
FOUNDING PARTNER
CARBON BLACK
ARM YOUR ENDPOINTS
Threat Hunting & Incident Response
SANS DFIR | Summit & Training
APR 18-25, 2017 | NEW ORLEANS
Will you be the hunter or the prey?

Threat Hunting & Incident Response

SANS DFIR | Summit & Training

SUMMIT:	TRAINING:	LOCATION:
April 18-19	April 20-25	New Orleans

Gather your incident response team – it's time to go hunting!

- **Two days of in-depth Threat Hunting & Incident Response Summit talks** Top experts will discuss specific methods and techniques that can be utilized to identify, contain, and eliminate adversaries targeting your networks.
- **Seven world-class SANS courses** Following the two-day Summit, choose from seven hands-on, immersion-style courses taught by real-world practitioners.
- **Exclusive networking opportunities and bonus evening sessions** Join your peers for a night out in New Orleans, DFIR NetWars, and SANS@Night talks.

"Awesome material and presenters with a wide degree of coverage and content on threat hunting."

-Dallas Moore, Threat Hunter, PepsiCo

SAVE $200

when you register and pay for the Summit by Feb 22nd – Use code **EarlyBird17**

@sansforensics

#ThreatHuntingSummit

DON'T BE THE PREY, REGISTER TODAY AT

www.sans.org/ThreatHunting

SANS Training Courses

April 20-25, 2017

FOR508: **Advanced Digital Forensics, Incident Response, and Threat Hunting**
Instructor: Jake Williams | Certification: GCFA

FOR526: **Memory Forensics In-Depth**
Instructor: Alissa Torres

FOR572: **Advanced Network Forensics and Analysis**
Instructor: Philip Hagen | Certification: GNFA

FOR578: **Cyber Threat Intelligence**
Instructors: Robert M. Lee & Scott Roberts

FOR610: **Reverse-Engineering Malware: Malware Analysis Tools and Techniques**
Instructor: Anuj Soni | Certification: GREM

SEC550: **Active Defense, Offensive Countermeasures, and Cyber Deception**
Instructor: Chris Pizor

MGT517: **Managing Security Operations: Detection, Response, and Intelligence** NEW!
Instructor: Christopher Crowley

SAVE $400
when you you register for the THIR Summit and a SANS course

DON'T BE THE PREY, REGISTER TODAY AT
www.sans.org/ThreatHunting

FEATURED THREAT HUNTING & IR SUMMIT TALKS

KEYNOTE PRESENTATION

Rob Lee
@robtlee
@sansforensics
Lead – DFIR Curriculum, SANS Institute

Rob Lee is a Fellow and the Digital Forensics and Incident Response curriculum lead at SANS. He graduated from the U.S. Air Force Academy and served as a founding member of the 609th Information Warfare Squadron. Prior to starting his own firm, Rob worked with a variety of government agencies and Mandiant, where he held digital forensics and incident response roles.

"The Threat Hunting and Incident Response Summit brings together many of the tactics and secrets that teams have used successfully in their own organizations. I'm honored to be a part of it!"

-Rob Lee

KEYNOTE PRESENTATION

JJ Guy
@jjguy
Senior Director and Founding Team, Carbon Black

J.J. Guy was part of the founding team of Carbon Black in November, 2012. Prior to Cb, he spent 12 years with various federal offensive network operations teams. He's been preaching about the inevitability of compromise (and thus the need for threat hunting and continuous incident response) since 2003. He's finally excited for the rest of the world to recognize the problem – so he's no longer "that crazy government guy."

"Last year's inaugural Threat Hunting & Incident Response Summit was an incredible event for a sold-out crowd and Carbon Black was very grateful to participate as a founding partner. There are many practitioners hunting threats every day who are anxious both to share their hunting strategies and learn from their colleagues. We are delighted to help shape the new community."

