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 | FOR500 | DEV522 |
| SEC506 | FOR508 | DEV541 |
| SEC511 | FOR518 | AUD507 |
| SEC542 | FOR526 | LEG523 |
| SEC560 | FOR572 | ICS410 |
| FOR578 |

To receive the discounted rate, you must sign up before Monday, September 18th at 8:00pm EDT.

Add to your order via your Portal Account: www.sans.org/account/login?url=history

Call or e-mail SANS Registration:
1-301-654-SANS (7267) | registration@sans.org

---

**TABLE OF CONTENTS**

- NetWars Tournaments ........................................ 1
- General Information ......................................... 2-3
- Course Schedule ............................................. 4-6
- GIAC Certifications ........................................... 7
- Bonus Sessions ............................................... 8-18
- Vendor Events ............................................... 19-22
- Future SANS events ......................................... 23
- Hotel Floorplans .............................................. 24-25

---

**Core NETWARS EXPERIENCE**

Hosted by Tim Medin
Wednesday, Sept 13 - Thursday, Sept 14
6:30pm - 9:30pm | Roman Ballroom

**DFIR NETWARS TOURNAMENT**

Hosted by Sarah Edwards & Heather Mahalik
Wednesday, Sept 13 - Thursday, Sept 14
6:30pm - 9:30pm | Florentine I/II

**CYBER DEFENSE NETWARS TOURNAMENT**

Hosted by Eric Conrad & Seth Misenar
Wednesday, Sept 13 - Thursday, Sept 14
7:15pm - 10:15pm | Milano VII/VIII

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

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

### Badge & Courseware Distribution

Location: Roman I Ballroom (Promenade Level)

- **Sat, Sept 9** (WELCOME RECEPTION) 5:00pm - 7:00pm
- **Sun, Sept 10 - Mon, Sept 11** 7:00am - 9:00am
  
  Location: Octavius Ballroom Foyer (Promenade South Level)
  
  - **Sat, Sept 16** (SHORT COURSES ONLY) 8:00am - 9:00am

### Registration Support

Location: Promenade Foyer (Promenade Level)

- **Sun, Sept 10 - Thu, Sept 14** 8:00am – 5:00pm
- **Fri, Sept 15** 8:00am - 2:00pm

### Internet Café

Location: Imperial Ballroom

- **Sun, Sept 10** Opens at noon
- **Mon, Sept 11 - Thu, Sept 14** Open 24 hours
- **Fri, Sept 15** 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 Sunday, September 10 in Milano VII/VIII.

### Photography Notice

SANS may take photos of classroom activities for marketing purposes. SANS Network Security 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
- **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™
SEC401: Security Essentials Bootcamp Style  
Stephen Sims ...................... Location: Neopolitan I  
Bootcamp Hours: 5:00pm - 7:00pm (Course days 1-5)

SEC503: Intrusion Detection In-Depth  
David Hoelzer ..................... Location: Octavius 20

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

SEC505: Securing Windows and PowerShell Automation  
Jason Fossen ....................... Location: Octavius 14

SEC506: Securing Linux/Unix  
Hal Pomeranz ...................... Location: Octavius 3

SEC511: Continuous Monitoring and Security Operations  
Bryan Simon ....................... Location: Octavius 17/18  
Bootcamp Hours: 5:15pm - 7:00pm (Course days 1-5)

SEC542: Web App Penetration Testing and Ethical Hacking  
Eric Conrad ....................... Location: Milano VII/VIII

SEC555: SIEM with Tactical Analytics  
Justin Henderson .................. Location: Octavius 6

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

SEC561: Immersive Hands-on Hacking Techniques  
Kevin Fiscus ....................... Location: Florentine III

SEC573: Automating Information Security with Python  
Michael Murr ...................... Location: Neopolitan II

SEC575: Mobile Device Security and Ethical Hacking  
Joshua Wright ..................... Location: Pompeian III

SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses  
Larry Pesce ......................... Location: Pompeian IV

SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques  
Adrien de Beaupre .................. Location: Florentine IV

SEC760: Advanced Exploit Development for Penetration Testers  
Jake Williams ...................... Location: Octavius 13  
Bootcamp Hours: 5:15pm - 7:00pm (Course days 1-5)

