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  SEC560  FOR572
SEC401  SEC566  FOR578
SEC501  SEC573  FOR585
SEC503  SEC575  FOR610
SEC504  SEC642  MGT414
SEC505  SEC660  MGT512
SEC506  FOR500  MGT514
SEC511  FOR508  DEV544
SEC542  FOR518  AUD507
SEC555  FOR526  LEG523

To receive the discounted rate, you must sign up before Wednesday, April 11th 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

**First Time at SANS?**

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

**Tuesday, April 3**
8:00-8:30 am

Location:
**Regency S** (CONVENTION LEVEL)
GENERAL INFORMATION

Badge & Courseware Distribution

Location: Orlando Ballroom M/N (CONVENTION LEVEL)
Mon, Apr 2 ........................................ 5:00pm - 7:00pm
Tue, Apr 3 ........................................ 7:00am - 9:00am

Location: Registration Desk (CONVENTION LEVEL)
Tue, Apr 3 - Sat, Apr 7 ......................... 9:00am - 5:00pm
Sun, Apr 8 ........................................ 9:00am - 2:00pm
Mon, Apr 9 ...................................... 8:00am - 12:00pm

Location: Rainbow Spring II (CONVENTION LEVEL)
Tue, Apr 10 ..................................... 9:00am - 5:00pm

Internet Café

Location: Regency Rotunda (CONVENTION LEVEL)
Tue, Apr 3 ......................................... Opens at Noon
Wed, Apr 4 - Sat, Apr 7 ....................... Open 24 hours
Sun, Apr 8 ........................................ 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. SANS 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:

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:** **Tuesday, April 3, 2018**  
*Time: 9:00am - 5:00pm (Unless otherwise noted)*

#### SEC301: Introduction to Cyber Security  
Keith Palmgren . . . . Location: Windermere Z (CONVENTION LEVEL)

#### SEC401: Security Essentials Bootcamp Style  
Bryce Galbraith . Location: Regency Ballroom V (CONVENTION LEVEL)  
**Bootcamp Hours:** 5:00pm - 7:00pm (Course days 1-5)

#### SEC501: Advanced Security Essentials - Enterprise Defender  
Paul A. Henry . . . Location: Celebration 1 (CONVENTION LEVEL)  
**Extended Hours:** 5:00pm - 7:00pm (Course day 1)

#### SEC503: Intrusion Detection In-Depth  
David Hoelzer . . . Location: Celebration 9/10 (CONVENTION LEVEL)  
**Bootcamp Hours:** 5:00pm - 7:00pm (Course days 1-5)

#### SEC504: Hacker Tools, Techniques, Exploits & Incident Handling  
John Strand . . . . Location: Windermere W (CONVENTION LEVEL)  
**Extended Hours:** 5:00pm - 7:15pm (Course day 1)

#### SEC505: Securing Windows and PowerShell Automation  
Jason Fossen . . . Location: Celebration 6 (CONVENTION LEVEL)

#### SEC506: Securing Linux/Unix  
Hal Pomeranz . . . Location: Blue Spring I (CONVENTION LEVEL)

#### SEC511: Continuous Monitoring and Security Operations  
Bryan Simon . . . Location: Celebration 14/15 (CONVENTION LEVEL)  
**Bootcamp Hours:** 5:15pm - 7:00pm (Course days 1-5)

#### SEC542: Web App Penetration Testing and Ethical Hacking  
Seth Misner . . . Location: Bayhill 23/24 (LOBBY LEVEL)

#### SEC545: Cloud Security Architecture and Operations  
Dave Shackleford . . . Location: Bayhill 17/18 (LOBBY LEVEL)

#### SEC555: SIEM with Tactical Analytics  
Justin Henderson . . . Location: Bayhill 22 (LOBBY LEVEL)  
**Bootcamp Hours:** 5:15pm - 7:00pm (Course days 1-5)

#### SEC560: Network Penetration Testing and Ethical Hacking  
Ed Skoudis . . . Location: Windermere X (CONVENTION LEVEL)  
**Extended Hours:** 5:00pm - 7:15pm (Course day 1)  
*Extended hours will be led by Michael Murr in the SEC504 classroom located in River*

