SANS DFIR

Threat Hunting & Incident Response Summit 2018

Program Guide

@sansforensics #ThreatHuntingSummit

Founding Partner

Carbon Black.

Agenda

All Summit Sessions will be held in the Grand Ballroom (unless noted).

All approved presentations will be available online following the Summit at ***sans.org/summit-archives/dfir***

Thursday, September 6

7:00-8:45 am	**Registration & Coffee** (LOCATION: ASTOR BALLROOM)
8:45-9:00 am	***Welcome & Opening Remarks*** ***Rob Lee*** *(@robtlee), DFIR Lead & Summit Co-Chair, SANS Institute* ***Phil Hagen*** *(@PhilHagen), Senior Instructor & Summit Co-Chair, SANS Institute, and DFIR Strategist, Red Canary*
9:00-9:45 am	***Opening Keynote: Lean Hunting*** (Threat) Hunting has been around long enough that most agree it should be part of any comprehensive information security program. In any cat and mouse game, tooling will never catch all evil. We need to apply creativity, analytical thinking, and keep humans in the loop. The challenge, of course, is that human hours are scarce and expensive. Most organizations cannot afford to staff hunt teams 24/7 (or at all), so what's the best way to deploy human attention to identify emerging threats? We'll explore how to take aspects of entrepreneurship and align organizations to achieve positive outcomes by building lean (threat) hunting capabilities. ***Ben Johnson*** *(@chicagoben), Co-Founder & CTO, Obsidian Security*
9:45-10:20 am	***Uncovering and Visualizing Malicious Infrastructure*** How much information about a threat can you find using a single IP address, domain name, or indicator of compromise (IOC)? What additional threats can you identify when looking at attacker and victim infrastructure? To discover and analyze the infrastructure behind large-scale malware activity, we'll look at known indicators from popular botnets spreading such threats as Locky, Globeimposter, and Trickbot. We will highlight co-occurring malicious activities observed on the infrastructure of popular botnets, and demonstrate practical techniques to find threats, analyze botnet and malware infrastructure in order to identify actor and victim infrastructure, and show how to pivot to discover additional IOCs using such techniques as passive DNS and OSINT. Finally, we will demonstrate how visualizing known IOCs helps to better understand the connections between infrastructure, threats, victims, and malicious actors. ***Josh Pyorre*** *(@joshpyorre), Security Research Analyst, Cisco Umbrella* ***Andrea Scarfo*** *(@AScarf0), Security Research Analyst, Cisco Umbrella*
10:20-10:45 am	**Networking Break** (LOCATION: ASTOR BALLROOM)

Thursday, September 6

10:45-11:20 am

The Fastest Way to Hunt Windows Endpoints

Threat hunting can be a daunting task, but there are a few ways to quickly discover key malicious artifacts or indicators of compromise (IOCs) that can then be fed into enterprise-hunting solutions to hunt globally. The WinNTI hacking group offers some fantastic enterprise tools for hunting. Until recently, it lacked a tool to quickly assess a suspect Windows system to harvest key artifacts or IOCs to feed back into enterprise hunting solutions. Experience with an advanced hacking group led to the development of a process and a tool that discovers key artifacts faster than any tools we had evaluated or could purchase. In Windows systems, we must be able to harvest properly configured and useful logs, compare a suspect system's filesystem and registry against trusted hashes and registry snapshots, and remove the good to find the bad. We all want to harvest artifacts that indicate a compromised system – such as large registry keys hiding malicious payloads, sticky keys exploits providing backdoors, suspicious PowerShell scripts executing downloads from the Internet, and WMI persistence. This talk focuses on solutions that have worked in hunting and detecting the activities of advanced hacking groups.

Michael Gough *(@HackerHurricane), Malware Archaeologist, Malware Archaeology*

11:20-11:55 am

Threat Hunting in Your Supply Chain

In 2017, the world experienced the most devastating cyber attacks to date as attackers used leaked National Security Agency (NSA) exploits to wreak havoc in Europe and beyond. Attackers gained initial entry to networks through supply-chain attacks, piggybacking on legitimate applications. It is more obvious than ever that supply-chain attacks need to be part of our threat models. But supply-chain risks don't lend themselves well to traditional threat hunting processes, since agreements with third parties often limit the amount of data available for threat hunting. Jake will introduce a model for including supply-chain risks (hardware, software, and service) into your threat hunting operations.

