SANS

Network Security 2018

Las Vegas | September 23-30

Program Guide

#SANSNetworkSecurity @SANSInstitute

SANS OnDemand

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	SEC555	FOR578
SEC401	SEC560	FOR585
SEC440	SEC566	FOR610
SEC455	SEC573	MGT414
SEC501	SEC575	MGT433
SEC503	SEC642	MGT512
SEC504	SEC660	MGT514
SEC505	FOR500	DEV522
SEC506	FOR508	DEV544
SEC511	FOR518	LEG523
SEC542	FOR526	ICS410
	FOR572	

To receive the discounted rate, you must sign up before Monday, Oct 1 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

TABLE OF CONTENTS

General Information 2-3
Course Schedule 4-6
GIAC Certifications 7
Bonus Sessions 8-14
SANS NetWars 14
Free SANS Resources 15
Vendor Events 16-18
Future SANS Training Events 19
Hotel Floorplans 20-21

First Time at SANS?

Please attend our **Welcome to SANS** talk designed to help you get the most from your SANS training experience.

Bryan Simon
Sunday, September 23
8:00am-8:30am

Location:
Roman III

GENERAL INFORMATION

Event Check-In | Badge & Courseware Distribution

Roman I Ballroom

Sat, September 22 (Welcome Reception) . . . . 5:00pm - 7:00pm
Sun, September 23. . . . . 7:00am - 9:00am

Octavius Ballroom Foyer

Sat, September 29 (2-Day Courses) . . . . . 8:00am - 9:00am

Registration Support

Registration Desk – Promenade Foyer

Sun, September 23. . . . . 9:00am - 7:00pm
Mon, September 24 – Thu, September 27 . . . . 8:00am - 5:00pm
Fri, September 28. . . . . 8:00am - 2:00pm

Internet Café

Imperial Boardroom

Sun, September 23 . . . . . Opens at Noon
Mon, September 24 – Thu, September 27 . . . . . Open 24 hours
Fri, September 28 . . . . . 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

Photography Notice

SANS may take photos of classroom activities for marketing purposes. Network Security 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 4-6.

Bootcamps (Attendance Mandatory)

SEC401: Security Essentials Bootcamp Style

SEC503: Intrusion Detection In-Depth

SEC511: Continuous Monitoring and Security Operations

SEC555: SIEM with Tactical Analytics

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

SEC760: Advanced Exploit Development for Penetration Testers

MGT414: SANS Training Program for CISSP® Certification

Extended Hours:

SEC455: SIEM Design & Implementation

SEC501: Advanced Security Essentials - Enterprise Defender

SEC504: Hacker Tools, Techniques, Exploits & Incident Handling

SEC560: Network Penetration Testing and Ethical Hacking

MGT512: SANS Security Leadership Essentials for Managers with Knowledge Compression™

COURSE SCHEDULE

START DATE: **Sunday, September 23, 2018**
Time: 9:00am - 5:00pm (Unless otherwise noted)

SEC301: Introduction to Cyber Security
Keith Palmgren . . . . . Florentine I (PROMENADE)

SEC401: Security Essentials Bootcamp Style
Bryan Simon . . . . . Milano VII/VIII (PROMENADE)
Bootcamp Hours: 5:00pm - 7:00pm (Course days 1-5)

SEC460: Enterprise Threat and Vulnerability Assessment
Tim Medin . . . . . Sorrento (PROMENADE)

SEC487: Open-Source Intelligence Gathering (OSINT) and Analysis
Micah Hoffman . . . . . Capri (PROMENADE)

SEC501: Advanced Security Essentials - Enterprise Defender
Bryce Galbraith . . . . . Octavius 1/2 (PROMENADE SOUTH)
Extended Hours: 5:00pm - 7:00pm (Course day 1)

SEC503: Intrusion Detection In-Depth
David Hoelzer . . . . . Milano I (PROMENADE)
Bootcamp Hours: 5:00pm - 7:00pm (Course days 1-5)

SEC504: Hacker Tools, Techniques, Exploits & Incident Handling
John Strand . . . . . Roman II (PROMENADE)
Extended Hours: 5:00pm - 7:15pm (Course day 1)

SEC505: Securing Windows and PowerShell Automation
Jason Fossen . . . . . Octavius 14 (PROMENADE SOUTH)

SEC506: Securing Linux/Unix
Hal Pomeranz . . . . . Octavius 15/16 (PROMENADE SOUTH)

SEC511: Continuous Monitoring and Security Operations
Seth Misenar . . . . . Octavius 17/18 (PROMENADE SOUTH)
Bootcamp Hours: 5:15pm - 7:00pm (Course days 1-5)

SEC530: Defensible Security Architecture
Eric Conrad . . . . . Octavius 21/22 (PROMENADE SOUTH)