FOR500: Windows Forensic Analysis  
Chad Tilbury ....................... Location: Florentine II

FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting  
Rob Lee ............................ Location: Florentine I

FOR518: Mac Forensic Analysis  
Sarah Edwards ..................... Location: Salerno

FOR526: Memory Forensics In-Depth  
Alissa Torres ...................... Location: Sorrento

FOR572: Advanced Network Forensics and Analysis  
Philip Hagen ...................... Location: Neopolitan III

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

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques  
Lenny Zeltser ...................... Location: Milano II

MGT414: SANS Training Program for CISSP® Certification  
Seth Misenar ...................... Location: Octavius 9/10  
Bootcamp Hours: 8:00am - 9:00am (Course days 2-6) & 5:00pm - 7:00pm (Course days 1-5)

MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep  
Jeff Frisk ......................... Location: Octavius 5

DEV522: Defending Web Applications Security Essentials  
Dr. Johannes Ullrich ............. Location: Octavius 19

AUD507: Auditing & Monitoring Networks, Perimeters, and Systems  
Clay Risenhoover .................. Location: Octavius 21/22

HOSTED: Physical Security Specialist – Full Comprehensive Edition  
The CORE Group .................. Location: Neopolitan IV

SEC301: Intro to Information Security  
Keith Palmgren .................... Location: Milano I

Paul A. Henry ...................... Location: Octavius 1/2

SEC550: Active Defense, Offensive Countermeasures and Cyber Deception  
Bryce Galbraith .................... Location: Octavius 23

SEC566: Implementing and Auditing the Critical Security Controls – In-Depth  
James Tarala ....................... Location: Milano III

SEC579: Virtualization and Software-Defined Security  
Dave Shackleford .................. Location: Octavius 11
COURSE SCHEDULE

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
James Lyne ................................ Location: Octavius 7/8
*Bootcamp Hours: 5:15pm - 7:00pm (Course days 1-5)*

FOR578: Cyber Threat Intelligence
Robert M. Lee ............................. Location: Milano IV

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

MGT514: IT Security Strategic Planning, Policy, and Leadership
Frank Kim ................................. Location: Milano V

MGT517: Managing Security Operations:
Detection, Response, and Intelligence
Christopher Crowley ...................... Location: Pompeian II

DEV541: Secure Coding in Java/JEE: Developing Defensible Applications
Gregory Leonard ........................ Location: Messina

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

LEG523: Law of Data Security and Investigations
Benjamin Wright .......................... Location: Pompeian I

ICS410: ICS/SCADA Security Essentials
Justin Searle .............................. Location: Octavius 15/16

START DATE: Saturday, September 16
*Time: 9:00am - 5:00pm (Unless otherwise noted)*

SEC440: Critical Security Controls: Planning, Implementing, and Auditing
Chris Christianson ...................... Location: Octavius 9/10

SEC546: IPv6 Essentials
Dr. Johannes Ullrich ....................... Location: Octavius 21/22

SEC580: Metasploit Kung Fu for Enterprise Pen Testing
Bryce Galbraith .......................... Location: Octavius 13

MGT415: A Practical Introduction to Cyber Security Risk Management
James Tarala ............................. Location: Octavius 20

MGT433: Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program
Lance Spitzner ............................ Location: Octavius 19

DEV531: Defending Mobile Applications Security Essentials
Gregory Leonard ........................ Location: Octavius 14

DEV534: Secure DevOps: A Practical Introduction
Frank Kim ................................. Location: Octavius 11

Add a GIAC Certification with your SANS training at SANS Network Security 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 Network Security 2017 for a savings of $360! After this event is over, the alumni bundle price goes to $1,049.*

Stop by the Registration Support Desk or via your Portal Account www.sans.org/account/login?url=history to add your GIAC certification attempt before the last day of class for the discount.

Find out more about GIAC at www.giac.org or call 301-654-7267.
Enrich your SANS experience! Morning and evening talks given by our faculty and selected subject matter experts help you broaden your knowledge, get the most for your training dollar, and hear from the voices that matter in network and computer security.

