SANS 2017

Orlando, FL April 7-14

PROGRAM GUIDE

@SANSInstitute #SANS2017

SANS OnDemand Bundle

Add an OnDemand Bundle to your course to get an additional four months of intense training! OnDemand Bundles are just $689 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	SEC566	FOR585
SEC401	SEC575	FOR610
SEC501	SEC579	MGT414
SEC503	SEC642	MGT512
SEC504	SEC660	MGT514
SEC505	FOR408	DEV522
SEC506	FOR508	DEV544
SEC511	FOR518	AUD507
SEC542	FOR572	LEG523
SEC560	FOR578	ICS410

Three ways to register!

Visit the registration desk onsite
Call (301) 654-SANS
Write to ondemand@sans.org

TABLE OF CONTENTS

Core NETWARS EXPERIENCE

Hosted by Tim Medin
Wednesday, April 12 – Thursday, April 13
6:30-9:30pm | Windermere X

DFIR NETWARS TOURNAMENT

Hosted by Alissa Torres & Chad Tilbury
Wednesday, April 12 – Thursday, April 13
6:30-9:30pm | Windermere Z

All students who register for a 4-6 day course will be eligible to play NetWars for FREE.
Register Now!
sans.org/event/sans-2017

GENERAL INFORMATION

Badge & Courseware Distribution

Location: Registration Desk (CONVENTION LEVEL)

Friday, April 7 (SHORT COURSES ONLY) 8:00-9:00am

Location: Orlando Ballroom (CONVENTION LEVEL)

Saturday, April 8 (WELCOME RECEPTION) 5:00-7:00pm

Sunday, April 9 . . . . . 7:00-9:00am

Registration Support

Location: Registration Desk (CONVENTION LEVEL)

Sunday, April 9 - Friday, April 14 . . . . . 8:00am - 5:00pm

Internet Café

Location: Regency Rotunda (CONVENTION LEVEL)

Sunday, April 9. . . . . Opens at noon - 24 hours

Monday, April 10 - Thursday, April 13 . . . . . Open 24 hours

Friday, April 14. . . . . Closes at 2:00pm

Course Times

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

Course Breaks

Morning Coffee. 7:00-9:00am

Morning Break 10:30-10:50am

Lunch (ON YOUR OWN) 12:15-1:30pm

Afternoon Break. 3:00-3:20pm

First Time at SANS?

Please attend our **Welcome to SANS** briefing designed to help newcomers get the most from your SANS training experience. The talk is from **8:00-8:30am** on **Sunday, April 9** at the **General Session** in *Windermere W*.

Photography Notice

SANS may take photos of classroom activities for marketing purposes. SANS 2017 attendees grant SANS all rights for such use without compensation, unless prohibited by law. Those who wish not to be photographed onsite should notify the photographer.

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 evening session and drop it in the evaluation box.

Wear Your Badge

To confirm you are in the right place, SANS door monitors 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

SEC511: Continuous Monitoring and Security Operations

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:

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™

COURSE SCHEDULE

START DATE: **Friday, April 7**
Time: 9:00am - 5:00pm (Unless otherwise noted)

SEC440: Critical Security Controls: Planning, Implementing, and Auditing
Randy Marchany . . . . . .Location: Bayhill 27

SEC524: Cloud Security Fundamentals
Jorge Orchilles . . . . . .Location: Bayhill 31/32

SEC567: Social Engineering for Penetration Testers
Dave Shackleford. . . . . .Location: Manatee Spring 1

SEC580: Metasploit Kung Fu for Enterprise Pen Testing
Bryce Galbraith . . . . . .Location: Discovery 46

MGT415: A Practical Introduction to Cyber Security Risk Management
James Tarala . . . . . Location: Manatee Spring 2

MGT433: Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program
Lance Spitzner . . . . . Location: Bayhill 29/30

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

SEC301: Intro to Information Security
Keith Palmgren. . . . . Location: Regency P

SEC401: Security Essentials Bootcamp Style
Bryan Simon . . . . . Location: Bayhill 23/24
Bootcamp Hours: 5:00-7:00pm (Course days 1-5)

SEC501: Advanced Security Essentials – Enterprise Defender
Paul A. Henry . . . . . Location: Regency Ballroom U

SEC503: Intrusion Detection In-Depth
Johannes Ullrich, Ph.D. . . . . Location: Regency Ballroom V

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

SEC505: Securing Windows and PowerShell Automation
Jason Fossen. . . . . .Location: Bayhill 31/32

SEC506: Securing Linux/Unix
Hal Pomeranz. . . . . Location: Celebration 4

SEC511: Continuous Monitoring and Security Operations
Eric Conrad . . . . . .Location: Coral Spring 1/2
Bootcamp Hours: 5:15-7:00pm (Course days 1-5)

SEC542: Web App Penetration Testing and Ethical Hacking
Pieter Danhieux . . . . . Location: Celebration 6

SEC550: Active Defense, Offensive Countermeasures and Cyber Deception
Bryce Galbraith . . . . . Location: Peacock Spring

SEC560: Network Penetration Testing and Ethical Hacking
Ed Skoudis . . . . . Location: Windermere X
Extended Hours: 5:00-7:15pm (Course Day 1 only)
Extended hours will be led by John Strand in the SEC504 classroom located in Windermere W

SEC561: Immersive Hands-On Hacking Techniques
Tim Medin . . . . . Location: Celebration 2

SEC566: Implementing and Auditing the Critical Security Controls – In-Depth
James Tarala . . . . . Location: Regency Ballroom T

SEC573: Automating Information Security with Python
Mark Baggett . . . . . Location: Celebration 9/10

SEC575: Mobile Device Security and Ethical Hacking
Joshua Wright . . . . . Location: Celebration 12/13

SEC579: Virtualization and Private Cloud Security
Dave Shackleford . . . . . Location: Bayhill 25/26

SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses
Larry Pesce . . . . . Location: Bayhill 33

SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques
Adrien de Beaupre . . . . . Location: Bayhill 17/18

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
Stephen Sims . . . . . Location: Celebration 5
Bootcamp Hours: 5:15-7:00pm (Course days 1-5)

SEC760: Advanced Exploit Development for Penetration Testers
Jake Williams . . . . . Location: Dicovery 46
Bootcamp Hours: 5:15-7:00pm (Course days 1-5)

