SANS

THREAT HUNTING & INCIDENT RESPONSE

SUMMIT & TRAINING

Will you be the hunter or the prey?

brought to you by

CARBON BLACK
ARM YOUR ENDPOINTS

&

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Hunting Season starts in April. Will you be the hunter or the prey?

Successful hunters know hunting seasons require a methodic preparation. This preparation is what puts them in the right place at the right time for the kill.

Learn to hunt down the enemy before it hunts you:

- Master the latest techniques needed to properly identify compromised systems
- Contain security breaches and rapidly remediate the incidents
- Stop adversaries from further compromising your enterprise systems

---

Don't be the prey, register today at sans.org/ThreatHuntingSummit

SCHEDULE

Threat Hunting & Incident Response Summit
20 Threat Hunting Focused Technical Talks and Speakers Across Two Days
Tue, Apr 12 - Wed, Apr 13

FOR508: **Advanced Digital Forensics and Incident Response**
Thu, Apr 14 - Tue, Apr 19

FOR572: **Advanced Network Forensics and Analysis**
Thu, Apr 14 - Tue, Apr 19

FOR578: **Cyber Threat Intelligence NEW!**
Thu, Apr 14 - Mon, Apr 18

MGT535: **Incident Response Team Management**
Thu, Apr 14 - Fri, Apr 15

SEC401: **Security Essentials Bootcamp Style**
Thu, Apr 14 - Tue, Apr 19

SEC504: **Hacker Tools, Techniques, Exploits, and Incident Handling**
Thu, Apr 14 - Tue, Apr 19

SAVE $400 OFF
any 5-6 day course by paying by March 9th

SAVE $500 OFF*
your Summit registration fee when purchased with a full-priced 5-6 day course!

*Does not qualify with EarlyBird discount

FOR508

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.

Advanced Incident Response

Instructor: Alissa Torres @sibertor

GATHER YOUR INCIDENT RESPONSE TEAM – IT'S TIME TO GO HUNTING

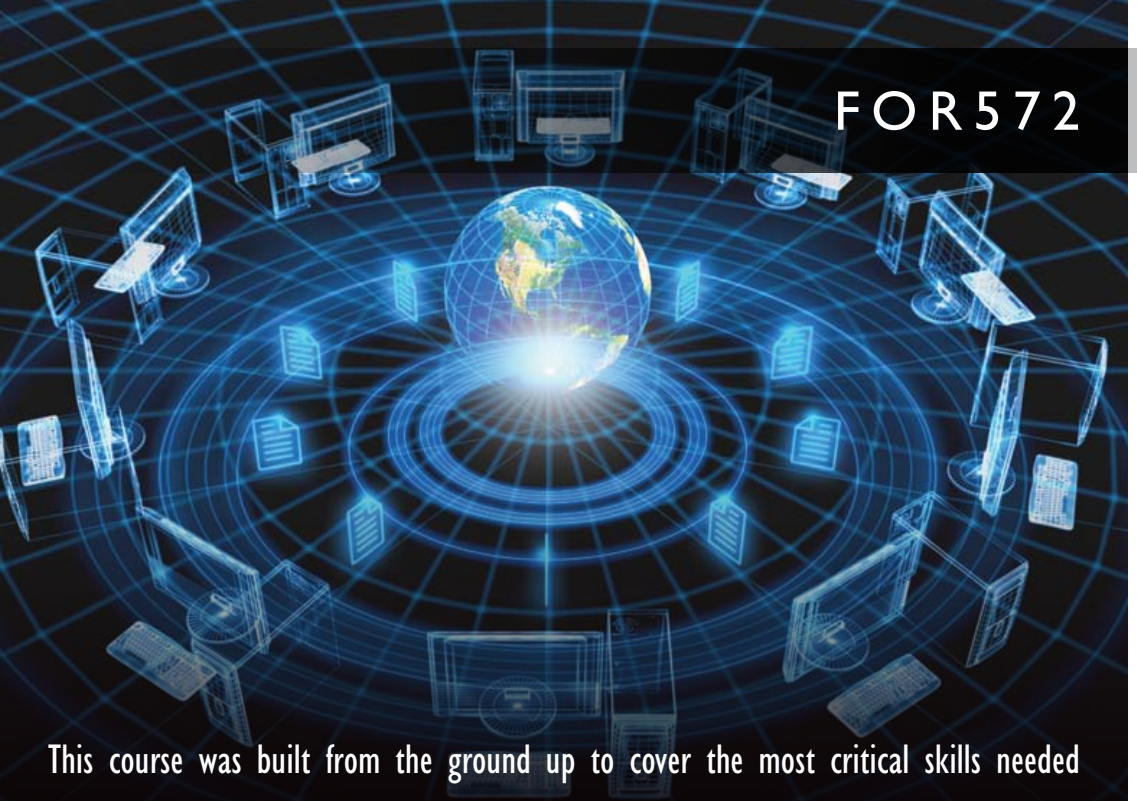
"The most in-depth, state-of-the-art IR course I can imagine. It's the first time I think defense can actually gain an advantage."
-Kai Thomsen, AUDI AG

- 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

sans.org/FOR508

GIAC CERTIFIED FORENSIC ANALYST GCFA

giac.org



FOR572

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.