SATURDAY, SEPTEMBER 9

SPECIAL EVENT
Welcome Reception
Saturday, Sept 9  |  5:00pm - 7:00pm
Location: Promenade Foyer

Check in early and network with your fellow students!

SUNDAY, SEPTEMBER 10

SPECIAL EVENT
General Session – Welcome to SANS
Speaker: Bryan Simon
Sunday, Sept 10  |  8:00am - 8:30am  |  Location: Milano VII/VIII

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
Actionable Detects: Blue Team Cyber Defense Tactics
Speaker: Seth Misenar
Sunday, September 10  |  7:15pm - 9:15pm  |  Location: Milano VII/VIII

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. Considering detection and defense against modern adversaries too costly to perform yourself can be a very expensive miscalculation considering the substantially increased price of response and recovery with breach duration. Seth Misenar’s ever evolving Actionable Detects presentation provides you thoughts, 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.

MONDAY, SEPTEMBER 11

SANS@NIGHT
The Cider Press: Extracting Forensic Artifacts from Apple Continuity
Speakers: Heather Mahalik & Sarah Edwards
Monday, Sept 11  |  7:15pm - 8:15pm  |  Location: Roman IV

Apple Continuity allows us to move between our devices without disruption in activity. Just think of the ultimate handoff where you can start browsing the Internet on your iPhone, continue on your Mac without the hassle of having to type a search a second time. Essentially, your devices work together enabling you to do less. Imagine how this looks on a Mac, iPhone or Apple Watch. Will you be able to tell which device the user conducted an activity on? What will the on-device forensic artifacts look like? Continuity requires inter-device communications, so what artifacts will be present on the WiFi and Bluetooth fronts? What if this feature would make or break your investigation?

SANS@NIGHT
The 14 Absolute Truths of Security
Speaker: Keith Palmgren
Monday, Sept 11  |  7:15pm - 8:15pm  |  Location: Milano II

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.

SANS@NIGHT
Introduction to Reversing with IDA
Speaker: Stephen Sims
Monday, Sept 11  |  7:15pm - 8:15pm  |  Location: Roman II

Have you ever been curious how to use the Interactive Disassembler (IDA) by Hex-Rays to reverse engineer applications, or just find the tool intimidating? Join me for an hour while I give a tour of IDA, its features, and automation through scripting. Various demonstrations will be performed to help tie the information being shared to real world examples. The concepts of disassembly and decompilation will also be addressed, as well as plug-ins and scripts that can be used to aide in exploit development and malware analysis.
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.

Industrial Control System Active Defense and Threat Intelligence

Speaker: Robert M. Lee

Monday, Sept 11 | 7:15pm - 8:15pm | Location: Florentine II

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 each environment is different so you, the customer, must tell them what you want the SIEM to do and then they’ll help with professional services or by replacing your current SIEM with something “better and more advanced.” This is hogwash. Organizations tend to have a lot of overlap through 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. This presentation is for you 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 Elasticsearch Stack, formerly ELK, most likely can beat what you have today. It is time to think outside the box, Come find out how one organization spent 14 months deploying a top magic quadrant SIEM solution only to have it beaten by ELK in two weeks.

Stuck in the Box: A SIEM’s Tale

Speaker: Justin Henderson

Monday, Sept 11 | 8:15pm - 9:15pm | Location: Roman II

There is an arms race between analysts and attackers. Modern malware obfuscates and subverts using techniques such as sophisticated code injection and anti-memory analysis mechanisms to destroy or corrupt volatile data. Examiners must have a deep understanding of memory internals and 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.

Increase Network Visibility: Methods to Feed IDS Sensors

Speaker: Brandon Peterson, Master’s Degree Candidate

Monday, Sept 11 | 8:15pm - 8:55pm | Location: Milano V

IDS sensors are a valuable tool for monitoring malicious activity on a network. However, to be useful, they must be fed with network traffic. This becomes challenging as most organizations no longer use a simple network architecture consisting of just an internal, DMZ, and external network. Instead, organizations split their internal network into many smaller segments, typically have multiple DMZs, and often utilize more than one ISP for Internet access. Additionally, most organizations will have multiple locations and may be using multiple cloud service providers. To inspect the traffic from multiple disparate environments, network security administrators need to understand the pros and cons of the many different methods of packet capturing available. This presentation discusses the most common methods available: Taps, SPANs, RSPANs, and ERSPAN. The discussion will also cover some of the tools and techniques used to benchmark these methods in your own environment. Understanding these methods will help ensure organizations can monitor their entire network in the most cost effective manner possible.