#### SEC561: Immersive Hands-on Hacking Techniques  
Tim Medin . . . Location: Bayhill 33 (LOBBY LEVEL)

#### SEC566: Implementing and Auditing the Critical Security Controls – In-Depth  
James Tarala . . . Location: Celebration 12/13 (CONVENTION LEVEL)

#### SEC573: Automating Information Security with Python  
Mark Baggett . . . Location: Bayhill 25/26 (LOBBY LEVEL)

#### SEC575: Mobile Device Security and Ethical Hacking  
Joshua Wright . . . Location: Bayhill 27 (LOBBY LEVEL)

#### SEC599: Defeating Advanced Adversaries – Implementing Kill Chain Defenses  
Erik Van Buggenhout . . . Location: Coral Spring I/II (LOBBY LEVEL)

#### SEC617: Wireless Penetration Testing and Ethical Hacking  
Larry Pesce . . . . Location: Manatee Spring I (LOBBY LEVEL)

#### SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques  
Adrien de Beaupre . . . Location: Celebration 11 (CONVENTION LEVEL)

#### SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking  
Stephen Sims, James Lyne . . . Location: Manatee Spring II (LOBBY LEVEL)  
**Bootcamp Hours:** 5:15pm - 7:00pm (Course days 1-5)

#### SEC760: Advanced Exploit Development for Penetration Testers  
Jake Williams . . . Location: Rock Spring (LOBBY LEVEL)  
**Bootcamp Hours:** 5:15pm - 7:00pm (Course days 1-5)

#### FOR500: Windows Forensic Analysis  
Chad Tilbury . . . Location: Regency Ballroom T (CONVENTION LEVEL)

#### FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting  
Rob Lee . . . Location: Regency Ballroom U (CONVENTION LEVEL)

#### FOR518: Mac and iOS Forensic Analysis and Incident Response  
Sarah Edwards . . . Location: Celebration 16 (CONVENTION LEVEL)

#### FOR526: Memory Forensics In-Depth  
Alissa Torres . . . Location: Peacock Spring (LOBBY LEVEL)

#### FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response  
Philip Hagen . . . Location: Celebration 4 (CONVENTION LEVEL)

#### FOR578: Cyber Threat Intelligence  
Peter Szczepankiewicz . . . Location: Windermere Y (CONVENTION LEVEL)

#### FOR585: Advanced Smartphone Forensics  
Heather Mahalik . . . Location: Regency S (CONVENTION LEVEL)

#### FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques  
Lenny Zeltser . . . Location: Celebration 5 (CONVENTION LEVEL)

#### MGT414: SANS Training Program for CISSP® Certification  
Eric Conrad . . . Location: Bayhill 21 (LOBBY LEVEL)  
**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™  
Ted Demopoulos . . . Location: Bayhill 29/30 (LOBBY LEVEL)  
**Extended Hours:** 5:00pm - 6:00pm (Course days 1-4)

#### MGT514: IT Security Strategic Planning, Policy, and Leadership  
Frank Kim . . . Location: Bayhill 31/32 (LOBBY LEVEL)
**Course Schedule**

**MGT517: Managing Security Operations: Detection, Response, and Intelligence**
Christopher Crowley  . Location: Bayhill 28 (LOBBY LEVEL)

**MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep**
Jeff Frisk  . Location: Bayhill 19/20 (LOBBY LEVEL)

**DEV540: Secure DevOps and Cloud Application Security**
Eric Johnson  . Location: Barrel Spring 1 (LOBBY LEVEL)

**DEV544: Secure Coding in .NET: Developing Defensible Applications**
Aaron Cure  . Location: Celebration 3 (CONVENTION LEVEL)

**AUD507: Auditing & Monitoring Networks, Perimeters, and Systems**
Clay Risenhoover  . Location: Celebration 2 (CONVENTION LEVEL)

**LEG523: Law of Data Security and Investigations**
Benjamin Wright  . Location: Barrel Spring II (LOBBY LEVEL)

**HOSTED: Physical Security Specialist – Full Comprehensive Edition**
The CORE Group  . Location: Blue Spring II (CONVENTION LEVEL)