Advanced Network Forensics and Analysis

Instructor: Philip Hagen @PhilHagen

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 then 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

sans.org/FOR572

GIAC Network Forensic Analyst GNFA

giac.org

FOR578

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, detect, scope, and stop intrusions and data breaches.

Cyber Threat Intelligence

Instructor: Mike Cloppert @mikecloppert

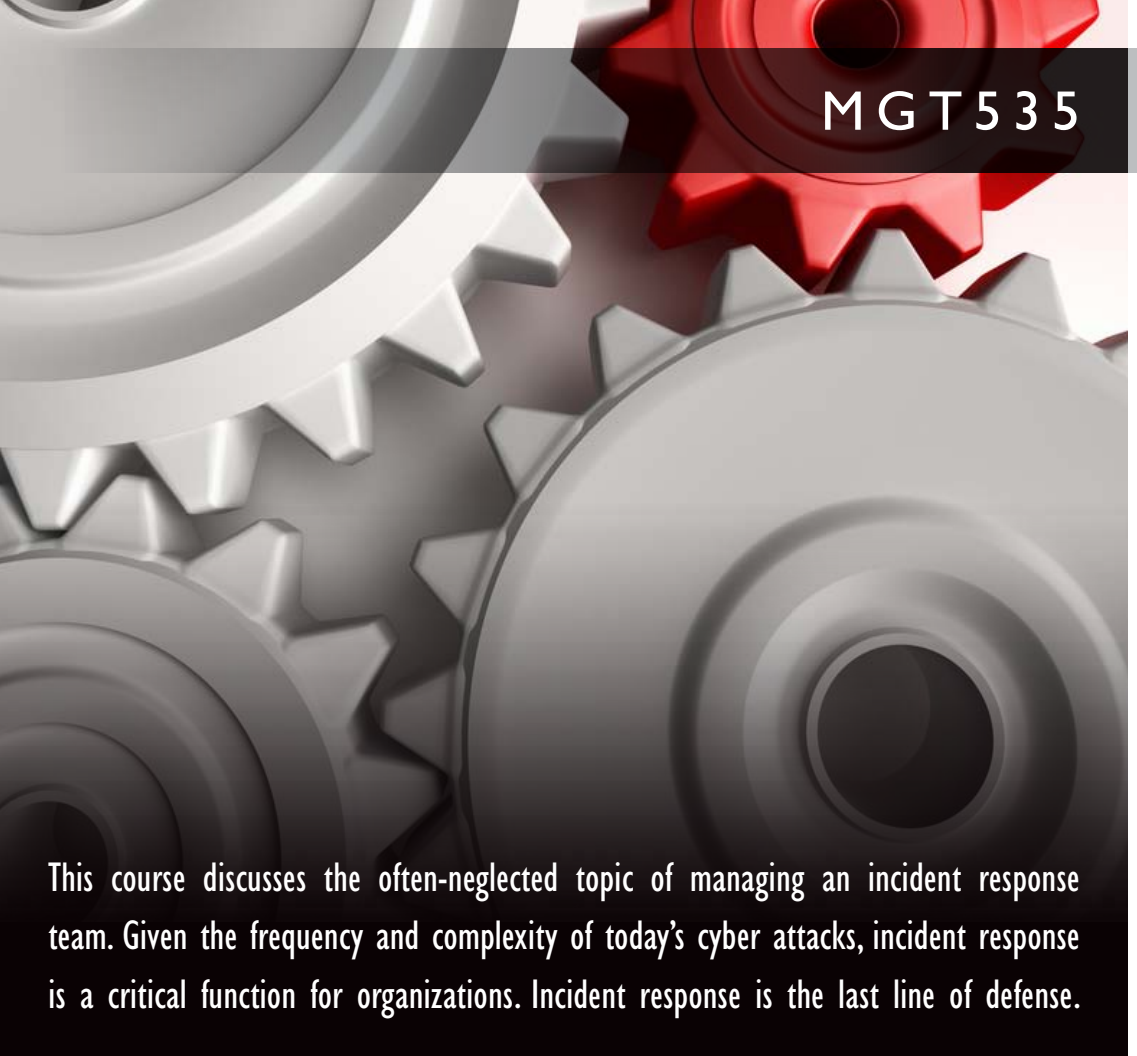
NEW

"In teaching this course, my goal is to create a colleague – someone I trust and who understands how to look at defending networks by leveraging the perspective of our adversary. This course represents my wish list for the baseline knowledge and experience I'd like to see among all the new colleagues I will meet throughout my career."

