CYBER THREAT INTELLIGENCE

SUMMIT & TRAINING

Program Guide

@sansforensics #CTISummit

Agenda

All Summit Sessions will be held in the Regency EF Ballroom (unless noted otherwise).
All approved presentations will be available online following the Summit at ***sans.org/summit-archives***

Sunday, January 19

5:00-7:00 pm

Bonus Sunday Night Workshop – CTI Answer & Question Night (LOCATION: KENNEDY/JEFFERSON)

Whether you're brand-new to CTI or an experienced intel analyst, you're not in jeopardy of missing out on anything! Join us for the SANS CTI Summit version of everyone's favorite answer-and-question game, hosted by our very own Alex TRebekah Brown and featuring some very special contestants, including David J. "Pyramid of Pain" Bianco and Sergio "Diamond Model" Caltagirone. This workshop is optional, and is included in your Summit registration.

Sponsored by:

CYBER THREAT ALLIANCE

Monday, January 20

7:00-9:00 am

Registration & Coffee (LOCATION: REGENCY FOYER)

9:00-9:15 am

Welcome & Opening Remarks

Rebekah Brown *@PDXBek*

Rick Holland *@rickhholland*

Katie Nickels *@likethecoins*

9:15-10:00 am

Keynote: Secret Squirrels and Flashlights: Legal Risks and Threat Intelligence

As threat intelligence matures into a more traditional security discipline and companies seek to better protect customers through threat intel products and services, there are growing pains. Often, those pains come when the freedom of the analyst intersects with the law, corporate promises, or contracts. In this talk, we'll explore those boundaries, and discuss strategies to help threat intelligence analysts identify and manage legal risks while hunting, investigating, and responding. Hear from Microsoft's lead attorney for the Microsoft Threat Intelligence Center and long-standing counsel to the Microsoft Security Response Center on how to leverage your lawyers as a part of a threat intelligence team. We will also consider legal consequences in information sharing, incident response, working with third parties, government engagements, and technology choices.

Cristin Flynn Goodwin *@cristingoodwin, Assistant General Counsel for Customer Security and Trust, Microsoft*

10:05-10:40 am

The Threat Intelligence EASY Button

If you build, manage, or provide threat intelligence services, this presentation was created with you in mind. Chris Cochran has spent over a decade building numerous threat intelligence capabilities for various organizations, including Netflix. He has designed a simple touchstone for teams of all skill levels that are looking to improve their threat operations. His four-point model is as follows: Elicit Requirements, Assess Collection Plan and Strive for Impact, and Yield to Feedback. In this presentation, Chris will discuss why these are his pillars of practice and what has gone right while building out his programs, as well as what has gone terribly wrong. Attendees will leave with a powerful model to leverage and execute impactful threat intelligence missions.

Chris Cochran *@chriscochrcyber, Threat Intelligence and Operations Lead, Netflix*

10:40-11:10 am

Networking Break (LOCATION: REGENCY FOYER)

Monday, January 20

11:15-11:50 am

Mexico Under Siege: A Look at Threat Activity South of the Border

Mexico is often overlooked when it comes to all things "cyber," as most security issues there making headlines seem related to drug trafficking and illegal immigration. However, Mexico exports its share of cyber-crime tech and techniques, and it is an attractive (and lucrative) sandbox for groups crafting sophisticated attacks targeted mostly against financial institutions. The scale of the attacks and the evolution of the threat actors make Mexico an interesting case study because many of the attacks there of late could well be reproduced in the United States. Attacks covered in this presentation include BANCOMEXT, the attack against SWIFT that almost resulted in the theft of $10 million; and attacks against multiple banks connected to the centralized payment system operated by the Central Bank of Mexico. We'll explain how attacks were executed and how the connection between cyber threat actors and organized crime works; review the TTPs and artifacts used by the threat actors behind the centralized payment system attack, as well as those used to exploit an industry-leading transaction processing switch; and how developing time-critical, in-house threat intelligence capabilities against a zero-day attack resulted in the successful anticipation of the next wave of attacks. We'll look at the current state of affairs in Mexico, lessons learned from previous attacks, what is being done in terms of CTI, and how Mexico's central government lacks a cybersecurity strategy and how that could affect the United States.

