Kick off your SANS Security East 2018 experience at the Welcome Networking Reception

January 7 | 6:00pm - 9:00pm

Location:
Fulton Alley
600 Fulton Street, New Orleans, LA 70130

Food and beverages provided for all registered SANS Security East 2018 attendees!

Network with industry peers, SANS instructors, and professionals in cybersecurity.

Engage and make connections. Get to know your fellow attendees. Reconnect with old friends and make new contacts.

Find out how to make the most of your week at SANS Security East 2018.

Attendees must pick up their event name badge at Registration Sunday, January 7 from 4:00pm-6:00pm. Event name badges are required for admission to the Welcome Networking Reception. If you are NOT able to pick up your badge from 4:00-6:00pm, SANS staff will be on-site to assist you with entry into the reception.
Hosted by Rob Lee & Jake Williams
Thu, Jan 11 & Fri, Jan 12
6:30pm - 9:30pm  |  Location: Compass

Hosted by Eric Conrad & Seth Misenar
Thu, Jan 11 & Fri, Jan 12
7:15pm - 10:15pm  |  Location: Chart A

All students who register for a 4-6 day course will be eligible to play NetWars for FREE.

Space is limited. Please visit the Registration Support desk to register today.
**GENERAL INFORMATION**

**Badge & Courseware Distribution**  
*Location: Riverside Registration*  
Sun, Jan 7 ........................................ 4:00pm - 6:00pm  
Mon, Jan 8 ........................................ 7:00am - 9:00am

**Registration Support**  
*Location: Bridge (Riverside)*  
Tue, Jan 9 - Sat, Jan 13 ......................... 9:00am - 5:00pm

**Internet Café**  
*Location: Riverside Foyer*  
Mon, Jan 8 ........................................ Opens at Noon  
Tue, Jan 9 - Fri, Jan 12 ....................... Open 24 hours  
Sat, Jan 13 ........................................ Closes at 2:00pm

**Course Times**  
*All full-day courses will run 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

**First Time at SANS?**  
Please attend our Welcome to SANS talk designed to help you get the most from your SANS training experience. The talk is from 8:00am - 8:30am on Monday, January 8 in River.
**Photography Notice**
SANS may take photos of classroom activities for marketing purposes. SANS Security East 2018 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 4–5.

*Bootcamps (Attendance Mandatory)*
- **SEC401**: Security Essentials Bootcamp Style
- **SEC511**: Continuous Monitoring and Security Operations
- **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, Exploits, and Incident Handling
- **SEC560**: Network Penetration Testing and Ethical Hacking
- **MGT512**: SANS Security Leadership Essentials for Managers with Knowledge Compression™
<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Instructor(s)</th>
<th>Location</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC301</td>
<td><strong>Intro to Information Security</strong></td>
<td>Keith Palmgren</td>
<td>Chart C (Riverside)</td>
<td></td>
</tr>
<tr>
<td>SEC401</td>
<td><strong>Security Essentials Bootcamp Style</strong></td>
<td>Bryan Simon</td>
<td>Kabacoff (Riverside)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Bootcamp Hours: 5:00pm - 7:00pm</td>
<td>(Course days 1-5)</td>
</tr>
<tr>
<td>SEC503</td>
<td><strong>Intrusion Detection In-Depth</strong></td>
<td>David Hoelzer</td>
<td>Quarter Deck B (Riverside)</td>
<td></td>
</tr>
<tr>
<td>SEC504</td>
<td><strong>Hacker Tools, Techniques, Exploits &amp; Incident Handling</strong></td>
<td>Michael Murr</td>
<td>River (Riverside)</td>
<td>Extended Hours: 5:00pm - 7:15pm (Course Day 1 only)</td>
</tr>
<tr>
<td>SEC511</td>
<td><strong>Continuous Monitoring and Security Operations</strong></td>
<td>Eric Conrad</td>
<td>Chart A (Riverside)</td>
<td>Bootcamp Hours: 5:15pm - 7:00pm (Course days 1-5)</td>
</tr>
<tr>
<td>SEC542</td>
<td><strong>Web App Penetration Testing and Ethical Hacking</strong></td>
<td>Moses Hernandez</td>
<td>Quarter Deck C (Riverside)</td>
<td></td>
</tr>
<tr>
<td>SEC555</td>
<td><strong>SIEM with Tactical Analytics</strong></td>
<td>Seth Misenar, Mick Douglas</td>
<td>Steering (Riverside)</td>
<td></td>
</tr>
<tr>
<td>SEC560</td>
<td><strong>Network Penetration Testing and Ethical Hacking</strong></td>
<td>Bryce Galbraith</td>
<td>Fulton (3rd Floor)</td>
<td>Extended Hours: 5:00pm - 7:15pm (Course Day 1 only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Extended hours will be led by Michael Murr in the SEC504 classroom located in River</td>
</tr>
<tr>
<td>SEC566</td>
<td><strong>Implementing and Auditing the Critical Security Controls – In-Depth</strong></td>
<td>James Tarala</td>
<td>Starboard (Riverside)</td>
<td></td>
</tr>
<tr>
<td>SEC573</td>
<td><strong>Automating Information Security with Python</strong></td>
<td>Mark Baggett</td>
<td>Eglinton Winton (2nd Floor)</td>
<td></td>
</tr>
</tbody>
</table>
SEC579: Virtualization and Software-Defined Security  
Dave Shackleford. Location: Quarter Deck A (Riverside)