-Mike Cloppert, FOR578 Course Author

- Determine the role of cyber threat intelligence in their jobs
- Know 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 improve success in defending against and responding to future intrusions
- Manage, share, and receive intelligence on APT actors

sans.org/FOR578



MGT535

This course discusses the often-neglected topic of managing an incident response team. Given the frequency and complexity of today's cyber attacks, incident response is a critical function for organizations. Incident response is the last line of defense.

Incident Response Team Management

Instructor: Christopher Crowley @CCrowMontance

YOU ARE THE TEAM CALLED UPON AT THE WORST TIME, BE PREPARED TO WIN THE BATTLE

"This course brings hands-on and very relevant information for everyone establishing or being part of an incident response team."

-Geir Lossius, Sparebanken Vest

- Incident Response – 6 Steps
- Creating Incident Response Requirements
- Developing Incident Handling Capabilities
- Reporting, SLAs, Cost of Incidents
- Setting up Operations
- Managing Daily Operations
- Navigating Executive Management

sans.org/MGT535

SEC401

Security Essentials Bootcamp Style

Instructor: Chris Christianson

SANS' flagship and most popular course! Written by renowned industry expert and SANS Instructor Dr. Eric Cole, this intensive six-day course focuses on the essential skills needed to protect and secure an organization's critical information assets and business systems. Key concepts covered include Networking, Defense-In-Depth, O/S Security, Secure Communications, and much more. Extended hours in a bootcamp format reinforce key concepts with hands-on labs. This course will challenge you!

PREVENTION IS IDEAL BUT DETECTION IS A MUST!

"SEC401 answers the why of a lot of my work practices, and asks why not for the practices my company doesn't follow."

-Thomas Petro, Southern California Edison

- Design and build a network architecture
- Create a security roadmap
- Build a network visibility map to harden a network
- Develop effective security metrics
- Analyze systems using Linux and Windows command-line tools
- Identify vulnerabilities in a system & configure the system to be more secure
- Utilize sniffers to analyze protocols to determine content and passwords

giac.org

sans.org/SEC401

SEC504

This course addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still so prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course includes a time-tested, step-by-step process for responding to computer incidents; a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them.

Hacker Tools, Techniques, Exploits, and Incident Handling

Instructor: Bryce Galbraith @brycegalbraith

KNOW YOUR ENEMY

"SEC504 opens your eyes to the real cyberworld. It encourages thinking about security of data and network access."

-Frank Munson, Virginia International Terminal

- Apply incident handling processes in-depth
- Analyze the structure of common attack techniques
- Learn how to accomplish operating system and application-level attacks
- Learn how to crack passwords
- Learn how to break into web applications
- Learn how to maintain access on a target

sans.org/SEC504

GIAC Certified Incident Handler GCIH

giac.org

SUMMIT AGENDA

Tuesday, April 12

9:00-9:20am **Welcome & Opening Remarks**

***Rob Lee**, Fellow, SANS Institute*

9:20-10:00am *Keynote to be announced*

10:30-11:15am *Hunting on the Cheap*

For organizations and individuals with limited security budgets, successfully hunting for cyber adversaries can be a daunting challenge. Threat Intelligence can be expensive and sometimes nothing more than IoCs or blacklists. In this talk, Endgame's threat research team will present a series of techniques that can enable organizations to leverage free or almost-free sources of data and open-source tools to "hunt on the cheap." They'll explain how to: retrieve attackers' tools from globally distributed honeynets that look like your organization or a juicy launching point to attackers; enrich the data past basic file/tool hashes to identify malicious command and control IPs/domains through automated binary analysis using open-source sandboxes and tools; and use passive DNS data to identify active infections and enrich existing data sets. Attendees will learn how to apply these three techniques to hunt for adversaries within their own networks. They will also learn about the various open-source solutions available, such as graph databases, that make these techniques inexpensive and within the scope of many organizations.

***Anjum Ahuja**, Senior Threat Researcher, Endgame*
***Jamie Butler**, Chief Scientist, Endgame*
***Andrew Morris**, Threat Researcher, Endgame*

11:15am-12:05pm *Title and Abstract to Come*

***Heather Adkins**, Information Security Manager, Google*

1:15-2:05pm *Using Open Tools to Convert Threat Intelligence into Practical Defenses*

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

***James Tarala**, Principal Consultant, Enclave Security; Senior Instructor, SANS Institute*

2:05-2:50pm *The Remediation Ballet: Performing the Delicate Dance of Cleanup*

The security industry focuses a great deal on defense, detection and investigation of advanced threats, but the red team always wins in the end. Once an attacker is on your network, it's imperative to have a formal and repeatable plan to quickly get them back out! This talk explores the difficulties involved in remediation such as when to kick-out, whether to clean up or rebuild, and suggests some methods by which IR teams can engage with ops and admins to more professionally accomplish remediation and return servers and networks to a known-trusted state.