Coffee & Donuts with the Graduate School

Speaker: Shelley Moore

Tuesday, Sept 12 | 7:30am-9:00am

Location: Promenade Foyer (Front of Registration Desk)

Join us for coffee, donuts, and conversation with graduate school staff and current students. Learn more about SANS’s regionally accredited graduate program which combines SANS technical training and certifications, with leadership and management curriculum specifically designed for the unique needs of aspiring leaders. Find out how the class you’re taking this week may be applied towards a master’s degree or graduate certificate program. Visit www.sans.edu for complete information on curriculum, admissions, and funding options.
SPECIAL EVENT

Women’s CONNECT Event
Hosted by the SANS COINS Program and ISSA WIS SIG
Tuesday, Sept 12   |   Location: Genoa
6:00pm - 7:30pm – Networking Reception
7:15pm - 9:15pm – SANS@Night Bonus Sessions

Joins SANS and the ISSA International Women In Security Special Interest Group (WIS SIG) as we partner with local association chapters and groups to foster an evening of connections. Association members and group representatives will be on hand to discuss their activities and the benefits of membership. From Jean Jennings Bartik to Diane Greene, women have always been a driving force in the field of information technology. Their experiences have been filled not only with stories of overcoming challenges but also ones of innovation and inspiration. Enjoy the connection building and camaraderie of your peers, while discussing the recent successes relating to local luminaries such as Joann Maguire, Sandra Rothenberg, Pam Shockley-Zalabak, and Judith Wagner, among MANY others.

SPECIAL EVENT

GIAC Program Presentation
Speaker: Jeff Frisk
Tuesday, Sept 12   |   6:15pm - 7:15pm   |   Location: Florentine II

Global Information Assurance Certification (GIAC) develops and administers the premier certifications for information security professionals. More than 30 GIAC certifications align with SANS training and ensure mastery in critical, specialized InfoSec domains. GIAC certifications provide the highest and most rigorous assurance of cybersecurity knowledge and skill available to industry, government, and military clients across the world. Join us for an informational presentation along with a Q and A session. We’ll cover everything from why you should get certified, what testing looks like, how to keep certifications current and more. GIAC staff will be present to answer your questions before and after the presentation.

SANS@NIGHT

Introducing DeepBlueCLI, a PowerShell Module for Hunt Teaming via Windows Event Logs
Speaker: Eric Conrad
Tuesday, Sept 12   |   7:15pm - 8:15pm   |   Location: Milano VII/VIII

A number of events are triggered in Windows environments during virtually every successful breach. These include 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 a majority of successful breaches, including use of malicious command lines including PowerShell.

SANS@NIGHT

The Seven Deadly Sins of Incident Response
Speaker: Jake Williams
Tuesday, Sept 12   |   7:15pm - 8:15pm   |   Location: Roman II

In this session, Jake will walk you through the seven deadly sins of incident response. Incident response is not for the faint of heart and it’s far easier to get wrong than it is to get right. Jake’s been in the trenches working incident response with a huge number of clients, ranging in size from a few credit card records to one case where hundreds of millions of dollars were at stake. You’ll take away some valuable lessons to help prevent an incident response catastrophe that you can’t walk back.

SANS@NIGHT

Control Things Platform
Speaker: Justin Searle
Tuesday, Sept 12   |   8:15pm - 9:15pm   |   Location: Milano VII/VIII

SamuraiSTFU was a great start to help Electric Utilities do penetration testing of their DCS and SCADA networks, however it just wasn’t enough. SamuraiSTFU has expanded its goals to include all control systems and IoT devices, thus requiring a name change and a complete rebuild of the pentest distribution. Come check out the new Control Things Platform, a pentesting platform to help you learn, calibrate, and perform security testing of control networks in any ICS organization.

