FOUNDING PARTNER

CARBON BLACK

Threat Hunting & Incident Response

SANS DFIR | Summit & Training

Program Guide

@sansforensics

#ThreatHuntingSummit

Agenda

All Summit Sessions will be held in BLAINE KERN BALLROOM (unless noted).

All approved presentations will be available online following the Summit at
https://digital-forensics.sans.org/community/summits

Tuesday, April 18	
8:00-9:00am	**Registration & Coffee** (LOCATION: BLAINE KERN BALLROOM FOYER)
9:00-9:45am	**Huntworld** Adversaries have been coming to our networks for nearly 20 years, repeating the same intrusions day after day, while we repeat more or less the same responses day after day. We'll kick off the second annual Threat Hunting & Incident Response Summit by exploring the hunting culture over the years and studying what works, what doesn't, and what the future holds. ***Rob Lee*** *(@robtlee), Lead – DFIR Curriculum, SANS Institute*
9:45-10:15am	**Networking Break & Vendor Expo** (LOCATION: BLAINE KERN BALLROOM FOYER)
10:15-10:50am	***Threat Hunting in Security Operations*** The Security Operations Center (SOC) is intended to be the nexus of protection for the organization. There are many things it must do. This talk will depict a model for security operations and the data flow of threat hunting within the SOC. This includes: inputs, outputs, staff members and technology necessary to accomplish the often misconstrued task of threat hunting. ***Chris Crowley*** *(@CCrowMontance), Principal Instructor, SANS Institute*
10:50-11:25am	***Real-Time Threat Hunting*** Normally the only option for threat hunting requires extensive data analysis by an experienced hunter. Machine learning has come a long way in the last few years. In this talk we'll cover a new tool for leveraging machine learning to take some of the capabilities of an experienced cyber hunter and show you how to leverage Bro and an open source tool to be released with this talk to achieve real-time detection on what would otherwise only be achievable with an experienced cyber hunter. Come learn how you can leverage machine learning to enhance your threat hunting efforts. ***Tim Crothers****, Senior Director – Cybersecurity, Target Corporation*

Tuesday, April 18

11:25am-12:00pm	***Biting into the Jawbreaker: Pushing the Boundaries of Threat Hunting Automation*** Threat Hunting has been commonly definable as a series of investigative actions that should be performed by human teams in order to cover detection gaps where automated tools fail. However, as those techniques become more and more popular and standardized, wouldn't it be the case that we are able to automate a large part of those common threat hunting activities, creating what is basicaly a definition oxymoron? In this session, we will demonstrate how some IOC-based threat hunting techniques can be automated or constructed to augment human activity by encoding analyst intuition into repeatable data extraction and processing techniques. Those techniques can be used to simplify the triage stage and get actionable information from potential threats with minimal human interaction. The more math-oriented parts will cover descriptive statistics, graph theory, and non-linear scoring techniques on the relationships of known network-based IOCs to an organization's log data. Our goal here is to demonstrate that by elevating the quality of data available to our automation processes we can effectively simulate "analyst intuition" on some of the more time consuming aspects of network threat hunting. IR teams can then theoretically more productive as soon as the initial triage stages, with data products that provide a "sixth sense" on what events are the ones worth of additional analyst time. ***Alex Pinto*** *(@alexcpsec), Chief Data Scientist, Niddel*
12:00-1:30pm	**Lunch & Learn** (LOCATION: BLAINE KERN BALLROOM)

Systemic Threat Hunting: Using Continuous Detection Improvement to Find Bad Things

CARBON BLACK

It is well accepted that threat research is foundational to the effectiveness of any threat hunting team. But many teams take IOC from a research report and immediately go on the hunt. There is a better way!

Leading threat hunting teams are using threat research to assess the effectiveness of their detection and prevention programs. These teams identify their gaps, improve their detection, and systemically hunt for threats using their detection tooling. It's more efficient and more reliable.