***Matt Linton**, Chaos Specialist, Google*

2:50-3:10pm *Train Like You Fight*

Too often, incident response talks are filled with glib advice: "assume compromise," "build a baseline," with little or no practical advice to offer. Our organization pursues aggressive testing and drills for our analysts and administrators, using real adversarial tactics and tool sets. We test our own environment with the intent to be caught and discovered. This is the best way to train your teams. These tests are cross-functional and have been proven highly effective. Your teams will learn what to look for, how these tools work, where their gaps are. From this talk you will come away with actual tactics and tools that you can use to mimic adversarial actions. We will explore how to conduct tests and counter-adversary operations with your teams. We'll explore what artifacts credential theft leaves on a system, and what command and control traffic looks like? The hope is that you will begin to train like you fight, to be ready to face the real threats.

***Casey Smith**, Threat Intelligence Analyst, FirstBank*

SUMMIT AGENDA (CONTINUED)

3:40-4:00pm *Collecting & Hunting for Indications of Compromise with Gusto & Style!*

In this session, SANS instructor Ismael Valenzuela will explain the methods and techniques used by world-class IR teams to leverage the power of open-source tools like Yara and Bro to do IOC hunting when reacting to emergency incidents. State-of-the-art techniques will be presented along with a new open-source tool called 'rastrea2r,' designed to assist with collecting and hunting for IOCs with gusto and style!

***Ismael Valenzuela**, Lead IR/Forensics Technical Practice Manager, Intel Security; Community Instructor, SANS Institute*

4:00-4:45pm *Must Collect IOCs... Now What?!*

Indicators of Compromise(IOCs) are hot commodities nowadays. Most of us have a metric ton of IOCs from a plethora of sources, but what do we do with them? After struggling to drink from the IOC firehose, we developed Overlord, an open-source project designed to provide automated searching and alerting on IOCs in a scaleable and robust manner to help us stay on top of the influx. In this talk, Phillips will examine how to utilize the Overlord Project to bridge the gap between IOC repositories and searching infrastructure. After getting a fresh IOC, besides the usual vetting, we would like to know about this IOC in our environment, ideally on an ongoing basis. Overlord allows us to achieve this by allowing each of its primary components to be modified or completely rewritten for each use-case, while still remaining easy to use.

***Williams M. Phillips IV**, Security Researcher, Salesforce*

Wednesday, April 13

9:00-9:45am *Hunting as a Culture (HaaC): Pursuing and Killing Threats via an Active, Adaptive Security Posture*

Cybersecurity is hard. Bombardment of attacks is paired with bombardment of data. The surface area is growing, the perimeter is deteriorating, and few organizations can hire enough defenders to moderately staff their ranks. But all is not lost. It's time to automate, it's time to orchestrate, and it's time to unite man and machine to enable team search and destroy missions to move closer to clean environments. 2016 is the year that hunting establishes itself as a first-class cyber defense strategy, and we will explore how to get you there.

***Ben Johnson**, Chief Security Strategist, Carbon Black*

PlugX and other favorite APT tools to show beginner to advanced YARA rules. Already familiar with YARA? Come learn how to improve rule signatures to catch different malware variants, all the while keeping false positives to a minimum. Arm yourself with the knowledge to go from hunted to hunter.

***Jay DiMartino**, Sr. Cyber Threat Researcher, Fidelis Cybersecurity*

2:05-2:50pm *Detecting and Responding to Pandas and Bears*

30% of incident response investigations conducted by our team over the past two years have had multiple attack groups operating at the same time within the same organization, and this number is likely to increase in the future. Do you know how to identify and remove multiple attackers within your environment? This presentation focuses on a recent investigation where the victim was simultaneously under attack by two separate attack groups, each with varying goals and TTPs. We'll demonstrate the critical role played by threat intelligence in identifying the attackers and how using this information allows responders and security teams to tailor their remediation tactics and implementation for success. We'll share approaches you can use and when to apply them. Attendees will also learn how to conduct adversary-based hunting operations using existing technology within your organization, improve authentication credential protection during live IR, and prepare for detection of future attacks.