SEC542: Web App Penetration Testing and Ethical Hacking
Hassan El Hadary . . . . . Verona (PROMENADE)

SEC545: Cloud Security Architecture and Operations
Dave Shackleford . . . . . Neopolitan IV (PROMENADE)

SEC555: SIEM with Tactical Analytics
Justin Henderson . . . . . Octavius 20 (PROMENADE SOUTH)
Bootcamp Hours: 5:15pm - 7:00pm (Course days 1-5)

SEC560: Network Penetration Testing and Ethical Hacking
Ed Skoudis . . . . . Roman IV (PROMENADE)
Extended Hours: 5:00pm - 7:15pm (Course day 1)
Extended hours will be led by John Strand in the SEC504 classroom located in Milano I (PROMENADE)

SEC566: Implementing and Auditing the Critical Security Controls – In-Depth
James Tarala . . . . . Florentine II (PROMENADE)

SEC573: Automating Information Security with Python
Mark Baggett . . . . . Milano V (PROMENADE)

SEC575: Mobile Device Security and Ethical Hacking
Joshua Wright . . . . . Octavius 7 (PROMENADE SOUTH)

SEC599: Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses
Erik Van Buggenhout . . . . . Milano III (PROMENADE)

SEC617: Wireless Penetration Testing and Ethical Hacking
Larry Pesce . . . . . Trevi (PROMENADE)

SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques
Adrien de Beaupre . . . . . Octavius 13 (PROMENADE SOUTH)

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
Brandon McCrillis, Stephen Sims . . Octavius 11 (PROMENADE SOUTH)
Bootcamp Hours: 5:15pm - 7:00pm (Course days 1-5)

SEC760: Advanced Exploit Development for Penetration Testers
Jake Williams . . . . . Octavius 6 (PROMENADE SOUTH)
Bootcamp Hours: 5:15pm - 7:00pm (Course days 1-5)

FOR500: Windows Forensic Analysis
Rob Lee . . . . . Florentine III (PROMENADE)

FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting
Chad Tilbury . . . . . Florentine IV (PROMENADE)

FOR518: Mac and iOS Forensic Analysis and Incident Response
Sarah Edwards . . . . . Pisa (PROMENADE)

FOR526: Memory Forensics In-Depth
Alissa Torres . . . . . Anzio (PROMENADE)

FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response
Philip Hagen . . . . . Neopolitan I (PROMENADE)

FOR578: Cyber Threat Intelligence
Peter Szczepankiewicz . . . . . Octavius 19 (PROMENADE SOUTH)

FOR585: Advanced Smartphone Forensics
Heather Mahalik . . . . . Neopolitan III (PROMENADE)

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Lenny Zeltser . . . . . Milano VI (PROMENADE)

MGT414: SANS Training Program for CISSP® Certification
David R. Miller . . . . . Octavius 9/10 (PROMENADE SOUTH)
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 . . . . . Milano II (PROMENADE)
Extended Hours: 5:00pm - 6:00pm (Course days 1-4)

MGT514: Security Strategic Planning, Policy, and Leadership
Frank Kim . . . . . Milano IV (PROMENADE)

COURSE SCHEDULE

MGT517: Managing Security Operations: Detection, Response, and Intelligence
Christopher Crowley . . . . . Turin (PROMENADE)

MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep
Jeff Frisk. . . . . Octavius 5 (PROMENADE SOUTH)

DEV522: Defending Web Applications Security Essentials
Dr. Johannes Ullrich. . . . . Salerno (PROMENADE)

DEV540: Secure DevOps and Cloud Application Security
Eric Johnson . . . . . Neopolitan II (PROMENADE)

DEV544: Secure Coding in .NET: Developing Defensible Applications
Aaron Cure . . . . . .Messina (PROMENADE)

LEG523: Law of Data Security and Investigations
Benjamin Wright . . . . . .Octavius 8 (PROMENADE SOUTH)

ICS410: ICS/SCADA Security Essentials
Justin Searle . . . . . Octavius 3 (PROMENADE SOUTH)

HOSTED: Physical Security Specialist – Full Comprehensive Edition
The CORE Group. . . . . Livorno (PROMENADE)

START DATE: **Saturday, September 29, 2018**
Time: 9:00am - 5:00pm (Unless otherwise noted)

SEC440: Critical Security Controls: Planning, Implementing, and Auditing
Chris Christianson . . . . . Octavius 9/10 (PROMENADE SOUTH)

SEC455: SIEM Design & Implementation
John Hubbard. . . . . Octavius 11 (PROMENADE SOUTH)
Extended Hours: 5:00pm - 6:00pm (Course day 1)
8:00am - 9:00am (Course day 2)

SEC524: Cloud Security Fundamentals
Jorge Orchilles . . . . . Octavius 14 (PROMENADE SOUTH)