FOR408: Windows Forensic Analysis
Rob Lee . . . . . Location: Windermere Y

FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting
Chad Tilbury . . . . . Location: Bayhill 29/30

FOR518: Mac Forensic Analysis
Sarah Edwards . . . . . Location: Challenger 40

COURSE SCHEDULE

FOR526: Memory Forensics In-Depth
Alissa Torres . . . . . Location: Celebration 1

FOR572: Advanced Network Forensics and Analysis
Philip Hagen . . . . . Location: Celebration 14/15

FOR578: Cyber Threat Intelligence
Robert M. Lee . . . . . Location: Bayhill 22

FOR585: Advanced Smartphone Forensics
Heather Mahalik . . . . . .Location: Bayhill 21

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Lenny Zeltser . . . . . Location: Windermere Z

MGT414: SANS Training Program for CISSP® Certification
Seth Misenar . . . . . .Location: Manatee Spring 1
Bootcamp Hours: 8:00-9:00am (Course days 2-6) & 5:00-7:00pm (Course days 1-5)

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

MGT514: IT Security Strategic Planning, Policy, and Leadership
Frank Kim . . . . . .Location: Regency O

MGT517: Managing Security Operations: Detection, Response, and Intelligence
Frank Kim . . . . . .Location: Bayhill 27

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

DEV522: Defending Web Applications Security Essentials
Jason Lam . . . . . .Location: Discovery 44

DEV544: Secure Coding in .NET: Developing Defensible Applications
Eric Johnson . . . . . Location: Celebration 3

AUD507: Auditing & Monitoring Networks, Perimeters, and Systems
Clay Risenhoover . . . . . .Location: Barrel Spring 2

LEG523: Law of Data Security and Investigations
Benjamin Wright . . . . . .Location: Barrel Spring 1

ICS410: ICS/SCADA Security Essentials
Justin Searle . . . . . Location: Challenger 41/42

HOSTED: Physical Security Specialist - Full Comprehensive Edition
The CORE Group. . . . . Location: Rock Spring

GIAC
CERTIFICATIONS

Add a GIAC Certification with your SANS training at SANS 2017 and

SAVE $360!

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 $689 when you bundle your certification attempt with your SANS training course during SANS 2017 for a savings of $360! After this event is over, the alumni bundle price goes to $1,049.

Stop by Registration and add your GIAC-affiliated certification before the last day of class for the discount.

Find out more about GIAC at www.giac.org or call 301-654-7267.

SPECIAL EVENTS

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, APRIL 8

Welcome Reception

Saturday, April 8 | 5:00-7:00pm
Location: Orlando Ballroom Foyer
Register early and network with your fellow students!

SUNDAY, APRIL 9

SPECIAL EVENT

General Session – Welcome to SANS

Speaker: Eric Conrad
Sunday, April 9 | 8:00-8:30am | Location: Windermere W

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.

SANS@NIGHT

KEYNOTE: Quality Not Quantity: Continuous Monitoring's Deadliest Events

Speaker: Eric Conrad
Sunday, April 9 | 7:15-9:15pm | Location: Windermere W

Most Security Operations Centers (SOCs) are built for compliance, not security. One well-known retail firm suffered the theft of over a million credit cards. Some 60,000 true positive events were reported to its SOC during that missed breach, but they were lost in the noise of millions. If you are bragging about how many events your SOC handles each day, you are doing it wrong. During this talk, we will show you how to focus on quality instead of quantity, and provide an actionable list of the deadliest events that occur during virtually every successful breach.

MONDAY, APRIL 10

SANS@NIGHT

Securing Your Kids

Speaker: Lance Spitzner

Monday, April 10 | 7:15-8:15pm | Location: Regency T

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.

SANS@NIGHT

Taking Control of Your Application Security

Speaker: Eric Johnson

Monday, April 10 | 7:15-8:15pm | Location: Regency U

Chances are, at any given moment, your organization's applications are under attack. The bad guys see your applications as the front door, and a single bad line of code allows them entry. Through a mobile app, web application, or REST API, attackers can pivot to a back-end database, your business partner's workstation, or even a payment processing vendor. As development teams continue to push new applications to web, mobile, and cloud environments, the need for an application security program is at an all-time high. Here's the problem: the application security space has nearly twice as many job openings as candidates. For every 100 developers, there are roughly 10 operations team members, and only and one security professional. With the shortage of capable experts, how do organizations take control of their application security? Get ready to explore the real-world impact of application security breaches, discuss some alarming statistics and trends, and walk through a series of practical steps for building security into applications from the beginning. Attendees will walk away with actionable ideas and recommended practical tools to help improve their application security program.

SPECIAL EVENTS

STI MASTER'S PRESENTATION

Indicators of Compromise Ransomware TeslaCrypt Malware

Speaker: Kevin Kelly, Master's Degree Candidate

Monday, April 10 | 7:15-7:55pm | Location: Regency V

Malware has become a growing concern in a society of interconnected devices and real-time communications. This presentation will analyze the effect of malware, how it is processed locally and within network traffic. The gathering of malware capabilities from different datasets, including process monitoring, flow data, registry key changes and others, will give indicators of compromise. These indicators will be collected and analyzed using various open source tools such as Sysinternals suite, Fiddler, Wireshark, Bro, and SiLK. Malware indicators of compromise will be collected to produce defensive countermeasures against unwanted advance adversary activity on a network. A virtual appliance platform with simulated production Windows 8 O/S will be created, infected with malware, a variant of a crypto locker malicious file, then processed to collect indicators to be used to detect similar infections.

SANS@NIGHT

The Three Cs to Building a Mature Awareness Program

Speaker: Lance Spitzner

Monday, April 10 | 8:15-9:15pm | Location: Regency T

After working with hundreds of organizations, we have found three common obstacles to a successful awareness program, what we call the three Cs: communication, collaboration, and culture. Learn how the most effective organizations are overcoming these three challenges and how you can apply their lessons learned to your own security awareness program.

SANS@NIGHT

Be the Cheatsheet. Know Memory.