***Christopher Scott**, Director, CrowdStrike Services*
***Wendi Whitmore**, VP, CrowdStrike Services*

2:50-3:10pm *Threat Intelligence Isn't Automatic*

Watching people struggle to determine which of their many sources had the "correct" threat intelligence was one of the motivations for building the ThreatExchange platform. The world is a complicated place and there is no one right answer, no matter what your vendor may tell you. But it is possible to maximize the value of that information by sharing context and experience with a trusted community. This talk will describe how ThreatExchange sharing works, how you can use the information shared with you, and how to make sense of all of that data.

***Jesse Kornblum**, Security Engineer, Facebook*

3:40-4:00pm *Proactive APT Hunting Style*

One of the biggest challenges for enterprises today is to have the capabilities available to determine and identify if a security incident has occurred and what systems that have already been compromised. The majority of enterprise network defense is reactive and heavily dependent on detection through mistakes by adversaries or benevolent 3rd parties alerting organizations to breaches within their network. This approach to detection is simply inexcusable and leads to attackers having control

9:45-10:30am *Casting a Big Net: Hunting Threats at Scale*

One of the biggest differentiators between a mature incident response team and one that is less experienced is the ability to triage hundreds to thousands of endpoints at once. The classic approach is to analyze one host at a time, attempt to connect the dots and determine patient zero. This approach is time consuming and leaves victims vulnerable while attackers are active in their network.

A much faster and more agile process is to collect, process, and analyze artifacts from all endpoints simultaneously. Known by various monikers such as sweeping, hunting, or stacking, being able to collect live response data quickly from endpoints is a crucial capability.

This talk demonstrates methods similar to those used by CrowdStrike's incident response consultants using a free tool, CrowdResponse, for collection and a free Splunk application for analysis at scale. Using real-world examples, we will show how to parse artifacts and identify anomalies from the registry, services, events, tasks, and file system at scale. Attendees will receive both the tools and expertise to put them on the fast track to identifying and ejecting adversaries from their network.

***Paul D. Jaramillo**, Principal Consultant, CrowdStrike*
***Reed Pochron**, Senior Consultant, CrowdStrike*

11:00-11:45am *Hunting and Dissecting the Weevely Web Shell*

Weevley (version 3) is an extendable PHP web shell that provides attackers a wide range of backdoor functionality via standard HTTP requests. This talk walks through techniques to find Weevely based on network analysis and, once located, how to dissect the host and network-based artifacts. This process includes reversing the custom command and control encryption used by Weevely. Once done, the analysis allows determining what actions were taken by the attacker, and what data was exfiltrated via the web shell. The PCAP from a simulated attack, host-based artifacts, and custom Python scripts used during the analysis will be made available afterwards.

***Kiel Wadner**, Information Security Analyst - Red Team, Blue Coat Systems*

11:45am-12:05pm *SANS Threat Hunting Survey Results*

1:15-2:05pm *To Catch an APT: YARA*

It's time to reclaim your networks and start hunting, armed with the open-source tool called YARA. Learn how to author YARA rule signatures with techniques used by malware researchers to mercilessly hunt down the elusive adversary of advanced threat actors, and how to apply those signatures in your organization or investigations using YARA-friendly tools. We will look at real-world case examples of of a network for months or years before they are noticed. This presentation will introduce a tool, developed by Advanced Security Center at EY, named "APT Hunter," which can be used to remotely collect large-scale system artifacts via Windows Management Instrumentation and potentially identify existing threats for enterprises. In addition, we will show some real cases where we used this tool to discover data-breach incidents. APT Hunter is an open-source tool and will be made available to Summit attendees after the event.

***Hao Wang**, Senior Penetration Tester & Incident Responder , EY*

4:00-4:20pm *DIY DNS DFIR: You're Doing it WRONG*

DNS is one of those protocols that we, as DFIR practitioners, take for granted. Operationally, if DNS resolution is working properly, we're happy. Many organizations, however, fail to utilize DNS logs and associated intelligence within their response and investigative activities. This is in part due to the perceived lack of value associated with DNS logs and its associated features, such as name server, WHOIS, and hosting information, and more often due to the unavailability of the logs. This talk will present several tools (both commercial and open source) to help manage the deluge of information on even the smallest of budgets. We will also discuss how to enrich your data with valuable intelligence from freely available sources. Finally, this talk will highlight some real-world investigative techniques where DNS and its associated features were used to add clarity to DFIR investigations.

***Andrew Hay**, CISO, DataGravity, Inc.*

4:20-4:40pm *A Longitudinal Study of the Little Endian that Could*

The 9002 malware, first seen during Operation Aurora in 2009, is a family of malware seen in use by threat actors based in China. What makes 9002 interesting is that over the last six years, the development of this malware has not been linear. Different threat groups have taken 9002 and customized it to suit their own needs, creating multiple, parallel development branches. By understanding the differences between these development branches we can gain an insight into the adversary's development process, allowing the creation of better criteria for detection for both current and future threats. This presentation will provide an overview of the 9002 malware, how the different development branches can be distinguished, how the development goals of the groups behind each branch differ, and how all of this information can be combined to better detect and respond to an intrusion.