SEC564: Red Team Operations and Threat Emulation
Joe Vest . . . . . Octavius 15/16 (PROMENADE SOUTH)

SEC580: Metasploit Kung Fu for Enterprise Pen Testing
Jeff McJunkin. . . . . Octavius 17/18 (PROMENADE SOUTH)

MGT415: A Practical Introduction to Cyber Security Risk Management
Brian Ventura . . . . . .Octavius 20 (PROMENADE SOUTH)

MGT433: SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program
Lance Spitzner . . . . . Octavius 19 (PROMENADE SOUTH)

DEV531: Defending Mobile Applications Security Essentials
Gregory Leonard . . . . . Octavius 13 (PROMENADE SOUTH)

BONUS SESSIONS

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.

SATURDAY, SEPTEMBER 22

SPECIAL EVENT

Network Security 2018 Welcome Reception

Saturday, September 22 | 5:00pm - 7:00pm | Promenade Foyer

Kick off your Network Security 2018 experience at the Network Security 2018 Welcome Reception taking place in the Promenade Foyer. 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 Las Vegas. Come join your colleagues for a fun, relaxing evening.

SUNDAY, SEPTEMBER 23

SPECIAL EVENT

General Session – Welcome to SANS

Speaker: Bryan Simon

Sunday, September 23 | 8:00am - 8:30am | Roman III

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.

SPECIAL EVENT

WMI Attacks: What You Don't Know CAN Hurt You

Speaker: Chad Tilbury

Sunday, September 23 | 7:15pm - 9:15pm | Roman III

In the spectrum of things that keep enterprise security teams up at night, Windows Management Instrumentation (WMI) should be heading to the forefront. Advanced adversaries are increasingly adding WMI-based attacks to their repertoires, and most teams are woefully unprepared to face this new threat. You need to understand what you are up against, and attendees will leave this presentation with a comprehensive overview of the state of WMI hacking, including real-world examples of nation-state and criminal actor tradecraft. Once you have a strong understanding of the threat, Chad will pivot to defense and discuss detection tools and analysis techniques. While parts of this presentation will necessarily be technical, even less technically oriented attendees will leave with a greater understanding of the threat and a checklist of actionable steps to better increase their organization's security posture.

MONDAY, SEPTEMBER 24

SANS@NIGHT

Traveling Paranoid (But Not Too Paranoid)

Speakers: Philip Hagen and Chris Crowley

Monday, September 24 | 7:15pm - 8:15pm | Florentine I

As every security professional knows, travel can be even more stressful when you're carrying multiple laptops, evidence drives, mobile devices, connection cables, and the like. Whether traveling domestically or internationally, your private data and those of your clients are arguably at the greatest risk when transiting customs or other airport screening points. You must realistically consider whether you would give up encryption passwords or forfeit your hardware at a border crossing, for example. Now, consider how people within your organization would deal with the same challenges. How should you equip them for international and domestic travel without creating an imposition on their busy schedules? How can you keep up with delivering information to traveling staff? What advice do you give them regarding foreign (or domestic) customs agents demanding passwords and data access? What sort of knowledge do you want to develop about attempts to access your information assets while your staff travels? This talk will cover various practical ways we can protect electronic interests in various common situations for you and your organization. We'll cover both preventive measures as well as mechanisms to detect whether your gear has been fiddled with while outside your immediate control. Measures for various operating systems will be addressed, while considering how to maintain practical paranoia without drawing attention to yourself.

SANS@NIGHT

Continuous Security: Monitoring and Active Defense in the Cloud

Speaker: Eric Johnson

Monday, September 24 | 7:15pm - 8:15pm | Florentine III

Monitoring and feedback loops from production is a critical tenant in DevOps for measuring performance, runtime errors, statistics, and changes. In the SecDevOps world, security teams can take advantage of DevOps monitoring tools to increase security visibility, identify anomalies, and respond swiftly to real-time attacks. Cloud providers are offering powerful infrastructure, development, and application continuous monitoring services that generate a wealth of data. But, building continuous security monitoring on top of the data can be challenging. Where are the log files? What is the log file format? What security events are captured? How do we display meaningful metrics? Can we detect and defend in real time? This talk will introduce attendees to a realistic AWS environment's monitoring and active defense system and discuss real data collected during a war-game exercise. Afterwards, we will walk through the postmortem, review the alerts raised during the incident, determine if there were any surprises, and identify opportunities to improve the system. Attendees will walk away with actionable techniques for building an active defense framework to help protect your organization's cloud resources.

BONUS SESSIONS

SANS@NIGHT

So, You Wanna Be a Pentester?

Speaker: Adrien de Beaupre

Monday, September 24 | 7:15pm - 8:15pm | Florentine II

This presentation will discuss the things that you will actually need to become a penetration tester. Be prepared for a no-fluff honest discussion. You will need attitude, aptitude, initiative, desire, dedication, discipline, integrity, ethics, experience, knowledge, and tools.

