SANS

SANS DFIR CYBER THREAT INTELLIGENCE Summit 2019

Program Guide

@sansforensics #CTISummit

Agenda

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

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

Sunday, January 20

5:00-8:00 pm

CTI 101: A Crash Course in Cyber Threat Intelligence Basics

New to the field of cyber threat intel? Eager to learn, but afraid that many of the Summit talks will go right over your head? Not sure of all the terminology and acronyms you've heard thrown around? The Summit advisory board will host a fun and interactive session on the eve of the Summit to bring you up to speed on key issues and trends. You'll also get a chance to ask all your questions in a more intimate setting, so you're primed for learning on Monday morning.

Featured topics include:

- ***Cyber Threat Intelligence: What is It? And Why Should You Care?***
  Robert M. Lee *(@RobertMLee), Summit Co-Chair*
- ***Effectively Communicating Threat Intel and Its Value***
  Rick Holland *(@rickhholland), Summit Co-Chair*
- ***Frameworks and Why We Use Them***
  Katie Nickels *(@likethecoins), ATT&CK Threat Intelligence Lead, The MITRE Corporation*
- ***Intelligence Consumption: Creating Threat Intelligence that Informs the Business***
  Kristen Dennesen*, Senior Manager – Cyber Threat Intelligence, Sony Pictures Entertainment*
- ***Network Defense: Integrating Threat Intel, Incident Response, and Hunting***
  Kris McConkey *(@smoothimpact), Threat Intel Lead, PwC*
- ***Ask Us Anything – Q&A with the advisory board***

Monday, January 21

7:00-9:00 am

Registration & Coffee (LOCATION: BALLROOM PRE-FUNCTION)

9:00-9:15 am

Welcome & Opening Remarks

Rick Holland *(@rickhholland), Summit Co-Chair*

Robert M. Lee *(@RobertMLee), Summit Co-Chair*

9:15-10:00 am

Keynote: Privacy vs. Security: It's a Log Story

Privacy and security are often lumped together as one subject with similar objectives. But as many security professionals know, these two subjects are often in tension with one another. This keynote will dig to the root of these tensions through an examination of logging practices to explore how privacy and security objectives operate in this new GDPR landscape. It will also provide practical, workable solutions to help lumber toward a better balance in your organization.

Whitney B. Merrill *(@wbm312), Hacker & Privacy Attorney, Electronic Arts (EA)*

10:00-10:30 am

Networking Break (LOCATION: BALLROOM PRE-FUNCTION)

Monday, January 21

10:30-11:00 am

Analytic Tradecraft in the Real World

Cyber threat intelligence is built on a traditional intelligence framework. Often, information security focuses on scientific concepts that entail a systematic approach that uses observable, testable, and repeatable data. However, understanding the application of traditional intelligence tradecraft and the value beyond collecting IOCs provides a foundation for a more robust, proactive response to threats. This presentation will highlight 10 analytic tradecraft skills derived from the CIA's Directorate of Intelligence and will show how these skills relate to real-world scenarios.

***Amy R. Bejtlich**, Cyber Threat Analyst, Dragos*

11:00-11:05 am

Q&A

11:05-11:35 am

Happy Hunting! Lessons in CTI Psychology from TV's Favorite Serial Killer

How often do you think about your thinking? Do you have internal discussions before coming to conclusions? What drives you to find answers and solve CTI mysteries? Explore metacognition, the science of thinking about your thinking, and how your bias, ulterior motives, and other psychological factors improve or destroy your threat intelligence products. Using her experience as a foreign language and intelligence analyst in the U.S. Army, NSA, and civilian sector, Charity Wright presents on the psychology of Cyber Threat Intelligence analysis. Lessons learned are gleaned from Dexter Morgan, TV's favorite serial killer and analyst and explores what it means to get inside the "bad guy's" head.