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking  
Tim Medin. Location: Chequers (2nd Floor)  
Bootcamp Hours: 5:15pm - 7:00pm (Course days 1-5)

FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting  
Rob Lee. Location: Compass (Riverside)

FOR578: Cyber Threat Intelligence  
Robert M. Lee. Location: Marlborough A (2nd Floor)

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques  
Jake Williams. Location: Prince of Wales (2nd Floor)

MGT414: SANS Training Program for CISSP® Certification  
David R. Miller. Location: Parish (3rd Floor)  
Bootcamp Hours: 8:00am - 9:00am (Course days 2-6) & 5:00pm - 7:00pm (Course days 1-5)

MGT512: SANS Security Leadership Essentials for Managers with Knowledge Compression™  
G. Mark Hardy. Location: Marlborough B (2nd Floor)  
Extended Hours: 5:00pm - 6:00pm (Course days 1-4)

MGT514: IT Security Strategic Planning, Policy, and Leadership  
Ted Demopoulos. Location: Port (Riverside)

DEV540: Secure DevOps and Cloud Application Security  
Eric Johnson. Location: Cambridge (2nd Floor)

ICS410: ICS/SCADA Security Essentials  
Paul (Monta) Elkins, Billy Rios. Location: Chart B (Riverside)
Add a GIAC Certification with your SANS training at SANS Security East 2018 and SAVE $370!

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 in the InfoSec industry.

Pay just $729 when you bundle your certification attempt with your SANS training course during SANS Security East 2018 for a savings of $370! After this event is over, the alumni bundle price goes to $1,099.

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.
Enrich your SANS experience!

Morning and evening talks given 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, JANUARY 7

SPECIAL EVENT

Welcome Networking Reception

Sunday, January 7 | 6:00pm - 9:00pm
Location: Fulton Alley, 600 Fulton Street, New Orleans, LA 70130

Kick off your SANS Security East 2018 experience at the Welcome Networking Reception taking place at Fulton Alley. 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 New Orleans. Come join your colleagues for a fun, relaxing evening.

Event name badges are required for admission to the Welcome Networking Reception. If you are NOT able to pick up your badge from 4:00pm - 6:00pm, SANS staff will be on-site to assist you with entry into the reception.

MONDAY, JANUARY 8

SPECIAL EVENT

General Session – Welcome to SANS

Speaker: Bryan Simon
Monday, January 8 | 8:00am - 8:30am | Location: River (Riverside)

Join us 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.
 Organizations relying on third parties to detect breaches can go almost a full year before finding out they have been compromised. Detect the breach yourself, and on average you will find it within about a month of the initial occurrence. Mistaking detection and defense against modern adversaries as “too costly” to perform can result in a very expensive miscalculation – especially when you consider the substantially increased price of response and recovery with breach duration. Seth Misenar’s ever-evolving Actionable Detects provides you with the tactics, techniques, and procedures to once again take pride in your Blue Team cyber capabilities. Not applying these lessons learned could prove costly in the face of adapting threat actors. Dig in and learn to hold your head high when talking about your defensive cyber operations capabilities.

Threat actors are not magic and there is not an unlimited, unique list of threats for every organization. Enterprises face similar threats from similar threat sources and threat actors, so why does every organization need to perform completely unique risk assessments and prioritized control decisions? This presentation will show how specific, community-driven threat models can be used to prioritize an organization’s defenses – without all the confusion. James Tarala will present a new, open, community-driven threat model that can be used by any industry to evaluate the risk they face. Then he will show how to practically use this model to prioritize enterprise defense and map to compliance requirements for organizations today. Whether you are in the Department of Defense or work for a small mom-and-pop retailer, you will be able to use this model to specifically determine a prioritized defense for your organization.
Blockchain: the New Digital Swiss Army Knife?

