Arlington, VA

TRAINING: Jan 25-30, 2017

SUMMIT: Jan 31-Feb 1, 2017

SANS DFIR CYBER THREAT INTELLIGENCE SUMMIT & TRAINING

SUMMIT:
Jan 31 - Feb 1, 2017

TRAINING:
Jan 25-30, 2017

LOCATION:
Arlington, VA

The Cyber Threat Intelligence Summit & Training is back for another year and it's set to be bigger and better than ever!

Check out what we have planned:

- **Two Days of In-Depth Cyber Threat Intelligence Talks:** The Summit features two days packed with trending talks and leading speakers covering the most innovative CTI topics.
- **Six World-Class SANS DFIR Courses:** Prior to the two-day Summit, choose from six hands-on DFIR training courses taught by expert SANS instructors.
- **Exclusive Networking Opportunities and Bonus Evening Sessions:** Join your peers for an evening reception, DFIR NetWars, and SANS@Night talks.

"One of very few events devoted solely to tradecraft of cyber threat analysis and intelligence. Essential to both newcomers and seasoned practitioners, and neither too fast nor too slow for either."

-Patton Adams, Verisign iDefense

SAVE $200
when you register and pay for the Summit by Dec 7th – Use code **EarlyBird17**

@sansforensics
#CTISummit

REGISTER TODAY AT **www.sans.org/CTI-Summit**

CTI TRAINING COURSES

FOR578
Cyber Threat Intelligence

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

FOR518
Mac Forensic Analysis

FOR572
Advanced Network Forensics and Analysis GNFA

FOR585
Advanced Smartphone Forensics GASF

FOR610
REM: Malware Analysis Tools and Techniques GREM

ALSO FEATURING

DFIR NETWARS TOURNAMENT

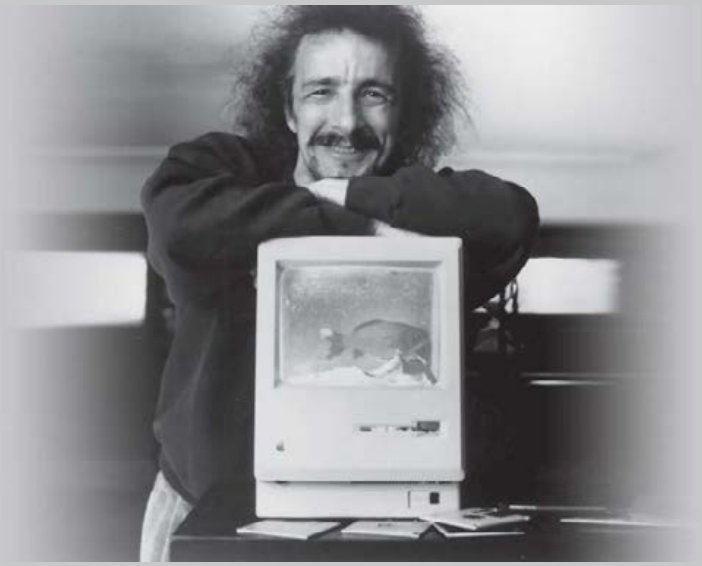
Jan 28-29, 2017

SAVE $400

when you register for the Cyber Threat Intelligence Summit and a SANS Course!

REGISTER TODAY AT **www.sans.org/CTI-Summit**

CTI SUMMIT KEYNOTE PRESENTATION



Clifford Stoll

Author, Astronomer, Skeptic

Clifford Stoll gained worldwide attention as a cyberspace sleuth when he wrote his bestselling book, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, the page-turning true story of how he caught a ring of hackers who stole secrets from military computer systems and sold them to the KGB. He has become a leading authority on computer security. His lecture presentations are energetic and entertaining, and showcase Clifford's dry wit and penetrating views. Clifford Stoll is a commentator for MSNBC and an astronomer at the University of California Berkeley.

The *Cuckoo's Egg* inspired a whole category of books on capturing computer criminals. He began by investigating a 75-cent error in time billing for the university computer lab for which he was systems manager and ended up uncovering a ring of industrial espionage. Working for a year without support from his employers or the government, he eventually tracked the lead to a German spy hacking into American computer networks involved with national security and selling the secrets to the KGB for money and cocaine.

Since catching the "Hanover Hacker" (Hanover, West Germany), Stoll has become a leading expert on computer security and has given talks for both the CIA and the National Security Agency, as well as the U.S. Senate.