Jake Williams *(@MalwareJake), Founder, Rendition InfoSec*

11:55 am - 1:15 pm

Lunch & Learn

Carbon Black.

Security Panel Discussion

Join Carbon Black and a panel of the world's top incident response experts as they discuss emerging threats and effective strategies for rapid incident response. Panelists will review key findings from a full day of discussions prior to the event where they took a close look at today's threat landscape, explored effective tools and processes to accelerate incident response, and compared their latest findings. The panel will be moderated by Rick McElroy, Carbon Black Security Strategist and well-known threat hunting and incident response expert.

1:15-1:50 pm

ATT&CKing the Status Quo: Threat-Based Adversary Emulation with MITRE ATT&CK

Every day, adversaries remind us that we need to evolve our defensive focus beyond indicators toward tactics, techniques, and procedures (TTPs), yet we struggle with how to do this. In this presentation, the MITRE ATT&CK team will discuss an end-to-end methodology for better organizing cyber threat intelligence and leveraging it to conduct adversary emulation and hunting. Threat analysts will gain an understanding of how to structure reporting in the form of ATT&CK techniques to increase the effectiveness of the products they create. Hunt teams, incident responders, and defenders will learn how to use that understanding of adversary TTPs to identify defensive gaps as well as prioritize hunting and mitigation activities.

Katie Nickels *(@likethecoins) (@MITREattack), ATT&CK Threat Intelligence Lead, The MITRE Corporation*

Cody Thomas *(@its_a_feature_), Adversary Emulation Engineer, The MITRE Corporation*

Thursday, September 6

1:50-2:25 pm	***Cyber Threat Hunting in the Middle East*** Cultural rifts and political divides are the norm, but cyber threat hunting in the Middle East involves a whole new level of challenges in this regard. After a number of years working in the Middle East, one comes to understand how the differences there have shaped the networks we hunt in. How hunting is conducted there and the types of access our advanced persistent threat (APT) adversaries have to these networks are much different than in the West. This session will provide details on threat hunting techniques adapted to the climate and temperatures of organizations and will explore how regional APT groups have shaped the type of hunting techniques adopted for the networks of clients that face constant disruptive attacks with an alarming trend of disabling networks. ***Kevin Albano**, Global Lead, Threat Intelligence, IBM X-Force IRIS*
2:25-2:55 pm	**Networking Break** (LOCATION: ASTOR BALLROOM)
2:55-3:30 pm	***Hunting for Lateral Movement Using Windows Event Logs*** Once an initial foothold has been obtained, it's likely that target information does not reside on that initial host. The Red Team needs to move laterally in order to achieve operational success. The Blue Team needs to know how lateral movement is achieved and how it can be prevented, detected, and hunted. This talk will describe the most common lateral movement techniques as well as the methods for detecting lateral movement. Attendees can expect to learn about the most common techniques used for lateral movement from an attacker's perspective and the key Windows event logs used for detecting lateral movement. ***Mauricio Velazco** (@mvelazco), VP – Threat Management, Blackstone*
3:30-4:05 pm	***Forecast: Sunny, Clear Skies, and 100% Detection*** *"Those who have knowledge, don't predict. Those who predict, don't have knowledge."* - Lao Tzu Attack simulations test the resilience of threat detection and response capabilities, and validate security implementations. They are an essential component of a solid threat hunting program. Is your internal team's forecast for detection of simulated adversary activity overly optimistic? Strong predictions of success prior to conducting attack simulations can uncover false pretenses and failed implementations. Learn how to incorporate forecasting and subsequent validations into your Blue Team hardening efforts. ***Alissa Torres** (@sibertor), Certified Instructor, SANS Institute*
4:05-5:00 pm	***Live Debates*** We'll wrap up the day with lively debates on topics from cybersecurity to Star Wars – but with a twist. Debaters won't know their topic – or what side they're on – until they're on stage. MODERATOR: ***Matt Bromiley**, Certified Instructor, SANS Institute; Principal Incident Response Consultant, Cylance*
6:00-8:00 pm	***Summit Night Out: Let the Good Times Roll*** NOLA's motto is "Laissez les bons temps rouler!" It probably didn't originally refer to bowling, but it does now! We'll hit the swankiest bowling alley in town for drinks, snacks, and good times. Wear your Summit badge for free entry and meet us at Fulton Alley, 600 Fulton Street. ***Sponsored by:*** Carbon Black. DOMAINTOOLS® THREATQUOTIENT

