SANS DFIR

Threat Hunting & Incident Response Summit 2019

Program Guide

@sansforensics #ThreatHuntingSummit

Agenda

All Summit Sessions will be held in the Salon A-E (unless noted otherwise).

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

Monday, September 30	
7:00-9:00 am	**Registration & Coffee** (LOCATION: MARDI GRAS BALLROOM PRE-FUNCTION)
9:00-9:15 am	***Welcome & Opening Remarks*** ***Matt Bromiley*** *@mbromileyDFIR, Summit Co-Chair, SANS Institute* ***Philip Hagen*** *@philhagen, Summit Co-Chair, SANS Institute*
9:15-10:00 am	***Keynote: Play Like a Kid, Protect Like a Champion: A Reservist Model*** Research has shown that play is crucial to the development of skills for children. This concept also applies to Olympic-caliber athletes, high-functioning military units, and cutting-edge cybersecurity programs. What if there was a way to simultaneously inject play/training into your security program, execute advanced cybersecurity functions (threat hunting, red teaming, and threat intelligence), and identify and close gaps in visibility and security posture? This talk will explore the Netflix framework to accomplish these goals. Netflix strives to find high-leverage activities that solve multiple challenges. For example, Netflix uses a reservist model to supplement crisis management and incident response with great success. This year, Netflix implemented a similar model to establish a purple team – a matrixed team of reservists to support threat hunting, red teaming, and intelligence operations. This presentation will explore how Netflix executes hunting via the red and intelligence teams, lessons learned, and steps you can start implementing today. It's time to play, have some fun, and develop championship-level security programs! ***Chris Cochran*** *Threat Intelligence & Operations Lead, Netflix*
10:05-10:40 am	***Evolving the Hunt: A Case Study in Improving a Mature Hunt Program*** As a major U.S. retailer with a strong cybersecurity focus, Target has long had a functional, mature threat hunting program. When David Bianco took over responsibility for the hunting program in early 2019, leadership's key question was "How can we do even better?" But what does "better" mean for a hunting program, and how do you get from where you are now to where you want to be? In this presentation, we'll talk about coming into an existing threat hunting program, prioritizing areas for improvement, and then implementing those improvements to make a great hunting program even better. Attendees will learn the key functions of a threat hunting program and how to evaluate the current hunting program maturity level, set an appropriate maturity improvement goal, identify and prioritize possible program changes to support the desired improvements, and understand how and why these efforts work (or don't work!). ***David J. Bianco*** *@davidjbianco, Principal Engineer – Cybersecurity, Target* ***Cat Self*** *@coolestcatiknow, Lead Information Security Engineer, Target*
10:40-11:20 am	**Networking Break** (LOCATION: SALON F/G/H)

Monday, September 30

11:20-11:55 am

My "Aha!" Moment

This presentation is designed as a personal journey through threat hunting to inspire others to embrace certain methods, tips, and lessons learned. When John Stoner joined this Splunk team in 2017, the team started working on the second version of what it called "Boss of the SOC" (BOTS). John will share his team's journey in threat hunting as it attempted to figure out where to start, at times found itself getting tangled in the data, and overcame distractions encountered during the hunting process. He'll cover how the team was able to conduct hunts, and he'll share some thoughts on gap analysis and operationalizing these findings. The presentation will also include some cautionary tales to help the threat hunting community assist security operations with operationalizing hunt data and not take all the great work that is out there and oversimplify it in such a way that it loses its impact. Attendees will come away with a better understanding of how to create a hunting hypothesis, build "guard rails" into your hunt to stay focused, and take hunting output and operationalize it. We'll also examine the importance of conducting gap analysis as part of the hunting activity to support the efforts of operations. Attendees will receive a data set and instructional application that they can take home and play with!

John Stoner *@stonerpsu, Principal Security Strategist, Splunk*

12:00-12:35 pm

Well, What Had Happened Was...