Speaker: G. Mark Hardy

Tuesday, January 9  |  7:15pm - 8:15pm  |  Location: Chart C (Riverside)

Now that the price of a single Bitcoin surpasses the price of an ounce of gold, is blockchain becoming a runaway train with businesses scrambling to hop on? If so, how can you take advantage of this opportunity, and will the mistakes be minor or catastrophic? Blockchain as a technology has been proposed as a solution to everything from frictionless currency transfer to tracking cargo on ships. With over $1 billion in venture funds invested and several hundred patents filed, every security professional must know the impact on organizations in terms of risk, volatility, and competitiveness. This talk will explore alternative uses for blockchain technology other than cryptocurrency, and provide a framework for utilizing and securing a technology considered as disruptive as the Internet was in the 1990s.

Infosec Rock Star: Geek Will Only Get You So Far

Speaker: Ted Demopoulos

Tuesday, January 9  |  8:15pm - 9:15pm  |  Location: Chart B (Riverside)

Some of us are so effective, and well known, that the term “Rock Star” is entirely accurate. What kind of skills do Rock Stars have and wannabe Rock Stars need to develop? Although we personally may never be swamped by groupies, we can learn the skills to be more effective, well respected, and well paid. Obviously it’s not just about technology; in fact most of us are very good at the technology part. The fact is that increasing our skills more on the social and business side will make most of us more effective at what we do than learning how to read hex better while standing on our heads, becoming “One with Metasploit,” or understanding the latest hot technologies.
Come attend this session and catch up with the latest InfoSec news and how it impacts your organization. In this session, we’ll talk about Russian election hacking, FBI investigative techniques, implications of the latest Shadow Brokers dumps, software product liability, DoJ protecting government exploits and more. Come hang with us for this session, and you’ll walk away bigger, badder, and smarter.

Web application development is a craft, and like all craftsmen, I sought to produce the highest-quality code I could as well as help the other developers around me produce higher quality code as well. I worked on my coding skills diligently and never stopped learning or practicing. And eventually I got my first introduction into the world of web application security. It was this that started me down a path of realizing that security and secure coding practices are an integral part to code quality. In this presentation, I will share my journey from developer to penetration tester, while pointing out the important lessons learned along the way. I will also be sharing tips and tools to help practice and hone your skills as well.

There have only ever been four pieces of ICS-tailored malware, and only one of those specifically targeted and disrupted a power grid: CRASHOVERRIDE. In this presentation, one of the security researchers who analyzed CRASHOVERRIDE will present the full timeline, including the 2015 and 2016 cyber attack on Ukraine’s power grid, analysis of the malware and what it is and is not capable of with relation to grid-impact scenarios, and detection and mitigation recommendations for defending against this and similar tradecraft. Participants can expect to leave the presentation with a deep appreciation of what security professionals must be doing as well as why the investments made into the security of infrastructure such as the power grid have so far put us in a great defensible situation.
SPECIAL EVENT

Coffee & Donuts with the Graduate Students

Thursday, January 11 | 7:30am - 9:00am | Location: Riverside Lobby Foyer

Get the inside scoop on what it’s like to pursue a graduate degree in cybersecurity from SANS from like-minded information security professionals currently enrolled in the SANS graduate programs. SANS’ regionally accredited graduate program, the SANS Technology Institute, combines SANS technical training and certifications, with leadership and management curriculum specifically designed for the unique needs of aspiring leaders. Find out how the class you’re taking this week may be applied towards a master’s degree or graduate certificate program. Visit www.sans.edu for complete information on curriculum, admissions, and funding options.

SPECIAL EVENT

Core NetWars Experience

Hosted by Bryce Galbraith

Thursday, January 11 & Friday, January 12 | 6:30pm - 9:30pm
Location: River (Riverside)

SANS Core NetWars Experience is a computer and network security challenge designed to test a participant’s experience and skills in a safe, controlled environment while having a little fun with your fellow IT security professionals. Many enterprises, government agencies, and military bases are using NetWars to help identify skilled personnel and as part of extensive hands-on training. With Core NetWars, you’ll build a wide variety of skills while having a great time.

SPECIAL EVENT

DFIR NetWars Tournament

Hosted by Rob Lee & Jake Williams

Thursday, January 11 & Friday, January 12 | 6:30pm - 9:30pm
Location: Compass (Riverside)

SANS DFIR NetWars Tournament is an incident simulator packed with a vast amount of forensic and incident response challenges covering host forensics, network forensics, and malware and memory analysis. It is developed by incident responders and analysts who use these skills daily to stop data breaches and solve crimes. Sharpen your team’s skills prior to being involved in a real incident.