-JJ Guy

The Myth of Automated Hunting and Case Studies in ICS/SCADA Networks

Robert M. Lee
@RobertMLee
CEO, Dragos; Certified Instructor, SANS Institute

Threat hunting is a human-focused process. Automation is an important part of being able to hunt effectively and consistently over time, but threat hunting cannot be fully automated. The important aspect of threat hunting is pitting the best human defenders against the human threats we face. This presentation makes the case that threat hunting cannot be fully automated. This will be done through a discussion on where the approach should exist in an organization's security maturity model and will be reinforced with examples of hunting inside of ICS/SCADA networks such as those that operate the power grid, oil facilities, and petrochemical environments.

Billions and Billions of Logs, Oh My!

Jack Crook
@jackcr
Principal Incident Responder, General Electric

There is no such thing as the perfect intrusion. Attackers will always leave behind traces of their activity as they move from system to system, trying to reach their objective. Unfortunately, traditional detection is never perfect either, and subtle signs are often missed by this technology. Adversaries can remain on your network for months or years, siphoning money or intellectual property, before they are eventually found. By adding a hunting program you stand a much greater chance of reducing dwell time and impact, but the question is, how do you wade through the vast amounts of log data to find the adversary in the haystack? Companies can consume enormous amounts of logs. Reviewing this data can be a daunting task when asked to find malicious behavior. This talk will focus on effective ways to implement hunts so that you can greatly reduce the amount of data you are analyzing while being more effective at finding bad.

Toppling the Stack: Outlier Detection for Threat Hunters

David Bianco
@davidjbianco
Incident Detection & Response Specialist, Sqrrl

So much of what we do as hunters is based on finding oddballs, but most published hunt procedures seem to rely on a single method: stack counting. In this session, we'll examine a few other ways of finding outliers in your data, with samples and use cases for each.

THREAT HUNTING & IR SUMMIT SPEAKERS

Heather Adkins
Google, Director of Information Security

Speaker & Summit Advisory Board

@argvee

Lesley Carhart
Motorola Solutions, Incident Response Team Lead

Summit Advisory Board

@hacks4pancakes

Jared Atkinson
Veris Group, Defensive Services Technical Lead

TALK TITLE:
Taking Hunting to the Next Level: Hunting in Memory

@jaredcatkinson

Michel Coene
NVISO, Senior Information Security Consultant

TALK TITLE:
So Many Ducks, So Little Time

@coenemichel

Matias Bevilacqua
Mandiant, Senior Incident Response Consultant

TALK TITLE:
ShimCache and AmCache Enterprise-wide Hunting: Evolving Beyond Grep

Jack Crook
General Electric, Principal Incident Responder

TALK TITLE:
Billions and Billions of Logs; Oh My!

@jackcr

David Bianco
Sqrrl, Incident Detection & Response Specialist

TALK TITLE:
Toppling the Stack: Outlier Detection for Threat Hunters

@davidjbianco

Maxim Deweerdt
NVISO, Senior Information Security Consultant

TALK TITLE:
So Many Ducks, So Little Time

@AlfaSec

Josh Bryant
Microsoft, Cybersecurity Architect

TALK TITLE:
Hunting Webshells on Microsoft Exchange Server

@FixTheExchange

JJ Guy
Carbon Black, Summit Advisory Board

Keynote

@jjguy

Sergio Caltagirone
Dragos, Inc., Director - Threat Intelligence & Analytics

TALK TITLE:
Deriving Successful Hunting Strategies with the Diamond Model

@cnoanalysis

THREAT HUNTING & IR SUMMIT SPEAKERS

Philip Hagen
Red Canary, DFIR Strategist; SANS Institute, Certified Instructor

Summit Advisory Board

@jessekornblum

Alex Pinto
Niddel, Chief Data Scientist

TALK TITLE:
Biting into the Jawbreaker: Pushing the Boundaries of Threat Hunting Automation