SANS@NIGHT

"Could We Have Stopped This?" Attack Simulations for Blue Team Hardening

Speaker: Alissa Torres

Monday, September 24 | 7:15pm - 8:15pm | Florentine IV

A post-compromise, post-remediation security team is made up of steely-eyed veterans, tempered by the fire of system ownage and soul-wrenching defense and detection failures. Their experience is invaluable, but arrived at with significant cost to the organization. How can we grow such a hardened blue team of this meddle without the cost and pain of time on the battlefield? Start by going beyond the tabletop walk-throughs and testing the "load bearing" capacity of your threat detection and response (TDR) people, process and technology. Throw your team into simulations of the hard stuff; real-world challenges that model complex multi-pronged attacks. Join Alissa Torres for this one-hour session walk-through of stress-test techniques that develop your blue team, and stop checking annual compliance boxes.

SANS@NIGHT

Hacking Dumberly, Just Like the Bad Guys

Speaker: Tim Medin

Monday, September 24 | 8:15pm - 9:15pm | Florentine II

Tim Medin will discuss the dumbest red team tricks and hacks he's encountered over the years. He is going to take the A out of APT, because so few attackers really need to use advanced techniques. He'll also discuss the simple defenses that make an attacker's life much more difficult.

SANS@NIGHT

Let's Go Hunting Bad Guys

Speaker: John Strand

Monday, September 24 | 8:15pm - 9:15pm | Florentine III

In this presentation, John will share with you custom free tools on hunting bad guys inside and outside of your network...with awesomeness and math. But mostly math.

SANS@NIGHT

Stuck in the Box, a SIEM's Tale

Speaker: Justin Henderson

Monday, September 24 | 8:15pm - 9:15pm | Florentine IV

Organizations often spend excessive amounts of money on Security Information and Event Management (SIEM) products only to end up with a log collection box when they thought they purchased a tactical detection system. Most organizations find themselves with a SIEM but unsure how to use its capabilities. Point solutions are quick to defend deficiencies by stating each environment is different so you, the customer, must tell them what you want the SIEM to do and then they'll help with professional services or by replacing your current SIEM with something "better and more advanced." This is complete hogwash. Organizations tend to have a lot of overlap such as the use of Windows systems or network protocols such as DNS. As such there are high-fidelity detects that can be implemented in every organization. Enough is enough. If you are looking for techniques and methods to get value out of your current SIEM or are interested in seeing how a new open-source big data solution such as the Elastic Stack, formerly ELK, most likely can beat what you have today, then this talk is for you. Fact is that it is time to think outside the box. Come find out how one organization spent 14 months deploying a top magic quadrant SIEM solution to have it beaten by ELK in two weeks.

TUESDAY, SEPTEMBER 25

SPECIAL EVENT

Coffee and Donuts with the Graduate Students

Tuesday, September 25 | 7:30am - 9:00am | Promenade 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

GIAC Overview Presentation

Speaker: Jeff Frisk

Tuesday, September 25 | 6:30pm - 7:15pm | Florentine IV

As the leading provider and developer of Information Security Certifications, GIAC tests and validates the ability of practitioners in cyber defense, pen testing, forensics, software security, management, and ICS. GIAC certification holders are recognized as experts in the IT industry and are sought after globally by government, military, and industry to protect the cyber environment. Join us for an informational presentation along with a Q&A session. We'll cover everything from why you should get certified, what testing looks like, how to keep certifications current and more. GIAC Certifications staff will be present to answer your questions before and after the presentation.

BONUS SESSIONS

SPECIAL EVENT

APAC Student Reception

Tuesday, September 25 | 6:30pm - 7:30pm | Turin

The SANS APAC Student Reception is an informal event to give APAC students the opportunity to meet up with some of your SANS APAC team, SANS instructors, and other students from the APAC region. Food and beverages will be served. ***RSVP by 9/24 to asiapacific@sans.org***

SPECIAL EVENT

An Evening of Hacking the Internet of Things (IoT)

Speakers: Stephen Sims, James Lyne, Tim Medin, and Jim Shewmaker

Tuesday, September 25 | 7:15pm - 10:00pm | Roman I/II

Join Steve, James, Tim, and Jim in this SANS special event. Somewhere along the line product developers thought it would be a good idea to connect things like pet food dispensers, BBQ grills, refrigerators, and many other "items" to the Internet. What could possibly go wrong? We will have a collection of "things" for you to try and find vulnerabilities in, as well as some guided exercises... If you find something interesting you may even be able to take the item home! We'll walk through an introduction of how to extract and analyze firmware, and the types of bugs that are most commonly found, along with some examples. What do you need to bring? A laptop with VMware Player, Workstation, or Fusion, and a copy of Kali Linux. We will have some USB sticks on it with Kali if you forget to bring a copy.