***Andrew White**, Senior Security Researcher, Dell Secureworks*

4:40-5:00pm **Closing Remarks**

***Rob Lee**, Fellow, SANS Institute*

MEET THE THIR SUMMIT SPEAKERS

Heather Adkins *Google* @argvee

Heather Adkins is a founding member of the Google Security Team. As Manager of Information Security, she has built a global team responsible for maintaining the security of Google's networks, systems and applications. The Google Security Team is involved in every facet of the business, including building security infrastructure, responding to security threats, and evangelism.

Anjum Ahuja *Endgame*

Anjum Ahuja is a Threat Researcher at Endgame, working on problems related to network security, malwares, and large-scale data analysis. He is currently focused on building threat detection systems based on network fingerprints of malwares, their infrastructures, and global traffic patterns. He has a background in computer networks, routing and IOT security, and holds multiple patents in these fields.

Jamie Butler *Endgame* @jamierbutler

Jamie Butler is the Chief Technology Officer and Chief Scientist at Endgame, where he leads Endgame's research on advanced threats, vulnerabilities and attack patterns. He has directed research teams at some of the most prominent and successful security companies of the last decade.

Jay DiMartino *Fidelis Cybersecurity*

Jay DiMartino is a Sr. Cyber Threat Researcher for Fidelis Cybersecurity. He has been doing Malware Reverse Engineering for over five years and also has several industry certifications including the GREM and GCFA.

Andrew Hay *DataGravity, Inc.* @andrewsmhay

Andrew Hay is the CISO at DataGravity where he is responsible for the development and delivery of the company's comprehensive information security strategy. Prior to that, Andrew was the Director of Research at OpenDNS (acquired by Cisco) and was the Director of Applied Security Research and Chief Evangelist at CloudPassage.

Andrew Morris *Endgame* @Andrew_Morris

Andrew Morris works on the Research and Development team at Endgame, specializing in developing cutting-edge security technologies and researching advanced adversary techniques. Prior to Endgame, Andrew spent several years consulting to various Fortune 100 companies, government agencies, and military customers providing red team support, penetration testing, and adversary emulation services.

William M. Phillips IV *Salesforce*

William Phillips is a recent graduate of Brown University and currently a Security Researcher for the Salesforce Threat Intelligence team where one of his projects is Overlord. Areas of interest include OS X forensics, iOS security, and Network Forensics.

Reed Pochron *CrowdStrike* @rpochron

Reed Pochron has over 5 years of experience in intrusion investigations, conducting incident response, and enterprise security operations. As a Senior Consultant with CrowdStrike out of the Saint Louis office, Reed participates in customer engagements ranging from breach response to proactive compromise and maturity assessments. Reed currently holds his CISSP, GCFA, GCFE, and GCIH certification.

Christopher Scott *CrowdStrike Services*

Christopher Scott has 18 years of Fortune 500/DoD/DIB business proficiency, including more than eight years of targeted threat detection and prevention expertise. Christopher supports a variety of engagements at CrowdStrike that include: proactive and reactive security services, incident response, data loss prevention, business continuity and disaster recovery processes.

Casey Smith *FirstBank* @subTee

Casey Smith is a Threat Intelligence Analyst in the Financial Industry. He has a passion for understanding and testing defensive systems.

Paul D. Jaramillo *CrowdStrike* @DFIR_Janitor

Paul is a Principal Consultant with CrowdStrike and previously worked in the government, energy, manufacturing and telecommunication sectors. Career highlights include breaking into a 2FA VPN as a pentester, successfully investigating an insider threat case across the globe as a forensics examiner, and ejecting nation state adversaries from corporate networks.

Ben Johnson *Carbon Black* @chicagoben

Ben Johnson is cofounder and chief security strategist for Carbon Black. In that role, he spends a lot of time strategizing with customers to improve cyber defenses across the stack. Ben worked in cyber at NSA and at a defense contractor and has two computer science degrees.

Jesse Kornblum *Facebook* @jessekornblum

Jesse Kornblum is a network security engineer on the Threat Infrastructure team at Facebook. He currently works on the ThreatExchange platform which enables organizations to share threat information with trusted partners within a vetted community. Previously, Kornblum was a computer forensics researcher and practitioner, writing tools such as ssdeep and md5deep. He is also a former Special Agent for the Air Force Office of Special Investigations.

Rob Lee *SANS Instititute* @robtlee @sansforensics

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 15 years of experience in computer forensics, vulnerability and exploit discovery, intrusion detection/prevention, and incident response.