Join Red Canary, Carbon Black, and a joint customer as they talk threat hunting best practices. You will learn:

- The difference between automation and hunting
- A process for continuous detection improvement
- Why endpoint telemetry is critical for your hunting efforts

***Jared Myers**, Threat Researcher, Carbon Black*

***Joe Moles**, Incident Response, Red Canary*

Tuesday, April 18

1:30-2:05pm	***The Myth of Automated Hunting and Case Studies in ICS/SCADA Networks*** Threat hunting is a human focused process. Automation is an important part to being able to hunt effectively and consistently over time but threat hunting cannot be fully automated. The important part about threat hunting is pitting the best human defenders against the human threats we face. In this presentation the case will be made that threat hunting cannot be fully automated. This will be done through a discussion on where the approach should exist in an organization's security maturity model and will be reinforced with examples of hunting inside of ICS/SCADA networks such as those that operate the power grid, oil facilities, and petrochemical environments. ***Robert M. Lee*** *(@RobertMLee), CEO, Dragos Inc.*
2:05-2:40pm	***So Many Ducks, So Little Time*** Threat hunting is time consuming, costly and highly specialized". The authors of this talk aim to completely contradict this statement and show you that you can start threat hunting with minimal time investment by leveraging free tools and clever techniques. While the need for proactive threat identification is getting traction within the security industry, many still see this as something that can only be achieved by investing in intelligent (and expensive) threat hunting software. Starting with baselining a subset of the systems in your environment and automating analysis through scripting, the authors were able to start their threat hunting efforts on a 4-hour budget. They will show you how they developed their methods and achieved quick wins. During the session, hands-on tips and lesson learned will be provided. A demonstration will show you how you can easily start looking for anomalies in your environment and uncover luring threats on a very small budget. ***Michel Coene*** *(@coenemichel), Senior Information Security Consultant, NVISO* ***Maxim Deweerdt*** *(@AlfaSec), Cyber Analyst, Center for Cyber Security Belgium (CCB/CERT.BE)*
2:40-3:15pm	**Networking Break & Vendor Expo** (LOCATION: BLAINE KERN BALLROOM FOYER)
3:15-3:50pm	***Hunting on AWS*** While 'hunting' has come to mean targeted searches for IOCs, I always considered it operations that perturb the environment in order to illuminate adversary activity. For instance you might bounce a server and see if they try to reacquire. This was risky in a traditional datacenter, but the modern methodologies embraced at Netflix, such as microservices and Continuous Deployment, make it tractable. In this presentation I will explore tools and tactics that enable a broad range of hunting activities on Amazon Web Services (AWS). We will discuss how to leverage native AWS APIs and services, as well as supplement them with Open Source tools on the host, and navigate the 'shared responsibility model' to hunt in a large scale production environment. ***Alex Maestretti*** *(@maestretti), Engineering Manager, Netflix* ***Forest Monsen*** *(@forestm), Senior Security Response Engineer, Netflix*

Tuesday, April 18

3:50-4:25pm	***Hunting Webshells on Microsoft Exchange Server*** Microsoft Exchange Servers are a high value target, making investigation of them during Incident Response vital, but where do you start? What should you look for? Backdoor implants in the form of webshells hiding in OWA 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, through real world examples. It's easier than you might think, and these techniques can help up your DFIR game in environments containing Exchange Servers! ***Josh Bryant*** *(@FixTheExchange), Cybersecurity Architect, Microsoft*
4:25-5:00pm	***Toppling the Stack: Outlier Detection for Threat Hunters*** So much of what we do as hunters is based on finding oddballs, but most published hunt procedures seem to rely on a single method: stack counting. In this session, we'll examine a few other ways of finding outliers in your data, with samples and use cases for each. ***David J. Bianco*** *(@davidjbianco), Principal Engineer, Cyber Security, Target*
5:00-5:15pm	***Day 1 Wrap-Up***
5:15-6:15pm	**Networking Reception & Vendor Expo** (LOCATION: BLAINE KERN BALLROOM FOYER)

6:30-9:30pm	**Fulton Alley Night Out** Join us at Fulton Alley (www.fultonalley.com) for a fun Threat Hunting Summit night out. A five-minute walk from the hotel – approximately three blocks away – Fulton Alley offers bowling, bocce ball, board games and other non-electric games. Perfect for a fun, relaxing evening mingling with your fellow attendees. Fulton Alley will be closed to the public for this event so only THIR summit attendees will be in attendance. Bowling fees, food, and beverages are included. Location: Fulton Alley | 600 Fulton Street

Night Out is sponsored by

CARBON BLACK · ANOMALI™ · ENDGAME. · illusive®

cybereason · DOMAINTOOLS® · sqrrl Target. Hunt. Disrupt. · INFOARMOR® DETECTION IS THE NEW PREVENTION

cisco Cisco Umbrella · Recorded Future · 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.