SANS@NIGHT

You’ve Got Ransomware!
Managing the Legal Risk of Cyber Fraud
Speaker: Benjamin Wright
Tuesday, Sept 12   |   7:15pm - 8:15pm   |   Location: Roman IV

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.

SANS@NIGHT

Lets Go Hunting Bad Guys
Speaker: John Strand
Tuesday, Sept 12   |   8:15pm - 9:15pm   |   Location: Roman II

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.
Ten Tenets of CISO Success
Speaker: Frank Kim
Tuesday, Sept 12 | 8:15pm - 9:15pm | Location: Roman IV

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.

How to Become a SANS Instructor
Speaker: Eric Conrad
Wednesday, Sept 13 | 12:30pm - 1:15pm | Location: Milano VII/VIII

This presentation is free of charge, but space is limited to the first 40 registrations. Please register online at www.sans.org/network-security

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.

SANS Core NetWars Experience
Hosted by Tim Medin
Wednesday, Sept 13 - Thursday, Sept 14
6:30pm - 9:30pm | Roman Ballroom

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.

SANS DFIR NetWars Tournament
Hosted by Sarah Edwards & Heather Mahalik
Wednesday, Sept 13 - Thursday, Sept 14
6:30pm - 9:30pm | Florentine I & II

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.

So, You Wanna be a Pentester?
Speaker: Adrien de Beaupre
Wednesday, Sept 13 | 7:15pm - 8:15pm | Location: Milano I

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.

Three Keys to Mobile Security: Are You Doing Everything You Can to Protect Your Apps?
Speaker: Gregory Leonard
Wednesday, Sept 13 | 7:15pm - 8:15pm | Location: Milano III

The threat landscape against mobile applications continues to grow. Malicious apps are still being discovered in the Apple and Google Play app stores, and questions continue to grow about how well-protected mobile users really are. To combat this increasing threat landscape, mobile devices are providing new hardware and software features to help protect users from exploitation. We will discuss how developers can use features such as fingerprint scanning, on-device cryptography, and MDM/MAM to provide a secure environment for users and their data.
will evolve and what to expect next. This attack vector, and we’ll venture predictions on how this “industry” “explosions” that went nowhere. We’ll offer insights into the future of and ACTUALLY WORK as evidenced by fully contained Ransomware. We’ll demonstrate tools and methodologies that are battle-proven the darn thing.” But what if you could stop Ransomware in its tracks? Costs far more than the average ransom, so executives just say, “Pay a billion dollar industry, and it’s getting even bigger. Lost productivity paralyzing your organization – we’ll show you how. Ransomware is a next is LOL! You can build defenses that prevent Ransomware from bypass traditional detection. This presentation will help you start learning how to turn malware inside out.

STI MASTER’S PRESENTATION
Don’t Always Judge a Packet by Its Cover
Speaker: Gabriel Sanchez, Master’s Degree Candidate
Wednesday, Sept 13 | 8:15pm - 8:55pm | Location: Milano II

This presentation is on research that tackles the challenges of honing in on packets of interest that may contain malicious intentions. Traditional approaches to this challenge typically rely on heuristics or signatures with a known bad which tend to be ineffective to the advanced attacker. This presentation will look at the approach of behavior analysis and profiling of packets to defend against attackers that bypass traditional detection.

SANS@NIGHT
Anti-Ransomware
Speaker: G. Mark Hardy
Wednesday, Sept 13 | 8:15pm - 9:15pm | Location: Milano I

OMG! We just got hit with Ransomware! What you don’t usually hear next is LOL! You can build defenses that prevent Ransomware from paralyzing your organization – we’ll show you how. Ransomware is a billion dollar industry, and it’s getting even bigger. Lost productivity costs far more than the average ransom, so executives just say, “Pay the darn thing.” But what if you could stop Ransomware in its tracks? We’ll demonstrate tools and methodologies that are battle-proven and ACTUALLY WORK as evidenced by fully contained Ransomware “explosions” that went nowhere. We’ll offer insights into the future of this attack vector, and we’ll venture predictions on how this “industry” will evolve and what to expect next.