Speaker: Alissa Torres

Monday, April 10 | 8:15-9:15pm | Location: Regency U

There is an arms race between analysts and attackers. Modern malware increasingly employs obfuscation and subversion techniques such as sophisticated code injection and anti-memory analysis mechanisms to destroy or subvert volatile data. Examiners must have a deep understanding of memory internals and the ability to choose the right tool for the job in order to identify the malware and discern the intentions of attackers or rogue trusted insiders. It's time to re-up your skills at hunting evil in memory. Attend this session, learn the newest memory forensics techniques, and tear into our memory images to find your own evil.

STI MASTER'S PRESENTATION

Learning Normal with the Kansa PowerShell Incident Response Framework

Speaker: Jason Simsay, Master's Degree Candidate
Monday, April 10 | 8:15-8:55pm | Location: Regency V

Preparation is a critical step in establishing an effective incident response program. Information security professionals that will be called upon to handle an incident have the opportunity to prepare ahead of time. Kansa is a PowerShell Incident Response framework developed by Dave Hull. The PowerShell Remoting feature is leveraged to establish a highly scalable and extensible system state collection platform. Once data is collected from across the Microsoft environment, an extensive set of frequency analysis scripts enable incident handlers to turn unknown unknowns into known unknowns and discover anomalies and indicators of compromise.

Learning and deploying the Kansa framework before an incident occurs is valuable preparatory work. Even more so, we can leverage Kansa during the preparation phase to baseline systems and establish familiarity with normal. This makes us much more adept at identifying abnormal activity, getting a jump on incident identification, and ideally, containing an incident with minimal damages. This presentation will explore leveraging the Kansa framework to facilitate documenting normal state baselines. We will build upon the frequency analysis capabilities to support profiling across various homogenous endpoint profiles deployed within the organization.

TUESDAY, APRIL 11

SPECIAL EVENT

Coffee & Donuts with the Graduate School

Tuesday, April 11 | 7:30-9:00am | Location: Regency Rotunda

Join us for coffee, donuts, and conversation with graduate school staff and current students.

The SANS Technology Institute (**www.sans.edu**) is the only graduate program designed by the world-class faculty at SANS. Our programs combine SANS technical training and certifications, recognized as the industry's best, with leadership and management curriculum specifically designed for the unique needs of aspiring leaders. Our master's degree programs provide high-potential cybersecurity professionals with the combination of cutting-edge knowledge and leadership skills that take careers to the highest levels. Graduate certificate programs offer a shorter, technically focused set of courses that sharpen your skills and keep your knowledge current. Questions? Contact us at **info@sans.edu**

SPECIAL EVENTS

SANS@NIGHT

Operating an ICS/SCADA Security Operations Center

Speaker: Robert M. Lee

Tuesday, April 11 | 7:15-8:15pm | Location: Regency T

The Security Operations Center (SOC) represents a centralized approach to enterprise security that contains functions such as alerting, triage, and incident response. As the ICS/SCADA community has moved towards interconnecting industrial control systems with traditional IT infrastructure, there has been increased attention on the utilization of a SOC. Questions that arise involve the types of personnel needed, the focus, the cost, and whether what is needed is a dedicated ICS SOC or an integrated approach with the enterprise. This presentation will examine case studies and best practices for building, structuring, and running an ICS SOC.

SANS@NIGHT

The Tap House

Speaker: Philip Hagen

Tuesday, April 11 | 7:15-8:15pm | Location: Regency U

Packets move pretty fast. The field of network forensics needs to move fast, too. Whether you are investigating a known incident, hunting unidentified adversaries in your environment, or enriching forensic findings from disk- and memory-based examinations, it's critical to stay abreast of the latest developments in the discipline. In this talk, Phil Hagen will discuss some of the latest technologies, techniques, and tools that you'll want to know in pursuit of forensication nirvana. This presentation will be helpful for those who wish to keep up-to-date on the most cutting-edge facets of Network Forensics. Phil is also an avid craft beer fan, so there's a good chance you'll learn something about a new notable national or interesting local beer in the process.

STI MASTER'S PRESENTATION

Arming SMB's Against Ransomware Attacks

Speaker: Timothy Ashford, Master's Degree Candidate
Tuesday, April 11 | 7:15-7:55pm | Location: Regency V

Ransomware has become one of the most serious cyber threats to small and medium businesses today. A recent variant permanently deletes files within one hour of infection. The situation grows increasingly dire: the FBI even encourages victims to make payment, though there is still no guarantee that owners will recover their data. Despite such threats, small and medium enterprises can follow recommended best practices to mitigate this risk. Businesses with tighter budgets and fewer security team members can adopt many of the protections available to the largest enterprises. The most important recommendation is the use of application whitelisting. In Windows environments, this can be accomplished through free tools within Active Directory. Other options will also be discussed, as well as a brief discussion of the future of ransomware.

SANS@NIGHT

Sarah's Apple Orchard

Speaker: Sarah Edwards
Tuesday, April 11 | 8:15-9:15pm | Location: Regency T

This talk series will feature freshly picked topics pertaining to Apple specific digital forensics. Topics may be from the smallest seedling like a recent subject in current news to something that has been baking for a while that requires advanced forensic analysis. These talks will get at the core of many Apple technologies in a wide variety of areas within software and hardware. Any juicy and delicious topic is fair game in Sarah's Apple Orchard.

SANS@NIGHT

The End of Banking as We Know It: How Crypto Currencies and e-Payments are Breaking Up a Centuries-Old Monopoly

Speaker: G. Mark Hardy
Tuesday, April 11 | 8:15-9:15pm | Location: Regency U

Are we finally ready to go mainstream with alt-currency? Bitcoin got off to a slow start but has attracted millions of VC dollars in the last two years. We'll look at this brave new world of electronic money to understand what it is, how it works, what it can (and cannot) do, and probabilities of success or failure. We'll examine spin-off technologies such as blockchains, and look into the mechanics behind electronic payment systems such as Apple Pay, CurrentC, and Softcard. We'll even talk about why crooks love Bitcoin for ransomware extortion, and dig into the mechanics of how credit card fraud works, and whether that might be going away as well.