@sansforensics **#ThreatHuntingSummit**

Wednesday, April 19

8:00-9:00am	**Registration & Coffee** (LOCATION: BLAINE KERN BALLROOM FOYER)
9:00-9:15am	***Day 2 Overview & Opening Remarks***
9:15-10:00am	***Sorry, But There Is No Magic Fairy Dust*** Every organization is desperately seeking solutions to the "inevitability of compromise." Despite increased investment in recent years, targeted attackers are still successful, and most organizations are struggling to keep up. Since so many practitioners still don't understand attackers and their methodologies, they're asking industry vendors to be the smart guys in the basement and sell them a magic bullet solution with secret-sauce-magic-fairy-dust that will make it go away. As threat hunters, we know there is no magic fairy dust, but we must stand up, cut through the FUD, and educate our organizations on the truth from the trenches. ***JJ Guy*** *(@jjguy), Senior Director & Founding Team, Carbon Black*
10:00-10:30am	**Networking Break & Vendor Expo** (LOCATION: BLAINE KERN BALLROOM FOYER)
10:30-11:05am	***ShimCache and AmCache enterprise-wide hunting, "evolving beyond grep"*** The presentation will focus around the open source release of a tool designed to efficiently process and analyse ShimCache and AmCache data at scale for enterprise-wide hunting purposes. The tool is designed as a framework with which to explore new analytics but will be released with some of our own custom-built analytics in it like: time execution correlation, Levenshtein distance analysis and time stacking to name a few. ***Matias Bevilacqua****, Senior Incident Response Consultant, Mandiant*
11:05-11:40am	***Deriving Successful Hunting Strategies with the Diamond Model*** Threat hunting is one of the most expensive and risky functions because in many cases hunters find little or nothing. A strong strategy underpins any successful hunt thereby increasing the chances of success and return on investment (ROI). The Diamond Model provides a foundation to all cyber threat analysis supporting incident response, threat intelligence, intrusion analysis, hunting, and other functions. Not really discussed before is the ability to derive threat hunting strategies from the Diamond Model. Using the Diamond Model to build a hunting strategy will ensure that the hunt is focused and properly aligned thereby increasing success. Sergio, the model's progenitor, will present the elements of a successful hunting strategy entails and how to use the Diamond Model to do this with examples. ***Sergio Caltagirone*** *(@cnoanalysis), Director, Threat Intelligence & Analytics, Dragos, Inc.*

Wednesday, April 19

11:40am – 12:15pm	***Taking Hunting to the Next Level: Hunting in Memory*** The vast majority of threat hunting takes place on easily visible and accessible system artifacts. These include log entries, network data, command line histories, persistence locations, and many other locations on a system or in the environment. Thanks to rule-based approaches and more advanced data analytics, it is relatively easy to detect outliers, surface suspicious artifacts, and discover anomalies on and across endpoints. Current hunt methodologies do a good job finding intrusions and reducing dwell times in many cases, but it still isn't good enough. Traditional hunting methods don't address one essential area: in memory-only attacks. Today's sophisticated adversaries are well aware of challenges in-memory only methods pose for defensive tools and methods (including threat hunting) and thus increasingly avoid disk during operations. It is generally not possible with today's tools to perform signature-less analysis of memory at the large scale necessary for effective hunting. Current memory analysis methods usually require collection of very large amounts of data and entail intensive analysis. Memory is largely a place for forensics as opposed to a datasource for real threat hunting at the speed and scale necessary for effective detection. We can do better. In this talk, we will describe both common and advanced stealth malware techniques which evade today's hunt tools and methodologies. Attendees will learn about adversary stealth and understand ways to detect some of these methods. Then, we will demonstrate and release a Powershell tool which will allow a hunter to automatically analyze memory across systems and rapidly highlight injected in-memory-only attacks across systems at scale. This will help move memory analysis from the domain of forensics to the domain of detection and hunting, allowing hunters to close the detection gap against in-memory threats, all without relying on without signatures. ***Jared Atkinson*** *(@jaredcatkinson), Defensive Services Technical Lead, Veris Group* ***Joe Desimone*** *(@dez_), Malware Researcher, Endgame*
12:15-1:30pm	**Lunch & Learn Sessions**