This presentation will cover the details and lessons learned from a cybersecurity incident involving a nation-state adversary that occurred in 2013. The nation-state threat actor group was named in an October 2018 indictment, so it can finally be discussed in a public forum. We will also present additional information that was not seen in this specific incident, but was part of a strategic operation that was traced all the way back to 2010. It is not often that a presentation can include not only the entire digital life cycle of an attack, from first infection method to last-ditch attempted persistence, but also insider threats, physical security, and more!

Todd Mesick *@tmesick1, Lead Forensic Analyst, Precision CastParts*

Brian Moran *@brianjmoran, Digital Strategy Consulting, BriMor Labs*

12:35-1:40 pm

Lunch & Learn Sessions

DOMAINTOOLS®

Domain and DNS-Based Adversarial Threat Intelligence in the SOC/CSIRT (LOCATION: BALCONY J/K)

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 and it doesn't have to be. Corin Imai of DomainTools will demonstrate straightforward methods and data sources to strengthen your security posture without breaking the bank, using real-world examples of DNS-based intelligence that exposed attack campaign infrastructure.

Corin Imai, *Senior Security Advisor & Senior Product Marketing Manager*

Evade Me If You Can: An Inside Look at Malware Evasion Techniques

(LOCATION: BALCONY L/M)

VMRAY

When traditional security products fail in preventing malware from infiltrating an organization, a malware sandbox is often the last hope. For years, malware authors have found ways to stay one step ahead in the arms race with sandbox vendors in this crucial security layer. Building on years of research, the VMRay team tracked and analyzed the evasion techniques that these malware authors use. Like Sun Tzu, we know our enemy and bring the battle to them. Join Ben Abbott, Solutions Engineer at VMRay, as he takes a deeper look at the techniques these malware authors use to evade analysis, and what steps can be taken for organizations to restore hope in their defenses.

Ben Abbott *@VMRay, Solutions Engineer*

Monday, September 30

1:45-2:20 pm

Who's that CARBANAKing at My Door? Hunting for Malicious Application Compatibility Shims

If an attacker clearly had backdoor access to a system, yet no malware can be found on disk and there is no sign of how the malware was loaded into memory, how would you even begin your forensic investigation? This was the obstacle Mandiant consultants faced while responding to an intrusion attributed to FIN7 in 2017. FIN7, a financially-motivated threat group, was able to stealthily use the CARBANAK backdoor as well as point-of-sale malware to steal thousands of payment card numbers. FIN7 remained undetected for months by using application compatibility shims to hide and execute its malware, a methodology that had rarely been seen prior to this intrusion. This presentation will recount that investigation from the perspective of the incident responders and share techniques for detecting and hunting malicious application compatibility shims in your own network. The number of threat actors using application shim persistence will likely continue to rise in the years ahead as network defenders become more effective at detecting traditional persistence mechanisms and more attackers are forced to take FIN7's lead. Raising industry awareness of this attacker methodology is critical before its use becomes prevalent. Attendees will come away with a technical understanding of how Microsoft uses shims to provide applications with backwards compatibility against the ever-changing Windows codebase, and how attackers have abused shim functionality to covertly execute malware and ways they will expand this abuse in the near future. Be prepared to come away locked and loaded, ready to hunt down malicious application compatibility shims that are likely already on your networks!

