them into action. Highly recommended!”

– Kyle McDaniel, Lenovo

Hosted by Jeff McJunkin
Thu, Feb 6 & Fri, Feb 7
6:30pm – 9:30pm
River (RIVERSIDE)

Hosted by Eric Conrad
Thu, Feb 6 & Fri, Feb 7
7:15pm – 10:15pm
Compass (RIVERSIDE)

Hosted by Heather Mahalik & Philip Hagen
Thu, Feb 6 & Fri, Feb 7
6:30pm – 9:30pm
Chart A (RIVERSIDE)

All students who register for a 5- or 6-day course are eligible to play NetWars for FREE.

Space is limited. Please visit the Registration Support desk to register today.
Add a GIAC Certification to your SANS training at Security East 2020 and **SAVE $300!**

In the information security industry, certification matters. GIAC Certifications offer skills-based certifications that go beyond high-level theory and test true hands-on and pragmatic skill sets that are highly regarded.

Pay just $799 when you bundle your certification attempt with your SANS training course during Security East 2020 for a savings of $300! After this event is over, the alumni bundle price goes to $1,149.

Stop by the Registration Support Desk or via your Portal Account www.sans.org/account/login?url=history to add your GIAC certification attempt before the last day of class for the discount.

*Find out more about GIAC at www.giac.org or call 301-654-7267.*
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scottsdale</td>
<td>Scottsdale, AZ</td>
<td>Feb 17-22</td>
</tr>
<tr>
<td>San Diego</td>
<td>San Diego, CA</td>
<td>Feb 17-22</td>
</tr>
<tr>
<td>Jacksonville</td>
<td>Jacksonville, FL</td>
<td>Feb 24-29</td>
</tr>
<tr>
<td>N. VA – Reston Spring</td>
<td>Reston, VA</td>
<td>Mar 2-7</td>
</tr>
<tr>
<td>St. Louis</td>
<td>St. Louis, MO</td>
<td>Mar 8-13</td>
</tr>
<tr>
<td>Dallas</td>
<td>Dallas, TX</td>
<td>Mar 9-14</td>
</tr>
<tr>
<td>Wild West Hackin Fest</td>
<td>San Diego, CA</td>
<td>Mar 10-11</td>
</tr>
<tr>
<td>Norfolk</td>
<td>Norfolk, VA</td>
<td>Mar 16-21</td>
</tr>
<tr>
<td>San Francisco Spring</td>
<td>San Francisco, CA</td>
<td>Mar 16-27</td>
</tr>
<tr>
<td>Seattle Spring</td>
<td>Seattle, WA</td>
<td>Mar 23-28</td>
</tr>
<tr>
<td>Philadelphia</td>
<td>Philadelphia, PA</td>
<td>Mar 30 – Apr 4</td>
</tr>
<tr>
<td>SANS 2020</td>
<td>Orlando, FL</td>
<td>Apr 3-10</td>
</tr>
<tr>
<td>Bethesda</td>
<td>Bethesda, MD</td>
<td>Apr 14-19</td>
</tr>
<tr>
<td>Minneapolis</td>
<td>Minneapolis, MN</td>
<td>Apr 14-19</td>
</tr>
<tr>
<td>Boston Spring</td>
<td>Boston, MA</td>
<td>Apr 20-25</td>
</tr>
<tr>
<td>Pen Test Austin</td>
<td>Austin, TX</td>
<td>Apr 27 – May 2</td>
</tr>
<tr>
<td>Baltimore Spring</td>
<td>Baltimore, MD</td>
<td>Apr 27 – May 2</td>
</tr>
<tr>
<td>Security West</td>
<td>San Diego, CA</td>
<td>May 6-13</td>
</tr>
<tr>
<td>N. VA – Alexandria</td>
<td>Alexandria, VA</td>
<td>May 17-22</td>
</tr>
<tr>
<td>San Antonio</td>
<td>San Antonio, TX</td>
<td>May 17-22</td>
</tr>
<tr>
<td>Atlanta Spring</td>
<td>Atlanta, GA</td>
<td>May 26-31</td>
</tr>
<tr>
<td>Nashville Spring</td>
<td>Nashville, TN</td>
<td>May 26-31</td>
</tr>
<tr>
<td>Chicago Spring</td>
<td>Chicago, IL</td>
<td>Jun 1-6</td>
</tr>
<tr>
<td>New Orleans</td>
<td>New Orleans, LA</td>
<td>Jun 8-13</td>
</tr>
<tr>
<td>Las Vegas Summer</td>
<td>Las Vegas, NV</td>
<td>Jun 8-13</td>
</tr>
<tr>
<td>SANSFIRE</td>
<td>Washington, DC</td>
<td>Jun 13-20</td>
</tr>
</tbody>
</table>
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.

Webcasts

Ask the Experts Webcasts
SANS experts bring current and timely information on relevant topics in IT security.

Analyst Webcasts
A follow-on to the SANS Analyst Program, Analyst Webcasts provide key information from our whitepapers and surveys.

WhatWorks Webcasts
The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT security issues.

Tool Talks
Tool Talks are designed to give you a solid understanding of a problem, and how a vendor’s commercial tool can be used to solve or mitigate that problem.

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)
Advance your career and protect your organization with cybersecurity training and GIAC certifications. Choose from 11 hands-on, immersion style courses.

SAVE $300! Register and pay by March 25th. Use code EarlyBird20.

Register Now: sans.org/san-antonio

Community SANS – Our Most Popular Courses Taught by Up-and-Coming Instructors in Small Classroom Settings in Local and Regional Areas Near You

With smaller classes, you get more direct interaction with your instructor, and the regional location means an easier, less expensive commute. View upcoming events or request a course that fits your organization’s needs.

“SANS offers the best value-for-money courses and content out there. I’ve learned so much from SANS and hope to learn more in the future.” ~Ashwin Venkat, F5 Networks

San Antonio 2020
May 17-22 | NET WARS

Learn More: sans.org/community
Do You Have the Skills to Become a Bounty Hunter?

Bug bounty programs are used by many IT companies, including the world’s largest firms such as Google, Microsoft, and Facebook. Researchers are full of ideas and know clever tactics from which much can be learned about mixing manual and automated techniques. In SEC552 you will learn how to apply modern attack techniques to discover and disclose tricky, logic-based application flaws that automated scanning tools will not reveal.

BETA COURSE
Learn More: sans.org/SEC552

SEC552:
Bug Bounties and Responsible Disclosure

Do You Have the Skills to Produce Actionable Intelligence in 90 Minutes or Less?

The new FOR498 course will teach you the skills to quickly and properly identify, collect, preserve, and respond to data from a wide range of storage devices and repositories, ensuring that the integrity of evidence is beyond reproach.

NEW COURSE
Learn More: sans.org/FOR498

FOR498: Battlefield Forensics & Data Acquisition

“This is a great course & would be especially beneficial for people just starting in the field.” — S. Lewis, U.S. Air Force
Security East 2021
Hyatt Regency New Orleans
January 11-18, 2021