---

**START DATE:** Monday, April 9, 2018  
Time: 9:00am - 5:00pm (Unless otherwise noted)

**SEC440: Critical Security Controls: Planning, Implementing, and Auditing**
Russell Eubanks  . Location: Celebration 11 (CONVENTION LEVEL)

**SEC455: SIEM Design & Implementation**
Justin Henderson  . Location: Celebration 16 (CONVENTION LEVEL)

**SEC524: Cloud Security Fundamentals**
Dave Shackleford  . Location: Bayhill 29/30 (LOBBY LEVEL)

**SEC564: Red Team Operations and Threat Emulation**
Joe Vest  . Location: Bayhill 27 (LOBBY LEVEL)

**SEC567: Social Engineering for Penetration Testers**
Micah Hoffman  . Location: Bayhill 28 (LOBBY LEVEL)

**SEC580: Metasploit Kung Fu for Enterprise Pen Testing**
Bryce Galbraith  . Location: Manatee Spring II (LOBBY LEVEL)

**MGT415: A Practical Introduction to Cyber Security Risk Management**
James Tarala  . Location: Coral Spring I/II (LOBBY LEVEL)

**MGT433: SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program**
Lance Spitzner  . Location: Bayhill 31/32 (LOBBY LEVEL)

**DEV531: Defending Mobile Applications Security Essentials**
Gregory Leonard  . Location: Blue Spring I (CONVENTION LEVEL)

---

**GIAC Certifications**

Add a GIAC Certification with your SANS training at SANS 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 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.*
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.

MONDAY, APRIL 2

SPECIAL EVENT
SANS 2018 Welcome Reception

Mon, April 2 | 5:00pm - 7:00pm
Location: Orlando Ballroom Foyer (CONVENTION LEVEL)

Kick off your SANS 2018 experience at the SANS 2018 Welcome Reception taking place in the Orlando Ballroom 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 Orlando. Come join your colleagues for a fun, relaxing evening.

TUESDAY, APRIL 3

SPECIAL EVENT
General Session – Welcome to SANS

Speaker: Bryan Simon
Tue, April 3 | 8:00am - 8:30am | Location: Regency S (CONVENTION LEVEL)

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.

KEYNOTE
Threat Hunting via Windows Event Logs

Speaker: Eric Conrad
Tue, April 3 | 7:15pm - 9:15pm | Location: Regency S (CONVENTION LEVEL)

Windows event logs continue to be the best source to centrally hunt malware in a Windows environment. Virtually all malware may be detected via event logs after making small tweaks to the logging configuration. Recent malware attacks leverage “fileless malware,” typically using PowerShell for post exploitation. Why? No EXE for antivirus or HIPS to squash, nothing saved to the filesystem, sites that use application whitelisting allow PowerShell, and little to no default logging. We will discuss DeepBlueCLI, an open-source Powershell framework for threat hunting via Windows Event Logs (including the latest PowerShell-fueled post exploitation). DeepBlueCLI will go toe-to-toe with the latest attacks; this talk will explore the evidence malware leaves behind, leveraging Windows command line auditing (now natively available in Windows 7+) and PowerShell logging. We will also discuss DeepWhite, an open-source detective application whitelisting framework that relies on Microsoft Sysinternals’s Sysmon and supports auto-submission of EXE, DLL and driver hashes via a free Virustotal Community API key.

WEDNESDAY, APRIL 4

LUNCH & LEARN
How to Become a SANS Instructor

Speaker: Eric Conrad
Wed, April 4 | 12:30pm - 1:15pm | Location: Bayhill 23/24 (CONVENTION LEVEL)

Have you ever wondered what it takes to become a SANS instructor? How does your SANS instructor rise to the top and demonstrate the talents to become part of the SANS faculty? Attend this session and learn how to become part of the faculty and learn the steps to make that goal a reality. A certified SANS instructor will share their experiences and show you how to become part of the SANS top-rated instructor team.

This presentation is free of charge, but space is limited to the first 40 registrations. Please register by clicking on the link below. There will also be a bulletin board on site for lunch and learn sign ups.

SPECIAL EVENT
GIAC Information Reception

Speaker: Jeff Frisk
Wed, April 4 | 6:30pm - 7:30pm | Location: Windermere X (CONVENTION LEVEL)

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.