"With his analytical, scientific mindset – and no experience at all – Cliff Stoll uncovered the first documented case of espionage on what became the internet. This event is what grew into what we call Cyber Threat Intelligence today, and the methodology he followed is as applicable today as it was in 1986. Cliff is an amazing speaker and a brilliant mind, and a man we can all thank for our careers today."

-Mike Cloppert, PriceWaterhouseCoopers, Senior Cyber Threat Analyst

"If you've read 'The Cuckoo's Egg' (and you should have), you know about the man who engaged in the first-ever documented nation-state hacker hunt. Even decades later, Cliff Stoll's story embodies so much of the mindset we need to successfully hunt attackers in today's networks. We can all learn something from Cliff's story of meticulous attention to logging data, breakthrough solutions to technical challenges, and working through international bureaucracy to hunt the original APT."

-Jake Williams, Principal Consultant, Rendition Sec

CTI SUMMIT FEATURED TALKS

Here's a small sampling of the Cyber Threat Intelligence Summit talks...

Integrating Cyber Threat Intelligence Using Classic Intel Techniques

Service providers frequently limit the scope of CTI to the dissemination of threat feeds, third-party analysis, and indicators. As the cyber industry moves away from this limited understanding and begins to more clearly define CTI as a full-spectrum endeavor spanning tactical, operational, and strategic threat intelligence areas, it is important to illustrate how organizations can effectively incorporate actual CTI into their business models. Through integration of the intelligence cycle into the cyber domain and appropriate tradecraft, this presentation will examine how other organizations can incorporate this model. The audience will learn how to incorporate classic intelligence techniques into their cyber threat model to provide analysts and decision-makers with actionable, predictive intelligence, and improved situational awareness. In addition, attendees will learn how integrating both tools and people (net defenders and cyber all-source analysts) within their CTI model is imperative to create a holistic cyber-threat picture. To achieve this, we will use case studies to challenge the notion that effective CTI is purely technical – it is not. Effective CTI is the marriage between net defense and all-source analysis.

***Elias Fox**, Cyber Threat Intelligence Analyst- R&D, Noblis-NSP*

***Mariangela Taylor**, Cyber Threat Intelligence Analyst- R&D, Noblis-NSP*

Using CTI to Profile and Defend Against the World's Most Successful Email Scam

In this talk, we will examine the various aspects of one of the world's most successful email campaigns: the business email scam. This campaign has stolen nearly $3.1 billion over the past three years, and shows no signs of slowing down. This presentation will analyze research spanning over three years across the globe involving multiple case studies and banks from North Carolina to Hong Kong. We will start by examining characteristics of the tools, context, and domains used by the attackers to trick companies. Using publicly-available and free tools, we will profile just how large this campaign is, what evidence is available, and how to extract valuable indicators from the data. The presentation will conclude with lessons on how the attendees can use these publicly-available free tools to build profiles on attacks such as this scam. We will discuss how to take seemingly arbitrary indicators and use them to protect our networks and business. Lastly, we will also briefly discuss open source tools that smaller teams can use to maintain and organize their indicators.

***Matt Bromiley**, Senior Consultant, Mandiant*

Hunting Cyber Threat Actors with TLS Certificates

This presentation will go over how net defenders and threat intel analysts can use TLS/SSL data from open-source sites like scans.io and censys.io to defend their networks and track threat actors that use TLS/SSL to encrypt their command and control, perform credential harvesting, or even manage their command and control infrastructure.

Most analysts know and use Whois registrant info to track domains threat actors create. However, a lot of threat actors have learned to use Domain Privacy Registration, which mitigates that tracking ability. Analysts also like to use passive DNS sources to track domains and IPs as actors move their infrastructure. Others analysts use things like VirusTotal to track threat actors based off their malware, but not everyone has access to VirusTotal. Using this technique, defenders and analysts can easily track malware command and control infrastructure as it moves and put the appropriate defense mitigations in place as needed.

