Cyber Defense Initiative 2017
Washington, DC | Dec 12-19

Program Guide

@SANSInstitute  #SANSCDI
Add an OnDemand Bundle to your course to get an additional four months of intense training! OnDemand Bundles are just $729 when added to your live course, and include:

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

**COURSES AVAILABLE:**

- SEC301
- SEC401
- SEC501
- SEC503
- SEC504
- SEC505
- SEC511
- SEC542
- SEC555
- SEC560
- SEC566
- SEC573
- SEC575
- SEC579
- SEC642
- SEC660
- FOR500
- FOR508
- FOR526
- FOR578
- FOR585
- FOR610
- MGT414
- MGT512
- MGT514
- DEV522
- ICS410
- ICS515
- FOR572

To receive the discounted rate, you must sign up before Friday, December 29th 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
**General Information**

**Badge & Courseware Distribution**
*Location: Coats Room (Terrace Level)*
*Tue, Dec 12 (SHORT COURSES ONLY) .................. 8:00am - 9:00am*

*Location: Terrace Foyer (Terrace Level)*
*Wed, Dec 13 .................................................. 5:00pm - 7:00pm*
*Thu, Dec 14 .................................................. 7:00am - 9:00am*

**Registration Support**
*Location: Coats Room (Terrace Level)*
*Thu, Dec 14 - Mon, Dec 18 ......................... 9:00am - 5:00pm*
*Tue, Dec 19 .................................................. 9:00am - 2:00pm*

**Internet Café**
*Location: Concourse Foyer*
*Thu, Dec 14 .................................................. Opens at noon*
*Fri, Dec 15 - Mon, Dec 18 ............................ Open 24 hours*
*Tue, Dec 19 .................................................. Closes at 2:00pm*

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

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

**First Time at SANS?**
Please attend our Welcome to SANS talk designed to help you get the most from your SANS training experience. The talk is from **8:00am - 8:30am** on **Thursday, December 14** in *International Ballroom Center*.

**Photography Notice**
SANS may take photos of classroom activities for marketing purposes. SANS Cyber Defense Initiative 2017 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
- **SEC511**: Continuous Monitoring and Security Operations
- **SEC555**: SIEM with Tactical Analytics
- **SEC660**: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
- **MGT414**: SANS Training Program for CISSP® Certification

**Extended Hours:**
- **SEC504**: Hacker Tools, Techniques, Exploits, and Incident Handling
- **SEC560**: Network Penetration Testing and Ethical Hacking
- **MGT512**: SANS Security Leadership Essentials for Managers with Knowledge Compression™
<table>
<thead>
<tr>
<th>COURSE SCHEDULE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>START DATE:</strong> Tuesday, December 12</td>
</tr>
<tr>
<td><strong>Time:</strong> 9:00am - 5:00pm (Unless otherwise noted)</td>
</tr>
</tbody>
</table>

**SEC440:** Critical Security Controls: Planning, Implementing, and Auditing  
Russell Eubanks  
Location: Holmead West

**SEC564:** Red Team Operations and Threat Emulation  
Joe Vest  
Location: Oak Lawn

**SEC573:** Automating Information Security with Python  
Mark Baggett  
Location: Holmead West

**SEC566:** Implementing and Auditing the Critical Security Controls – In-Depth  
James Tarala  
Location: Holmead East

**SEC504:** Hacker Tools, Techniques, Exploits & Incident Handling  
Michael Murr  
Location: Columbia Hall 1/2  
Extended Hours: 5:00pm - 7:15pm (Course Day 1 only)

**SEC505:** Securing Windows and PowerShell Automation  
Jason Fossen  
Location: Columbia Hall 11

**SEC511:** Continuous Monitoring and Security Operations  
Eric Conrad  
Location: Jefferson East  
Bootcamp Hours: 5:15pm - 7:00pm (Course days 1-5)