Benjamin Wiley *@benwiley, Associate Consultant, Mandiant*

2:25-3:00 pm

Threat Hunting in the Enterprise with Winlogbeat, Sysmon, and ELK

While threat prevention is critical to reduce an organization's security risk, it is not enough. Blue teamers must assume that at some point a threat is going to evade defenses and get an initial foothold in the organization. So it is important to have the means to detect those attacks at an early stage to contain the threat and reduce its impact. Defenders also need to perform retrospective investigations and do enterprise-wide searches, analyzing information of multiples devices at once. This presentation will show how to enhance endpoint visibility by using free tools such as Sysmon, Winlogbeat, and ELK. By using ATT&CK as a reference model, blue teamers can create detections for several attack techniques based on the endpoint events. By targeting threat behavior, defenders can more effectively detect adversaries, even when they change their artifacts or infrastructure. Several examples will show how the system can be used to detect various attack techniques such as live-off-the-land attacks (attackers using tools available on the endpoints such as wmic, cscript, net, PowerShell, net scripts); fileless attacks through PowerShell scripts (detections for PowerShell Empire and Unicorn will be shown); lateral movement (PSEXEC, wmic); password spraying attacks (based on Windows' successful and failed logins visualization in Kibana); persistence creation via the Windows registry, new services, and other techniques; command and control callbacks; actions on objective, such as looking for passwords on the file system and Windows registry for lateral movement and privilege escalation, in addition to Kibana, elasticsearch, and ELK API; and known threats based on specific functions used in code (TTP), rather than file hash, IP address, or domain, which allows for better detection and is harder for attackers to evade. While the human analyst is focusing on detecting TTPs, ELK API allows analysts to automate the search for indicators of compromise such as IP addresses, domains, and hashes to programmatically detect known evil. We will also show how to integrate this solution with the MISP Threat Intelligence Platform through API for automatic detection of Indicators of Compromise.

David Bernal Michelena *@d4v3c0d3r, Lead Security Researcher, Scitum*

Patricio Sánchez*, Head of SCILabs, Scitum*

3:05-3:40 am

Networking Break (LOCATION: SALON F/G/H)

Monday, September 30

3:45-4:20 pm

Once Upon a Time in the West: A Story on DNS Attacks

Just like in movies about the Old West, we are going through a land riddled with well-known gunmen – OceanLotus, DNSpionage, and OilRig, among others – who roam at ease while the security cowboys sleep. This presentation will uncover the toolset and techniques used by these gunmen, taking a closer look at their big guns and behavioral patterns. We will explore the attacks involving DNS that took place during the last decade to examine the latest techniques discovered to improve detection and dodge the bullets the bad guys are firing in our direction.

Ruth Esmeralda Barbacil*, Cyber Intelligence Analyst, Deloitte*

Valentina Palacin*, Cyber Intelligence Analyst, Deloitte*

4:25-5:00 pm

BZAR – Hunting Adversary Behaviors with Zeek and ATT&CK

Lately, threat hunters have been obsessed with endpoint data, and for good reason. Endpoint sensing is great for finding behaviors that happen exclusively on a single host. It has traditionally been neglected, yet it is a critical part of any threat hunter's arsenal. At the same time, adversaries need to move around the internal network. Whether via SMB, RDP, or some other method, moving laterally is a critical part of most adversaries' attacks. Adversaries can also use mechanisms like RPC to execute code, evade defenses, and access credentials. This means that internal network monitoring can also be a valuable asset for a threat hunter.
This presentation will first describe what adversaries do that is visible via internal network monitoring. This will be framed using the ATT&CK knowledge base: which techniques are always, usually, or sometimes visible in network traffic? As an example, Windows Admin Shares will almost always be visible in network traffic, while Scheduled Task creation might sometimes be visible when done in a certain way. The presentation will describe BZAR (Bro/Zeek ATT&CK-Based Analytics and Reporting), a set of Bro/Zeek scripts utilizing the Server Message Block (SMB), and Remote Procedure Call (RPC) protocol analyzers to detect post-exploit adversary behaviors. We'll focus not just on what BZAR can do, but also on how it works, how to deploy network sensors that can feed it, and lessons learned in building it out. We'll also examine another approach to BZAR-style analytics. Rather than doing analytics in Zeek directly, they can be implemented in a SIEM by sending the relevant Zeek logs to the SIEM and implementing analytics there. BZAR has the advantage of detecting events in real time with less ingest into the SIEM, and the SIEM has the advantage of being able to correlate events after the fact, across network and endpoint events, and across larger time frames.