@alexcpsec

Jesse Kornblum
Facebook, Network Security Engineer

Summit Advisory Board

@jessekornblum

Chris Sanders
Fireye, Senior Analyst

TALK TITLE:
The Mind of a Hunter: A Cognitive, Data-Driven Approach

@chrissanders88

Rob Lee
SANS Instititute, SANS Fellow

Summit Chair & Keynote

@robtlee
@sansforensics

Joseph Ten Eyck
Target Corporation, Lead Information Security Analyst

TALK TITLE:
Framing Threat Hunting in the Enterprise

@joseph.teneyck

Rob M. Lee
Dragos, CEO; SANS Institute, Certified Instructor

TALK TITLE:
The Myth of Automated Hunting and Case Studies in ICS/SCADA Networks

@RobertMLee

Bamm Visscher
General Motors, CIRT Manager

Summit Advisory Board

@bammv

Alex Maestretti
Netflix, Engineering Manager

TALK TITLE:
Hunting on AWS

@maestretti

Austin Whisnant
Software Engineering Institute, Member of the Technical Staff

TALK TITLE:
Threat Hunting with Network Flow

Chris McCann
Uber, Senior Security Engineer

Summit Advisory Board

FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting

Instructor: Jake Williams @MalwareJake

This in-depth incident response course provides responders with advanced skills to hunt down, counter, and recover from a wide range of threats within enterprise networks, including APT adversaries, organized crime syndicates, and hactivism.

THE ADVANCED PERSISTENT THREAT IS IN YOUR NETWORK – IT'S TIME TO GO HUNTING!

"The most in-depth, state-of-the-art IR course I can imagine. It's the first time I think defense can actually gain an advantage."

-Kai Thomsen, AUDI AG

- Learn how to track advanced persistent threats in your enterprise
- Perform incident response on any remote enterprise system
- Examine memory to discover active malware
- Perform timeline analysis to track the steps of an attacker on your systems
- Discover unknown malware on any system
- Perform deep-dive analysis to discover data hidden by anti-forensics

www.sans.org/THIR-FOR508

GIAC Certified Forensic Analyst GCFA

www.giac.org/gcfa

FOR526: Memory Forensics In-Depth

Instructor: Alissa Torres @sibertor

Memory analysis is now a crucial skill for any incident responder who is analyzing intrusions. The malware paradox is key to understanding that while intruders are becoming more advanced with anti-forensic tactics and techniques, it is impossible to hide their footprints completely from a skilled incident responder performing memory analysis.

MALWARE CAN HIDE, BUT IT MUST RUN

"Totally awesome, relevant and eye opening. I want to learn more every day."

-Matthew Britton, Blue Cross Blue Shield of Louisiana

- Utilize stream-based data parsing tools to extract AES-encryption keys
- Capture, examine and analyze physical memory image and structures
- Windows, Mac, and Linux Memory Analysis Covered
- Conduct Live System Memory Analysis
- Extract and analyze packed and non-packed PE binaries from memory
- Gain insight into the latest anti-memory analysis techniques and how to overcome them

sans.org/THIR-FOR526

FOR572: Advanced Network Forensics and Analysis

Instructor: Philip Hagen @PhilHagen

This course was built from the ground up to cover the most critical skills needed to mount efficient and effective incident response investigations. We focus on the knowledge necessary to expand the forensic mindset from residual data on the storage media from a system or device to the transient communications that occurred in the past or continue to occur.

BAD GUYS ARE TALKING – WE'LL TEACH YOU TO LISTEN

"I research ICS/SCADA environments. I think FOR572 presents a better approach at detecting malware than a more traditional approach does."

-Niklas Vilhelm, Norwegian National Security Authority

- Extract files from network packet captures and proxy cache files
- Use historical NetFlow data to identify relevant past network occurrences
- Reverse engineer custom network protocols
- Decrypt captured SSL traffic to identify attackers' actions
- Incorporate log data into a comprehensive analytic process
- Learn how attackers leverage man-in-the-middle tools
- Analyze network protocols and wireless network traffic