SPECIAL EVENT
APAC Student Reception at SANS 2018

Wed, April 4 | 7:15pm - 8:15pm | Location: Windermere W (CONVENTION LEVEL)

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.
BONUS SESSIONS

SANS@NIGHT
Stuck in the Box, a SIEM’s Tale
Speaker: Justin Henderson
Wed, April 4 | 7:15pm - 8:15pm | Location: Regency S (CONVENTION LEVEL)
Organizations often spend excessive amounts of money on 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 that each environment is different, so you, the customer, must tell them what you want the SIEM to do, then they’ll help with professional services or replace your current SIEM with something “better and more advanced.” This is complete hogwash. Organizations tend to have a lot of overlap in 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), can most likely beat what you have today, then this talk is for you. 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.

SANS@NIGHT
Infosec Rock Star: Geek Will Only Get You So Far
Speaker: Ted Demopoulos
Wed, April 4 | 7:15pm - 8:15pm | Location: Regency T (CONVENTION LEVEL)
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 on the social and business side will make most of us more effective at what we do, rather than learning how to read hex better while standing on our heads, becoming “One with Metasploit,” or understanding the latest hot technologies.

SANS@NIGHT
Hacking Dumberly, Just Like the Bad Guys
Speakers: Tim Medin and Derek Banks
Wed, April 4 | 7:15pm - 8:15pm | Location: Regency V (CONVENTION LEVEL)
Tim Medin and Derek Banks will discuss the dumbest red team tricks and hacks we’ve encountered over the years. We are going to take the A out of APT, because so few attackers really need to use advanced techniques. We’ll also discuss the simple defenses that make an attacker’s life much more difficult.

SANS@NIGHT
Malware Vaccination: Its Potential and Limitations
Speaker: Lenny Zeltser
Wed, April 4 | 7:15pm - 8:15pm | Location: Regency U (CONVENTION LEVEL)
Some malicious software is designed to avoid infecting the system more than once by looking for predefined infection markers. Incident responders can vaccinate endpoints against such malware families by distributing the corresponding markers. The vaccines can take the form of specific registry keys, file names, mutex objects, and so on. Enterprises already know to treat such artifacts as indicators of compromise (IOCs). Vaccination entails using some IOCs to not only detect, but also prevent infections. This session will examine the potential for and limitations of malware vaccination and will explore several malware samples that could be controlled using this technique.

SANS@NIGHT
SIEM Field Guide
Speaker: Peter Szczepankiewicz
Wed, April 4 | 7:15pm - 8:15pm | Location: Windermere Z (CONVENTION LEVEL)
Come join our lively discussion on real life incidents that I have detected through the use of several Security Information and Event Managers (SIEMs) over the past 15 years. Generally, Chief Information Security Officers (CISO’s) use a SIEM as an instrument in the Security Operations Center (SOC). The main purpose is to find a live incident and pass it on to the Incident Handlers. We’ll discuss some of the technical use cases that have born fruit. Lately, the SIEM has been used for more than discovery, but also for detective work. Cyber Threat Intelligence analysts are able to glean a lot of information from the Incident Response (IR) team as well as the SOC. We’ll discuss the use of several different models, such as instrumentation into the SIEM, to the Pyramid of Pain, to the Kill Chain and Diamond Model. The focus of this talk is on security operations, but we’ll discuss some architectural strategies that always place you squarely in control over your SIEM.

SANS@NIGHT
So, You Wanna be a Pentester?
Speaker: Adrien de Beaupre
Wed, April 4 | 8:15pm - 9:15pm | Location: Regency S (CONVENTION LEVEL)
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
Let’s Go Hunting Bad Guys
Speaker: John Strand
Wed, April 4 | 8:15pm - 9:15pm | Location: Regency T (CONVENTION LEVEL)
In this presentation, John will share custom free tools with you to hunt bad guys inside and outside of your network – with awesomeness and math. But mostly math.
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.