Matt Bromiley *@_bromiley, Principal Consultant, FireEye Managed Defense; Certified Instructor, SANS Institute*

Enrique Vaamonde *@_ejvm, Co-Founder, Tekium*

11:55 am – 12:30 pm

Threat Intelligence and the Limits of Malware Analysis

Threat intelligence is guided (and limited) by the availability and nature of underlying data for analysis. As a result, threat intelligence reporting is shaped by the sources from which it emerges: incident data, fusion of multiple sources, and technical analysis. One of the most frequently produced threat intelligence reports consists of malware analysis and conclusions (or assumptions) drawn from technical functionality. Yet, such analyses are limited to a narrow view of events that may not be accurate or relevant to broader operations. This presentation will examine how different views of event information – with an emphasis on malware analysis – influence and shape subsequent threat intelligence reporting. Overall, the goal is to demonstrate to consumers and practitioners the boundaries that specific technical analysis sometimes places on conclusions and subsequent decisions. By understanding specifically how technical malware analysis as a discipline contributes to overall threat intelligence functions – and its limitations, ranging from attribution to specific adversary tracking – threat intelligence consumers and practitioners can gain a more accurate understanding of its relevance to actual defensive operations.

Joe Slowik *@jfslowik, Principal Adversary Hunter, Dragos*

12:30-1:40 pm **Networking Lunch** (LOCATION: REGENCY FOYER)

Join your fellow attendees for a networking lunch as you relax between sessions. A special thanks to our Summit sponsors for hosting this event.

ANALYSTPLATFORM INTELLIGENT CYBER DEFENSE

ANOMALI®

CROWDSTRIKE

CYBER THREAT ALLIANCE

DOMAINTOOLS®

EclecticIQ

ThreatConnect™

THREATQUOTIENT

Monday, January 20

1:45-2:20 pm	***Automation: The Wonderful Wizard of CTI (Or Is It?)*** Is automation the wizard of Cyber Threat Intelligence (CTI)? Let's travel down the yellow brick road to find the answer! In the age of machine learning and artificial intelligence, it seems we're always searching for a way to automate and make our jobs easier. This is no different for CTI analysts. Admittedly, our desire to do less manual work and more CTI analysis motivates us to automate extraction of adversary behaviors by creating such tools as Threat Report ATT&CK Mapping (TRAM). In this presentation, we'll examine problems MITRE faced with backlogged reports, how its team uses TRAM to keep up with CTI, and why this type of automation, while important, can fall short if not accompanied by human analysis. We'll review MITRE's tool creation methodology, discuss challenges with automation, and look at why the wizard behind the curtain may just be an illusion. Finally, we'll demonstrate how anyone can download TRAM and use it to analyze multiple reports, extract MITRE ATT&CK techniques, and operationalize CTI in their organizations. Attendees will learn not just how to use the tool, but also ways in which automation can be an effective tool for CTI. ***Jackie Lasky**, Cyber Security Engineer, The MITRE Corporation* ***Sarah Yoder** @sarah_yoder, Cyber Security Engineer, The MITRE Corporation*
2:25-3:00 pm	***Hack the Reader: Writing Effective Threat Reports*** Drawing on best practices covered in his SEC402 course, Cybersecurity Writing: Hack the Reader, Lenny will break down strategies for compiling concise and compelling threat reports. ***Lenny Zeltser** @lennyzeltser, CISO, Axonius*
3:00-3:30 pm	**Networking Break** (LOCATION: REGENCY FOYER)
3:35-5:30 pm	***CTI Summit Analysis Workshop*** You've spent the day soaking up wisdom from awesome presentations, and now you'll have the chance to put your CTI analysis skills to the test! In an all-new hands-on team workshop, you'll be presented with a real-world-inspired scenario that will let you pivot through data while responding to your consumer's requirements and synthesizing what you learn into finished analysis. We'll introduce you to all the tools and concepts you need for the workshop, so no matter what your experience level, you'll be able to contribute to your team! If you'd like to participate, please bring a laptop (a virtual machine of any operating system is recommended if you want to make sure you don't accidentally click on adversary domains). ***Katie Nickels** @likethecoins, Summit Co-Chair, SANS Institute*
5:30-6:30 pm	***Networking Reception*** (LOCATION: REGENCY FOYER) Join Summit sponsors for drinks and networking before you settle in for movie night.
6:30-8:30 pm	***Summit Night In: Mystery CTI Theatre 2020*** (LOCATION: REGENCY FOYER) The weather outside may be frightful, but our viewing selections are delightful. Join us for some hyper-realistic cinematic representations of cybersecurity and threat intel on screen. As a bonus, you'll learn secret Hollywood tradecraft for identifying and taking down threat actors in 45 minutes or less. Snacks and drinks are on us. Audience participation is encouraged.