***Mark Parsons**, DevOps/ThreatIntel, Punch Cyber Analytics*

To view the entire Summit agenda, visit www.sans.org/CTI-Agenda

CTI SUMMIT SPEAKERS

Rob Lee
SANS Instititute, SANS Fellow

Summit Advisory Board

@robtlee
@sansforensics

Mike Cloppert
PriceWaterhouseCoopers,
Senior Cyber Threat Analyst

Summit Advisory Board

@mikecloppert

Juan Andrés Guerrero-Saade
Kaspersky Lab - GReAT,
Senior Security Researcher

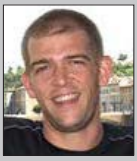
TALK TITLE:
Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks

@juanandres_gs

Rob Dartnall
Security Alliance Ltd,
Director of Cyber Intelligence

TALK TITLE:
The Use of Conventional Intelligence Analysis Methodologies in Cyber Threat Intelligence

@cyberfusionteam



Brian Bartholomew
Kaspersky Lab - GReAT,
Senior Security Researche

TALK TITLE:
Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks

@Mao_Ware

Elias Fox
Noblis-NSP,
Cyber Threat Intelligence Analyst

TALK TITLE:
Integrating Cyber Threat Intelligence Using Classic Intel Techniques

Matt Bromiley
Mandiant, Senior Consultant;
SANS Institute, Instructor

TALK TITLE:
Using CTI to Profile and Defend Against the World's Most Successful Email Scam

@505Forensics

Dave Herrald
Splunk, Security Architect

TALK TITLE:
The Threat Intel Victory Garden: Creating, Capturing, and Using Your Own Threat Intelligence Using Open-Source Tools

@daveherrald

Rebekah Brown
Rapid7, Threat Intelligence Lead;
SANS Institute, Instructor

Summit Advisory Board

@PDXbek

Rick Holland
SANS Institute, Summit Co-Chair

TALK TITLE:
Inglorious Threat Intelligence

@agnu

Sergio Caltagirone
Microsoft, Director,
Threat Intelligence Analysis

TALK TITLE:
Threat Intelligence at Microsoft: A Look Inside

@cnoanalysis

Jeremy Johnson
Ford Motor Company,
Cyber Threat Intelligence Analyst

TALK TITLE:
Using Intelligence to Heighten Your Defense Mobile Forensics

@agnu

Lincoln Kaffenberger
IMF, Information Technology Officer

TALK TITLE:
Location-Specific Cyber Risk: Where You Are Affects How Badly You'll Be Hacked

@LincolnKberger

Ryan Kovar
Splunk Inc., Staff Security Strategist

TALK TITLE:
The Threat Intel Victory Garden: Creating, Capturing, and Using Your Own Threat Intelligence Using Open-Source Tools

@meansec

CTI SUMMIT SPEAKERS

John Kupcinski

KPMG, Director

TALK TITLE:

Location-Specific Cyber Risk: Where You Are Affects How Badly You'll Be Hacked

Rob M. Lee

Dragos, CEO;
SANS Institute, Certified Instructor

TALK TITLE:

Knowing When to Consume Intelligence vs. Generate It

@RobertMLee

Scott Roberts

GitHub, Bad Guy Catcher;
SANS Institute, Instructor

Summit Advisory Board

@sroberts

Kyle Maxwell

Verisign iDefense, Senior Researcher

TALK TITLE:

Accurate Thinking: Analytic Pitfalls and How to Avoid Them

@kylemaxwell

Aaron Shelmire

Anomali, Principal Threat Researcher

TALK TITLE:

Effective Threat Intel Management

@ashelmire

Christian Paredes

Booz Allen Hamilton,
Threat Intelligence Analyst

TALK TITLE:

Pen-To-Paper and the Finished Report: The (Often Overlooked) Key To Generating Threat Intelligence

@cyint_dude

Mariangela Taylor

Noblis-NSP, Principal Investigator/
Cyber All-Source Analyst

TALK TITLE:

Integrating Cyber Threat Intelligence Using Classic Intel Techniques

@DaLastCenturion

Mark Parsons

King and Union,
DevOps/ThreatIntel

TALK TITLE:

Hunting Cyber Threat Actors with TLS Certificates

Ronnie Tokazowski

PhishMe, Senior Researcher

TALK TITLE:

Reversing Threat Intelligence: Fun with Strings in Malware

@iHeartMalware

Alex Pinto

Niddel, Chief Data Scientist

TALK TITLE:

Beyond Matching: Applying Data-Science Techniques to IOC-based Detection

@alexcpsec

Jake Williams

Rendition Infosec, Principal Consultant;
SANS Institute, Certified Instructor

Summit Advisory Board

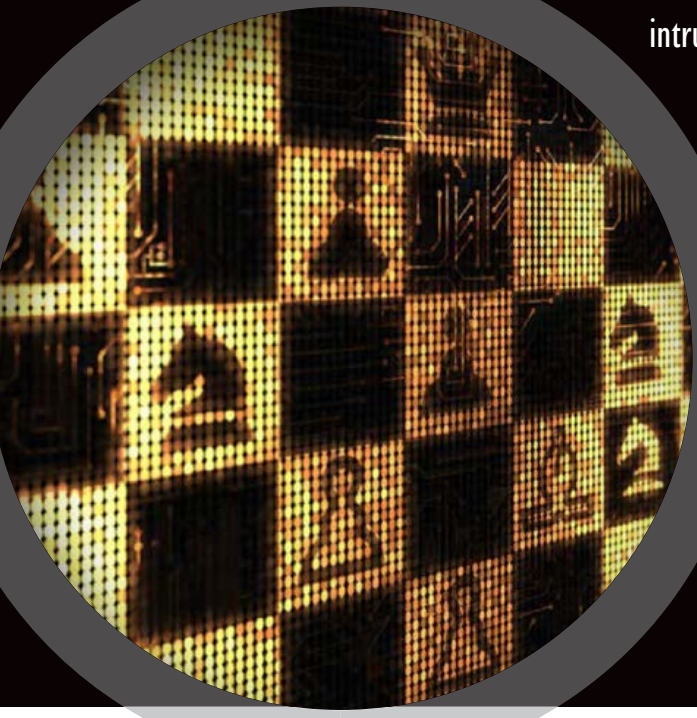
@MalwareJake

FOR578: Cyber Threat Intelligence

Instructors:

Rebekah Brown @PDXBek | Robert M. Lee @RobertMLee

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.



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/CTI-FOR578

FOR508: Advanced Incident Response and Threat Hunting

Instructor: Rob Lee @robtlee, @sansforensics

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/CTI-FOR508

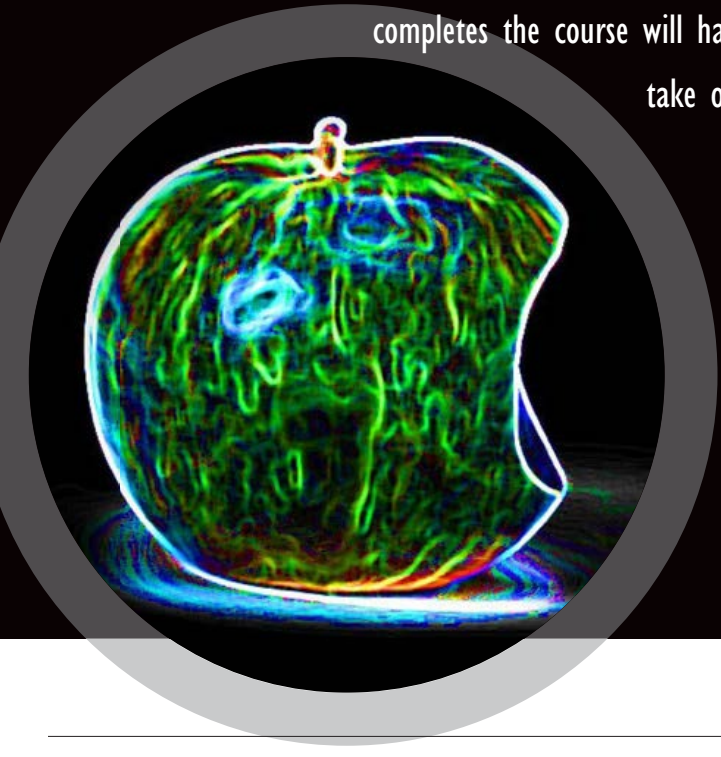
GIAC CERTIFIED FORENSIC ANALYST GCFA

www.giac.org/gcfa

FOR518: Mac Forensic Analysis

Instructor: Sarah Edwards @iamevltwin

This course aims to form a well-rounded investigator by introducing Mac forensics into a Windows-based forensics world. The course focuses on topics such as the HFS+ file system, Mac-specific data files, tracking user activity, system configuration, analysis and correlation of Mac logs, Mac applications, and Mac-exclusive technologies. A computer forensic analyst who successfully completes the course will have the skills needed to take on a Mac forensics case.



FORENSICATE DIFFERENTLY!