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat or turn them in to the SANS registration desk.

Friday, September 7

7:00-8:45 am	**Registration & Coffee** (LOCATION: ASTOR BALLROOM)
8:45-9:00 am	***Day 2 Opening Remarks*** ***Rob Lee*** *(@robtlee), DFIR Lead & Summit Co-Chair, SANS Institute* ***Phil Hagen*** *(@PhilHagen), Senior Instructor & Summit Co-Chair, SANS Institute, and DFIR Strategist, Red Canary*
9:00-9:45 am	***Keynote: Differentiating Evil from Benign in the Normally Abnormal World of InfoSec*** Have you ever been positive you had found evil, only to realize it was normal after hours of triage and work? We have all heard and love "KNOW NORMAL FIND EVIL," but how hard is it to actually know normal? The MITRE ATT&CK Framework gives defenders a better map to "find evil," but how can this framework be used to "know normal"? Rick will discuss how knowing normal in a world of abnormal is harder than one thinks, and how addressing the actual root cause of evil can improve the technology industry as a whole. ***Rick McElroy****, Security Strategist, Carbon Black*
9:45-10:20 am	***How to Submit a Threat Profile to MITRE ATT&CK*** The MITRE Corporation's framework to describe the behavior of cyber adversaries operating within enterprise networks – known as Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) – is growing fast. It is also being adopted by more and more security solutions and vendors, including big names like Microsoft and Splunk. The framework draws on years' worth of detailed forensic reports on cyber attacks that have not been fully taken advantage of up until now. The security industry has largely been focused on sharing and utilizing indicators of compromise (IOCs). By focusing on techniques and tactics of adversaries, the ATT&CK framework has gone deeper and is increasingly being used to help organizations identify gaps known to be exploited by cyber adversaries. This presentation will detail what it takes to collect public information security, threat intelligence, and forensic reports on a security threat group, and then submit all of the adversarial tactics and techniques to MITRE for inclusion in the ATT&CK framework. ***Walker Johnson*** *(@wjohnsonsled), Senior Security Engineer, Financial Services Industry*
10:20-10:45 am	**Networking Break** (LOCATION: ASTOR BALLROOM)
10:45-11:20 am	***Threat Hunting Using Live Box Forensics*** In a threat landscape characterized by targeted attacks, file-less malware, and other advanced hacking techniques, the days of relying solely on traditional "dead box" forensics for investigations are...well, dead. Live forensics, a practice considered a dangerous and dark art just a decade ago, has now become the de facto standard. However, many Computer Security Incident Response Teams still struggle with this type of threat hunting. We will discuss the benefits and pitfalls of and best practices for performing live box forensics as a threat hunting tool. John will introduce and demo a free and publicly available command-line tool for Windows that automates the execution and data acquisition from other live forensics tools in a more secure and easier-to-maintain manner. ***John Moran****, Senior Product Manager, DFLabs*

Friday, September 7

11:20-11:55 am

Viewing the Nodes in the Noise: Leveraging Data Science to Discover Persistent Threats

CenturyLink has been working on three algorithms that identify previously unknown malicious traffic by using the timestamps and packet attributes of Domain Name Server traffic. This presentation will look at the successes we have had in identifying threats through the use of our pattern, exposure, and DGA algorithms.