**SEC542:** Web App Penetration Testing and Ethical Hacking  
Micah Hoffman  
Location: Georgetown West

**SEC545:** Cloud Security Architecture and Operations  
Dave Shackleford  
Location: Columbia Hall 5

**SEC555:** SIEM with Tactical Analytics  
Seth Misenar  
Location: Columbia Hall 4

**SEC560:** Network Penetration Testing and Ethical Hacking  
Stephen Sims  
Location: Columbia Hall 8  
Bootcamp Hours: 5:15pm - 7:00pm (Course days 1-5)

**SEC566:** Implementing and Auditing the Critical Security Controls – In-Depth  
James Tarala  
Location: Holmead East

**SEC575:** Mobile Device Security and Ethical Hacking  
Christopher Crowley  
Location: Kalorama

**SEC501:** Advanced Security Essentials – Enterprise Defender  
Paul A. Henry  
Location: Columbia Hall 3

**SEC503:** Intrusion Detection In-Depth  
David Hoelzer  
Location: Lincoln East

**FOR500:** Windows Forensic Analysis  
Ovie Carroll  
Location: Columbia Hall 12
FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting  
Chad Tilbury .......................... Location: Monroe

FOR526: Memory Forensics In-Depth  
Alissa Torres ......................... Location: Gunston East

FOR572: Advanced Network Forensics and Analysis  
Philip Hagen ........................ Location: Georgetown East

FOR578: Cyber Threat Intelligence  
Jake Williams ........................ Location: International Ballroom East

FOR585: Advanced Smartphone Forensics  
Heather Mahalik ........................ Location: Morgan

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques  
Lenny Zeltser ......................... Location: Columbia Hall 9/10

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

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

MGT514: IT Security Strategic Planning, Policy, and Leadership  
Frank Kim ............................. Location: Columbia Hall 7

DEV522: Defending Web Applications Security Essentials  
Dr. Johannes Ullrich .................. Location: Fairchild East

DEV540: Secure DevOps and Cloud Application Security  
Eric Johnson .......................... Location: Gunston West

ICS410: ICS/SCADA Security Essentials  
Billy Rios ............................. Location: Lincoln West

ICS515: ICS Active Defense and Incident Response  
Robert M. Lee ........................ Location: Oak Lawn

---

GIAC CERTIFICATIONS

Add a GIAC Certification with your SANS training at SANS Cyber Defense Initiative 2017 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 Cyber Defense Initiative 2017 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.

WEDNESDAY, DECEMBER 13

SPECIAL EVENT
Welcome Reception
Wed, Dec 13 | 5:00pm - 7:00pm | Location: International Terrace West
Check in early and network with your fellow students!

THURSDAY, DECEMBER 14

SPECIAL EVENT
General Session – Welcome to SANS
Speaker: Bryan Simon
Thu, Dec 14 | 8:00am - 8:30am | Location: International Ballroom Center
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
Exploitation 101: Stacks, NX/DEP, ASLR and ROP!
Speaker: David Hoelzer
Thu, Dec 14 | 7:15pm - 9:15pm | Location: International Ballroom Center
In this two-hour talk we will begin with basic stack overflows, then introduce the various protections one at a time and demonstrate how they are defeated. The talk will cover stack overflows, bypassing DEP/NX (non-executable stacks), defeating ASLR, and defeating code signing with ROP. While the talk covers technical topics, even those with less of a technical background will walk away with an appreciation of just how easy exploit development actually is!

SPECIAL EVENT
APAC Student Reception
at SANS Cyber Defense Initiative 2017
Thu, Dec 14 | 7:00pm - 8:00pm | Location: Lincoln East
The APAC Student Reception is an informal event, an opportunity for students to meet up with your SANS APAC team, SANS instructors, and other students from the Asia Pacific region.