"The most comprehensive Mac class I've taken."
-DANIEL MILLS, NASA

- Analyze and parse the Hierarchical File System (HFS+) file system by hand and recognize the specific domains of the logical file system and Mac-specific file types
- Understand and profile users through their data files and preference configurations.
- Determine how a system has been used or compromised by using the system and user data files in correlation with system log files.
- Understand and analyze many Mac-specific technologies, including Time Machine, Spotlight, iCloud, Versions, FileVault, AirDrop, and FaceTime.

www.sans.org/CTI-FOR518

FOR572: Advanced Network Forensics and Analysis

Instructor: Ryan Johnson @ForensicRJ

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/CTI-FOR572

GIAC NETWORK FORENSIC ANALYST GNFA

www.giac.org/gnfa

FOR585: Advanced Smartphone Forensics

Instructor: Cindy Murphy @cindymurph

Mobile devices are often a key factor in criminal cases, intrusions, IP theft, security threats, and more. Understanding how to leverage the data from the device in a correct manner can make or break your case and your future as an expert. FOR585: Advanced Smartphone Forensics will teach you those skills.

SMARTPHONE DATA CAN'T HIDE FOREVER – IT'S TIME TO OUTSMART THE MOBILE DEVICE!

"FOR585 provides forensics with the mentality and set of tools required to forensically examine most types of devices."

-STEVE BONE, MOD

- Select the most effective forensic tools, techniques, and procedures for critical analysis of smartphone data
- Reconstruct events surrounding a crime using information from smartphones, including timeline development and link analysis (e.g., who communicated with whom, where, and when)
- Understand how smartphone file systems store data, how they differ, and how the evidence will be stored on each device
- Interpret file systems on smartphones and locate information that is not generally accessible to users

www.sans.org/CTI-FOR585

GIAC ADVANCED SMARTPHONE FORENSICS GASF

www.giac.org/gasf

FOR610: REM: Malware Analysis Tools and Techniques

Instructor: Lenny Zeltser @lennyzeltser

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 GUNNERSON, 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/CTI-FOR610

GIAC REVERSE ENGINEERING MALWARE GREM

www.giac.org/grem

SANS CTI INSTRUCTORS

Rebekah Brown *SANS Instructor*

Rebekah Brown is the threat intelligence lead for Rapid7, supporting incident response, analytic response, global services and product support. She is a former NSA network warfare analyst, U.S. Cyber Command training and exercise lead, and Marine Corps crypto-linguist who has helped develop threat intelligence programs at the federal, state, and local levels as well as in the private sector at a Fortune 500 company. She has an Associates in Chinese Mandarin, a B.A. in International Relations, and is wrapping up a M.A in Homeland Security with a Cybersecurity focus and a graduate certificate in intelligence analysis. @PDXBek

Sarah Edwards *Certified Instructor*

A self-described Mac nerd, Sarah Edwards is a forensic analyst, author, speaker, and both author and instructor of SANS FOR518: Mac Forensic Analysis. She has been a devoted user of Apple devices for many years and has worked specifically in Mac forensics since 2004, carving out a niche for herself when this area of forensics was still new. Although Sarah appreciates digital forensics in all platforms, she has a passion for working within Apple environments and is well known for her work with cutting-edge Mac OS X and iOS, and for her forensic file system expertise. Sarah has more than 12 years of experience in digital forensics, and her passion for teaching is fueled by the ever-increasing presence of Mac devices in today's digital forensic investigations. Sarah has worked with federal law enforcement agencies on a variety of high-profile investigations in such areas as computer intrusions, criminal cases, counter-intelligence, counter-narcotics, and counter-terrorism. Her research and analytical interests include Mac forensics, mobile device forensics, digital profiling, and malware reverse engineering. @iamevltwin

Ryan Johnson *SANS Instructor*

Ryan Johnson is the Head of CSIRT Readiness and Investigations at PricewaterhouseCoopers. In this role, Ryan is responsible for global CSIRT readiness, insider threat, and strategic threat intelligence. Previously, Ryan was a Senior Director and lead incident responder in the Cyber Division of consulting firm Alvarez & Marsal. Ryan has been investigating crimes in the digital realm for more than 12 years including performing media exploitation for the U.S. Army in Iraq. Ryan has run multiple large-scale breach investigations and has also provided clients with proactive assessments that assisted them in identifying both security gaps, and identifying systems which are already compromised. Ryan taught digital forensics for the US State Department's Anti-Terrorism Assistance program and was a co-author of several of their digital forensics courses. Ryan also co-authored *Mastering Windows Network Forensics and Investigations, Second Edition*. Ryan's industry credentials include: GIAC Network Forensic Analyst (GNFA), GIAC Continuous Monitoring Certification (GMON), GIAC Certified Incident Handler (GCIH), Certified Information System Security Professional (CISSP), Certified Forensic Computer Examiner (CFCE), Digital Forensics Certified Professional (DFCP), EnCase Certified Examiner (EnCE), and Payment Card Industry Professional (PCIP). He has earned an M.S. from Dalhousie University and two Bachelor's degrees from Queen's University. @ForensicRJ