SANS@NIGHT
Secure DevOps: A Puma’s Tail
Speaker: Aaron Cure
Wed, April 4 | 8:15pm - 9:15pm | Location: Regency U (CONVENTION LEVEL)
DevOps is changing the way that organizations design, build, deploy, and operate online systems. Engineering teams are making hundreds or even thousands of changes per day, and traditional approaches to security are struggling to keep up. Security must be reinvented in a DevOps world to take advantage of the opportunities provided by continuous integration and delivery pipelines. In this talk, we start with a case study of an organization trying to leverage the power of Continuous Integration (CI) and Continuous Delivery (CD) to improve its security posture. After identifying the key security checkpoints in the pre-commit, commit, acceptance, and deployment lifecycle phases, we will explore how unit testing and static analysis fit into SecDevOps. Live demonstrations will show how to identify vulnerabilities inside the Visual Studio development environment before they are committed to source control, and how to enforce security unit tests and static analysis in a Jenkins CI build pipeline. Attendees will walk away with a better understanding of how security fits into DevOps and an open-source .NET static analysis engine to help secure their organization’s applications.

STI MASTER’S PRESENTATION
Container Centric Intrusions: Assessing the Efficacy of Intrusion Detection and Analysis Methods for Container Based Environments
Speaker: Alfredo Hickman
Wed, April 4 | 8:15pm - 8:55pm | Location: Regency V (CONVENTION LEVEL)
This presentation is on practical research that empirically and comparatively assesses the efficacy of typical types of intrusion detection and analysis methods applicable to Linux application-container environments. This presentation will look at Cyber Kill Chain®-based attack-and-analysis experiments that were conducted to provide realistic scenarios that can assist security professionals in conceptualizing, developing, and operating more effective intrusion detection and analysis methods in Linux application container environments.

THURSDAY, APRIL 5
SPECIAL EVENT
Coffee and Donuts with the Graduate Students
Thu, April 5 | 7:30am - 9:00am | Location: Regency Rotunda (CONVENTION LEVEL)
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
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.
**BONUS SESSIONS**

**SANS@NIGHT**

**Three Keys for SecDevOps Success**

Speaker: Frank Kim

Thu, April 5 | 8:15pm - 9:15pm | Location: Regency T (CONVENTION LEVEL)

Learn three things that security teams can do to get to “yes” with DevOps teams that are striving to move at an even more rapid pace. Traditional application security practices can’t keep up with the speed of modern development organizations. Hear how you can start to make a difference for your organization.

**SATURDAY, APRIL 7**

**SANS@NIGHT**

**Speaking to the Board on Cybersecurity**

Speaker: Lance Spitzner

Sat, April 7 | 7:15pm - 8:15pm | Location: Regency S (CONVENTION LEVEL)

Time and time again we understand the need for leadership support on cybersecurity. However it can be challenging communicating to senior leaders, especially Board members, in their terms. How do you translate the technical world of cyber into concise business terms? Who is a Board member, how do they think and what do they want to know? Learn how senior leaders think and operate, what their priorities are, and how you can effectively engage them. Make your security program a success by gaining the support you need.

**SANS@NIGHT**

**Securing Your Kids**

Speaker: Lance Spitzner

Sat, April 7 | 8:15pm - 9:15pm | Location: Regency S (CONVENTION LEVEL)

Technology is an amazing tool. It allows our kids to access a tremendous amount of information, meet new people, and communicate with friends around the world. In addition, for them to be successful in the 21st century they have to know and understand how to leverage these new tools. However, with all these capabilities come a variety of new risks, risks that as parents you may not understand or even be aware of. In this one-hour presentation we cover the top three risks to kids online and the top steps you can take to protect them.

**VENDOR EVENTS**

**Vendor Solutions Expo**

Thu, April 5 | 12:00pm - 1:30pm | 5:30pm - 7:30pm

Location: Regency Rotunda (CONVENTION LEVEL)

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**

Thu, April 5 | 12:00pm-1:30pm

Location: Regency Rotunda (CONVENTION LEVEL)

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.

*Lunch sponsors are:*

- LogRhythm
- Sophos
- Cylance
- Garrison Technology, Ltd.
- Tripwire
- Risk IQ
- Qualys
- Rapid7
- Garrison Technology, Ltd.
- Tripwire
- Risk IQ
- Anomali
- ExtraHop
- Demisto
- Awake Security
- Corelight
- Terbium Labs
- MobileIron
- F5 Networks
- Anomali
- Terbium Labs
- MobileIron
- F5 Networks

**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 below are located on the are located at the Vendor Registration Desk.