SPECIAL EVENT

Cyber Defense NetWars Experience

Hosted by Eric Conrad & Seth Misenar

Thursday, January 11 & Friday, January 12 | 7:15pm - 10:15pm
Location: Chart A (Riverside)

The all-new NetWars Defense Competition is a defense-focused challenge aimed at testing your ability to solve problems and secure your systems from compromise. With so much focus on offense, NetWars Defense is a truly unique experience and opportunity to test your skills in architecture, operations, threat hunting, log analysis, packet analysis, cryptography, and much more!
Add an OnDemand Bundle to your course to get an additional four months of intense training! OnDemand Bundles are just $729 when added to your live course, and include:

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

**COURSES AVAILABLE:**

- SEC301
- SEC401
- SEC501
- SEC503
- SEC504
- SEC511
- SEC542
- SEC555
- SEC560
- SEC566
- SEC573
- SEC579
- SEC660
- FOR508
- FOR578
- FOR610
- MGT414
- MGT512
- MGT514
- ICS410

To receive the discounted rate, you must sign up before Monday, January 15th at 8:00pm EDT

Add to your order via your Portal Account: www.sans.org/account/login

Call or e-mail SANS Registration:
1-301-654-SANS (7267) | registration@sans.org
Measure your organization's human security risk and educate staff to avoid security threats with SANS Security Awareness training.

1300+ organizations

6.5+M people trained

Learn more at securingthehuman.sans.org
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 (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) how recent attacks worked, and (4) 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.

Other Free Resources

(No portal account is necessary)
- InfoSec Reading Room
- Top 25 Software Errors
- 20 Critical Controls
- Security Policies
- Intrusion Detection FAQs
- Tip of the Day
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)
### Future Training Events

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Location</th>
<th>Dates</th>
<th>#Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>Northern VA Winter</td>
<td>Reston, VA</td>
<td>Jan 15-20</td>
<td>#SANSReston</td>
</tr>
<tr>
<td>Las Vegas</td>
<td>Las Vegas, NV</td>
<td>Jan 28 - Feb 2</td>
<td>#SANSLasVegas</td>
</tr>
<tr>
<td>Miami</td>
<td>Miami, FL</td>
<td>Jan 29 - Feb 3</td>
<td>#SANSMiami</td>
</tr>
<tr>
<td>Scottsdale</td>
<td>Scottsdale, AZ</td>
<td>Feb 5-10</td>
<td>#SANSScottsdale</td>
</tr>
<tr>
<td>Southern California – Anaheim</td>
<td>Anaheim, CA</td>
<td>Feb 12-17</td>
<td>#SANSAAnaheim</td>
</tr>
<tr>
<td>Dallas</td>
<td>Dallas, TX</td>
<td>Feb 19-24</td>
<td>#SANSDallas</td>
</tr>
<tr>
<td>New York City Winter</td>
<td>New York, NY</td>
<td>Feb 26 - Mar 3</td>
<td>#SANSNYC</td>
</tr>
<tr>
<td>San Francisco Spring</td>
<td>San Francisco, CA</td>
<td>Mar 12-17</td>
<td>#SANSSanFrancisco</td>
</tr>
<tr>
<td>Northern VA Spring – Tysons</td>
<td>McLean, VA</td>
<td>Mar 17-24</td>
<td>#SANSTysons</td>
</tr>
<tr>
<td>Pen Test Austin</td>
<td>Austin, TX</td>
<td>Mar 19-24</td>
<td>#SANSAustin</td>
</tr>
<tr>
<td>Boston Spring</td>
<td>Boston, MA</td>
<td>Mar 25-30</td>
<td>#SANSBoston</td>
</tr>
<tr>
<td><strong>SANS 2018</strong></td>
<td>Orlando, FL</td>
<td>Apr 3-10</td>
<td>#SANS2018</td>
</tr>
<tr>
<td><strong>Baltimore Spring</strong></td>
<td>Baltimore, MD</td>
<td>Apr 21-28</td>
<td>#SANSBaltimore</td>
</tr>
<tr>
<td><strong>Seattle Spring</strong></td>
<td>Seattle, WA</td>
<td>Apr 23-28</td>
<td>#SANSSeattle</td>
</tr>
<tr>
<td>Security West</td>
<td>San Diego, CA</td>
<td>May 11-18</td>
<td>#SANSSecurityWest</td>
</tr>
</tbody>
</table>

### Future Summit Events

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Location</th>
<th>Dates</th>
<th>#Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Threat Intelligence</td>
<td>Bethesda, MD</td>
<td>Jan 29 - Feb 5</td>
<td>#SANSCTISummit</td>
</tr>
<tr>
<td>Cloud Security</td>
<td>San Diego, CA</td>
<td>Feb 19-26</td>
<td>#SANSCloudSummit</td>
</tr>
<tr>
<td>ICS Security</td>
<td>Orlando, FL</td>
<td>Mar 19-26</td>
<td>#SANSICSSummit</td>
</tr>
</tbody>
</table>
Join us again next year!

Security East 2019
New Orleans, LA | February 4-9, 2019

Save the Date!