Robert M. Lee *Certified Instructor*

Robert M. Lee is the CEO and Founder of Dragos Security LLC, a critical infrastructure cybersecurity company, where he pursues his passion for control system traffic analysis, incident response, and threat intelligence research. Rob is the course author of SANS ICS515: ICS Active Defense and Incident Response, and the co-author of SANS FOR578: Cyber Threat Intelligence. He is also a non-resident National Cyber Security Fellow at New America focusing on policy issues relating to the cybersecurity of critical infrastructure, and a PhD candidate at Kings College London. For his research and focus areas, he was named one of Passcode's Influencers and awarded EnergySec's 2015 Cyber Security Professional of the Year. Rob was also named to the 2016 class of Forbes "30 Under 30" for Enterprise Technology as one of "the brightest entrepreneurs, breakout talents, and change agents" in the sector. Robert obtained his start in cybersecurity serving as a Cyber Warfare Operations Officer in the U.S. Air Force. He has performed defense, intelligence, and attack missions in various government organizations including the establishment of a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Robert routinely writes articles in publications such as Control Engineering and the Christian Science Monitor's Passcode and speaks at conferences around the world. Lastly, Robert, is author of the book "SCADA and Me" and the weekly web-comic Little Bobby (www.littlebobbycomic.com). @RobertMLee

SANS CTI INSTRUCTORS

Rob Lee *Faculty Fellow*

Rob Lee is an entrepreneur and consultant in the Boston area, specializing in information security, incident response, threat hunting, and digital forensics. Rob is currently the curriculum lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 18 years of experience in digital forensics, vulnerability and exploit discovery, intrusion detection/prevention, and incident response. Rob graduated from the U.S. Air Force Academy and served in the U.S. Air Force as a founding member of the 609th Information Warfare Squadron, the first U.S. military operational unit focused on information operations. Later, he was a member of the Air Force Office of Special Investigations (AFOSI) where he led a team conducting computer crime investigations, incident response, and computer forensics. Prior to starting his own firm, he directly worked with a variety of government agencies, U.S. Department of Defense, and intelligence communities as the technical lead for a vulnerability discovery and an exploit development team, lead for a cyber forensics branch, and lead for a digital forensic and security software development team. Rob was also a director for MANDIANT, a company focused on investigating advanced adversaries, such as the APT, for five years prior to starting his own business. Rob co-authored the book *Know Your Enemy, 2nd Edition*. Rob earned his MBA from Georgetown University in Washington DC. Rob is also a co-author of the MANDIANT threat intelligence report M-Trends: The Advanced Persistent Threat. @robtlee, @sansforensics

Cindy Murphy *Certified Instructor*

Cindy Murphy served in law enforcement for more than 30 years, including 24 years as a detective with the Madison Police Department in Wisconsin. During 17 of those years she worked as a certified digital forensics examiner. During her time as an investigator, she saw firsthand the emergence of mobile devices as the primary source of evidence in investigations. This pushed her to grow into the mobile forensics expert she is today and enabled her to co-author the SANS FOR585 Advanced Smartphone Forensics course. Just recently, Cindy took a leave of absence from the Madison Police Department to launch Gillware Digital Forensics, where she is co-owner and serves as president and lead examiner. As a life-long police officer, Cindy knows the transition from the public to the private sector to private will present new challenges, but she's looking forward to broadening her professional experience even further, which will benefit both Cindy and her students. @cindymurph