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 21

7:00-9:00 am	**Registration & Coffee** (LOCATION: REGENCY FOYER)
9:00-9:15 am	***Welcome & Opening Remarks*** ***Rebekah Brown*** *@PDXBek* ***Rick Holland*** *@rickhholland* ***Katie Nickels*** *@likethecoins*
9:15-10:00 am	***Keynote: Achieving Effective Attribution: A Case Study on ICS Threats with Perceived Iranian Motivations*** This presentation will cover an alternative method to achieving the value of true attribution without the analytical and resource cost associated with government attribution and the risks it carries. The talk will look at ICS threats and the current geopolitical tension with Iran as an example of what success can look like. ***Robert M. Lee*** *@robertmlee, Founder & CEO, Dragos; Senior Instructor, SANS Institute*
10:05-10:40 am	***Cyber Order of Battle: Revealing the Composition, Disposition, and Strength of MuddyWater*** Cyber Order of Battle (CYOB) is an adaption of traditional military intelligence's Order of Battle, which is an assessment tool used to analyze enemy capabilities for combat. CYOB builds on the traditional military framework to determine the hierarchical organization, command structure, strength, disposition of personnel, equipment of units, and formations of armed forces. In the case of CYOB, some of these issues are directly applicable, such as the disposition of personnel, while others have a specific cyber analogy, where strength and equipment may translate to capability as defined in the Diamond Model. CYOB provides analysts with forecasting abilities by determining a threat actor's intelligence cycle and linking it to geopolitical events that impact an actor's grand strategy. This presentation examines a CYOB assessment of the Iran-based threat actor commonly tracked as MuddyWater. Working with their central intelligence team out of the United Kingdom, PwC Netherlands has analyzed MuddyWater's operations since 2017, including examining the number of countries targeted and the amount of lures per country in a single period. In examining MuddyWater's OPSEC failures and overt objectives as an Iran-based threat actor, the analysis provide information about its command structure, disposition of personnel, composition, and capabilities. ***Curtis Hanson****, Senior Associate CTO-NL, PwC Netherlands* ***Konrad Ten Holter****, Senior Manager CTO-NL, PwC Netherlands*
10:40-11:10 am	**Networking Break** (LOCATION: REGENCY FOYER)

Tuesday, January 21

11:15-11:50 am

Every Breath You Take: A CTI Review of Stalkerware

A common misconception is that Cyber Threat Intelligence is just for Corporate America or governments. Let's challenge that assumption with a practical application of CTI to the issue of stalkerware. Security professionals might consider stalkerware a tool for overly-controlling partners or parents, but what if I told you there's more? Stalkerware presents a hostile actor with a (questionably) legal, commoditized, and easily consumable "software" that has many of the same features of backdoors and other malware we all fight to keep out of our environments, and what wrongdoer wouldn't take advantage of that? In fact, stalkerware has already been linked to nation-state governments spying on dissidents and journalists. As awareness continues to grow about stalkerware, it is only a matter of time before more people take it seriously. Malicious actors clearly are, and it is time that defenders respond seriously as well. In this talk, you'll get additional insights into stalkerware; what it is, how it works, who it targets, CTI hypotheses and suggested RFIs to other teams, and of course, no CTI review would be complete without a discussion of the various hostile actors that leverage stalkerware and their tradecraft. Takeaways include glimpses into the dark side of humanity and a report for your threat intelligence platform, as well as ideas of how security professionals can start to tackle this problem as a part of their CTI program.