***David Evenden**, Senior Vulnerability Exploitation Analyst, CenturyLink*

11:55 am - 1:15 pm

Lunch & Learn

Practical Application of Network Intel for Analysts and Threat Hunters (LOCATION: TOULOUSE B)

DOMAINTOOLS®

Threat Intelligence and hunting hold great potential for helping network defenders block adversaries who have not yet breached them, and for finding evidence regarding those who may have. While external threat intel feeds can be great, most organizations also are sitting on a potential gold mine of useful forensic data. However, making practical and impactful use of the data can be tricky. It doesn't have to be. Tim Helming of DomainTools will demonstrate straightforward methods and data sources to strengthen your security posture without breaking the bank, using real-world examples of network and DNS-based threat hunts that exposed attack campaign infrastructure. The talk concludes with a simple five-point checklist you can apply immediately to begin your organization's threat intel evolution.

***Tim Helming**, Director of Product Management*

Know Your Enemy: Proactive Cyber Threat Intelligence and Threat Hunting (LOCATION: BIENVILLE)

IBM Security

During this workshop you will learn how to use cyber threat intelligence to proactively hunt advanced threats that evade detection. Discover how military intelligence analysis methodologies are now being adopted by the SOC to defeat advanced adversaries in cyberspace. We will share critical information that will help you to proactively hunt threats and gain greater intelligence including: How to define the threat landscape; How to define your adversary; How to conduct proactive cyber threat intelligence analysis against your adversary. Battle-tested threat hunter Sid Pearl, Worldwide i2 Safer Planet Cyber SME as well Chief Cyber Intelligence Officer for the International Association of Certified Information Sharing and Analysis Organizations (ISAO) will lead this informative discussion.

***Sidney Pearl**, Global i2 Cyber Leader at IBM*

Stalking the Modern Adversary (LOCATION: ST. ANN)

red canary

Learn about the techniques most often employed in successful attacks, including an increasing reliance on trusted system resources and memory residence. We'll examine prevalent, highly-effective techniques that are not easily mitigated. And we'll follow by looking at the detection engineering and analysis approach employed to detect and respond effectively to these threats.

***Joe Casazza**, Technical Account Manager, Red Canary*

Friday, September 7

11:55 am - 1:15 pm	**Lunch & Learn (Continued)** Cisco Umbrella ***Investigating and Dissecting a High-Profile Breach*** (LOCATION: IBERVILLE) In today's world, detecting and responding effectively to malware requires a range of tools able to detect and eradicate malware from inside an organization's IT infrastructure. This session will start by dissecting a high-profile breachbreach: what happened, and how did we investigate it? We will review an integrated security architecture, and discuss how threat intelligence, and malware analysis are exponentially more powerful when endpoint and network security are paired, to reduce the time needed to detect and enable further threat hunting in your environment. The session will take a look at Cisco's endpoint and cloud security solutions from the viewpoint of the architect and reverse engineer. We will discuss the technologies and philosophies behind the products and discuss lessons learned as they relate to detecting malware at scale. We will also discuss how we leverage telemetry from various sources to proactively hunt threats, turning this information into timely intelligence, detection and prevention capabilities. Finally, we will show you how you can reduce complexity and provide faster response to threats by answering critical questions such as how, who and what was impacted in your organization. ***Eric Hulse**, Sr Reverse Engineer Advanced Threat Solutions – AMP Threat Grid* ***David Lamb** , Director - Technical Services, Americas Region*
1:15-1:50 pm	***Hunting Webshells: Tracking TwoFace*** Microsoft Exchange Servers are a high-value target for many adversaries, which makes the investigation of them during Incident Response vital. Backdoor implants in the form of webshells and IIS modules on servers are on the rise. Find out how to hunt webshells and differentiate between legitimate use and attacker activity, using default logging available on every exchange server. The presentation will feature real-world examples carried out by an adversary group using web-based backdoors to breach and maintain access to networks of targeted organizations in the Middle East. ***Josh Bryant** (@FixtheExchange), Director of Technical Account Management, Tanium* ***Robert Falcone**, Threat Researcher, Palo Alto Unit 42*
1:50-2:25 pm	***Who Done It? Gaining Visibility and Accountability in the Cloud*** Every day, more enterprises are incorporating cloud services and workflows. Moving data to the public cloud has numerous advantages, but it also brings new risks and challenges for the security team. While traditional techniques and controls apply in many cases, there are also new areas involving cloud native services and APIs unique to this environment. This presentation will explore several use cases, techniques, and tools that can be applied to address the risks and challenges of using the public cloud. ***Ryan Nolette**, Security Technologist, Amazon Web Services*
2:25-3:00 pm	***Quantify Your Hunt: Not Your Parents' Red Team*** The security marketplace is saturated with product claims of detection coverage that have been almost impossible to evaluate, all while intrusions continue to make headlines. To help organizations better understand the detection provided by a commercial or open-source technology platform, a framework is necessary to measure depth and breadth of coverage. This presentation builds on the MITRE ATT&CK framework by explaining how to measure the coverage and quality of ATT&CK, while demonstrating open-source Red Team tools and automation that generate artifacts of post-exploitation. ***Devon Kerr** (_devonkerr_), Principal Threat Researcher, Endgame* ***Roberto Rodriguez** (@cyb3rward0g), Senior Threat Hunter, SpecterOps*
3:00-3:30 pm	**Networking Break** (LOCATION: ASTOR BALLROOM)