Lenny Zeltser *Senior Instructor*

Lenny Zeltser is a seasoned business and tech leader with extensive information security expertise. As a product portfolio owner at NCR, he delivers the financial success and expansion of the company's security services and SaaS products. Beforehand, as the national lead of the security consulting practice at Savvis (acquired by CenturyLink), he managed the US team of service professionals, aligning their expertise to the firm's cloud solutions. Lenny helped shape global infosec practices by teaching incident response and malware defenses at SANS Institute and by sharing knowledge through writing, public speaking and community projects. Lenny has earned the prestigious GIAC Security Expert professional designation and developed the Linux toolkit used by malware analysts throughout the world. His approaches to business and technology are built upon work experience, independent research, a Computer Science degree from the University of Pennsylvania and an MBA degree from MIT Sloan. Lenny's expertise is strongest at the intersection of business, technology and information security and spans incident response, infosec cloud services and business strategy. To get a sense for his thought process and knowledge areas, take a look at his blog at https://zeltser.com. @lennyzeltser

DFIR NetWars

Are you one of the top Digital Forensics & Incident Response Professionals?

2 Nights of DFIR NetWars at SANS CTI SUMMIT 2017!

SAT, JAN 28 - SUN, JAN 29 6:30-9:30 PM

Come and join us for this exciting event to test your skills in a challenging and fun learning environment. Registration for DFIR NetWars is **FREE OF CHARGE TO ALL STUDENTS AT SANS CTI SUMMIT 2016**. 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/CTI-Summit

ALSO CHECK OUT

SANS@NIGHT EVENING TALKS

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.

KEYNOTE:

Intel All the Things! 2016 a Year in Review

Robert M. Lee

This past year saw a host of new companies, methodologies, and case studies in the cyber threat intelligence community. Some were exciting (first cyber attack leading to outages in a power grid), some were entertaining (Guccifer and the Democratic National Convention), and some were a mix of both (Norse anyone?). This presentation will give a no-holds-barred look at 2016, including all of the pitfalls and opportunities, as we hit 2017 running. The community is getting larger and as such it is more critical than ever to extract the right lessons learned to move forward.

iOS Location Forensics

Sarah Edwards

It is no secret iOS devices can track a user's every move, providing location data that can be a major factor in many types of investigations. This valuable information can be found in a variety of areas on the iOS device. In this webcast, we will walk you through native iOS databases, plist files, and third-party applications where this information is kept and tracked. We will also introduce you to scripts created to make data analysis easier by allowing you to do fast-data correlation and build a historical map of locations.

Threat Hunting & Incident Response

SANS DFIR | Summit & Training

APRIL 18-25, 2017 | NEW ORLEANS

SAVE THE DATE!

www.sans.org/ThreatHunting

Will you be the Hunter or the Prey?

SAVE THE DATE!

SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

SUMMIT & TRAINING

JUNE 22-29, 2017 | AUSTIN, TX

www.sans.org/dfirsummit

Hotel Information

Training Campus

Renaissance Arlington Capital View Hotel

2800 South Potomac Ave
Arlington, VA 22202
703-413-1300
www.sans.org/cti-location

Special Hotel Rates Available

A special discounted rate of $174.00 S/D will be honored until January 3, 2017 based on space availability.

A limited number of government per diem rate rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate.

Reservations must be made directly with Marriott via telephone at 703-413-1300 by January 3, 2017 and refer to SANS Institute. All reservations after this date are subject to rate and space availability.

In the past, the event hotel has sold out several weeks prior to the event – so book early!

Top 5 reasons to stay at Renaissance Arlington Capital View Hotel

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 Renaissance Arlington Capital View Hotel, you 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 Renaissance Arlington Capital View Hotel that you won't want to miss!
5. Everything is in one convenient location!

Registration Information

Register online at
www.sans.org/CTI-Summit

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	12-7-16	$200.00	12-28-16	$100.00
FOR A COURSE ONLY	**DATE**	**DISCOUNT**	**DATE**	**DISCOUNT**
Pay & enter code before	12-7-16	$400.00	12-28-16	$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 December 30, 2016 – processing fees may apply.

SANS DFIR

CYBER THREAT INTELLIGENCE

SUMMIT & TRAINING

SUMMIT: Jan 31 - Feb 1 TRAINING: Jan 25-30

FOR578: Cyber Threat Intelligence
Robert M. Lee & Rebekah Brown

FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting
Rob Lee | GIAC Cert: GCFA

FOR518: Mac Forensic Analysis
Sarah Edwards

FOR572: Advanced Network Forensics and Analysis
Ryan Johnson | GIAC Cert: GNFA

FOR585: Advanced Smartphone Forensics
Cindy Murphy | GIAC Cert: GASF

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Lenny Zeltser | GIAC Cert: GREM

REGISTER AT
www.sans.org/CTI-Summit