Matt Linton *Google* @0xMatt

Matt is an incident responder with experience throughout the security process, from architecture through penetration. He is formally trained in disaster management and specializes in rapid response, remediation and hardening of compromised environments.

James Tarala *Enclave Security* @isaudit

James Tarala is a founder and principal consultant with Enclave Security and a senior instructor with the SANS Institute. James presently serves as a technical editor for the Center for Internet Security's Critical Security Controls and the Open Threat Taxonomy projects.

Ismael Valenzuela *Intel Security* @aboutsecurity

Ismael Valenzuela (SANS Instructor & GSE #132), accumulates +15 years of international experience in cybersecurity consulting, teaching and public speaking. He currently works as Practice Manager at Intel Security, leading the delivery of SOC, Incident Response, Forensics and Threat Research services for major public and private organizations in North America.

Kiel Wadner *Blue Coat Systems* @kielwadner

Kiel works on an internal Red Team at Blue Coat Systems evaluating products and internal networks. Previously he was a security researcher on Blue Coat's Global Intelligence Network building back-end detection systems and tracking threats. He is a graduate of the SANS Technology Institute and holds numerous GIAC certifications.

Hao Wang *Ernst & Young*

Hao Wang is a senior in Ernst & Young's Advanced Security Center. Hao joined Ernst & Young after he graduated from Information Security Institute of Johns Hopkins. Hao is currently responsible for performing Attack & Penetration assessments involving internal as well as external network assessments, and Incident Response involving both network- and host-based forensics, and threat hunting.

Andrew White *Dell Secureworks*

Andrew White, Ph.D. is a senior security researcher at Dell Secureworks with over five years of experience in digital forensics research. When not responding to targeted intrusions, Andrew performs research into memory forensics, targeted malware, credential theft and malware-less intrusions. Current holder of the DFIR Netwars high-score record.

Wendi Whitmore *CrowdStrike Services* @wendilou2

Wendi Whitmore has over 15 years of experience in the computer security industry. As the Vice President of Services for CrowdStrike, Wendi is responsible for all professional services offered by the company. Along with her team, Wendi responds to critical security breaches and provides customers with solutions to complex adversary problems.

MEET THE THIR COURSE INSTRUCTORS

Chris Christianson

SANS Instructor

Chris Christianson is an Information Security Analyst and Network Engineer who lives and works in Northern California. He currently works in the financial industry and is the Assistant Vice President of Network Services for one of the nation's largest credit unions. With more than fifteen years of experience, Chris has spoken at conferences, contributed articles for magazines, and obtained many technical certifications including: CCSE, CCDP, CCNP, GSEC, CISSP, IAM, GCIH, CEH, IEM, GCIA, GREM, GPEN, and GWAPT. He has also earned a Bachelor of Science in Management Information Systems.

Mike Cloppert

SANS Instructor

Michael is the lead analyst for Lockheed Martin CIRT's Intel Fusion team, charged with collecting and managing intelligence on adversaries intent on stealing the organization's intellectual property, and development of new detection and analysis techniques. Michael has worked as a security analyst in various sectors including the Financial, Federal Government, and Defense industries. He has an undergraduate degree in Computer Engineering from the University of Dayton, an MS in Computer Science from The George Washington University, has received a variety of industry certifications including SANS GCIA, GREM, and GCFA, and is a SANS Forensics and IR blog contributor. Michael's past speaking engagements include the DC3 Cybercrime Conference, IEEE, and SANS amongst various others. @mikecloppert

Christopher Crowley

Certified Instructor

Christopher Crowley has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. His work experience includes penetration testing, computer network defense, incident response, and forensic analysis. Mr. Crowley is the course author for SANS MGT535: Incident Response Team Management and holds the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GREM, GMOB, and CISSP certifications. His teaching experience includes SEC401, SEC503, SEC504, SEC560, SEC575, SEC580, FOR585, and MGT535; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor of the year award, which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities. @CCrowMontance

Bryce Galbraith

Principal Instructor

As a contributing author of the internationally bestselling book Hacking Exposed: Network Security Secrets & Solutions, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. Bryce has held security positions at global ISPs and Fortune 500 companies, he was a member of Foundstone's renowned penetration testing team and served as a senior instructor and co-author of Foundstone's Ultimate Hacking: Hands-On course series. Bryce is currently the owner of Layered Security where he provides specialized vulnerability assessment and penetration testing services for clients. He teaches several of the SANS Institute's most popular courses and develops curriculum around current topics. He has taught the art of ethical hacking and countermeasures to thousands of IT professionals from a who's who of top companies, financial institutions, and government agencies around the globe. Bryce is an active member of several security-related organizations, he holds several security certifications and speaks at conferences around the world. @brycegalbraith