FRIDAY, DECEMBER 15

SPECIAL EVENT
Girls and Women in Tech
Presented in partnership with ISSA Women in Security SIG, Women’s Society of Cyberjutsu, ISACA and WITI
Fri, Dec 15 | 5:30pm - 7:00pm | Location: Columbia Foyer West
SANS will be hosting approximately 80 girls scouts and middle schoolers for an afternoon of challenges created by Ed Skoudis and Women’s Society of Cyberjutsu. The young ladies will then join our regular Women’s CONNECT networking reception and have access to evening events. We invite SANS attendees who are interested to join our Women’s CONNECT networking reception. As always, this event is an opportunity to network with each other, the special young guests, and various partner organizations from the local area who are working to support women in STEM initiatives.

SPECIAL EVENT
GIAC Program Presentation
Speaker: Scott Cassity
Fri, Dec 15 | 6:15pm - 7:15pm | Location: Georgetown West
GIAC Certifications is 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.

SANS@NIGHT
Actionable Detects: Blue Team Cyber Defense Tactics
Speaker: Seth Misenar
Fri, Dec 15 | 7:15pm - 8:15pm | Location: Monroe
Organizations relying on third parties to detect breaches can go almost a full year before finding out they have been compromised. Detect the breach yourself, and on average you will find it within about a month of the initial occurrence. Mistaking detection and defense against modern adversaries as “too costly” to perform can result in a very expensive miscalculation – especially when you consider the substantially increased price of response and recovery with breach duration. Seth Misenar’s ever-evolving Actionable Detects provides you with the tactics, techniques, and procedures to once again take pride in your Blue Team Cyber capabilities. Not applying these lessons learned could prove costly in the face of adapting threat actors. Dig in and learn to hold your head high when talking about your defensive cyber operations capabilities.
The Three C’s to Building a Mature Awareness Program

Speaker: Lance Spitzner
Fri, Dec 15  |  7:15pm - 8:15pm  |  Location: Jefferson West

After working with hundreds of organizations, we have found three common obstacles to a successful awareness program, what we call the three C’s: 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.

Using an Open-Source Threat Model for Prioritized Defense

Speaker: James Tarala
Fri, Dec 15  |  7:15pm - 8:15pm  |  Location: Lincoln East

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

The 14 Absolute Truths of Security

Speaker: Keith Palmgren
Fri, Dec 15  |  7:15pm - 8:15pm  |  Location: Lincoln West

Keith Palmgren has identified 14 absolute truths of security – things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these 14 absolute truths and how they affect a security program can lead to the success of that program. Failing to recognize these truths will spell almost certain doom. Here we will take a non-technical look at each of the 14 absolute truths in turn, examine what they mean to the security manager, what they mean to the security posture, and how understanding them will lead to a successful security program.
Now that the price of a single Bitcoin surpasses the price of an ounce of gold, is blockchain becoming a runaway train with businesses scrambling to hop on? If so, how can you take advantage of this opportunity, and will the mistakes be minor or catastrophic? Blockchain as a technology has been proposed as a solution to everything from frictionless currency transfer to tracking cargo on ships. With over $1 billion in venture funds invested and several hundred patents filed, every security professional must know the impact on organizations in terms of risk, volatility, and competitiveness. This talk will explore alternative uses for blockchain technology other than cryptocurrency, and provide a framework for utilizing and securing a technology considered as disruptive as the Internet was in the 1990s.

SANS@NIGHT

An Interactive Look at Defeating Advanced Adversaries and Implementing Kill Chain Controls
Speaker: Stephen Sims
Fri, Dec 15  |  8:15pm - 9:15pm  |  Location: Lincoln West
SANS has a new Cyber Defense Essentials course – SEC599: Defeating Advanced Adversaries and Implementing Kill Chain Controls. After over a decade of penetration testing and exploit writing, Stephen Sims has partnered with Erik Van Buggenhout of nViso to leverage their experience and arm cyber defenders with the skills necessary to prevent attackers. Join Stephen and discuss the current threat landscape while observing demos from the new course.