Mark Fernandez*, Lead Cybersecurity Engineer, The MITRE Corporation*

John Wunder *@jwunder, Principal Cybersecurity Engineer, The MITRE Corporation*

6:00-8:00 pm

Summit Night Out (LOCATION: BARCADIA)

Take a 10-minute walk to **Barcadia** (@barcadianola) for food, drinks, networking, and vintage arcade games. (Tron! Galaga! MS. PAC MAN!) Barcadia is located at 601 Tchoupitalas.

SPONSORED BY:

VMRAY

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.

Tuesday, October 1

7:00-9:00 am	**Registration & Coffee** (LOCATION: MARDI GRAS BALLROOM PRE-FUNCTION)
9:00-9:05 am	***Day 2 Opening Remarks*** ***Matt Bromiley*** *@mbromileyDFIR, Summit Co-Chair, SANS Institute* ***Philip Hagen*** *@philhagen, Summit Co-Chair, SANS Institute*
9:05-9:50 am	***Keynote: Classifying Evil: Lessons from Hunting Human Traffickers*** Global Emancipation Network is the leading data analytics and intelligence nonprofit dedicated to countering all forms of human trafficking across the globe. We track children across the web and international borders. We monitor and reconstruct timelines of trafficker's online personas and real-world locational data. We develop and provide cutting-edge tools to counter-trafficking stakeholders to disrupt international criminal organizations. Join us as we explore the parallels between hunting human traffickers and cyber criminals from aggregating siloed data to adapting to changing adversary tradecraft to the latest efforts in image analysis and open source intelligence. ***Sherrie Caltagirone****, Executive Director, Global Emancipation Network @GblEmancipation*
9:50-10:25 am	***Jupyter Notebooks and Pre-recorded Datasets for Threat Hunting*** How many times have you thought about a more efficient, intuitive, or creative way to analyze the security events your organization collects, but feel limited to the capabilities of a one language-dependent search bar with basic Boolean search capabilities? In addition, how much time do you usually spend preparing for the simulation of specific adversarial techniques? What if you could expedite the process to validate the detection of those techniques in a more efficient and affordable way? In this talk, we will introduce the concept of utilizing Jupyter Notebooks for a more dynamic, flexible, and language-agnostic way to analyze security events, and at the same time help your team document, standardize, and share detection playbooks. We will go over the architecture, deployment, and capabilities of Jupyter Notebooks and present a few use cases covering multiple techniques to analyze data while performing research. In addition, we will show how to use pre-recorded datasets from a new open-source project named Mordor to expedite simulation of adversarial techniques and validation of data analytics. The final part of the presentation will cover a methodology used to collect and consume pre-recorded security events in a controlled lab environment with specific security log auditing configurations that can also be used to identify gaps and provide recommendations for data collection strategies in production environments. ***Roberto Rodriguez*** *@Cyb3rWard0g, Security Researcher* ***Jose Luis Rodriguez*** *@Cyb3rPandaH, Security Researcher*
10:25-10:55 am	**Networking Break** (LOCATION: SALON F/G/H)

Tuesday, October 1

11:00-11:35 am

Don’t Miss the Forest for the Trees: How to Translate Too Much Data from Too Many Intrusions into Strategic Hunting Value

The global pace of targeted intrusion activity is as rapid as ever, but improvements in monitoring, detection, and forensics technologies currently provide threat hunters with unprecedented visibility. How can we manage the seemingly exponential growth in the number of breaches and amount of relevant intrusion data even as we still have to develop a useful strategic threat picture over time? This talk will provide insights from an industry-leading threat hunting team on ways to approach this problem. Recommendations will include ways to effectively capture the most relevant takeaways from intrusions to help analysts create better hunting leads and build threat assessments with robust context. Armed with these foundations, threat hunters can better partner with their threat intelligence counterparts to harness tactical data when building strategic assessments of adversaries. The talk will also present unique strategic trends and threat hunting findings identified using these methods.