STI MASTER'S PRESENTATION

Impediments to Adoption of Two-Factor Authentication by Home End-Users

Speaker: Preston Ackerman, Master's Degree Candidate

Tuesday, April 11 | 8:15-8:55pm | Location: Regency V

Cyber criminals have proven to be both capable and motivated to profit from compromised personal information. The FBI has reported that victims have suffered over $3 billion in losses through compromise of email accounts alone (IC3 2016). One security measure, which has been demonstrated to be effective against many of these attacks, is two-factor authentication (2FA). The FBI, the Department of Homeland Security US Computer Emergency Readiness Team (US-CERT), and the internationally recognized security training and awareness organization, the SANS Institute, all strongly recommend the use of two-factor authentication. Nevertheless, adoption rates of 2FA are low.

This study introduced 2FA to a group of millennials as an easily accessible security tool to protect their accounts against takeover by cyber criminals. They were introduced to the purpose of 2FA and provided resources to help begin using it. This presentation discusses the factors that influenced the participants' decisions to adopt or not adopt 2FA. The findings of this study will help organizational security awareness programs and 2FA service providers focus their efforts on more persuasive messages and, possibly, enhanced technologies that can improve the use of 2FA services among millennials in the future.

WEDNESDAY, APRIL 12

LUNCH & LEARN

How to Become a SANS Instructor

Speaker: Eric Conrad

Wednesday, April 12 | 12:30-1:15pm | Location: Coral Springs 1/2

This presentation is free of charge, but space is limited to the first 40 registrations. Please register on line or on site where there will be a bulletin board for lunch and learn sign ups.

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. Eric Conrad, a SANS Certified Instructor, will share his experiences and show you how to become part of the SANS top-rated instructor team.

Core NetWars Experience

Host: Tim Medin

Wed, April 12 & Thu, April 13 | 6:30-9:30pm | Location: Windermere X

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.

DFIR NetWars Tournament

Hosts: Chad Tilbury & Alissa Torres

Wed, April 12 & Thu, April 13 | 6:30-9:30pm | Location: Windermere Z

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.

SANS@NIGHT

Cyber Hygiene and Standards of Care: Practical Defenses Against Advanced Attacks

Speaker: James Tarala

Wednesday, April 12 | 7:15-8:15pm | Location: Regency O

There is no question that organizations are struggling to stop attacks. Yet hackers are not magic, though we pretend that they are and that special secret knowledge is required to stop them. In this presentation, James Tarala, a contributor to the CIS Critical Security Controls, will discuss standards of cybersecurity care and why the Controls are quickly becoming the gold standard for organizations. He will also share practical tips for implementing the Controls and overcoming the barriers to implementation. Attendees should expect to leave the presentation with practical advice for using these Controls to stop even the most advanced attacks on their organization.

SPECIAL EVENTS

SANS@NIGHT

You Have Ransomeware! Managing the Legal Risk of Cyber Fraud

Speaker: Benjamin Wright

Wednesday, April 12 | 7:15-8:15pm | Location: Regency P

Today, most fraud has a cyber component, and most fraud investigations involve digital evidence. Cyber fraud like ransomware can trigger a legal crisis for your firm or your client. Mr. Wright will share insights on how to manage the legal risk. He will examine legal measures such as disclaimers, cyber insurance and invocation of attorney confidentiality rules.

STI MASTER'S PRESENTATION

Influence and Implementation

Speaker: Wesley Earnest, Master's Degree Candidate

Wednesday, April 12 | 7:15-7:55pm | Location: Regency T

Information security is a difficult job. Practitioners have to defend against every possible scenario and attackers only have to find one hole in the defenses in order to compromise an organization. Often times, InfoSec practitioners know what needs to be done and have ample technical skills to achieve success, yet end users or "The Business" veto the implementation of practical controls necessary to secure the environment. Learn how one small community bank overcame these challenges and enjoyed the successes of transitioning from an environment of constant reactionary troubleshooting to implementing an information security strategy that focused not only on improving the information technology environment but also business operations and regulatory compliance for the bank.

SANS@NIGHT

Prioritizing Your Security Program

Speaker: Keith Palmgren

Wednesday, April 12 | 8:15-9:15pm | Location: Regency P

Building a cybersecurity program is easy. Building a cybersecurity program that is effective is seriously hard! When faced with a seemingly insurmountable task, prioritization is vital. Investing time and money in the right place at the right time is the difference between success and being the next cyberbreach headline. Whether you are new to cybersecurity or an old hand, you may feel lost in the storm. If so, this talk is for you. Cybersecurity's five historic and current pitfalls that prevent organizations from building an effective IT Security platform will be discussed: poor passwords, vulnerabilities, malware/crimeware, insider threat, and mismanagement. Every organization needs a cybersecurity strategy. An effective strategy requires that you understand the problems as well as the solutions to those problems. Only then can you prioritize your limited cybersecurity resources. Managers and technicians alike will gain valuable insight in this non-technical talk.

SANS@NIGHT

Mobile Application Assessment

Speaker: Chris Crowley

Wednesday, April 12 | 8:15-9:15pm | Location: Regency O

Mobile devices are ubiquitous. The variety of mobile applications present on these devices is incredible, with both the Google Play market and Apple App store offering over two million applications each. While each app store vets applications to help protect consumers, there have been overtly malicious applications in the stores, as well as applications that exhibit less desirable behavior. In this talk we'll explore the SANS top eight mobile steps, one of which is performing application assessments. We discuss a methodology taught in SEC575, the application report card, for organizations to look at aspects of Android and iOS mobile applications in order to protect the organization's interests. There are some tools available to perform assessments of mobile applications, but we also need analysts who are competent at wielding those tools. This talk will bring awareness to those who haven't had a peek behind the details of mobile applications. Additionally, it will provide technical specifics to people who want to assess mobile applications.

STI MASTER'S PRESENTATION

SS7: Teleco's Fallen Wall

Speaker: Hassan Mourad, Master's Degree Candidate

Wednesday, April 12 | 8:15-8:55pm | Location: Regency T

For decades, the security of one of the fundamental protocols in telecommunications networks, Signaling System No. 7 (SS7), has been solely based on the mutual trust between the interconnecting operators. Operators relied on their trust in other operators to play by the rules, and the SS7 network has always been regarded as a closed trusted network. This notion of trust and security has recently changed after several security researchers announced major vulnerabilities in the SS7 protocol suite that threatens user's privacy and can lead to user location tracking, fraud, denial of service, or even call interception. In this talk we will discuss SS7 attacks from the operator's perspective and examine the possibility of using some of the critical security controls to protect against those attacks. We will finalize our discussion by examining possible precautions from the end user perspective to mitigate or reduce the impact of such attacks.