SANS@NIGHT
Secure DevOps: Static Analysis & the Puma’s Tail
Speaker: Eric Johnson
Wednesday, Sept 13 | 8:15pm - 9:15pm | Location: Milano III

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 and take advantage of the opportunities provided by continuous integration and delivery pipelines. In this talk, we will explore how static analysis fits into Secure DevOps and introduce you to Puma Scan, an open-source .NET static analysis rules engine. Live demonstrations will show Puma Scan identifying vulnerabilities inside Visual Studio and in a Jenkins continuous integration (CI) build pipeline. Attendees will walk away with a better understanding of the role static analysis play in DevOps and a .NET static analysis engine to help secure your organization’s applications.

THURSDAY, SEPTEMBER 14

SANS@NIGHT
The Three Cs to Building a Mature Awareness Program
Speaker: Lance Spitzner
Thursday, Sept 14 | 7:15pm - 8:15pm | Location: Milano II

After working with hundreds of organizations we have found three common obstacles to a successful awareness program, which 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.

STI MASTER’S PRESENTATION
Selling Your Information Security Strategy
Speaker: David Todd, Master’s Degree Candidate
Thursday, Sept 14 | 7:15pm - 7:55pm | Location: Milano V

It is the information security leader’s responsibility to identify the gaps between the most significant security threats and vulnerabilities, compared with the organization’s current state. The information security leader should develop a strategy that aligns with the strategic goals of the organization and sells the gap mitigation strategy to executive management and the board of directors. Before embarking on this new adventure, clearly articulate what success looks like to your organization. What is the result you are driving to accomplish? Then develop a strategy to get you there. Take a play directly from the sales organization’s playbook - know yourself; know your customer; and know the benefits from your customer’s perspective. Following this simple strategy will help the information security leader close the deal of selling your information security strategy.
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.

Privacy and Legal Dimensions in Increasingly Connected Digital World

Speaker: Muzamil Riffat, Master’s Degree Candidate
Thursday, Sept 14 | 8:15pm - 8:55pm | Location: Milano V

The benefits of the reliance on the Internet and Digital Communication for our day-to-day activities are accompanied by complex privacy and legal related challenges. In the realm of privacy, there are subjective interpretations of the concept that are not universally accepted. Therefore, what privacy really means or entails is influenced by auxiliary factors such as culture, location, use of technology and perceived benefits from information sharing. The legal apparatus is inherently slow and not able to keep up with the rapid changes in the technology landscape. As technology is becoming more and more integral to our daily life, it was always feared that legal apparatus will sooner or later be tested with the cases involving information technology and privacy considerations. The presentation will explain the definition of privacy in the light of US constitution as well as what does it really mean to have a “reasonable” expectation of privacy. A case-study about the recent high-profile legal cases will be used to illustrate the complexities involved in such cases from information security and privacy perspectives.

Vendor Solutions Expo

Tuesday, Sept 12 | 12:00pm - 1:30pm | 5:30pm - 7:30pm
Location: Octavius Ballroom 24/25

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, Sept 12 | 12:00pm-1:30pm | Location: Octavius Ballroom 24/25

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.

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.

Vendor-Sponsored Lunch & Learns

Anomali
Bracket Computing
Bricata
Corelight
Crossmatch
Cylance
Datacom Systems
Forcpoint
ForeScout Technologies
InfoArmor
Kaspersky Labs
LogRhythm
Minerva Labs
Pwnie Express
Qualys
RiskIQ
SecurityZONES/Spamhaus
Sophos
Terbim Labs
VM Ray

18
19
The 2017 NSS Labs NGFW Test reports that many of the leading next generation firewalls are vulnerable to Advanced Evasion Techniques (AETs) that can let exploits and malware (including aggressive ransomware attacks like WannaCry) into your network undetected. Michael Knapp will demonstrate how well your firewalls and IPS defenses stand up to evasions with Evader, the world’s premier software-based testing environment for evasions. Watch how Evader by Forcepoint lets you interactively throw different types of attacks at firewalls and IPS devices to see whether they do their job – or just give lip service to security.