SANS@NIGHT

Responding to the European Union's New General Data Protection Regulation

Speaker: Ben Wright

Tuesday, September 25 | 7:15pm - 8:15pm | Florentine I

The European Union has long been a leader in privacy law. It has now advanced the law with a sweeping new regulation that applies to a broad range of companies around the world, even those that do not have a physical presence in Europe. We will discuss how to manage risk under this new regulation.

SANS@NIGHT

Defense Is Doable: Breaking The Cyber Kill Chain

Speakers: Erik Van Buggenhout & Stephen Sims

Tuesday, September 25 | 7:15pm - 8:15pm | Florentine II

Recent security incidents and breaches often make it look like there's no way of preventing adversaries from compromising your environment. During this fast-paced presentation, Erik Van Buggenhout (SANS Certified Instructor) and Stephen Sims (SANS Fellow) will discuss how advanced adversaries are attempting to penetrate your environment and what you can do to stop or detect them. The talk will focus on principles and techniques that are readily available to all (or most) organizations, WITHOUT breaking the bank to purchase a myriad of commercial tools. The material covered is a sample of the content in our new course, SANS SEC599: Defeating Advanced Adversaries – Implementing Kill Chain Defenses.

SPECIAL EVENT

Women's Connect & SANS Summits Workshop: How to Write Presentation Proposals for Cybersecurity Conferences

Speakers: Alissa Torres, Heather Mahalik, My-Ngoc Nguyen, Phil Hagen, and Sarah Edwards

Tuesday, September 25 | 7:15pm - 8:15pm | Roman III

Just in case no one has said this to you yet, you have an interesting, unique, and important perspective on cybersecurity that is worth sharing. Yes, YOU. The agenda at many cybersecurity events looks like a line-up of the usual suspects. But the community needs to hear diverse viewpoints. While it may feel intimidating to throw your hat into the ring, and no one likes rejection, we need your voice. SANS is committed to identifying and developing talented cybersecurity professionals. In this workshop, some of the top SANS instructors and seasoned industry speakers will arm you with the tools to draft presentation proposals that make it onto the agenda. Join Alissa Torres, Heather Mahalik, My-Ngoc Nguyen, Phil Hagen, and Sarah Edwards, who will share their experience and advice. This is your chance to work through the ideas you've been percolating and get answers to all the questions you haven't been able to ask until now. This workshop is open to anyone interested in building the skills and confidence to deliver presentations at cybersecurity events.

SANS@NIGHT

What is NetWars? Why Play? Feel Intimidated?

Speaker: Jeff McJunkin

Tuesday, September 25 | 7:15pm - 8:15pm | Florentine III

You have NetWars questions... we have NetWars answers! Come to this interactive SANS@Night session with Chief NetWars Challenge Architect, Jeff McJunkin, as he gives an overview of what Netwars is, how it is played, why you shouldn't feel intimidated, and how you can get the most out of your SANS NetWars Experience. We are also looking for experienced NetWars players who would like to be mentors to new players and to lead teams.

SANS@NIGHT

Nation State-Level Honeypotting: Emulating Vulnerable Applications at Scale

Speaker: Dr. Johannes Ullrich

Tuesday, September 25 | 8:15pm - 9:15pm | Florentine I

Honeypots have been used for a long time to learn more about how attackers are targeting and exploiting vulnerable systems. Web applications in particular have been one of the primary targets of attackers and honeypots have been used to understand these attacks better. However, applications are very diverse. Hundreds if not thousands of different vulnerable applications can easily be exploited, and new once are added to the list. In this talk, you will learn how you can participate in our large scale agile honeypot network. A network that can easily be tuned to detect and collect metrics for the attack of the day and a network large enough to rival the size of some nations infrastructure.

BONUS SESSIONS

SANS@NIGHT

Blockchain 101

Speaker: G. Mark Hardy

Tuesday, September 25 | 8:15pm - 9:15pm | Florentine II

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.

NETWARS EXPERIENCE

Hands-On Information Security Challenges

CORE NETWARS EXPERIENCE

Hosted by Jeff McJunkin
Wed, Sept 26 & Thu, Sept 27
6:30pm – 9:30pm
Roman Ballroom

DFIR NETWARS TOURNAMENT

Hosted by Sarah Edwards & Heather Mahalik
Wed, Sept 26 & Thu, Sept 27
6:30pm – 9:30pm
Florentine III/IV

CYBER DEFENSE NETWARS TOURNAMENT

Hosted by Eric Conrad & Seth Misenar
Wed, Sept 26 & Thu, Sept 27
7:15pm – 10:15pm
Florentine I/II

ICS NETWARS EXPERIENCE

Hosted by Tim Conway
Wed, Sept 26
6:30pm – 9:30pm
Pisa

All students who register for a 4-, 5-, or 6-day course will be eligible to play NetWars for FREE. *Space is limited. Please visit the Registration Support desk to register today.*

Sign into your SANS account to enjoy these ***free*** resources at **www.sans.org/account**

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.