Friday, September 7

3:30-4:05 pm	***Launching Threat Hunting from Almost Nothing*** Many organizations that don't have sophisticated hunting teams wonder how to incorporate threat hunting functions into their current security operations. Would it even be of value for them to have such a function? We had the exact same questions upon hearing the term "threat hunting" for the first time. After having launched our hunting activities starting virtually from scratch, we can now say, "Yes, it's worth pursuing." In this presentation we'll explain why threat hunting was considered of value for us, what threat hunting functions were carried out, and how we have been improving our security operations. The hunting operations enabled us to identify some significant attacks that had gone undetected by several security measures. As a result, we have been making continuous improvements to make hunting a scalable mechanism that does not depend on a few advanced experts. This session will provide case studies that focus on threat hunting in enterprise security operations. ***Takahiro Kakumaru**, Security Researcher, NEC*
4:05-4:40 pm	***Threat Hunting or Threat Farming: Finding the Balance in Security Automation*** There is nearly a consensus in the broader security community that threat hunting is a fundamentally human activity. But even the most vocal proponents of this view believe that automation is necessary to continuously improve upon an existing security program and make the hunting activity scalable. When organizations can use automation to pull together the seams in their security program and extend the current hunting framework, they see immediate gains in their security posture and enable junior analysts to operate at a level near that of more experienced analysts. In this presentation, two speakers with opposing views on the subject will define the boundaries of what are fundamentally human activities (threat hunting) and what can be reasonably automated (threat farming). This distinction allows for hunters to be continuously "fed" what is necessary for a robust security detection and response program. It also provides them with the resources and capacity to go out and hunt the big game. This presentation will cover traditional network-based and ICS hunting, both manual and automated, in order to showcase examples where automation enabled the capabilities to hunt even more exciting and critical potential incidents. We'll also look at a case or two where lousy automation meant everyone had a bad day. ***Robert M. Lee** (@RobertMLee), CEO, Dragos, Inc.* ***Alex Pinto** (@alexcpsec), Lead Security Data Scientist, Verizon Enterprise Services*
4:40-5:15 pm	***Lightning Talks*** Enjoying the Summit talks? Think you've got something to add? Here's your chance to share a big idea and wow the crowd in five minutes or less! Sign-up details will be available on day 1 of the Summit. MODERATOR: ***David J. Bianco** (@davidjbianco), Principal Engineer, Cyber Security, Target*

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat or turn them in to the SANS registration desk.

SPEAKERS

***Kevin Albano**, Global Lead, Threat Intelligence, IBM X-Force IRIS*
Kevin Albano has more than 17 years of experience working in information technology, law enforcement, and security consulting. Throughout his career, he has focused on investigating computer network intrusions, notifying impacted organizations, and disrupting some of the largest cyber espionage campaigns. At IBM, Kevin is responsible for threat intelligence collections, managing advanced threat research and directing information analysis – all focused on helping customers understand their cyber threat risk and make decisions to protect their organizations. Prior to IBM, Kevin held prominent roles at the Federal Bureau of Investigation and Mandiant. As a Special Agent at the Los Angeles FBI Field Office, Kevin developed the investigative process for examining computer network attack operations.