Xena Olsen *@ch33r10, Cyber Threat Analyst, Financial Services Industry*

11:55 am – 12:30 pm

Collection Overload: Understanding and Managing Collection to Support Threat Intelligence Analysis

Fear of missing out when collecting information is very real. Traditional intelligence practitioners often assume that their goal is to gather as much information as possible to formulate a more comprehensive picture of threats, and this is a common problem in cyber threat intelligence as well. However, this approach can hamper the accuracy, timeliness, and relevancy of analysis. In truth, excessive collection will likely lead to information overload on both the individual and institutional levels that can result in skewed analysis and assessments. Unfettered and undermanaged intelligence collection of raw, exploited, and production data can affect both data-driven analysis and conceptually-driven analysis. It has been shown that an analyst only needs minimum information to make an informed judgement. Common issues deriving from collection overload include overconfidence (a result of circular reporting or having too many information sets to evaluate); reinforcement of collection bias; and unchecked collection, which may cause analytic paralysis that leads to a high noise-to-signal ratio that in turn results in indecision and an inability to conduct effective structured analysis. This presentation proposes best practices to mitigate such issues by producing a realistic collection management framework and sustainable intelligence requirements; starting with a minimal viable collection strategy; collecting what you need and growing it only as needed; conducting source review and evaluation; evaluating exploited and production data via a framework such as an admiralty system; and counting the times a source is used to enforce an assessment in order to uncover collection bias. Finally, we'll look at upgrading analysis models as the best way to improve analysis and mitigate issues deriving from over-collection.

Sherman Chu*, Cyber Intelligence Analyst, New York City Cyber Command*

Tuesday, January 21

12:30-1:40 pm	**Lunch**
	Lunch & Learn Session: ***One-Stop Shopping: Intel Enrichment and Integration*** (LOCATION: KENNEDY) We've all seen it – dozens of browser tabs open, each offering some insight into an observable you are investigating. Twitter feeds reporting the latest malware detections. Without a doubt, there is tremendous benefit in bringing more automation to your repeatable research processes. But not all external data sources are created equally. As platforms become more open, integration options are seemingly endless. I'll suggest a simple framework for evaluating the value in integrating with external enrichment sources. ***Thomas Graves**, Senior Sales Engineer, Anomali*
	Lunch & Learn Session: ***One-Stop Shopping: It's Not Just Play Books – Digging Deeper on Orchestration*** (LOCATION: JEFFERSON) Providing musicians with sheet music that is arranged for their specific instrument results in the entire orchestra playing together in harmony. Delivering cybersecurity information should follow a similar approach. This talk will present different approaches to orchestrating, automating and integrating both the technologies/security infrastructure and people/teams within companies that are too often siloed and disparate. Companies are struggling to adopt new approaches like the MITRE ATT&CK framework, which offers real world knowledge of TTP's, detection and mitigation. Orchestration has become as buzzy of a term as 'cyber' itself, but it's no longer just the play books many think of. We will explore the concept of intel teams delivering their "product" to these desperate groups, and leveraging the work that the domain experts in each group performs to capture further context, thereby creating an intelligence refinement loop through machine to machine communication. ***Chris Jacob** @TheChrisJacob, Global VP, Threat Intelligence Engineers, ThreatQuotient*
1:45-2:20 pm	***Strategic Takeaways: Forging Compelling Narratives with Cyber Threat Intelligence*** This presentation will cover the various cyber threat intelligence methods and techniques that can be used to deliver effective and strategic cyber threat reports and briefings to middle management, executives, and C-level officers in medium-size to large organizations. The presentation will cover preparation, determination of scope, story-telling, intelligence briefing styles (e.g., styles based on timelines, threats, industry, or geography), filtering the intelligence that matters, fusing risk information with threat intelligence, industrial control system threat intelligence considerations, and how to avoid common pitfalls with strategic intelligence briefings. ***Abdulrahman Alsuhaimi** @aasuh88, Cyber Threat Intelligence Analyst, Saudi Aramco*

