SANS strives to present the most relevant, timely, and valuable content. As a result, this agenda is subject to change. Please check back frequently for changes and updates.

Thursday, September 6	
8:45-9:00 am	*Welcome & Opening Remarks* ● **Rob Lee (@robtlee), DFIR Lead & Summit Co-Chair, SANS Institute** ● **Phil Hagen (@PhilHagen), Certified Instructor & Summit Co-Chair, SANS Institute, and DFIR Strategist, Red Canary**
9:00-9:45 am	*Opening Keynote* To be announced
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, this session begins by looking at known indicators from popular botnets spreading such threats as Locky, Globeimposter, and Trickbot. The presentation will highlight co-occurring malicious activities observed on the infrastructure of popular botnets. We will 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**
10:45-11:20 am	**This Is the Fastest Way to Hunt Windows Endpoints** Threat hunting can be a daunting task, and there are 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, but what was lacking until recently was a tool that could quickly assess a suspect Windows system to harvest key artifacts or IOCs to feed back into enterprise hunting solutions. What came out of dealing with an advanced hacking group and the speed with which these groups spread within an environment was 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. Where do we start? What do we look for? What can we glean from a suspect system that could be used to hunt? This talk focuses on solutions that have worked in hunting and detecting the activities of advanced hacking groups. It looks at the gaps we had to quickly evaluate on a suspect Windows endpoint in order to discover key malicious artifacts or IOCs. We'll also discuss how those gaps were closed by developing a new tool that hunters can use to quickly evaluate a Windows endpoint to harvest key artifacts and IOCs that can be used as stand-alones or fed into enterprise-hunting solutions to improve the speed and quality of your hunts. **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 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. In this talk, Jake will introduce a model for including supply-chain risks (hardware, software, and service) into your threat hunting operations in order to ensure that your organization does not overlook this critical area of security. **Jake Williams (@MalwareJake), Founder, Rendition InfoSec**
11:55 am-1:15 p.m.	**Lunch & Learn, *Presented by*** Carbon Black.
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 how to better organize cyber threat intelligence and leverage it to conduct adversary emulation and hunting using ATT&CK. 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. Red

	Teamers will also benefit by learning how to leverage that same intel on adversary TTPs to plan operations, communicate with defenders, and perform adversary emulation. **Katie Nickels (@likethecoins) (@MITREattack), ATT&CK Threat Intelligence Lead, The MITRE Corporation** **Cody Thomas (@its_a_feature_), Adversary Emulation Engineer, The MITRE Corporation**
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. Join Stuart Davis in this brief but informative session on threat hunting techniques adapted to the climate and temperatures of organizations that Mandiant works with on a day-to-day basis. We 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. **Stuart Davis, Director – EMEA, Mandiant**
2:25-2:45 pm	**Networking Break**
2:45-3:20 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. The purpose of this talk is to describe the most common lateral movement techniques as well as the methods the Blue Team can put in place to detect lateral movement. Mauricio will also introduce a tool called Oriana that he developed to hunt for lateral movement. Attendees can expect to learn about the most common techniques used for lateral movement from an attacker's perspective, as well as the most relevant Windows event logs that can be used to detect lateral movement. **Mauricio Velazco (@mvelazco), VP – Threat Management, Blackstone**
3:20-3:45 pm	**Networking Break**
4:00-4:35 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), Incident Response Manager, Cargill; Certified Instructor, SANS Institute**
4:35-5:10 pm	**Live Debates** 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; Cylance**

[

Friday, September 7	
8:45-9:00 am	*Day 2 Opening Remarks* ● **Rob Lee (@robtlee), DFIR Lead & Summit Co-Chair, SANS Institute** ● **Phil Hagen (@PhilHagen), Certified Instructor & Summit Co-Chair, SANS Institute, and DFIR Strategist, Red Canary**
9:00-9:45 am	*Keynote* **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. This is likely to continue because the framework draws on years' worth of detailed forensic reports on cyber-attacks and attackers 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. The framework focuses on the inevitable post-compromise, which forces cyber adversaries to change not only surface level and trivial IOCs but also their tactics and techniques, which are much more difficult to change. 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**
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. This session will discuss the benefits, pitfalls, 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**
11:20-11:55 am	**Viewing the Nodes in the Noise: Leveraging Data Science to Discover Persistent Threats** Century Link has been working on three algorithms that identify previously unidentified malicious traffic by using the timestamps and packet attributes of Domain Name Server traffic. This presentation will ok at the success 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 p.m.	**Lunch**
1:15-1:50 pm	**Hunting Webshells: Tracking TwoFace** Microsoft Exchange Servers are a high-value target for many adversaries, which makes investigation of them during Incident Response vital. Where do you start? What should you look for? 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. During this presentation, we will use 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), Cybersecurity Architect, Microsoft** **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**
2:25-2:45 pm	**Networking Break**
2:45-3:20 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. Attendees will gain new or improved abilities to measure detection capabilities. Finally, the presentation will articulate a call to action for the industry: Adopt this common language that describes these detection capabilities in a tangible and quantifiable way. **Devon Kerr (_devonkerr_), Principal Threat Researcher, Endgame** **Roberto Rodriguez (@cyb3rward0g), Senior Threat Hunter, SpecterOps**
3:20-3:45 pm	**Launching Threat Hunting from Almost Nothing** Many organizations that don't have very 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 exactly same questions upon hearing the term "threat hunting" for the first time. After having launched out 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 were 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**
3:45-4:00 pm	**Networking Break**
4:00-4:35 pm	**Threat Hunting or Threat Farming: Finding the Balance in Security Automation** There is near 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 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), Security Data Scientist, Niddel (a Verizon company)**
4:35-5:10 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 5 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**

Speaker Biographies

Josh Bryant (@FixtheExchange), Cybersecurity Architect, Microsoft
Josh is a Cybersecurity Architect (Senior Consultant Cyber II) at Microsoft, where he is currently focused on delivering cybersecurity services ranging from compromise and strategic recovery to advanced threat analytics implementation, risk assessments, and more to customers in a variety of industries around the world.

Stuart Davis, Director – EMEA, Mandiant
Bio to come

David Evenden, Senior Vulnerability Exploitation Analyst, CenturyLink
Bio to come

Robert Falcone, Threat Researcher, Palo Alto Unit 42
Robert is a Threat Intelligence Analyst with Palo Alto Networks' Unit 42 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.

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.

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.

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.

Alex Pinto (@alexcpsec), Security Data Scientist, Niddel (a Verizon company)
Alex is a Security Data Scientist at Niddel and the lead of the MLSec Project. He has been working on threat hunting automation with machine learning and data science techniques for the last five years, and has been working in Information Security for 20 years.

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 Oblivious Domain Name Servers 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), Incident Response Manager, Cargill; Certified Instructor, SANS Institute
Alissa works as Incident Response Manager at Cargill, where threat hunting is central to Command Center operations. She is a SANS Certified Instructor specializing in host-based forensics analysis with a passion for hunting evil in system memory. A huge fan of GIAC, Alissa holds numerous 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 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.