SANS@NIGHT

Introducing DeepBlueCLI, a PowerShell Module for Hunt Teaming Via Windows Event Logs
Speaker: Eric Conrad
Sat, Dec 16  |  7:15pm - 8:15pm  |  Location: Monroe
A number of events are triggered in Windows environments during virtually every successful breach, including service creation events and errors, user creation events, extremely long command lines, compressed and base64 encoded PowerShell functions, and more. Microsoft has added a wealth of BlueTeam tools to its operating systems, including native support of logging the full command line used to launch all processes, without requiring third-party tools (or Sysmon). KB3004375 adds this feature to Windows 7 and Server 2008R2. DeepBlueCLI can automatically determine events that are typically triggered during most successful breaches, including use of malicious command lines including PowerShell.

SANS MASTER’S DEGREE PRESENTATION

Cloud Security Testing
Speaker: Edward Zamora – Master’s Degree Candidate
Fri, Dec 15  |  8:15pm - 8:55pm  |  Location: Georgetown East
Cloud technology use has increased exponentially in the last few years. Many companies have adopted the use of the cloud for reduction of costs and increased efficiencies and collaborative opportunities. These same companies have questioned whether they can trust that their information is protected. Organizations have legitimate concerns regarding the security of their intellectual property and other private data. Statistics show that data loss is among the top concerns for businesses in all industries. Information security professionals in these companies need to be able to assess the risks to an organization’s cloud, particularly if they are hosting it. In this talk, an overview of typical cloud components that make up a cloud will be given and examples will be provided showing how security testing methodologies can be applied.
SANS@NIGHT

Building an Effective Security Monitoring Program
Speaker: Jake Williams
Sat, Dec 16 | 7:15pm - 8:15pm | Location: Lincoln East

Security monitoring is hard, really hard. So hard that we fail at it regularly. Most breaches aren’t detected for months, many aren’t detected for years. This isn’t surprising since most defenders implement monitoring programs that are geared towards achieving compliance rather than catching attackers. But those goals need not be mutually exclusive. In this talk, Jake will share his years of experience architecting monitoring programs to help you build one that doesn’t suck, catches attackers, and will virtually guarantee your next promotion.

SANS@NIGHT

Malware Analysis for Incident Responders: Getting Started
Speaker: Lenny Zeltser
Sat, Dec 16 | 7:15pm - 8:45pm | Location: Jefferson West

Knowing how to analyze malware has become a critical skill for incident responders and forensic investigators. A good way to get started is to examine how malicious software behaves in a controlled laboratory environment. In this 90-minute briefing, Lenny Zeltser demonstrates key aspects of this process, walking you through behavioral analysis of a malware specimen by using several free tools and even peeking into the world of code analysis. You will see practical techniques in action and understand how malware analysis will help you triage the incident to assess key capabilities of the malicious software. You will also learn how to determine ways of identifying this malware on systems in your environment by establishing indicators of compromise. This presentation will help you start learning how to turn malware inside out.

SANS@NIGHT

Three Keys for SecDevOps Success
Speaker: Frank Kim
Sat, Dec 16 | 7:15pm - 8:15pm | Location: Georgetown West

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.

SANS@NIGHT

Industrial Control System Active Defense and Threat Intelligence
Speaker: Robert M. Lee
Sat, Dec 16 | 8:15pm - 9:15pm | Location: Lincoln West

Industrial control systems (ICS) are some of the most defensible environments on the planet. Sure, ICS tend to have legacy equipment and numerous vulnerabilities, but if you really want to make the lights blink, it’s going to take more than an exploit. In this presentation, the course author for ICS515: ICS Active Defense and Incident Response and FOR578: Cyber Threat Intelligence, will talk about what it means to make a defensible environment a defended one by leveraging active defense best practices such as threat hunting and network security monitoring. In addition, what types of threat intelligence are applicable to such environments will be covered with use-cases highlighting lessons learned for both good and bad practices. Ultimately, defending these industrial environments requires a human focus.