***Charity Wright**, Cyber Threat Intelligence Fusion Analyst, Ernst & Young Global*

11:35-11:40 am

Q&A

11:40 am – 12:10 pm

ATT&CK™ Your CTI with Lessons Learned from Four Years in the Trenches

As a community, we struggle with how to make threat intelligence actionable. We fall back to indicators of compromise because they're easy to apply to defenses, but we know we need to track adversary behavior to make our defenses less fragile. MITRE ATT&CK can help. The presenters will explain how you can use ATT&CK to classify adversary behavior and apply that intel to your defenses – and then provide the data to ensure that this process really works. This presentation will start by explaining how you can use ATT&CK to organize the threat intelligence you're already collecting. The presenters will walk through examples of how to "extract" ATT&CK techniques from your data, and then suggest ideas for how you can use that intel to prioritize defenses in your organization. Next, the presenters will take the theoretical process and make it real. They will provide an exclusive first look at a rich multi-year data set of confirmed threats based on ATT&CK-mapped detection criteria. The presenters will give an overview of the methodology (including bias and limitations), then discuss what they learned from the data. Topics covered include the top techniques observed, key technique trends, and how to improve your hunting and detection based on those observations. Attendees will learn how to shift their thinking about threat intel toward tracking behavior and gain perspective on where they should prioritize their detections based on threat intel from years of confirmed threats. Analysts will learn how to structure original reporting in the form of ATT&CK techniques to increase the effectiveness and usability of the products they create for defenders.

***Brian Beyer**, CEO & Co-Founder, Red Canary*

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

12:10-12:15 pm

Q&A

Monday, January 21

12:15-1:30 pm

Lunch & Learn Sessions

The Intelligence Driven Response Process (LOCATION: STUDIO A)

Many people are taking advantage of threat intelligence today to help generate alerts, but may not have the processes in place to know how it complements the IR process. This talk will provide education and strategies on how users can apply threat intelligence to drive incident response processes in their own environment. By leveraging the Intelligence Cycle, organizations can implement an effective use of intelligence capabilities. The use of F3EAD and OODA can allow your organization to support incident response and make quick decisions to mitigate risks.

Teddy Powers*, Senior Cybersecurity Architect*

Overcoming Vulnerability Overload. Using Predictive Prioritization to Effectively Protect Your Business. (LOCATION: STUDIO B)

Overcoming the problem of vulnerability overload is critical to reducing cyber risk. In this session you'll learn how predictive prioritization of vulnerabilities will improve your vulnerability management efforts to reduce risk and close your Cyber Exposure gap.

By attending you will learn:

- How to move the most dangerous vulnerabilities up your priority list using threat intelligence
- The resources required to effectively assess your environment and prioritize your efforts
- Practices that help ensure the results of your vulnerability assessments will allow you to take appropriate actions to make your organization more secure.

Al Ring*, Territory Manager, Tenable*

Threat Intelligence Workshop (LOCATION: STUDIO D)

In this workshop we will present practical ways to build your own threat intelligence, enrich your investigations, and walk through some hands-on practice profiling adversary infrastructure.

Corin Imai, *Senior Security Advisor*

1:30-2:00 pm

Language and Culture in Threat Intelligence

Language serves as the required medium for every form of communication, whether it be via email, a phone call, or face-to-face conversation. For its part, Cyber threat intelligence (CTI) is the study of adversaries and their approaches to the compromise and disruption of communications infrastructure. As such, language and associated cultures have an incredible influence on CTI. Cultural and linguistic knowledge of potential and actual adversarial regions shape the way an analyst must shape a CTI program or engagement. Using his background in Chinese threat intelligence paired with fluency in Mandarin Chinese and a continuing academic background concerning Chinese history, politics, and culture, Mitchell Edwards will highlight the role that the Chinese language and culture has in the unique Chinese threat. Using China as a case study, the presentation will highlight the importance of studying the culture and history of potential and actual adversarial regions, as well as the importance of native fluency in threat intelligence programs and engagements targeting these areas.