Karl Scheuerman *@KarlScheuerman, Senior Strategic Intrusion Analyst, CrowdStrike*

Piotr Wojtyla*, Senior Researcher, CrowdStrike*

11:40 am – 12:15 pm

Open the Pod Bay Doors Please, HAL

Modern threat hunting has focused on tooling that enables hunters to be more efficient in finding correlated events and bringing the relevant data to their fingertips. As data volumes have increased – with new logs, alerts, telemetry, and intelligence blossoming at rates that make Moore’s Law look quaint – machine learning and machine intelligence systems have taken over the bulk of the “business as usual” and anomaly hunts. At the same time, the first generation of cloud SIEM complete with automated threat hunting and incident response capabilities has only just been launched. Subsequent generations will evolve both rapidly and in a way that will force organizations into rethinking their hunting and response requirements. This session looks at where “cloud effects” will be leveraged by cloud SIEM, how automation will default to autonomous, why machine intelligence will visibly succeed, and how the role of the threat hunter will evolve over the next few years.

Gunter Ollmann *@gollmann, Chief Security Officer, Microsoft*

12:15-1:25 pm

Lunch & Learn Sessions

cisco Cisco Umbrella

The Anatomy of an Attack (LOCATION: BALCONY L/M)

Cisco Threat Response integrates threat intelligence from Cisco TALOS and third-party sources to automatically research indicators of compromise (IOCs) and confirm threats quickly. This is the unifying force powering the Cisco integrated security architecture including Advanced Malware Protection, Umbrella, Email, FirePower and more. It’s a single console that automates integrations across Cisco security products and threat intelligence sources. Come hear about how this tool can help provide you a way to orchestrate and automate your Threat Hunting Efforts.

Daniel Bates, *Systems Architect*

Tuesday, October 1

12:15-1:25 pm

Lunch & Learn Sessions (CONTINUED)

Gain the Upper Hand: Leveraging Telemetry and Response Actions to Close the "Breakout" Window (LOCATION: BALCONY J/K)

ENDGAME.

As organizations implement additional tools and security controls, security operations teams gain increased visibility into their environment that can be leveraged during threat detection, hunting, and incident response. However, as the volume and types of telemetry increases, security analysts can be overwhelmed and struggle to find the signal in the noise. Security operations teams that understand their telemetry and what "normal" looks like in their environment, can focus on hunting for and detecting malicious behavior before their organization's assets are impacted. Join Endgame's lunch and learn session where we will discuss how security practitioners can:

- Understand the telemetry that is available to them before hunting for adversary behavior in their environment
- Use Endgame's Reflex™ technology along with the publicly released Event Query Language (EQL) to alert, hunt, and even prevent malicious activity
- Form additional hypotheses for threat hunting after analyzing a real intrusion campaign

***David French**, Threat Researcher*

1:30-2:05 pm

Live Debates!

Back by popular demand! This fast-paced, fun session pits friends and colleagues against one another in a (mostly) friendly competition with a twist: debaters don't know the topics – or whether they're pro or con – until they get on stage. Laugh along with them as they're put on the spot to defend their positions on a variety of hunting and IR topics.

REFEREE: ***Matt Bromiley** @mbromileyDFIR, Summit Co-Chair, SANS Institute*

2:10-2:45 pm

Remote Access Tools: The Hidden Threats Inside Your Network

Many remote access tools are used legitimately and not considered malware. However, these tools actively bypass network controls, obscuring which parties are communicating, when, and how. This ability to fly under the radar is attractive to malicious insiders and outside attackers alike. This presentation will discuss common techniques these tools use and how security teams can find and understand them.