The Evolution of Ransomware

ANOMALI™

The percentage of ransomware attacks doubled during the period July to December 2016, to account for 10.5% of all recognized malware attacks during that time. Thus far, 2016 has brought with it increasingly high-profile examples, most notably, the case of Hollywood Presbyterian Medical Center, a 434-bed hospital whose network was frozen after hackers breached the system. After briefly relying on pen and paper records, Hollywood Presbyterian paid the 40 bitcoin ($17,000) ransom to regain control of its network. In this session we will provide a history and the evolution of ransomware, the future of this growing threat, and incorporate the psychological aspect and how to defend against it.

Presenter: ***Teddy Powers****, Solutions Engineer*

Location: Fulton, 2nd Floor

Enrich All the Things: The Future of Threat Hunting

DOMAINTOOLS®

In this session, you'll get an overview of how to take indicators from your network, including domain names and IP addresses, and connect them with nearly every domain on the internet. These connections enable your threat hunting efforts by providing you much-needed context on threat actors and their motivations.

Presenter: ***Mark Kendrick****, Director of Business Development, DomainTools*

Location: River Bend 1, 2nd Floor

Wednesday, April 19

12:15-1:30pm	**Lunch & Learn Sessions**

Turning the Tables: Engaging an Adversary with Deception

Rather than simply waiting for the inevitable data breach to occur, many organizations are taking a more aggressive approach to security in actively hunting for bad actors. This capability requires highly skilled talent combined with the use of threat intelligence, behavioral analytics and a number of security tools and know how to effectively hunt down. The goal of course is to identify, isolate, determine scope, and remediate the threats before the adversary makes it to sensitive data.

- What if you can actively engage the adversary and change the economics of an attack in your favor?
- What if using the attackers' own techniques can create a highly reliable way to identify the adversary?
- What if lateral movements and APT can become an opportunity for the defense instead of purely benefitting the attacker?

In our session, we explore how using deception to actively engage an adversary can do just that and how illusive can help hunters identify a threat before critical information is exfiltrated from the business.

Presenter: ***Chad Gasaway***

Location: River Bend 2, 2nd Floor

Threat Hunting With Marty

Threat hunting is critical to detection and prevention, but it's also challenging with the pure volume of data, human-driven review processes, complex attacker methods, and constantly evolving threats. Using Recorded Future, we'll explore hunting for threats in open source data, closed/vetted access criminal forums, and technical signatures. We will also share some of our current hunting procedures and results.

Presenters: ***Daniel Hatheway****, Senior Threat Intelligence Analyst, Recorded Future*
Levi Gundert*, Vice President of Intelligence and Strategy, Recorded Future*

Location: New Levee, 2nd Floor

1:30-1:45pm	***SANS Threat Hunting Survey Results*** The results of SANS' 2nd annual Threat Hunting Survey will be released in a two-part webcast on April 26th & April 27th, but Summit attendees will get an exclusive sneak peek at the results. Included will be data and feedback on the tools organizations are using for threat hunting; the top skills hunters need to succeed; and how threat hunting affects and is affected by security budgets. ***Rob Lee*** *(@robtlee), Lead – DFIR Curriculum, SANS Institute*