SPECIAL EVENTS

THURSDAY, APRIL 13

SANS@NIGHT

The Internet of Things Is Turning Against Us

Speaker: Johannes Ullrich, Ph.D.

Thursday, April 13 | 7:15-8:15pm | Location: Regency V

Over the last few years, we have seen devices like cameras, routers, and printers being used in attacks. While you were wasting your time pentesting and securing the "known networks," your coworkers were building a network of buggy and exploitable devices that are ripe for the picking by attackers. If you don't have the ability to centrally manage these devices, they won't be covered by regular patch schedules and automatically applied hardened configurations. This presentation will show you some of the attacks against devices being used right now to penetrate corporate networks, launch denial of service attacks, and adjust your living room temperature. Learn enough to be scared, and maybe if I feel like it, I will throw you a bone to help you secure some of this mess.

SANS@NIGHT

Breaking Next Next (Next?) Gen Security Software

Speaker: John Strand

Thursday, April 13 | 7:15-8:15pm | Location: Regency U

Let's go over some tips and techniques for bypassing "advanced" security components like whitelisting, next gen firewalls, *Advanced* AV engines and User Behavioral Analytics.

Because sharing is caring!

STI MASTER'S PRESENTATION

Simple Approach to Access Control: Port Control and MAC Filtering

Speaker: William Knaffl, Master's Degree Candidate

Thursday, April 13 | 7:15-7:55pm | Location: Regency T

It seems that every day a new and more frightening data breach goes public. These attacks seem to run the gamut; everything from international banks, government agencies, private companies, educational institutions, and even non-profit organizations are targets. With each attack the confidentiality, integrity and availability of our data is diminishing. The use of the "Critical Controls" is one part of the defense in depth approach to data security. By approaching security from the perspective of these controls, we can reduce the threat vectors, reduce detection time, and expose attacks to the overall security posture. This presentation will review one such attack and show how implementation of the critical controls would have reduced the impact to the company.

SANS@NIGHT

HTTPDeux

Speaker: Adrien de Beaupre

Thursday, April 13 | 8:15-9:15pm | Location: Regency U

This talk will discuss the HTTP/2 protocol that has only recently been approved and published. The agenda will include reasons for the new protocol to be developed, how it is implemented, tools that can use it, and challenges it presents to penetration testers.

SANS@NIGHT

Ten Tenets of CISO Success

Speaker: Frank Kim

Thursday, April 13 | 8:15-9:15pm | Location: Regency V

The era of CISO-as-dictator is at an end. The increased importance of cybersecurity as a vital component of business growth requires that security leaders find new ways to work with executive leaders, business partners, and their own team members. Learn 10 tenets that CISOs and security leaders can utilize to go beyond technical skills, successfully lead organizations through change, and ultimately get to "yes" with the business.

STI MASTER'S PRESENTATION

Database Activity Monitoring (DAM): How It Works, And What You Need To Know To Implement It

Speaker: Charles Brodsky, Master's Degree Candidate

Thursday, April 13 | 8:15-8:55pm | Location: Regency T

If your CISO said "We think a DBAs account was hacked, can you tell if they downloaded anything from the production database?" would you have an answer? As more and more data is consolidated into databases, this is a challenge many information security professionals face. One of the uses for Database Activity Monitoring systems is trying to answer that type of question.

In this presentation we discuss how Database Activity Monitoring works, what it needs to be effective, and the challenges you'll face when implementing it. We go beyond the 'feature list' in a sales brochure and dig into deciding what to monitor, getting stakeholder 'buy in' and what can go wrong after you deployed it. We will also discuss one vendor's product for doing this, Imperva's SecureSphere.

If you are considering Database Activity Monitoring, or just want to get a better understanding of database security, this presentation is for you.

VENDOR EVENTS

Vendor Solutions Expo

Tuesday, April 11 | 12:00-1:30pm | 5:30-7:30pm
Location: Regency Rotunda

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, April 11 | 12:00-1:30pm | Location: Regency Rotunda

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 are:

PLATINUM

Malwarebytes

GOLD

Anomali	Cybereason	MobileIron	Sophos Inc.
Cisco Systems Inc.	Ensilo	Qualys	Terbium Labs
	F5 Networks, Inc.	RiskIQ	

SILVER

CrossMatch	Illusive Networks	LogRhythm
Datacom Systems, Inc.	InfoArmor	NH&A, LLC.
Event Tracker	Kaspersky Lab	Pwnie Express

Vendor Welcome Reception: PRIZE GIVEAWAYS!!! – Passport to Prizes

Tuesday, April 11 | 5:30-7:30pm | Location: Regency Rotunda

This informal reception allows you to visit exhibits and participate in some exciting activities. This is a great time to mingle with your peers and experience firsthand the latest in information security tools and solutions with interactive demonstrations and showcase discussions. Enjoy appetizers and beverages and compare experiences with other attendees regarding the solutions they are using to address security threats in their organization. Attendees will receive a Passport-to-Prizes entry form. Visit each sponsor to receive a stamp, and then enter to win exciting prizes.

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 Community Bulletin Board at Student Registration.

LUNCH AND LEARN

Threat Hunting 102: Beyond the Basics, Maturing Your Threat Hunting Program

Speaker: Jayson Wehrend, Solutions Engineer
Monday, April 10 | 12:30-1:15pm | Location: Coral Springs 9/10

The ever-escalating battle: cyber criminals are becoming more imaginative in their approaches and techniques and the defenders need to consistently boost security programs to stay alert and deliver on the promise of protecting it all. In this reality, thereâs no way to prevent all attacks and the concept of “penetration is inevitable” is...well...inevitable. The goal then of security teams should be to mitigate the damage of any unfortunate security breaches that do occur. Threat hunting is the best, proactive approach. But, excelling at threat hunting, discovering adversaries takes time, patience, planning, and some serious skills. In this session, you’ll learn how to elevate your current threat hunting program.

LUNCH AND LEARN

DDoS, Password Policies, and Spam: What Do They All Have in Common?