Mitchell Edwards *(@Viking_Sec), Virtual Operations Specialist, CrowdStrike*

Monday, January 21

2:00-2:05 pm	***Q&A***
2:05-2:35 pm	***Meet Me in the Middle: Threat Indications and Warning in Principle and Practice*** Discussions on threat intelligence often get bogged down between "machine speed" ingestion of atomic indicators and in-depth analysis of activity taking weeks (or months) to produce. Left in the cold in such debates is a very important but seldom considered middle ground: time-sensitive and incomplete but enriched threat intelligence. In the U.S. Navy and similar services, this is referred to as threat "indications and warning" (I&W) – a step beyond a simple observable refined to ensure accuracy and timely receipt. The goal of I&W is to get actionable, important information to those in need of it most as quickly, efficiently, and accurately as possible, even if as a result some context or other insights are lost. As a result of this activity, consumers are better armed and equipped to deal with and counter threats as they emerge, rather than either reacting to items with no context whatsoever or only reading about their challenges weeks after the fact in a complete intelligence report. This discussion will explore the concept of threat I&W within the context of network security generally and threat intelligence specifically to identify this topic as a shamefully ignored middle ground between extremes. The presentation will explore the conceptual background behind this idea, then transition to real-life examples of I&W drawn from the speaker's past activity in threat intelligence, incident response, and military operations. Attendees will walk away with two key lessons: first, do not let "perfect" (finished, complete intelligence) be the enemy of the "good" (actionable, if incomplete, information) when it comes to network defense; second, network defense consists of multiple phases of activity, from tactical to strategic, but ignoring the spaces "in between" results in fractured and incomplete operations. As a result of this discussion, attendees will be better armed and equipped to ask critical questions of their threat intelligence providers and have an enhanced set of expectations for what threat intelligence can do to support defensive operations. ***Joe Slowik*** *(@jfslowik), Principal Adversary Hunter, Dragos Inc.*
2:35-2:40 pm	***Q&A***
2:40-3:10 pm	***Unsolved Mysteries – Revisiting the APT Cold Case Files*** No matter how fascinating the advanced persistent threats (APTs) we discover, we often find that there's never enough time for adequate study. The next blog release is forthcoming…a deadline is missed…resources must be diverted elsewhere. In the process of chasing the PR high, we often find that intriguing questions fall through the cracks and certain mysteries are left unsolved. Moreover, at no fault of the analysts, it turns out some of these mystery cases were ahead of their time – a time when we lacked the technology to dig deeper, span wider datasets, and understand the nature of the threat at hand. Let's correct this. While vendors continue to race one another for the next hot thing, let's instead take pause and revisit the cold cases and the unsolved mysteries. Let's find ways to hunt, cluster, and perhaps even attribute yesterday's rarest intrusion sets. In the process of leveraging these to find our culprits, we'll learn to value the techniques and solutions developed over the past half-decade of private sector APT hunting. ***Juan Andres Guerrero-Saade*** *(@juanandres_gs), Researcher, Chronicle Security*
3:10-3:15 pm	***Q&A***
3:15-3:45 pm	**Networking Break & Vendor Expo** (LOCATION: BALLROOM PRE-FUNCTION)

Monday, January 21

3:45-4:15 pm

A Brief History of Attribution Mistakes

This presentation will examine the analytic mistakes the infosec community has made over the past ten years when attributing nation-state cyber attacks. We will contrast successful and failed attempts at attribution to identify the root causes of failures. The talk will cover basic logical fallacies (eg, mirror imaging and cherry picking) and briefly explain pivoting pitfalls when observing TTPs like dynamic DNS sites or tor exit nodes. Lastly, we'll explore historic examples of attribution mistakes and identify unexpected sources of those failures.

Sarah Jones *(@sj94356), Principal Analyst, FireEye*

4:15-4:20 pm

Q&A

4:20-4:50 pm

Quality Over Quantity: Determining Your CTI Detection Efficacy

You've collected a lot of indicators of compromise, but is your cyber threat intelligence (CTI) process serving you well? Quantity alone doesn't tell the whole story. What kinds of intel are you collecting and how useful is it for identifying incidents? What are your strongest areas and where are your gaps? Do you know enough about your priority threats to feel confident in your detection? These are hard questions to answer, and there's little existing guidance for answering them. Using models such as the MITRE ATT&CK framework and the Pyramid of Pain, attendees will learn analysis and visualization techniques to help them evaluate the quality of their collected CTI information, not just it's quantity.

David J. Bianco *(@DavidJBianco), Principal Engineer – Cybersecurity, Target Corporation*

4:50-4:55 pm

Q&A

6:00-8:00 pm

Summit Night Out (LOCATION: THE HIGHLINE RXR – 2010 CRYSTAL DRIVE – ARLINGTON, VA 22202)

We're all heading out to The Highline RxR, an upscale beer hall located at 2010 Crystal Drive, for complimentary food and drinks, networking and fun. It's an easy 10-minute walk.