**Unmasking the Fog: Improving Situational Awareness**

Speaker: Brian Roy, Sr. Sales Engineer

Wed, April 4 | 12:30pm - 1:15pm | Location: Regency S (CONVENTION LEVEL)

Situational awareness is a key factor in good threat intelligence. There is no such thing as perfect intelligence, as humans need to make decisions with incomplete data. The session will discuss how your organization can improve its situational awareness with a few techniques to include the aid of people, process and technology.
Identity Awareness: Do We Have It? Do We Need It?
Speaker: Nathan McKay, Security Solutions Engineer
Wed, April 4  |  12:30pm - 1:15pm  |  Location: Celebration 9/10  (CONVENTION LEVEL)

With the millions upon millions of identities, passwords, and accounts compromised every year, it is safe to say that we don’t – at least not all of us do, and not in practice in the real world. We’ll discuss what constitutes “identity” today, and how it is used out in the wild. What does it mean to be able to identify someone and why does it actually matter? How has technology allowed us to make better use of identity and how has it failed us? We will also challenge some current assumptions about identity and discuss how the rapid rise of technologies such as blockchain can impact or augment the idea of verifiable identity.

Navigating the Dark Web: A Case Study in Fraud and Risk Exposure
Speaker: Tyler Carbone, Chief Product Officer
Wed, April 4  |  12:30pm - 1:15pm  |  Location: Regency T  (CONVENTION LEVEL)

Terbium Labs and its customer, Baxter Credit Union (BCU), will discuss the problem of establishing a risk baseline as a medium-sized enterprise, and the necessity of ongoing visibility into exposure of payment card, financial, and personal data which may leak to, or be for sale, on the dark web. In this session, BCU will walk through its initial pain points and reasons for seeking a dark web data provider.

The Next Evolution of Protection: Introduction to Deep Learning
Speaker: Brandon Carden, Enterprise Sales Engineer
Wed, April 4  |  12:30pm - 1:15pm  |  Location: Regency U  (CONVENTION LEVEL)

Sophos has over 30 years of experience in creating an effective defense against ever-changing threats. One constant truth is that there is no silver bullet in security, solutions need to evolve to adapt the ever-changing threat landscape. In this presentation we review the latest trends, and how implementing the best Deep Learning techniques can combat these threats.

The New Cyber Security Ecosystem
Speaker: Laura Seletos, Technical Account Manager, Post-Sales
Wed, April 4  |  12:30pm - 1:15pm  |  Location: Regency V  (CONVENTION LEVEL)

Digital transformation is allowing companies to rapidly disrupt markets with new products and services that leverage cloud, mobile and IoT technology. This talk looks at the expanding ecosystem of cybersecurity products that help companies focus on evolving their security strategy along with business to accommodate common challenges this introduces.

Today’s Mobility and Cloud Cybersecurity Mission
Speaker: Loay Oweis, Federal Mobility Specialist
Fri, April 6  |  12:30pm - 1:15pm  |  Location: Regency U  (CONVENTION LEVEL)

The world today is evolving with burgeoning technology and business transformations. We can login to any user endpoint from a mobile device to a laptop, and have the same applications and content at our disposal to complete the daily tasks from anywhere. This is the experience we are growing accustomed to and are learning to expect to become ubiquitous from the workplace to the home place. Technology vendors are striving to standardize what once was innovation to become an expectation.

ICS Down...it’s go time!
Speaker: Jason DelyTechnical Director, ICS and Critical Infrastructure
Fri, April 6  |  12:30pm - 1:15pm  |  Location: Regency V  (CONVENTION LEVEL)

For years, we have read about security risks to companies that produce what we need that help run our society. Time and money have been spent, precautions have been taken and protections are in place. The moment of truth has now arrived to put security investments to the test. Yet, there’s direct evidence we’re not ready to defend and respond. Where have we gone wrong? Did we prepare for the right attacks? Have we admired threats yet ignored our ability to respond and recover? Direct from the battlefield, let’s examine where we are and how ready we are for a fight.
Save the Date and Join us again in 2019!

SANS 2019
Orlando, Florida
April 1-6