www.sans.org/THIR-FOR572

GIAC NETWORK FORENSIC ANALYST GNFA

www.giac.org/gnfa

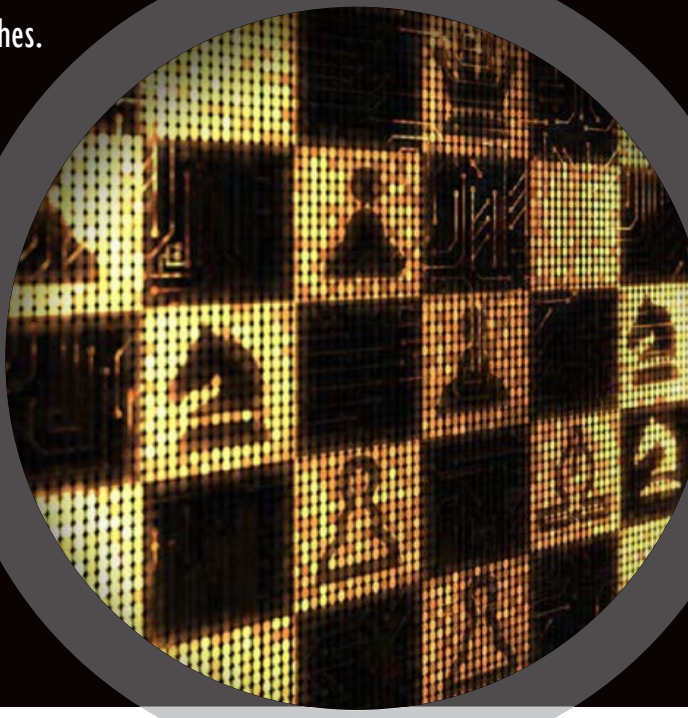
FOR578: Cyber Threat Intelligence

Instructors:

Robert M. Lee @RobertMLee & Scott Roberts @sroberts

During a targeted attack, an organization needs the best incident response and hunting team in the field, poised to combat these threats and armed with intelligence about how they operate. FOR578: Cyber Threat Intelligence will train you and your team to respond to, detect, scope, and stop intrusions and data breaches.

Now Available OnDemand



THERE IS NO TEACHER BUT THE ENEMY!

"What is threat intelligence? When am I ready for it? How do I use it? This class answers these questions and more at a critical point in the development of the field of threat intelligence in the wider community."

-Robert M. Lee, FOR578 Co-author

- Determine the role of cyber threat intelligence in your job
- Know when the analysis of an intrusion by a sophisticated actor is complete
- Identify, extract, prioritize, and leverage intelligence from advanced persistent threat (APT) intrusions
- Expand upon existing intelligence to build profiles of adversary groups
- Leverage collected intelligence to be more successful in defending against and responding to future intrusions
- Manage, share, and receive intelligence on APT actors

www.sans.org/THIR-FOR578

FOR610: REM: Malware Analysis Tools and Techniques

Instructor: Anuj Soni @asoni

This popular malware analysis course has helped forensic investigators and incident responders acquire practical skills for examining malicious programs that target Microsoft Windows. This training also teaches how to reverse-engineer web browser malware implemented in JavaScript, as well as malicious documents such as PDF and Microsoft Office files.

TURN
MALWARE
INSIDE OUT

"FOR610 should be required training for all forensic investigators. It is necessary for awareness, analysis, and reporting of threats."

-Paul G., U.S. Army

- Build an isolated lab for analyzing malicious code
- Employ network and system-monitoring tools for malware analysis
- Examine malicious JavaScript and VB Script
- Use a disassembler and debugger to analyze malicious Windows executables
- Bypass a variety of defensive mechanisms designed by malware authors
- Derive Indicators of Compromise (IOCs) from malicious executables
- Utilize practical memory forensics techniques to understand malware capabilities

www.sans.org/THIR-FOR610

GIAC REVERSE ENGINEERING MALWARE
GREM

www.giac.org/grem

SEC550: Active Defense, Offensive Countermeasures and Cyber Deception

Instructor: Chris Pizor @chris_pizor

This course is based on the Active Defense Harbinger Distribution live Linux environment funded by the Defense Advanced Research Projects Agency (DARPA). This virtual machine is built from the ground up for defenders to quickly implement Active Defenses in their environments. The course is very heavy with hands-on activities – we won't just talk about Active Defenses, we will work through labs that will enable you to quickly and easily implement what you learn in your own working environment.