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
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

VENDOR EVENTS

Vendor Solutions Expo

Tuesday, September 25 | 12:00pm - 1:30pm | 5:15pm - 7:15pm
Octavius 25 (Entrance through Octavius 4 – Promenade South)

All attendees are invited to meet with established and emerging solution providers as they reveal the latest tools and technologies critical to information security. The SANS Vendor Expo showcases product offerings from key technology providers in the commercial tools and services market. Vendors arrive prepared to interact with a technically savvy audience. You'll find demonstrations and product showcases that feature all the best that the security industry has to offer!

Vendor-Sponsored Lunch Session

Tuesday, September 25 | 12:00pm-1:30pm
Octavius 25 (Entrance through Octavius 4 – Promenade South)

Sign up at the SANS vendor table to receive a ticket for a free lunch brought to you by sponsoring vendors. Please note, by accepting a lunch ticket your badge will be scanned and your contact information shared with the sponsoring vendors. Join these sponsoring vendors and others on the expo floor for an introduction to leading 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.

Luncheon sponsors include:

Anomali
Awake Security
Corelight
Cylance
Graylog
LogRhythm
Panda Security
Pulse Secure
Qualys
Risk IQ
ShieldX
Sophos Terbium Labs
Swimlane
Tripwire
VMRay

Vendor-Sponsored Lunch & Learns

Since SANS course material is product neutral, these presentations provide the opportunity to evaluate vendor tools in an interactive environment to increase your effectiveness, productivity, and knowledge gained from the conference. These sessions feature a light meal or refreshments provided by the sponsor. Sign-up sheets for the events on pages 16-18 are located at the Vendor Registration Desk.

ANOMALI®

LUNCH AND LEARN

The Art of Collaboration

Speaker: Joe Gehrke, Senior Sales Engineer
Monday, September 24 | 12:30pm - 1:15pm | Milano II

Enterprise threat intelligence programs are becoming more common, but how has sharing evolved to support this function? This presentation will examine the current state of sharing and how it's changing to support today's analysts.

TERBIUM LABS
Data Intelligence

LUNCH AND LEARN

Anatomy of How Stolen Data Appears on the Dark Web (and Why You Should Care)

Speaker: Tyler Carbone, Chief Product Officer
Monday, September 24 | 12:30pm - 1:15pm | Milano IV

The dark web is a structured economy which hosts various marketplaces, some dedicated exclusively to trading and selling stolen data. Security organizations are responsible for specific data that is important and valuable to their companies, as well as to criminals who look to monetize that same data. This includes everything from personal data (PII and account credentials) to financial data (payment card details, payroll records) to broader corporate data (employee, executive, and board member personal information, proprietary data, intellectual property, and source code). How data is sold, how it appears, and how it is valued on the dark web are key factors to consider when updating security measures at a network level. With a comprehensive understanding of how illegal marketplaces are structured and operated, organizations can proactively place the right assets under monitoring and reactively confirm if detected data under monitoring leaked from their systems or from a third party, speeding up the remediation time and decreasing overall damage. You can't stop everything, but by using data intelligence, organizations can have visibility into their exposure on the dark web, helping to reduce the risk of the inevitable data exposure.

graylog

LUNCH AND LEARN

Tapping Wires: Easy DNS Security Analysis

Speaker: Lennart Koopmann, Founder
Monday, September 24 | 12:30pm - 1:15pm | Milano III

There are multiple ways to defend against attackers on outside network perimeters and detect intrusions inside your network. One way that's used less often, but is highly effective, is to collect and analyze DNS requests. DNS lookups are often generated when attackers use domain names rather than IP addresses to attempt to infect your IT infrastructure or to establish command and control channels. The classic approach to collecting DNS requests is to write requests from the DNS servers to a log file and transfer those logs into a log management solution. However, a newer approach of using a network tap or mirror port for listening to the wire data that goes to your DNS servers instead has numerous advantages and gives you better information faster. Come find out how analyzing DNS wire data works better to more comprehensively protect your network.

VENDOR EVENTS

LUNCH AND LEARN

Adaptive Defense 360: Differentiating Values in Endpoint Visibility and Control

Speaker: Rui Lopes, North America Pre-Sales Engineering Manager
Monday, September 24 | 12:30pm - 1:15pm | Milano I

Cyber criminals and actors need to reach endpoints – or at least one endpoint – to gather information, stake credentials, and hit additional targets. Malware campaigns are now part of much more elaborated plots requiring total visibility and control to be properly addressed. Panda Security will unveil its innovative IT security model, Adaptive Defense, and demonstrate its differentiating values bringing intelligent cybersecurity to the endpoint with the ability to plan ahead.