Speaker: Nathan McKay, Security Marketing Solutions Architect
Monday, April 10 | 12:30-1:15pm | Location: Regency T

DDoS, password policies, and spam: it’s 2017 and they’re still a thing, and still annoying. We’ll be focusing on DDoS, examining what constitutes an effective attack today and what the industry is doing about it. Spam has by and large been relegated to an annoyance; will we ever get to that point with DDoS? Can we do better and actually eliminate some attack types such as volumetric? We’ll take a closer look at some of the industry-wide collaboration that is underway to make DDoS as mundane as spam and as effective as Nigerian 419 scams.

Malwarebytes

LUNCH AND LEARN

Launch, Detect, Evolve: The Mutation of Malware

Speaker: Michael Hernandez, Senior Sales Engineer, Malwarebytes
Monday, April 10 | 12:30-1:15pm | Location: Regency U

In order to hit their targets, malware developers need to constantly evolve their tactics. This evolution is frequently done in very small incremental changes to known malware attacks. Today, malicious developers know their malware has a short half-life before detection. In order to optimize their efforts, cyber criminals now modify their "products" just enough to evade detection a little bit longer. The threat landscape is constantly changing. This is your opportunity to hear what you can expect to hit you networks and how you can prepare.

LUNCH AND LEARN

Digital Threat Management (DTM): Advanced Hunter and Defender Techniques

Speaker: Benjamin Powell, Technical Marketing Manager
Monday, April 10 | 12:30-1:15pm | Location: Regency V

80% of attacks happen outside of your firewall. How can you further optimize external threat investigation and understand your active attack surface? In this session, you will learn how to more rapidly correlate digital breadcrumbs to hunt down attackers, exploits and infrastructure. Examining recent publicized attacks with RiskIQ DTM platform, we will dive into the attack, adversary and analysis.

LUNCH AND LEARN

Perils of Shadow IT 2.0: The Mobile App-to-Cloud Security Gap

Speaker: James Plouffe, Lead Solutions Architect, MobileIron
Monday, April 10 | 12:30-1:15pm | Location: Regency P

Cyber Criminals are increasingly exploiting the Internet services to build agile and resilient infrastructures, and consequently to protect themselves from being exposed and taken over. This session will explain how the correlation of Internet data on multiple levels (DNS, BGP, ASN, Prefixes/IPs) can be used to build and deliver a new model of security that is pervasive and predictive, and that allows us to expose the attackers' infrastructure. Detection models that can be built and applied (such as co-occurrences, NLPRank, and Spike Detectors), and how the different detectors can be integrated to expose malicious infrastructures and advanced persistent threats.

LUNCH AND LEARN

Keep Calm and Prioritize: Five Requirements for Streamlining Vulnerability Remediation

Speaker: Jimmy Graham, Director of Product Management
Wednesday, April 12 | 12:30-1:15pm | Location: Windermere Z

IT organizations face an abundance of vulnerabilities, some of which are trivial and some of which pose a significant risk. Without knowledge of what to tackle first, organizations become overwhelmed, and high-risk vulnerabilities can easily remain unaddressed. In this presentation, you'll learn the five key elements for successfully prioritizing vulnerability remediation. Then learn best practices for using tools that allow you to take full control of evolving threats by correlating active threats against your vulnerabilities, so you know which vulnerabilities to remediate first.

LUNCH AND LEARN

The Dark Web: What It Is, What's On It, and How to Find It

Speaker: Tyler Carbone, COO Terbium Labs
Wednesday, April 12 | 12:30-1:15pm | Location: Windermere W

From stolen credit cards to drugs to grilled cheese, the Dark Web covers the spectrum from threatening to funny. In this talk, Tyler will discuss the range of content on the dark web, how to access and navigate it, and how to find what you need – whether it's threats against your organization, stolen data, or "Under 21" Fake IDs for a cheap gym membership.

LUNCH AND LEARN

Stop the Exploits. Stop the Attacks. Keep Threats Off Your Devices, Before They Can Run

Speaker: Steve Weber, Sales Engineer, Sophos, Inc.
Wednesday, April 12 | 12:30-1:15pm | Location: Regency T

Ransomware is one of the biggest threats facing organizations today. The security industry has traditionally struggled to keep up with this sophisticated, ever-changing attack. Until now. Sophos Intercept X is a brand new solution that stops ransomware in its tracks. Deploying a range of innovative next-gen technologies to block all kinds of advanced attacks. It gives you comprehensive protection from ransomware, rootkits, zero-day vulnerabilities, malicious traffic, and everything in-between.

VENDOR EVENTS

ANOMALI™

LUNCH AND LEARN

So You've Got Threat Intelligence - Now What?

An introduction to making use of indicator expansion, workflows, and context

Speaker: Daniel Katz , Sales Engineer

Wednesday, April 12 | 12:30-1:15pm | Location: Windermere X

At this point the industry can agree that the idea of monitoring Threat Intelligence is here to stay, and that bringing that data into relevant security technologies is a crucial part of making use of it. But what can become a bit more convoluted, is how to prioritize, understand, and organize the resulting alerts. This session delves into the value of efficient workflows, "indicator expansion," and making use of the context around IOC's to help tackle the biggest problems first.

ENSILO

LUNCH AND LEARN

The Night of the Living XP: Attacks on Legacy and Embedded Systems

Speaker: Paul Schofield, Director of Customer Experience

Wednesday, April 12 | 12:30-1:15pm | Location: Windermere Y

The insecurity of legacy and embedded systems affects the financials, medical and critical infrastructure industries. We demonstrate how a threat actor targets these systems without the use of any 0-day, just by using a 10-year-old exploit to penetrate a critical device, disrupt its activities and tamper with its controls.

CISCO™

LUNCH AND LEARN

Anatomy of an Attack

Speaker: Mark Stanford, Systems Engineer Manager, Cisco

Wednesday, April 12 | 12:30-1:15pm | Location: Regency O

Cyber Criminals are increasingly exploiting the Internet services to build agile and resilient infrastructures, and consequently to protect themselves from being exposed and taken over. This session will explain how the correlation of Internet data on multiple levels (DNS, BGP, ASN, Prefixes/IPs) can be used to build and deliver a new model of security that is pervasive and predictive, and that allows us to expose the attackers' infrastructure. Detection models that can be built and applied (such as co-occurrences, NLPRank, and Spike Detectors), and how the different detectors can be integrated to expose malicious infrastructures and advanced persistent threats.