***David J. Bianco** (@davidjbianco), Principal Engineer, Cyber Security, Target*
David has more than 20 years of experience in the information security field, with a particular focus on incident detection and response. He is active in the DFIR and Threat Hunting community, speaking and writing on the subjects of detection planning, threat intelligence and threat hunting. He is the principal contributor to The ThreatHunting Project (http://ThreatHunting.net) and a member of the MLSec Project (http://www.mlsecproject.org). You can follow him on Twitter or subscribe to his blog, "Enterprise Detection & Response" (http://detect-respond.blogspot.com).

***Matt Bromiley**, Certified Instructor, SANS Institute; Principal Incident Response Consultant, Cylance*
Matt Bromiley is a principal incident response consultant at a top digital forensics and incident response (DFIR) firm where he assists clients with incident response, digital forensics, and litigation support. He also serves as a SANS GIAC Advisory Board member, a subject-matter expert for the SANS Securing The Human Program, and a technical writer for the SANS Analyst Program. Matt brings his passion for digital forensics to the classroom as a SANS instructor for FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting; and FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response, where he focuses on providing students with implementable tools and concepts.

***Josh Bryant** (@FixtheExchange), Director of Technical Account Management, Tanium*
Josh Bryant is currently a Director of Technical Account Management at Tanium where he helps customers conduct rapid Threat Hunting data collection on a very large scale. Prior to joining Tanium, he was a Cybersecurity Architect at Microsoft where he focused on delivering Cybersecurity services ranging from Tactical and Strategic Recovery to Advanced Threat Analytics implementations, Risk Assessments, and more, to customers in a variety of industries around the world. Josh is also a Master Sergeant in the Illinois Air National Guard, where he manages a team of Systems Administrators that maintain an Air Operations Center. He has over 19 years in IT specializing in Cybersecurity and Messaging, and spent some of his Active Duty U.S. Air Force time as a Network Security Manager, performing vulnerability assessments and penetration testing.

***David Evenden**, Senior Vulnerability Exploitation Analyst, CenturyLink*
David Evenden is an experienced offensive security operator/analyst with over 12 years of active work experience inside the Intelligence Community (IC). During his time inside the IC, he learned Persian Farsi, worked at NSA Red Team and was a member of an elite international team operating in conjunction with coalition forces to aid in the ongoing efforts in the Middle East. He works at CenturyLink on the ECS in conjunction with DHS to aid in the efforts of enhancing the bidirectional sharing relationship between the US Government and Commercial entities.

SPEAKERS

***Robert Falcone**, Threat Researcher, Palo Alto Unit 42*
Robert is a Threat Intelligence Analyst with Palo Alto Networks' Unit42 focusing on malware analysis, reverse engineering, and tracking advanced threat actors. Prior to joining Unit42, he was a Malware Research Engineer at iDefense focusing primarily on malware analysis and tracking threat actors associated with cyber espionage activity. He also worked as a Security Engineer within a Security Operations Center for a managed security service provider focused on intrusion detection and prevention.

***Michael Gough** (@HackerHurricane), Malware Archaeologist, Malware Archaeology*
Michael is a Malware Archaeologist, Blue Team defender, Incident Responder, and logoholic who has developed several Windows logging cheat sheets to help the security industry understand Windows logging, where to start, and what to look for. He is also the co-developer of LOG-MD, a free tool that audits the settings, harvests, and reports on malicious Windows log data and malicious system artifacts.

***Phil Hagen** (@PhilHagen), Senior Instructor & Summit Co-Chair, SANS Institute, and DFIR Strategist, Red Canary*
Phil's career has spanned the full attack life cycle – from tool development to deployment, operations, and investigative aftermath – giving him rare and deep insight into the artifacts attackers leave behind. Phil has covered deep technical tasks, managed an entire computer forensic services portfolio, and handled executive responsibilities. He's managed a team of forensic professionals in the national security sector and provided forensic consulting services for law enforcement, government, and commercial clients.