**Using DNS to Choke Malware, Botnets, and Ransomware**

*Speakers: Matt Stith, Spamhaus Technology; Arnie Bjorklund, SecurityZones*

Learn the best practices from Spamhaus: threat intelligence to choke botnets, mitigate ransomware, and block connections to malicious domains. Prevent the resolution of known, bad domains within your DNS resolver. DNS RPZ is a proven, cost effective, way to choke botnets, malware and mitigate DDoS attacks and it lets you apply policy, deny access, and control DNS resolution on your infrastructure, stopping connections to malicious domains and IPs.

**How to Beat Evasive Malware at Its Own Game**

*Speaker: Lenny Zeltser, VP Products*

Developing sophisticated attacks takes time and requires heavy investment. Attackers safeguard their methods by designing malicious software to remain unnoticed by security tools for as long as possible. This educational session discusses some of the common evasive techniques that malware authors incorporate into their creations. Moreover, it proposes several innovative approaches for turning such capabilities against malware to defend endpoints, turning adversaries’ strengths into weaknesses. Attend this session to learn how evasive malware achieves its objectives and to consider methods for defending against such threats without relying on signatures, behavioral patterns or machine learning models.

**Looking Beyond Your Four Walls: Periphery Threat Intelligence**

*Speaker: Josh Fu, Senior Sales Engineer*

Over 63% of the breaches last year involved compromised credentials and phishing scams. As such, organizations need to strongly consider the importance of looking beyond their four walls vital to protecting your organization. This presentation will teach you about the various ways that adversaries can and will use these techniques against you and what you can do to proactively protect yourselves.

**Does Your Current Firewall Rise Above the Evasion Gap?**

*Speaker: Michael Knapp, Director, Network Security Architects for the Americas and Office of the CISO*

The 2017 NSS Labs NGFW Test reports that many of the leading next generation firewalls are vulnerable to Advanced Evasion Techniques (AETs) that can let exploits and malware (including aggressive ransomware attacks like WannaCry) into your network undetected. Michael Knapp will demonstrate how well your firewalls and IPS defenses stand up to evasions with Evader, the world’s premier software-based testing environment for evasions. Watch how Evader by Forcepoint lets you interactively throw different types of attacks at firewalls and IPS devices to see whether they do their job – or just give lip service to security.

**How ForeScout Supports the Critical Security Controls**

*Speaker: Peter Underwood, Systems Engineer, ForeScout Technologies*

Automated endpoint visibility and control is a consistent theme in the Critical Security Controls (CSCs). Without the ability to see and effectively manage the diverse and growing population of devices that access your network resources, securing them is impossible. How can you streamline CSC adoption without cutting corners? During this session, we will explain how businesses are using an agentless visibility and control solution to accelerate this process with quick wins in the first four steps of this multistep process. We will also discuss the role agentless visibility and control plays in 13 other critical security controls.

**Data Breaches on the Dark Web: Between Defense and Response**

*Speaker: Alex Viana, VP of Engineering*

Data breaches are a constant threat, even to organizations that follow data security best practices. Once a breach is detected, incident response protocols kick in to mitigate their effect. But between breach and response, an interval estimated to be over 300 days on average, is an entire world of hidden forums, economic incentives, anonymous actors, and even marketing campaigns. This presentation will provide some insight into what happens to certain types of data between breach and response as briefly show how Terbium Lab’s Matchlight tool can help close this gap.

**Matchlight tool can help close this gap.**
ICS Down...It's Go Time!
Speaker: Jason Dely, Professional Services Technical Director, ICS and Critical Infrastructure
Wednesday, Sept 13  |  12:30pm - 1:15pm  |  Location: Milano IV

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.

Visibility and Security in the Age of Digital Transformation
Speaker: Gill Langston, Director of Product Management
Wednesday, Sept 13  |  12:30pm - 1:15pm  |  Location: Milano II

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.

Using In-Memory Techniques to Battle Linux Malware
Speaker: Nolan Karpinski, Product Lead
Wednesday, Sept 13  |  12:30pm - 1:15pm  |  Location: Milano VI

Linux malware increased 300% from 2015 to 2016*, and the threat is growing as organizations move more workloads to the cloud. Worse, malware is becoming increasingly sophisticated. Yet the common approach is to double down on existing signature and behavior-based detection techniques, which don’t prevent zero day attacks. Such malware will eventually beat your perimeter defenses. We need to be ready. Attendees will learn about the use of guest introspection technology to prevent common Linux malware techniques like in-memory privilege escalation, rootkits, and file-level persistence.