***David Pearson** @davidp0508, Head of Threat Research, Awake Security*

2:50-3:25 pm

Worm Charming: Harvesting Malware Lures for Fun and Profit

Client-side attacks are a common source of compromise for many organizations. Web browser and e-mail-borne malware campaigns target users by way of phishing, social engineering, and exploitation. Office suites from vendors such as Adobe and Microsoft are ubiquitous and provide a rich and ever-changing attack surface. Poor user awareness and clever social engineering tactics frequently result in users consenting to the execution of malicious embedded logic such as macros, JavaScript, ActionScript, and Java applets. In this talk, we'll explore a mechanism for harvesting a variety of these malware lures for purposes of dissection and detection: worm charming (also known as grunting or fiddling). Worm charming is an increasingly rare real-world skill used to attract earthworms from the ground. A competitive sport in East Texas, it uses methods that involve vibration of the soil, which encourages the worms to surface. In our context, we'll apply a series of YARA rules to charm interesting samples to the surface from the nearly 1 million files uploaded to Virus Total daily. Once the samples are aggregated, we'll explore mechanisms for clustering and identifying " interesting" samples. Specifically, we're on the hunt for malware lures that can provide a heads-up to defenders on upcoming campaigns as adversaries frequently test their lures against anti-virus consensus.

***Will MacArthur** @Anti_Expl0it, Threat Research & Intelligence Lead, InQuest.net*

3:25-3:45 am

Networking Break (LOCATION: SALON F/G/H)

Tuesday, October 1

3:50-4:25 pm

Hunting Is Sacred, But We Never Do It for Sport!

Hunting is sacred, little brother. It's our right, but we never do it for sport!" Bagheera teaches Mowgli that jungle law during a hunt. Predators have to FIND preys and KILL in order to survive, and they do it instinctually. Threat Hunting and Incident Response (THIR) practitioners also have to do both effectively in order to survive. In cybersecurity, threat hunting (FIND) and incident response (KILL) practices are interrelated but at the same time distinct in nature. When a hunt sortie identifies a threat (prey) in the environment, it has to be followed by an effective incident response. Sounds straightforward, but the details and the overlooked seams between the two practices are underestimated and may lead to failure. Are the two THIR practices conducted by one team? Or two different teams? Internal or external? When do you switch from TH to IR? Does the first true positive come from the TH? How are the new injects from the TH cycle integrated into an already running IR cycle? How do you synchronize and integrate the two practices? We have good models and practices to run and manage THIR, but for the most part separately. We need to do more to seamlessly integrate the two practices and mend the seams between them. In this session we'll present examples when THIR has failed due to the overlooked seams between the two practices. Attendees will learn how to run the two practices seamlessly as one process – that is, stitch the seams between the two practices – as well as how the original Kill Chain (F2T2EA) model can be used to run an effective THIR.

Ashraf M. Abdalhalim*, Incident Response and Forensics, Senior Consultant, FireEye*

4:30-5:05 pm

There's an Actor in My Pocket!

Did you ever have the feeling there's a WASKET in your BASKET? Or an actor in your logs? Threat hunting is a human-driven approach to taking hunches like these and tracking them down to find threat actors lurking in your environment. A well-structured hunt includes inputs (for example, a hunch, internal incident learnings, threat intel), outcomes, and hypotheses to avoid going down rabbit holes when exploring large datasets. Join this session as we walk through multiple hunting examples with varying outcomes – from uncovering an incident to nothing – and share queries that you can use to hunt down bad guys in your own environment. We'll examine the tools and data sources used in threat hunting, including log aggregators (for example, SIEM) that create a playing ground for hunters to correlate events across data sources. And we'll also look at the rules or queries that are used to make sense of the data and help prove or disprove a hypothesis.

Jennifer Chavarria*, Threat Hunting Analyst, Shell Oil*

Daniel Garcia*, Threat Hunting Analyst, Shell Oil*

5:05-5:15 pm

Wrap-Up

Matt Bromiley *@mbromileyDFIR, Summit Co-Chair, SANS Institute*

Philip Hagen *@philhagen, Summit Co-Chair, SANS Institute*