DINING OPTIONS

Hyatt Regency

B-Line Diner OPEN 24 HOURS

The B-Line Diner is open 24 hours serving breakfast, lunch and dinner as well as a late night menu. The B-Line Diner also offers carry-out service at the B-Line Express window. The B-Line Diner features a marble dining counter, an exhibition kitchen, homemade ice cream, desserts, and a display case featuring a wide variety of sumptuous homemade cakes, pastries and other confections. High energy, prompt service and fine food quality are the B-Line Diner's hallmarks.

Fiorenzo Italian Steakhouse 6-10 PM, MON-SAT

Fiorenzo, located on the Lobby level of the International Tower, combines the fun and excitement of an authentic Italian restaurant and the tradition of a great American steak house. An open kitchen and pizza oven set the stage for the on-site preparation of new and traditional Italian favorites, great steaks, chops and fish. In addition to viewing the creation of delicious grilled steaks, seafood entrées, creative pizzas and pasta dishes, guests may gather at the Milan-inspired lounge and select wines from our extensive, award-winning wine cellar. Each day, Fiorenzo features a Chef 's Special in addition to a wide assortment of the freshest fish, pasta, seafood and steaks. Reservations are recommended.

Lobby Bar OPEN 7 DAYS A WEEK – 11 AM – 8 PM

Located in the heart of the International Tower Lobby, the Lobby Bar offers great viewing of sporting events or a secluded cocktail with friends in the alcoves. Offering full beverage service and a selection of favorite finger foods.

Urban Tide Restaurant OPEN 7 DAYS A WEEK

BREAKFAST BUFFET 6-10:30 AM | LUNCH 11 AM - 2:30 PM MON-FRI | DINNER 6-10 PM

Fresh from our bountiful coast, Urban Tide features Florida seafood and chic coastal cuisine. Seasonal favorites are celebrated, and elevated with bold flavors served in a stylish setting. Pair lunch or dinner with a classic or our current take on favorite handcrafted cocktails, or select from a distinctive collection of craft beers and fine wines.

Rocks Lounge OPEN 7 DAYS A WEEK | 4 PM - 1:30 AM

Located off the Main Lobby, Rocks is the spot to see and be seen in! A chic, architecturally inspired lounge showcasing a premiere, world-class ambience of unparalleled service, passionately crafted modern cocktails and creative bar food offerings.

Coffee, Etcetera OPEN 7 DAYS A WEEK AT 5 AM

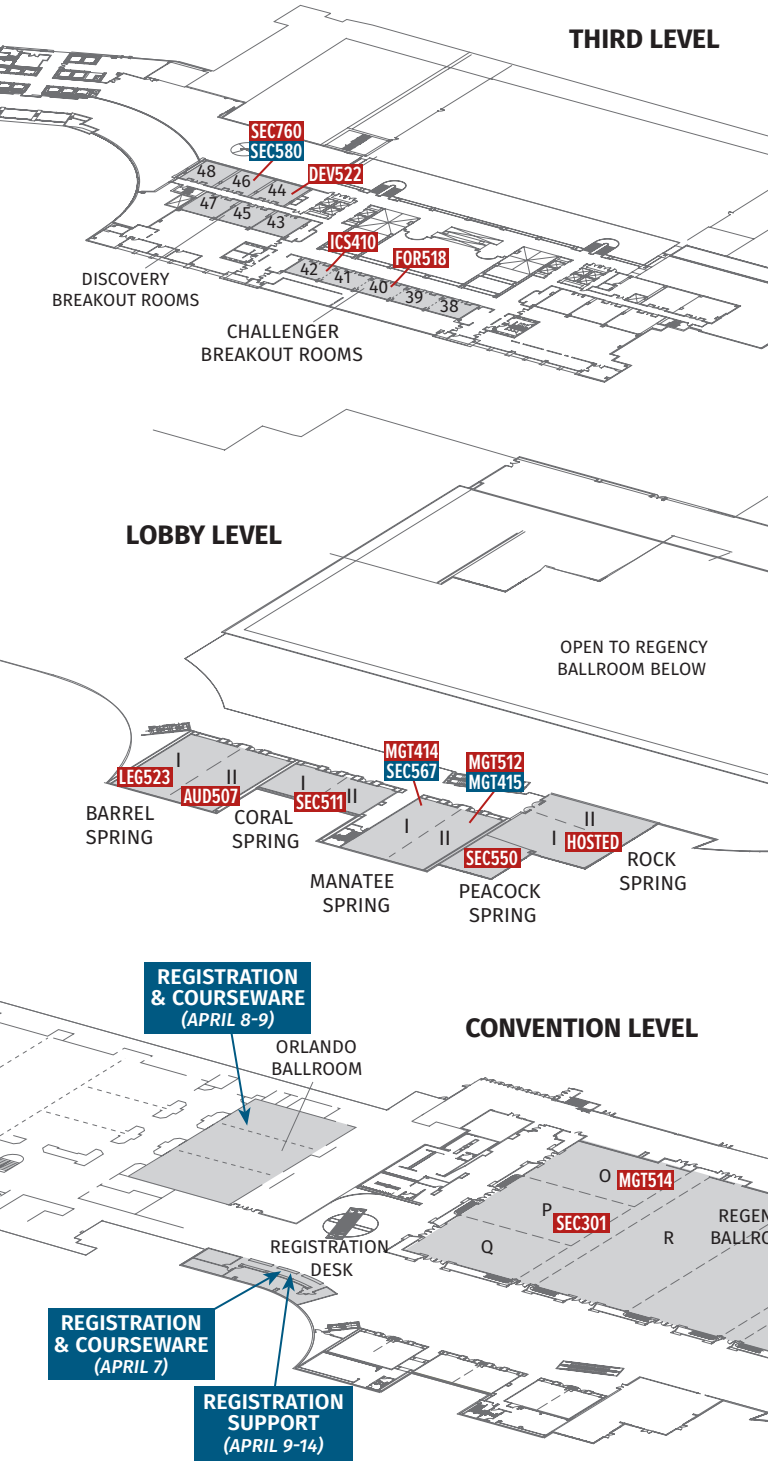
For those on the go, a full line of gourmet coffees and light bites can be found at the counter of Coffee, Etcetera!!