Creating a Self-Service AppSec Program: Automate Testing During Development

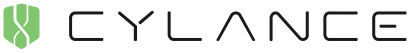
Speaker: Ed Arnold, Solution Architect
Wednesday, September 26 | 12:30pm - 1:15pm | Milano III

Organizations are facing a shift in application development and delivery. A far greater number of web applications, mobile applications and APIs are being created with tighter release cycles. All of these applications require some level of security testing and it is difficult for understaffed security teams to keep up with this pace. Learn how the Qualys Cloud Platform, integrated Cloud Apps including Web Application Scanning and the robust Qualys API can assist in creating a self-service model that enables your program for success.

Defense Against Targeted Custom Malware with Deep Learning For Whom the Malware Tolls: Introduction to Deep Learning

Speaker: Cameron Byers, Sales Engineer
Wednesday, September 26 | 12:30pm - 1:15pm | Milano IV

Sophos has over 30 years of experience in creating an effective defense against ever-changing threats. Your security defense solutions need to evolve to adapt to the ever changing threat landscape that customizes targeted attacks against your users, network, and data. In this presentation we review the latest trends, and how implementing the best Deep Learning techniques can keep your business assets protected.



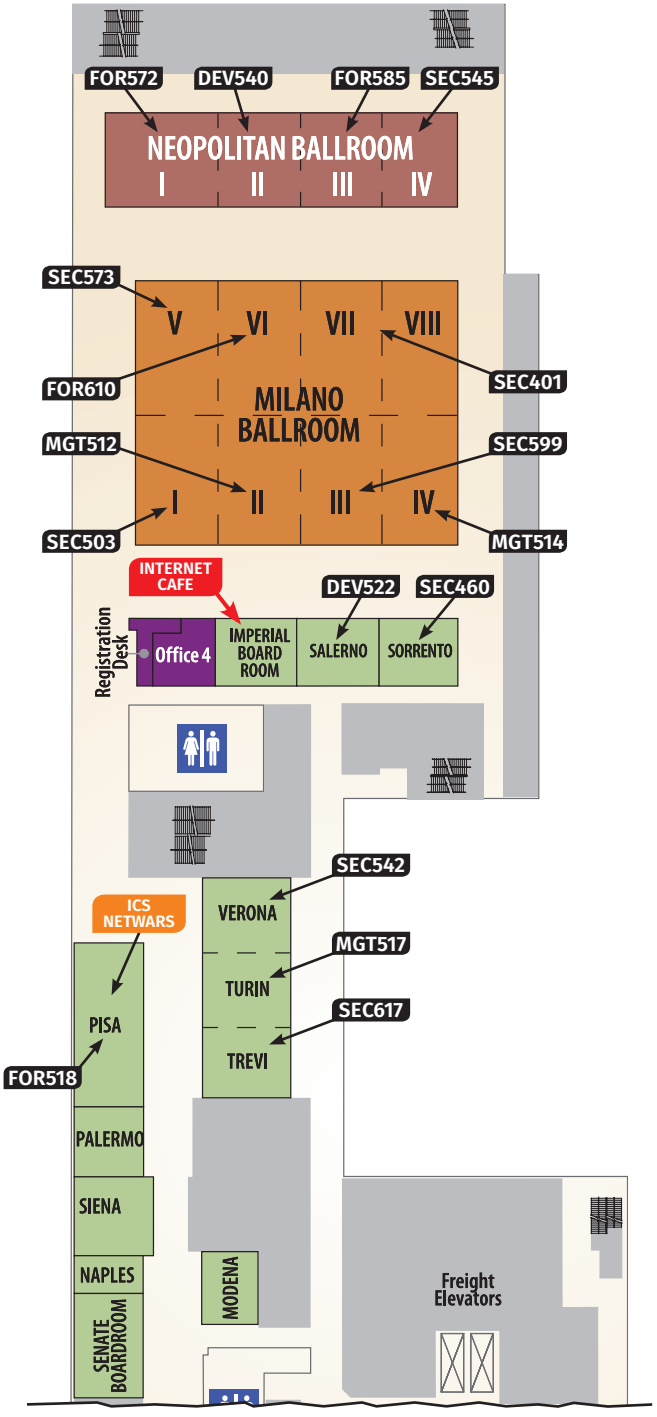
Wednesday, September 26 | 12:30pm - 1:15pm | Milano II