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, January 22

8:00-9:00 am	**Registration & Coffee** (LOCATION: BALLROOM PRE-FUNCTION)
9:00-10:00 am	***Keynote: Applying WWII-Era Analytic Techniques to CTI*** In World War II, Sherman Kent developed much of the analytic process that led to the planning of the Allied invasion of North Africa. Later, Kent codified his analysis methodologies into a set of tenets known today as "Kent's Analytic Doctrine." Principles of his doctrine are still used today by the US intelligence community and by intelligence agencies worldwide. Many cyber threat intelligence (CTI) professionals lack formal intelligence training and try to reinvent the wheel. Even among those with formal intelligence training, many find Kent's Analytic Doctrine difficult to apply to cyber threats. In this session, you'll learn the nine tenets of Kent's Analytic Doctrine and how to successfully apply them to CTI. You'll be armed with actionable takeaways that you can use to up your intelligence game and make better, more consistent, and more reliable CTI assessments. ***Jake Williams*** *(@malwarejake), Principal Consultant, Rendition Infosec; Senior Instructor, SANS Institute*
10:00-10:30 am	**Networking Break** (LOCATION: BALLROOM PRE-FUNCTION)
10:30-11:00 am	***BEC Revisited: Dropping By on Our Favorite Prince*** Two years ago, at this very Summit, we had a discussion about one of the world's most successful email scams. Since that time, the attackers have grown a little smarter but a lot richer; and they show no signs of stopping. This talk will examine how the attacks and techniques have changed over the past few years – and how these changes have impacted intelligence gathering and response. But attackers don't deserve all of my stage time. We will also discuss how a community of CTI warriors has emerged from these types of attacks, and the coordinated global effort to lay these scams to rest. ***Matt Bromiley*** *(@mbromileyDFIR), Certified Instructor, SANS Institute; Principal Incident Response Consultant, Cylance*
11:00-11:05 am	***Q&A***
11:05-11:35 am	***How to Get Promoted: Developing Metrics to Show How Threat Intel Works*** Many organizations have operationalized threat intelligence as part of a well-rounded security program, but we often struggle to show the return on investment. This talk will focus on developing measures of effectiveness whether your program is just getting started or is pretty well established, independent of what tools or vendors you use. Based on multiple surveys of threat intelligence practitioners, directors, and cybersecurity decision-makers, the presentation will show where the disconnects are between those roles and how to focus on those metrics that are most useful when explaining the value of threat intelligence to decision-makers in your organization. ***Marika Chauvin****, Senior Threat Intelligence Researcher, ThreatConnect* ***Toni Gidwani*** *(@t_gidwani), Director of Research, ThreatConnect*