DEVELOPING NEW STRATEGIES TO DEFEND OURSELVES

"SEC550 is the next step in the evolution of cyber defense – learning to make the hackers' job harder, track their movement, and get attribution."

-Mick Leach, Nationwide

- Track bad guys with callback Word documents
- Use Honeybadger to track web attackers
- Block attackers from successfully attacking servers with honeyports
- Block web attackers from automatically discovering pages and input fields
- Understand the legal limits and restrictions of Active Defense
- Obfuscate DNS entries
- Create non-attributable Active Defense Servers
- Combine geolocation with existing Java applications

www.sans.org/THIR-SEC550

MGT517: Managing Security Operations: Detection, Response, and Intelligence

Instructor: Christopher Crowley @CCrowMontance

NEW!

This course covers the design, operation, and ongoing growth of all facets of the security operations capabilities in an organization. An effective Security Operations Center (SOC) has many moving parts and must be designed with the ability to adjust and work within the constraints of the organization. To run a successful SOC, managers need to provide tactical and strategic direction and inform staff of the changing threat environment as well as provide guidance and training for employees.

ARMED WITH A ROADMAP TO DESIGN AND OPERATE AN EFFECTIVE SOC

"SANS coursework is not only conceptual, but also hands-on, showing you what to do, why you do it, and how you can apply what you learn to real-world solutions to problems."

-Duane Tucker, Barmark Partners

- Design security operations to address all needed functions for the organization
- Select technologies needed to implement the functions for a SOC
- Maintain appropriate business alignment with the security capability and the organization
- Develop and streamline security operations processes
- Strengthen and deepen capacity
- Collect data for metrics, report meaningful metrics to the business, and maintain internal SOC performance metrics

www.sans.org/THIR-MGT517

INSTRUCTOR BIOS

Christopher Crowley

Christopher Crowley has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. Christopher is the course author for SANS MGT535: Incident Response Team Management, and holds several information security certifications. @CCrowMontance

Philip Hagen

Philip Hagen has been working in the information security field since 1998, running the full spectrum including deep technical tasks, management of an entire computer forensic services portfolio, and executive responsibilities. Phil started his security career while attending the U.S. Air Force Academy. He served in the Air Force as a communications officer at Beale AFB and the Pentagon. @PhilHagen

Robert M. Lee

Robert obtained his start in cybersecurity serving as a Cyber Warfare Operations Officer in the U.S. Air Force. He is a SANS Certified Instructor, the course author of SANS ICS515: Active Defense and Incident Response, and the co-author of SANS FOR578: Cyber Threat Intelligence.
@RobertMLee

Chris Pizor

Chris Pizor is a civilian employee working for the U.S. Air Force as the lead curriculum designer for cyber warfare operations training. Chris served on active duty in the USAF as a Network Intelligence Analyst before retiring in 2010. He was part of the initial cadre of the NSA Threat Operations Center and helped develop tactics to discover and eradicate intrusions into U.S. government systems. @chris_pizor

Scott Roberts

Scott Roberts is an incident responder, manager, and developer at GitHub, the world's code collaborative development platform. Scott has worked major investigations involving criminal fraud and abuse and nation-state espionage while with Symantec, Mandiant, and others. He is an author of O'Reilly's upcoming Intelligence Driven Incident Response. @sroberts

Anuj Soni

Anuj Soni is a Senior Incident Responder at Booz Allen Hamilton, where he leads forensic, malware, and network analysis efforts to investigate security incidents. He received his bachelors and masters degrees from Carnegie Mellon University and holds several information security certifications. @asoni

Alissa Torres

Alissa Torres is a certified SANS instructor specializing in advanced computer forensics and incident response. Her industry experience includes serving in the trenches as part of the Mandiant Computer Incident Response Team (MCIRT) as an incident handler and working on an internal security team as a digital forensic investigator. She holds a bachelors degree from the University of Virginia and a masters from the University of Maryland in information technology. @sibertor

Jake Williams

Jake Williams is a Principal Consultant at Rendition Infosec. He has more than a decade of experience in secure network design, penetration testing, incident response, forensics, and malware reverse engineering. Before founding Rendition Infosec, Jake worked with various cleared government agencies in information security roles. @MalwareJake

DFIR NETWARS

Are you one of the top DFIR professionals?