FUTURE SANS TRAINING EVENTS

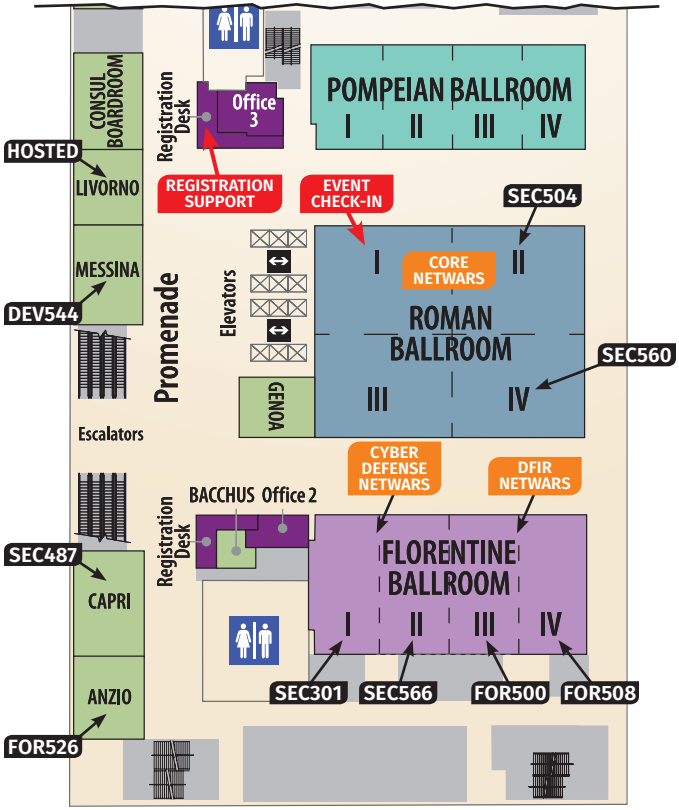
Northern VA Fall – Tysons	McLean, VA	Oct 13-20
Denver	Denver, CO	Oct 15-20
Seattle Fall	Seattle, WA	Oct 15-20
Secure DevOps	Denver, CO	Oct 22-29
Houston	Houston, TX	Oct 29 - Nov 3
Dallas Fall	Dallas, TX	Nov 5-10
DFIRCON Miami	Miami, FL	Nov 5-10
San Diego Fall	San Diego, CA	Nov 12-17
Pen Test HackFest	Bethesda, MD	Nov 12-19
Austin	Austin, TX	Nov 26 - Dec 1
San Francisco Fall	San Francisco, CA	Nov 26 - Dec 1
Nashville	Nashville, TN	Dec 3-8
Santa Monica	Santa Monica, CA	Dec 3-8
Tactical Detection and Data Analytics	Scottsdale, AZ	Dec 4-11
Cyber Defense Initiative	Washington, DC	Dec 11-18
Sonoma	Santa Rosa, CA	Jan 14-19, 2019
Miami	Miami, FL	Jan 21-26
Cyber Threat Intelligence	Arlington, VA	Jan 21-28
Las Vegas	Las Vegas, NV	Jan 28 - Feb 2
Security East	New Orleans, LA	Feb 2-9
Anaheim	Anaheim, CA	Feb 11-16
Northern VA Spring – Tysons	McLean, VA	Feb 11-16
Dallas	Dallas, TX	Feb 18-23
New York Metro Winter	Jersey City, NJ	Feb 18-23
Scottsdale	Scottsdale, AZ	Feb 18-23
Reno Tahoe	Reno, NV	Feb 25 - Mar 2
Open-Source Intelligence	Alexandria VA	Feb 25 - Mar 3
Baltimore Spring	Baltimore, MD	Mar 2-9

HOTEL FLOOR PLAN

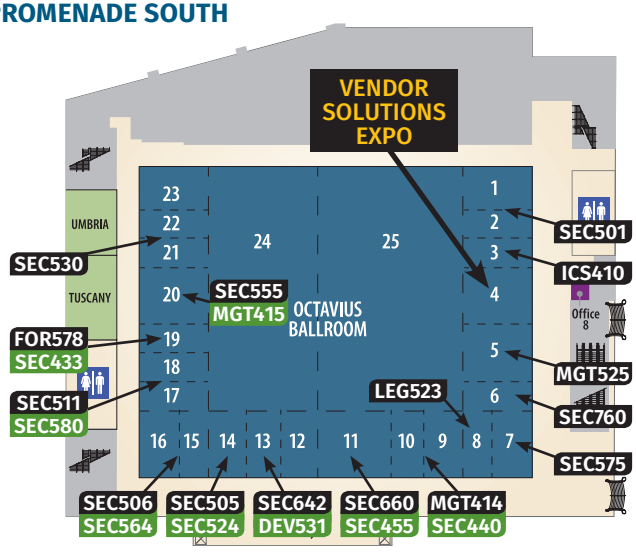
PROMENADE LEVEL



PROMENADE LEVEL (CONTINUED)



PROMENADE SOUTH



Save the Date!

Network Security 2019

Caesars Palace – Las Vegas

September 8-15