Tuesday, January 22

11:35-11:40 am	***Q&A***
11:40 am – 12:10 pm	***Schroedinger's Backslash: Tracking the Chinese APT Goblin Panda with RTF Metadata*** The APT Group Goblin Panda (aka, Conimes and China 1937CN Team) is an active threat to government and diplomatic organizations in the Asia-Pacific region, specifically in nations located along the South China Sea. This threat, which is thought to be aligned with the Chinese state and its espionage interests in the region, most commonly targets Vietnam, Malaysia, the Philippines, Indonesia, and India, utilizing historic exploits like CVE-2012-0158 delivered via phishing attachments. This presentation seeks to demonstrate through the examination of metadata in Goblin Panda CVE-2012-0158 RTF phishing lures that a single phishing builder has been in continuous use by the group since 2010. Despite having undergone at least one major overhaul, the phishing builder creates unique RTF Tags within the phishing lures that analysts can leverage to correlate campaigns across diverse targets in different geographic regions. This presentation will demonstrate the geographic areas targeted by Goblin Panda, the varying nature of targeted victims (government, military, diplomatic, civil society/dissidents), and the evolution of the phishing builder from 2010 through 2018. ***Michael Raggi*** *(@aRtAGGI), Senior Cyber Intelligence Analyst, Anomali*
12:10-12:15 pm	***Q&A***
12:15-1:30 pm	**Vendor Expo Lunch** (LOCATION: BALLROOM PRE-FUNCTION)
1:30-2:00 pm	***Cloudy with Low Confidence of Threat Intelligence: How to Use and Create Threat Intelligence in an Office 365 World*** Everyone is moving to the cloud, specifically Microsoft Cloud. Microsoft expects to have 66 percent of its Office business customers in the cloud by 2019. Doing so makes sense: it's easier than having on-premises mail servers, it (theoretically) reduces costs, and Microsoft Office 365 has one of the best security teams in the world. However, there is a downside, which is that it's hard to protect what you can't see or access. As of today, it is extremely difficult (or impossible, depending on your subscription level) to apply your externally created threat intelligence into Microsoft Office 365 detections. It is even more frustrating to try and search for known indicators on a platform that is not designed to help the security community. This talk will describe methods and release open-source code to enhance your Office 365 security by analyzing email metadata, attachments, and even full content with tools like stoQ or LaikaBOSS and by looking at how to use that information to research and create actionable threat intelligence via platforms like Splunk. ***Dave Herrald*** *(@daveherrald), Staff Security Strategist, Splunk* ***Ryan Kovar*** *(@meansec), Principal Security Strategist, Splunk*
2:00-2:05 pm	***Q&A***

Tuesday, January 22

2:05-2:35 pm	숨은 영웅 ***– Hidden Heroes and Other Gangsters from 39 North*** 숨은 영웅 – Hidden Heroes, and Other Gangsters from 39 North is an illumination of the Democratic People's Republic of Korea's (DPRK) military and civilian cyber Order of Battle. The talk will examine the infamous and frequently misattributed Unit 121 and provide an expanded understanding of the many operational and active cyber-capable units within the DPRK's Reconnaissance General Bureau and Korea Workers Party. We will also look at the historical path of those entities, from more traditional criminal activity to revenue generation in the world of cyber fraud. Finally, the talk will also examine the pitfalls of researching DPRK activity due to South Korean intelligence activities, the far-reaching aspects of the Korean diaspora, and signals that often allow DPRK actors to blend in with non-DPRK actors. ***Tom Creedon*** *(@n300trg), Senior Managing Director – Asia Pacific, LookingGlass*
2:35-2:40 pm	***Q&A***
2:40-3:00 pm	**Networking Break & Vendor Expo** (LOCATION: BALLROOM PRE-FUNCTION)
3:00-3:30 pm	***Untying the Anchor: Countering Unconscious Bias in Threat Intelligence Analysis*** Bias is an unavoidable facet of an analyst's life, but it is something that good analysis techniques can help to remedy. Anchoring is just one of the many forms of bias that with which an analyst must grapple. Anchoring involves focusing on a piece of information to the exclusion of others, and it can cause analysts to stop looking further or to disregard otherwise relevant information. To avoid this common dilemma, the PricewaterhouseCoopers LLP team has looked at ways that to untie this anchor in everyday analysis and view the vast sea of data from a fresh perspective. This talk will cover how the team has applied traditional intelligence techniques into its ways of working, including introducing "surges" and how these have helped challenge the team's assessments. A case study will be presented that shows how a variety of different analysis techniques have been applied to avoid bias, as well as the lessons learned from their application. This talk will not only provide attendees with practical examples of analytical techniques in action and how they can refocus threat actor attribution, but will also explore how recognizing bias can support threat intelligence being used effectively by security teams. ***Rachel Mullan*** *(@jadedmuse), Strategic Threat Intelligence Lead, PricewaterhouseCoopers LLP* ***Jason Smart****, Technical Threat Intelligence Lead, PricewaterhouseCoopers LLP*
3:30-3:35 pm	***Q&A***
3:35-4:45 pm	***Cyber Threat Intel Unplugged*** After two days of practitioner talks with actionable lessons, you should be fired up and feeling pretty smart about analyzing your intel. Here's your chance to take the stage for a 5-minute talk of your own. Share a current project, a problem you'd like advice on, your top takeaway from the Summit and how you plan to implement it; anything goes! The camera will be turned off and slides are not required, so give it a go.
4:45-4:50 pm	***Q&A***

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.