SANS@NIGHT

The Security Impact of IPv6
Speaker: Johannes Ullrich, Ph.D.
Sat, Dec 16 | 8:15pm - 9:15pm | Location: Monroe

IPv6 is more than just lots of addresses. IPv6 is protocol moving IP into the modern world of gigabit networks connecting billions of machines with gigabytes of RAM. In many ways, this transition is similar to the “DC” to “AC” power conversion in the late 1890s. While we still use DC in many places, AC has shown to be more flexible and scalable. Its initial adoption was hindered by security concerns, and DC supporters like Edison went to great lengths to demonstrate the security problems by stealing pets and electrocuting them in public displays. The fear of IPv6 is in many ways a fear of the unknown. IPv6 has some inherent risks, in particular if the protocol’s opportunities are not well understood, and if IPv4 thinking is applied to its deployment. We will discuss the impact of IPv6 on security architecture, intrusion detection, and network forensics, without harming anybody’s pet.

SANS@NIGHT

When IoT Attacks: Understanding the Safety Risks Associated With Connected Devices
Speaker: Billy Rios
Sat, Dec 16 | 8:15pm - 9:15pm | Location: Lincoln East

The Internet of Things (IoT) is all around us, making our lives more convenient. However, we’ve seen IoT devices being taken over to conduct DDoS attacks. We’ve heard about connected refrigerators being used to SPAM users and baby monitors being used to scream obscenities at infants. But could an IoT device be repurposed to physically attack an unsuspecting user? Let’s find out.
CORE  
NETWARS EXPERIENCE  

Hosted by Jeff McJunkin  
Sun, Dec 17 and Mon, Dec 18 | 6:30pm - 9:30pm  
Location: International Ballroom Center  

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  

Hosted by Alissa Torres & Jake Williams  
Sun, Dec 17 and Mon, Dec 18 | 6:30pm - 9:30pm  
Location: International Ballroom East  

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.

CYBER DEFENSE  
NETWARS TOURNAMENT  

Hosted by Eric Conrad & Seth Misenar  
Sun, Dec 17 and Mon, Dec 18 | 7:15pm - 10:15pm  
Location: International Ballroom West  

The all-new NetWars Defense Competition is a defense-focused challenge aimed at testing your ability to solve problems and secure your systems from compromise. With so much focus on offense, NetWars Defense is a truly unique experience and opportunity to test your skills in architecture, operations, threat hunting, log analysis, packet analysis, cryptography, and much more!

SANS@NIGHT  
Fortune 100 InfoSec on a Budget  
Speaker: Eric Capuano  
Sun, Dec 17 | 7:15pm - 8:15pm | Location: Georgetown West  

A common misconception is that it takes spending millions to be good at security. Not only is this untrue, but I will share ways that you can increase security posture while actually reducing spending. This talk outlines many of the tricks and mindsets to doing security well without breaking the bank. This is not the typical “Problem, problem, problem...” talk. This is a solution-based talk that goes back to many of the basic challenges facing SOC teams everywhere.

SANS@NIGHT  
Implementing an Enterprise Phishing Program  
Speaker: Serge Borso  
Sun, Dec 17 | 7:15pm - 8:15pm | Location: Jefferson West  

Phishing is the most prevalent variety of social attacks according to the 2017 Verizon DBIR. This talk will explain how to institute an enterprise-wide phishing program, for security awareness training of course : ), detailing critical elements to ensure success including:

- Technical approach to link and attachment based campaigns
- Web Development and Certificate integration for spear phishing campaigns
- Dealing with SPF records and troubleshooting SMTP issues
- Automation of sending, tracking, alerting and reporting
- Handling complaints and users
- Identifying goals, getting buy-in and handling backdoors/shells
- Adding value and ROI
- Tips and tricks for easier campaign creation and successful rollout
Vendor Solutions Expo
Fri, Dec 15  |  12:00pm - 1:30pm  |  5:30pm - 7:30pm
Location: International Terrace West
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
Fri, Dec 15  |  12:00pm-1:30pm  |  Location: International Terrace West
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:

- ThreatConnect
- HP
- Recorded Future
- LogRhythm
- ThreatQ
- ZeroFox
- InfoArmor
- Swimlane
- Cisco
- Kaspersky Labs
- NC4
- RedCanary
- NSS Labs
- VMRay
- Qualys
- Digital Guardian
- Domain Tools

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 at the Vendor Registration Desk.