Tuesday, January 21

2:25-3:00 pm	***Stop Tilting at Windmills: Three Key Lessons that CTI Teams Should Learn from the Past*** Since the publication of Mandiant's APT1 report in 2013, cyber threat intelligence (CTI) has been widely adopted by private organizations all over the world. There have been both successes and failures in trying to develop cyber threat capabilities and add value to businesses. As a community, it is critical to capture the relevant lessons learned from these experiences and conduct a status check on these first years of applied CTI. This presentation aims to identify areas where organizations should put more focus in order to stop tilting at windmills. We will deep dive into three major areas where most current CTI teams struggle: (1) intelligence direction (specifically, stakeholder identification and collection of intelligence requirements); (2) intelligence reporting and dissemination; and (3) the skills sets of CTI analysts. Takeaways for attendees will include recognizing the significance of requirements for the intelligence cycle; identifying key stakeholders; understanding how classic intelligence approaches can be applied to CTI production/reporting; learning from success stories on disseminating intelligence products and capturing feedback; understanding the variety of competencies of CTI teams; and improving ways to work within CTI teams comprised of analysts with different backgrounds and experience levels. ***Andreas Sfakianakis*** *@asfakian, Cyber Threat Intelligence Analyst*
3:00-3:30 pm	**Networking Break** (LOCATION: REGENCY FOYER)
3:35-4:10 pm	***The Importance of Cultural and Social Intelligence*** Far too often, threat intelligence professionals focus exclusively on intelligence elements that can be immediately put to use. Organizations do not exist in a vacuum and our adversaries all over the world represent a diverse set of cultural and social norms and motivations. To get a complete picture of the threat environment and provide additional context to threat intelligence, organizations should also strive to improve their understanding of the cultural and social underpinnings of attacker behaviors. This presentation will focus on certain examples along these lines, including understanding the Russian military culture under its current Chief of Staff General Valery Vasilyevich Gerasimov; the cultural and social pressures on adversaries in China that are driving their intelligence requirements; the concept of mirror imaging, that is, understanding why certain parties don't think like us; and cognitive biases and cultural intelligence. The goal is to examine cybersecurity and intelligence requirements outside of a technical realm and incorporate other models of analysis to enrich our understanding of the threat and better inform our risk assessments. ***Gerard Johansen****, CISSP, GCTI, Cisco Systems, Senior Incident Response Consultant*
4:15-4:50 pm	***CTI to Go: Your Takeaways and To Do List*** Hopefully after two days of talks, fortified by informal learning through networking with your peers, you're fired up to get back to the office and put these ideas to work. Rick will help you distill the key themes and advice from the Summit and organize them into manageable, actionable tasks that yield real results. ***Rick Holland*** *@rickhholland, Summit Co-Chair, 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 #CTISummit

FREE EVENT

SANS Cyber Threat Intelligence Solutions Forum

When: **Friday, March 27, 2020** | **8:30AM - 12:30PM** | Location: **Washington, D.C.**

Chairman
Robert M. Lee

The SANS Cyber Threat Intelligence (CTI) Solutions Forum will showcase the latest CTI tools and techniques and how organizations can leverage different types of CTI to meet their needs. Attend this free event with SANS certified instructor Robert M. Lee and guest speakers to learn how you can get the most out of CTI.

Earn 4 CPE Credit hours for attending. Networking lunch to follow after the forum.

Free to cybersecurity professionals with discount code
CTIForum2020

Reserve Your Seat: http://www.sans.org/u/YRI

NOTES