Philip Hagen

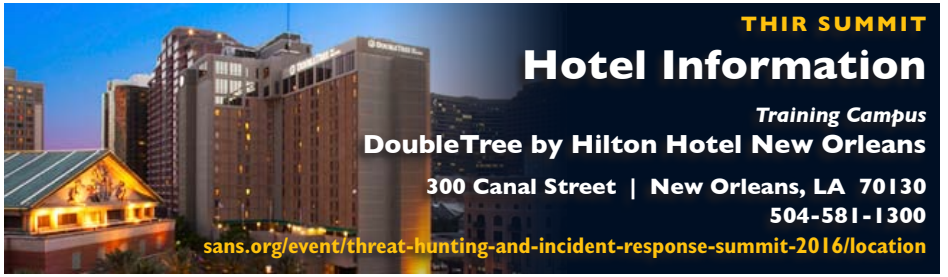
Certified Instructor

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. Currently, Phil is an Evangelist at Red Canary, where engages with current and future customers of Red Canary's managed threat detection service to ensure their use of the service is best aligned for success in the face of existing and future threats. Phil started his security career while attending the US Air Force Academy, with research covering both the academic and practical sides of security. He served in the Air Force as a communications officer at Beale AFB and the Pentagon. In 2003, Phil shifted to a government contractor, providing technical services for various IT and information security projects. These included systems that demanded 24x7x365 functionality. He later managed a team of 85 computer forensic professionals in the national security sector. He has provided forensic consulting services for law enforcement, government, and commercial clients prior to joining the Red Canary team. Phil is also a certified instructor for the SANS Institute, and is the course lead and co-author of FOR572, Advanced Network Forensics and Analysis. @PhilHagen

Alissa Torres

Certified Instructor

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 a internal security team as a digital forensic investigator. She has extensive experience in information security, spanning government, academic, and corporate environments and holds a Bachelors degree from University of Virginia and a Masters from University of Maryland in Information Technology. Alissa has taught as an instructor at the Defense Cyber Investigations Training Academy (DCITA), delivering incident response and network basics to security professionals entering the forensics community. She has presented at various industry conferences and numerous B-Sides events. In addition to being a GIAC Certified Forensic Analyst (GCFA), she holds the GCFE, GPEN, CISSP, EnCE, CFCE, MCT and CTT+. @sibertor



THIR SUMMIT

Hotel Information

Training Campus

DoubleTree by Hilton Hotel New Orleans

300 Canal Street | New Orleans, LA 70130

504-581-1300

sans.org/event/threat-hunting-and-incident-response-summit-2016/location

Special Hotel Rates Available

A special discount rate of $209 S/D will be honored based on space availability until Friday, March 18, 2016.

This rate includes high-speed Internet in your room. Click here to make a reservation. For ease of booking, your attendees may book their accommodations by contacting our DoubleTree Hotel New Orleans reservations at any time by dialing our toll free number at 1-800-222-TREE, using **group code SIR**. For added convenience, reservations can also be made online using your personalized web-link:
https://resweb.passkey.com/go/SANSinternational

U.S. Government Reservations

Please check **www.fedrooms.com** for Government Per Diem availability in the area. Note, you may need to reserve your accommodations online as these rates may not be available by contacting the hotel directly. However, if the rates are not available online, please feel free to contact the hotel.

Advantages of staying at the DoubleTree by Hilton Hotel New Orleans

- Complimentary WiFi in guest room
- Located in downtown New Orleans, directly across the street from the French Quarter, on the streetcar line and a short distance to exciting area attractions and historic sites
- No need to factor in daily cab fees, parking expense and the time associated with travel to alternate hotels
- And more...

THIR SUMMIT

Registration Information

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

Register online at sans.org/ThreatHuntingSummit

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.

Use code **EarlyBird16** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**3-9-16**	**$400.00**	**3-18-16**	**$200.00**

Some restrictions apply.

Bundle and Save

SAVE $500 off **your Summit registration fee when purchased in conjunction with a full-priced 4-6 day course!** Does not qualify with EarlyBird discount

Group Savings (Applies to tuition only)

To obtain a group discount, complete the discount code request form at sans.org/security-training/discounts prior to registering.

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 31, 2016 – processing fees may apply.

THREAT HUNTING & INCIDENT RESPONSE

SUMMIT & TRAINING

"I am discovering new techniques, tools, and solutions that my team is not familiar with."
-Chris Kulakowski, General Motors

"Bleeding-edge knowledge – AWESOME people."
-Anthony Layton, Stout Risius Ross, Inc.

"Awesome opportunity to meet and learn what my peers are involved in."
-William Jeskey, TCCD

Follow @sansforensics and join the conversation #ThreatHuntingSummit to hear the latest news.

SANS
5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407

BROCHURE CODE

Save $400 when you pay for any long course and enter the code "EarlyBird16" before March 9th.