***Ben Johnson** (@chicagoben), CTO & Co-Founder, Obsidian Security*
Ben Johnson is CTO and co-founder of Obsidian Security. Prior to founding Obsidian, he co-founded Carbon Black and most recently served as the company's Chief Security Strategist. As the company's original CTO, he led efforts to create the powerful capabilities that helped define the next-generation endpoint security space. Prior to Carbon Black, Ben was an NSA computer scientist and later worked as a cyber engineer in an advanced intrusion operations division for the intelligence community. Johnson has extensive experience building complex systems for environments where speed and reliability are paramount. His background also includes a great deal of technical "agility," having worked on advanced operational teams supporting US national security missions, to advising cyber security start-ups and the Department of Justice to writing complex calculation engines for the financial sector. Johnson earned a bachelor's degree in computer science from the University of Chicago and a master's degree in computer science from Johns Hopkins University. He lives in Newport Beach, CA with his wife and three sons.

***Walker Johnson** (@wjohnsonsled), Senior Security Engineer, Wells Fargo*
Walker is a Senior Security Engineer on the Wells Fargo Cyber Threat Forensics team within Enterprise Information Security. He previously served as a Senior Consultant and Incident Responder at Deloitte. As a forensic examiner working for the South Carolina Law Enforcement Division, Walker helped state and federal law enforcement agencies investigate numerous computer crimes.

***Takahiro Kakumaru**, Security Researcher, NEC*
Takahiro is an Assistant Manager in the NEC Corporation's Cybersecurity Strategy Division. His research interests lie in the areas of cyber threat intelligence, threat hunting, honeypots, and cyber threat intelligence sharing. He is active on OASIS CTI-TC and OpenC2 TC, and he holds the CISSP certification.

SPEAKERS

***Devon Kerr** (_devonkerr_), Principal Threat Researcher, Endgame*
Devon is a member of Endgame's research & development group, where he designs and implements enterprise detection and response capabilities. Prior to Endgame, Devon spent more than six years as a member of the Mandiant Incident Response practice.

***Rob Lee** (@robtlee), DFIR Lead & Summit Co-Chair, SANS Institute*
Rob Lee is the Curriculum Lead and an author for SANS' digital forensic and incident response training. He earned his MBA from Georgetown and graduated from the U.S. Air Force Academy. As a member of the Air Force Office of Special Investigations, Rob led crime investigations and worked directly with government agencies as a technical lead. He was also a director at MANDIANT, the commercial firm focused on responding to advanced adversaries such as the APT.

***Robert M. Lee** (@RobertMLee), CEO, Dragos, Inc.*
Robert is the founder as well as the CEO of his own company, Dragos, Inc., which provides cybersecurity solutions for industrial control system networks. He is also a SANS course author (FOR578 and ICS515) and Certified Instructor.

***Rick McElroy**, Security Strategist, Carbon Black*
Rick McElroy, security strategist for Carbon Black, has more than 15 years of information security experience educating and advising organizations on reducing their risk posture and tackling tough security challenges. He has held security positions with the U.S. Department of Defense, and in several industries including retail, insurance, entertainment, cloud computing, and higher education. McElroy's experience ranges from performing penetration testing to building and leading security programs. He is a Certified Information Systems Security Professional (CISSP), a Certified Information Security Manager (CSIM), and Certified in Risk and Information Systems Control (CRISC). As a United States Marine, McElroy's work included physical security and counterterrorism services. A fierce advocate for privacy and security who believes education and innovation are the keys to improving the security landscape, McElroy is program chair for the Securing Our eCity Foundation's annual CyberFest, a San Diego event dedicated to educating public and private sector security and IT professionals and business executives on the realities of security.

***John Moran**, Senior Product Manager, DFLabs*
John is a security operations and incident response expert. He has served as a Senior Incident Response Analyst for NTT Security, Computer Forensic Analyst for the Maine State Police Computer Crimes Unit, and Computer Forensics Task Force Officer for the U.S. Department of Homeland Security. John currently holds GCFA, CFCE, EnCE, CEH, CHFI, CCLO, CCPA, A+, Net+, and Security+ certifications.