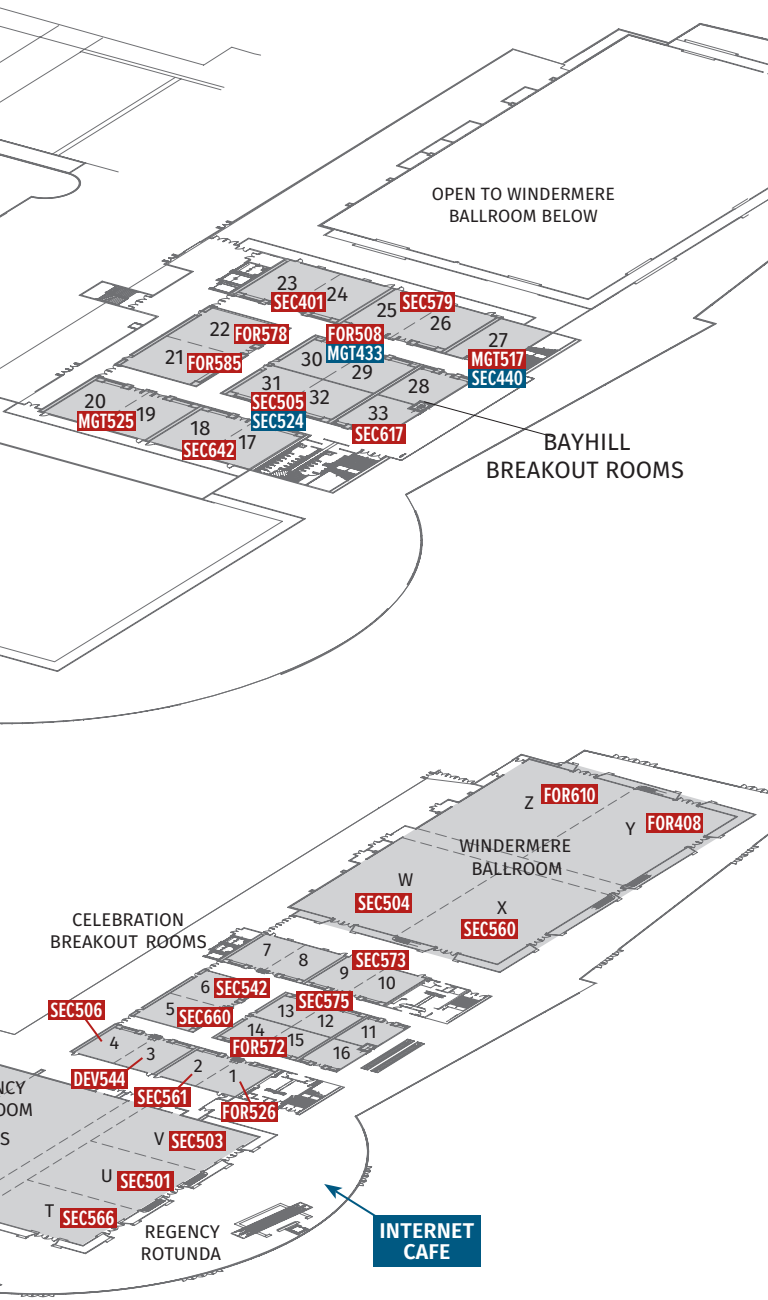
Coconuts Pool Side Bar & Grill OPEN 7 DAYS A WEEK

(WEATHER PERMITTING) 11 AM – SUNSET

Located poolside on the Pool level of the Regency Tower, enjoy the grilled foods, salads and sandwiches of the tropics along with your favorite cold beverage under swaying palm trees.

HOTEL FLOORPLANS




OPEN TO WINDERMERE
BALLROOM BELOW
23
24
SEC401
25
SEC579
26
22
FOR578
FOR508
27
21
FOR585
30
MGT433
MGT517
29
SEC440
31
SEC505
32
28
20
MGT525
19
SEC524
33
18
SEC617
17
SEC642
BAYHILL
BREAKOUT ROOMS

Z
FOR610
Y
FOR408
WINDERMERE
BALLROOM
W
SEC504
X
SEC560
CELEBRATION
BREAKOUT ROOMS
7
8
SEC573
9
10
6
SEC542
SEC506
5
SEC660
SEC575
13
12
4
14
11
3
15
FOR572
16
DEV544
2
1
SEC561
FOR526
V
SEC503
U
SEC501
T
SEC566
REGENCY
ROTUNDA
INTERNET
CAFE

Free SANS Resources

Stay connected with these FREE resources

WEBCASTS

Ask The Expert 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.

NEWSLETTERS

NewsBites – Twice weekly, high-level executive summary 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

Future Training Events

Baltimore Spring		
Baltimore, MD	April 24-29	#SANSBaltimore
Security West		
San Diego, CA	May 9-18	#SANSSecurityWest
Northern Virginia – Reston		
Reston, VA	May 21-26	#SANSReston
Atlanta		
Atlanta, GA	May 30 - June 4	#SANSAtlanta
Houston		
Houston, TX	June 5-10	#SANSHouston
San Francisco Summer		
San Francisco	June 5-10	#SANSSanFrancisco
Rocky Mountain		
Denver, CO	June 12-17	#SANSRocky
Charlotte		
Charlotte, NC	June 12-17	#SANSCharlotte
Minneapolis		
Minneapolis, MN	June 19-24	#SANSMinneapolis
Columbia		
Columbia, MD	June 26 - July 1	#SANSColumbia
ICS Energy – Houston		
Houston, TX	July 10-15	#ICSHouston
Long Beach		
Long Beach, CA	July 10-15	#SANSLongBeach
SANSFIRE		
Washington, DC	July 22-29	#SANSFIRE

Future Summit Events

Threat Hunting and IR		
New Orleans, LA	Apr 18-25	#ThreatHuntingSummit
Automotive Cybersecurity		
Detroit, MI	May 1-8	#SANSAutoSummit
DFIR		
Austin, TX	June 22-29	#DFIRSummit
Security Awareness		
Nashville, TN	July 31 - Aug 9	#SecAwareSummit

Information on all events can be found at
sans.org/security-training/by-location/all

Join us again next year!

SANS 2018

Orlando, FL

April 3-10 2018

Save the Date!

Hands-on, intensive cybersecurity training courses for highly seasoned InfoSec professionals as well as those new to the field or transitioning from more general IT roles.