2 Nights of DFIR NetWars at Threat Hunting & Incident Response Summit 2017

APRIL 23-24 | 6:30-9:30 PM

Join us for this exciting event to test your skills in a challenging and fun learning environment. Registration for NetWars is **FREE OF CHARGE TO ALL STUDENTS AT SANS THREAT HUNTING & IR SUMMIT 2017**. External participants are welcome to join for an entry fee of $1,520.

SANS DFIR NetWars Tournament is an incident simulator packed with a vast amount of forensic and incident response challenges for individual or team-based "firefights." It is developed by incident responders and forensic analysts who use these skills daily to stop data breaches and solve complex crimes. DFIR NetWars Tournament allows each player to progress through multiple skill levels of increasing difficulty, learning first-hand how to solve key challenges they might experience during a serious incident. DFIR NetWars Tournament enables players to learn and sharpen new skills prior to being involved in a real incident.

www.sans.org/ThreatHunting

EVENING BONUS SESSIONS

Enrich your SANS training experience!

Evening talks by our instructors and selected subject-matter experts help you broaden your knowledge, hear from the voices that matter in computer security, and get the most for your training dollar.

What Aren't You Seeing (Yet) in Memory Examinations: Examining Writeable Process Memory

Jake Williams and Alissa Torres

When I reach into my tool bag, I rarely find exactly the right tool for the job. In this session, we'll walk through identifying a problem experienced in an investigation, identifying potential work arounds, and writing a tool to solve the problem. Then we'll use the new tool to do some examination of writable process memory and see what we can find (the answer is A LOT). This will be an interactive session with example memory images. Bring a laptop if you want to work along – as long as you have a SIFT with volatility 2.5 you will be ready to play.

Opening a Can of Active Defense and Cyber Deception to Confuse and Frustrate Attackers

Chris Pizor

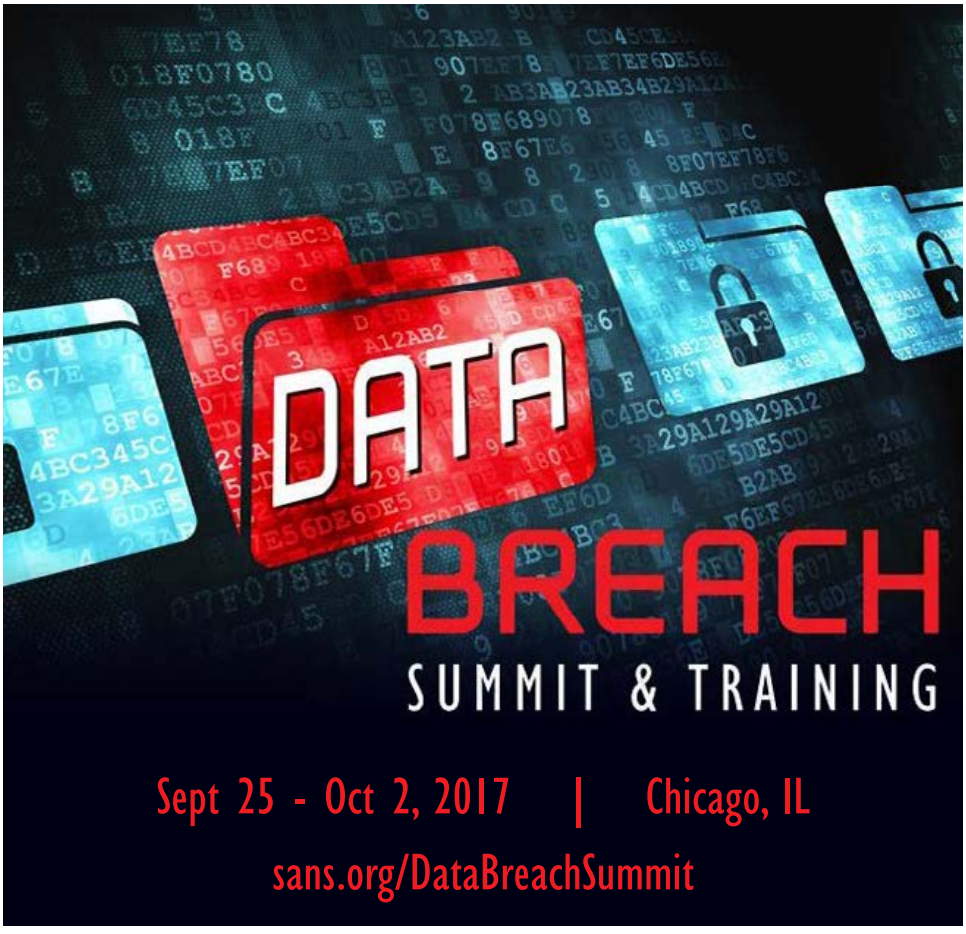
You're convinced that something just isn't right in your environment and you're tired of hearing that there hasn't been any A/V, IDS, IPS, or firewall alerts. It's time to smash the easy button and take a more proactive stance to security. To do this, you decide to employ Active Defense and Cyber Deception techniques to get better visibility. Join us as we discuss some practical approaches for deploying these techniques and the associated OPSEC considerations. We will talk about how we can increase the visibility of attacker actions in the lower levels of our network. We'll also discuss Honeypot OPSEC and some common pitfalls you need to avoid, as well as some easy changes that can be made to improve their likelihood of success in identifying attacker activity. It's time to take back your house!