***Katie Nickels** (@likethecoins), Lead Cyber Security Engineer, The MITRE Corporation*
As the Threat Intelligence Lead for the ATT&CK team, Katie focuses on applying cyber threat intelligence to ATT&CK and evangelizing how that helps analysts. She has worked in threat intelligence and network defense for nearly a decade, with much of that time spent helping Security Operations Centers navigate how to apply intel to defenses.

***Ryan Nolette**, Security Technologist, Amazon Web Services (AWS)*
Ryan is Amazon's primary AWS security technologist and expert. He has previously held a variety of roles, including in threat research, incident response consulting, and every level of security operations. With over a decade in the InfoSec field, Ryan has been on the product and operations side of companies such as Sqrrl, Carbon Black, Crossbeam Systems, SecureWorks and Fidelity Investments. Ryan writes and speaks frequently about threat hunting and endpoint security.

SPEAKERS

***Alex Pinto** (@alexcpsec), Lead Security Data Scientist Verizon Enterprise Services*
Alex is responsible for data science, analytics and machine learning capabilities of the Verizon Autonomous Threat Hunting product. He joined Verizon through the acquisition of Niddel, where Alex was Co-Founder and Chief Data Scientist. Alex has over 20 years of experience in build security solutions and products and the last 5 of those years have been solely dedicated to the application of machine learning in cybersecurity detection and threat hunting activities. He also holds multiple cybersecurity certifications, such as CISSP-ISSAP, CISA, CISM, and was previously PMP and PCI-QSA certified. Before founding Niddel, Alex was a founder of Cipher Security, a global full-solution provider of Brazilian origin. He was born in Rio de Janeiro, but for a twist of fate can't play any soccer. His spirit animal is the capybara.

***Josh Pyorre** (@joshpyorre), Security Research Analyst, Cisco Umbrella*
Josh has worked in security for 14 years. He's been a threat analyst at NASA and also helped to build the Security Operations Center at Mandiant. His professional interests involve network, computer, and data security.

***Roberto Rodriguez** (@cyb3rward0g), Senior Threat Hunter, SpecterOps*
As a Senior Threat Hunter for SpecterOps, Roberto specializes in data analytics, threat hunting, and Incident Response. He is the author of the Threat Hunter Playbook and the HELK platform.

***Andrea Scarfo** (@AScarf0), Security Research Analyst, Cisco Umbrella*
Andrea worked as a Sysadmin for 12 years and has worked with Hewlett Packard and the city of Danville, CA. She began working with Open DNS in 2015 and has worked tirelessly to make the Internet a safer place.

***Cody Thomas** (@its_a_feature_), Senior Cyber Security Engineer, The MITRE Corporation*
Cody is the creator of ATT&CK for Linux and Mac, and he also serves as an Adversary Emulation Engineer. His work includes leading adversary emulation operations, developing Red-Team-oriented tools, and spreading the word on the power of purple teaming.

***Alissa Torres** (@sibertor), Certified Instructor, SANS Institute*
Alissa is a Certified SANS instructor, specializing in advanced computer forensics and incident response. Her industry experience spans government, academic and corporate environments and includes incident handling with the Mandiant CIRT and internal investigations for a large government contractor. A huge fan of GIAC, Alissa holds the GCFA, GCFE, GCIH, GCIA, GSEC, CISSP, and EnCE certifications.

***Mauricio Velazco** (@mvelazco), VP – Threat Management, Blackstone*
Mauricio is an Information Security specialist with more than eight years of results-driven experience in designing and executing security projects. He is also an experienced security instructor who has taught students in many countries in critical fields of computer and application security. Mauricio currently leads the Blue Team at Blackstone, the largest private equity firm in the world.

***Jake Williams** (@MalwareJake), Founder, Rendition InfoSec*
Jake is a SANS Senior Instructor and course author. He founded Rendition InfoSec, where he runs a Security Operations Center. He also provides Incident Response, threat intelligence, and other InfoSec consulting services. Jake is also a certified Shadow Brokers protagonist.