Why a Holistic Approach is Crucial in Cybersecurity
Speaker: Keith Buswell, Sales Engineer
Wednesday, Sept 13  |  12:30pm - 1:15pm  |  Location: Milano III

Learn how log analytics can help you dive deeper into the attack phases.

Future Training Events

<table>
<thead>
<tr>
<th>Event</th>
<th>Dates</th>
<th>Location</th>
<th>#Hashtag</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baltimore Fall</td>
<td>Sep 25-30</td>
<td>Baltimore, MD</td>
<td>#SANSBaltimore</td>
</tr>
<tr>
<td>Rocky Mountain Fall</td>
<td>Sep 25-30</td>
<td>Denver, CO</td>
<td>#SANSRocky</td>
</tr>
<tr>
<td>Phoenix – Mesa</td>
<td>Oct 9-14</td>
<td>Mesa, AZ</td>
<td>#SANSMesa</td>
</tr>
<tr>
<td>Tysons Corner Fall</td>
<td>Oct 14-21</td>
<td>McLean, VA</td>
<td>#SANSTysons</td>
</tr>
<tr>
<td>San Diego</td>
<td>Oct 30 - Nov 4</td>
<td>San Diego, CA</td>
<td>#SANSSanDiego</td>
</tr>
<tr>
<td>Seattle</td>
<td>Oct 30 - Nov 4</td>
<td>Seattle, WA</td>
<td>#SANSSeattle</td>
</tr>
<tr>
<td>Miami</td>
<td>Nov 6-11</td>
<td>Miami, FL</td>
<td>#SANSMiami</td>
</tr>
<tr>
<td>San Francisco Winter</td>
<td>Nov 27 - Dec 2</td>
<td>San Francisco, CA</td>
<td>#SANSSanFrancisco</td>
</tr>
<tr>
<td>Austin Winter</td>
<td>Dec 4-9</td>
<td>Austin, TX</td>
<td>#SANSAustin</td>
</tr>
<tr>
<td>Cyber Defense Initiative</td>
<td>Dec 12-19</td>
<td>Washington, DC</td>
<td>#SANSCDI</td>
</tr>
<tr>
<td>Security East</td>
<td>Jan 8-13</td>
<td>New Orleans, LA</td>
<td>#SANSSecurityEast</td>
</tr>
<tr>
<td>Northern VA Winter</td>
<td>Jan 15-20</td>
<td>Reston, VA</td>
<td>#SANSReston</td>
</tr>
<tr>
<td>Las Vegas</td>
<td>Jan 28 - Feb 2</td>
<td>Las Vegas, NV</td>
<td>#SANSLasVegas</td>
</tr>
<tr>
<td>Miami</td>
<td>Jan 29 - Feb 3</td>
<td>Miami, FL</td>
<td>#SANSMiami</td>
</tr>
<tr>
<td>Scottsdale</td>
<td>Feb 5-10</td>
<td>Scottsdale, AZ</td>
<td>#SANSScottsdale</td>
</tr>
</tbody>
</table>

Future Summit Events

<table>
<thead>
<tr>
<th>Event</th>
<th>Dates</th>
<th>Location</th>
<th>#Hashtag</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pen Test Hackfest</td>
<td>Nov 13-20</td>
<td>Bethesda, MD</td>
<td>#SANSHackfest</td>
</tr>
<tr>
<td>SIEM &amp; Tactical Analytics</td>
<td>Nov 28 - Dec 5</td>
<td>Scottsdale, AZ</td>
<td></td>
</tr>
<tr>
<td>Cyber Threat Intelligence</td>
<td>Jan 29 - Feb 5</td>
<td>Bethesda, MD</td>
<td></td>
</tr>
</tbody>
</table>

*Source: SANS Institute
Join us again next year!

NETWORK SECURITY 2018

Las Vegas, NV

Sept 23-30, 2018

Save the Date!

Returning to Caesars Palace!