How Threat Intelligence Helps You Calculate Risk to Obtain the Security Resources You Really Need
Speaker: Levi Gundert, Vice President of Threat Intelligence
Thu, Dec 14  |  12:30pm - 1:15pm  |  Location: Lincoln West
Cyber threat intelligence sounds intuitive to defenders, but creating a valuable practice that benefits the business is difficult. Threat intelligence only works to decrease risk in advance if risk is being quantitatively assessed on an ongoing basis. Do you know where there’s potential for real loss in your business? This session will enumerate a cyber threat taxonomy for risk with specific and recent examples to practically explore the implications (or lack thereof) for threat relevance and business loss, using Recorded Future as a case study.

The Future of Cyber Security
Speaker: Dr. Tommy Gardner, PE – CTO of HP Federal
Thu, Dec 14  |  12:30pm - 1:15pm  |  Location: Monroe
This talk will look at the potential for enhancing end point security, the threat and possibilities of quantum computing, algorithms, and encryption and then explore different facets of AI, such as machine learning, deep learning, neural networks and expert systems. Finally, we will look at the underlying technology driving cryptocurrencies and examine the role blockchain will play in protection of future systems. The goals will be to start thinking now how to design cyber protection into our systems to protect against a future threat.

Defeating Sandbox Evasion Techniques Used By Malware
Speaker: Ian Richardson – Sales Engineer, VMRay
Thu, Dec 14  |  12:30pm - 1:15pm  |  Location: Lincoln East
Join Ian Richardson, Sales Engineer at VMRay, as he takes a deeper look at the techniques malware authors use to evade sandbox detection, and what steps can be taken for organizations to restore hope in their malware sandbox.
2017 Security Trends
Speaker: Joey Muniz, Technical Solutions Architect
Thu, Dec 14 | 12:30pm - 1:15pm | Location: Georgetown East
This presentation will discuss how security trends are changing and what you can do to protect yourself from today and future threats. Know the best practices before, during, and after an attack.

Visibility and Security in the Age of Digital Transformation
Speaker: Gill Langston, Director of Product Management, Qualys
Thu, Dec 14 | 12:30pm - 1:15pm | Location: Jefferson East
As the move to digitally transform accelerates, IT and security teams face entirely new challenges. From securing devices beyond the traditional perimeter, to establishing security in the “shared responsibility model” of public clouds, IT organizations of all sizes are struggling to achieve visibility and prioritization across multiple platforms and resources. Learn about processes and technologies that will help you keep pace with this acceleration, and about best practices to ensure the most secure environment for you and your customers.

The Power of the Pivot: Poking the Bear with DomainTools
Speaker: Taylor Wilkes-Pierce, Sales Engineer
Thu, Dec 14 | 12:30pm - 1:15pm | Location: Jefferson West
In this session, you’ll get an overview of how to take indicators from your network, including domain names and IP addresses, and connect them with nearly every domain on the internet. Also walk through a deep-dive investigation into one of 2017’s most notorious phishing attacks to learn how to use domain data and pivoting to profile threat actors and prevent future attacks.
**Newsletters**

**NewsBites**
Twice-weekly, high-level executive summaries of the most important news relevant to cybersecurity professionals.

**OUCH!**
The world’s leading monthly free security awareness newsletter designed for the common computer user.

**@RISK: The Consensus Security Alert**
A reliable weekly summary of (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) how recent attacks worked, and (4) other valuable data.

**Webcasts**

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

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

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

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

**Other Free Resources**

(No portal account is necessary)
- InfoSec Reading Room
- Top 25 Software Errors
- 20 Critical Controls
- Security Policies
- Intrusion Detection FAQs
- Tip of the Day
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)
Cyber Defense Initiative 2018
Washington, DC | Dec 13-18

Join us again next year!

Save the Date!