Wednesday, April 19

1:45-2:20pm	***The Mind of a Hunter: A Cognitive, Data-Driven Approach*** Security investigations are a mental labyrinth. There are countless paths that can be chosen, with each decision point influencing the decisions made later. Analysts are hopeful they choose the right path that leads to an accurate depiction of the events that occurred, but that doesn't always happen. Even when it does, sometimes it takes quite a bit of backtracking and wandering around before the analyst gets there. The conclusion is important, but so is the path. What makes an analyst choose a particular path? That's the question I've sought to answer with a data-driven approach, based in principles of cognitive psychology. In this presentation, I will present original research produced from case studies where I interacted with 50+ analysts while performing security investigations and hunting. By observing searches, pivots, aggregations and more in real investigations and simulations, I've gathered and summarized data that provides insight into the inner workings of the mind of an analyst. I'll discuss answers to questions like, "Is hunting really that different from an alert-driven investigation?", "Is PCAP always the best place to start an investigation?", "Is it harmful to pivot through too many data sources at once?," and "What data transformations usually led to the most success for providing hunting input?." You should walk away from this discussion with a greater understanding of your underlying cognitive process, and actionable ideas for improving your ability to find evil and stop bad guys in a timely manner. ***Chris Sanders*** *(@chrissanders88), Senior Analyst, FireEye*
2:20-2:55pm	***Framing Threat Hunting in the Enterprise*** There is a tendency to focus on the purely technical solutions to the problem of unknown attackers in our networks. This completely ignores the need to be able to justify the high cost of technical solutions and technical people. By wrapping a proper hunting framework around the technical expertise we can satisfy both the need to be technical proficient but also to generate the necessary support and communication to ensure the maturation of the hunting program and the growth of the organization as a whole. The introduction of the Threat Hunting Framework provides an evidence based methodology to ensure these goals. This talk will focus on how to take hunting that is being done in your environment and leveraging that for the growth of the org. Beyond the technical challenges of hunting, of which are many, there also lies organizational challenges surrounding how we approach hunting on a programmatic level. At the root of hunting lies cost to the organization which may hamper the growth and maturation of an organizations hunting efforts. This talk will address a systemic way to frame hunting within the organization that will enable technical staff to take the weekly activities of hunting and leverage that to promote maturation of the hunting program, the ability of an organization to further detect threats, and overall growth of an organization. ***Joseph Ten Eyck*** *(@joseph.teneyck), Lead Information Security Analyst, Target Corporation*
2:55-3:25pm	**Networking Break & Vendor Expo** (LOCATION: BLAINE KERN BALLROOM FOYER)

Wednesday, April 19

3:25-4:00pm	***Threat Hunting with Network Flow*** Advanced persistent threats often pass through standard network defense capabilities undetected, requiring significant manual analysis or specialized tools for detection. Many of these require full network packet capture, which is storage and processing intensive. Small record size and long storage time make network flow a great supplement to full packet capture. Furthermore, the ability to query on multiple fields in different combinations over a long period of time makes network flow much more flexible than signature matching tools. The focus of this presentation will be on how to incorporate network flow analysis into your threat hunting toolkit. We will cover topics such as anomaly discovery versus signature matching, IP expansion, longitudinal analysis of threat actors, how network flow relates to the Cyber Kill Chain, and where network flow analysis should sit in the threat hunting cycle. We will look at real world examples of the effects of these techniques in discovering malicious actors on networks. ***Austin Whisnant**, Member of the Technical Staff, Software Engineering Institute*
4:00-4:35pm	***Hunting: From Fudd to Terminators*** Haven't we always been hunting? Haven't we always been like Elmer Fudd, hunting for rabbits: sifting through data, unsure what we're looking for, yet knowing that buried in the abyss of data available to us something unknown lurks? Isn't that what we did in the 90s before we had log aggregation, IDS and SIEMs? Probably, yes. So why have we come back to this old idea of threat hunting and what about it makes it so attractive? In this talk I will run through our history as an industry, lay out the arguments for threat hunting and posit that we need to reframe our thinking about what such teams should do. I'll revisit an idea I presented last year around the lifecycle of incidents and threat hunting to suggest a model whereby these analysts should become exacting specialists in codifying research and doing test-driven development of new detection ideas. I will give examples of how this can work by observing how Google's security engineers approach their field. ***Heather Adkins**, Director of Information Security, Google*
4:35-4:45pm	***Closing Remarks*** ***Rob Lee** (@robtlee), Lead – DFIR Curriculum, SANS Institute*

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.

@sansforensics **#ThreatHuntingSummit**