The Tap House

Philip Hagen

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 @Night talk, Phil Hagen will discuss some of the latest technologies, techniques, and tools that you'll want to know in pursuit of forensication nirvana. 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.


SAVE THE DATE!
DFIR
SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE
SUMMIT & TRAINING
JUNE 22-29, 2017 | AUSTIN, TX
www.sans.org/dfirsummit


DATA
BREACH
SUMMIT & TRAINING
Sept 25 - Oct 2, 2017 | Chicago, IL
sans.org/DataBreachSummit

SANS THREAT HUNTING AND IR SUMMIT 2017

Hotel Information

Training Campus

New Orleans Downtown Marriott at the Convention Center

859 Convention Center Blvd | New Orleans, LA 70130
504-613-2888
www.sans.org/event/threat-hunting-and-incident-response-summit-2017/location

Find just the right balance of work and play at New Orleans Downtown Marriott at the Convention Center. The hotel is housed in a renovated 19th century cotton mill that now boasts modern amenities. Discover unique accommodations and event spaces that are the perfect pairing for your work or leisure visit to the historic Crescent City.

Special Hotel Rates Available

A special discounted rate of $216.00 S/D will be honored based on space availability. These rates include high-speed Internet in your room but are only available through March 27, 2017. To make reservations, please call 504-613-2888; you must mention that you are attending the SANS event to get the discounted rate.

Top 5 reasons to stay at the New Orleans Downtown Marriott at the Convention Center

1. All SANS attendees receive complimentary high-speed Internet when booking in the SANS block.
2. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
3. By staying at the New Orleans Downtown Marriott at the Convention Centeryou gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
4. SANS schedules morning and evening events at the New Orleans Downtown Marriott at the Convention Center that you won't want to miss!
5. Everything is in one convenient location!

Registration Information

Register online at
www.sans.org/ThreatHunting

We recommend you register early to ensure you get your first choice of courses.

Select your course or courses and indicate whether you plan to test for GIAC certification. If the course is still open, the secure online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

Save $400 when you register for the summit and a course!

Pay Early and Save

FOR THE SUMMIT ONLY	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**2-22-17**	**$200.00**	**3-8-17**	**$100.00**
FOR A COURSE ONLY	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**2-22-17**	**$400.00**	**3-8-17**	**$200.00**

Some restrictions apply. Discount offers cannot be combined.

Use code **EarlyBird17** when registering early

Cancellation You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by March 28, 2017 – processing fees may apply.