SANS

SANS DFIR CYBER THREAT INTELLIGENCE SUMMIT

Program Guide

@sansforensics  #CTISummit

Agenda

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

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

Monday, January 29

8:45-9:00 am	***Welcome and Introductions*** *Rick Holland (@rickhholland), Summit Co-Chair, SANS Institute* *Robert M. Lee (@RobertMLee), CEO, Dragos Inc.; Summit Co-Chair, Author, Certified Instructor, SANS Institute*
9:00-10:00 am	***Keynote: Survival Heuristics: My Favorite Techniques for Avoiding Intelligence Traps*** In a 32-year plus career in the Intelligence Community, Carmen Medina made many different types of intelligence mistakes and suffered the consequences of faulty thinking. But along the way she learned a thing or two, and she is now eager to share these learnings with other intelligence professionals. In an entertaining and practical talk, she will share her favorite shortcuts and intelligence process hacks to help analysts think better and communicate their findings more effectively to their clients. *Carmen Medina, Retired, CIA; Author, Rebels At Work: A Handbook for Leading Change from Within*
10:00-10:30 am	**Networking Break** (LOCATION: REGENCY FOYER)
10:30-11:05 am	***There Is MOAR To Structured Analytic Techniques Than Just ACH!*** As private sector intelligence capabilities and tradecraft continue to evolve, structured analytic techniques are being incorporated into intelligence programs. Analysis of competing hypotheses (ACH) is perhaps the most featured structured analytic technique in use today. ACH is most effective when looking back an event; it is not as useful for forecasting future events. Structured analytic techniques constitute a toolbox, and you need to pick the right tool for the job. This talk will highlight additional structured analytic techniques that can be leveraged to reduce uncertainty within intelligence analysis. Structured analytic techniques such as quadrants and the cone of plausibility will be broken down to align with tactical, operational, and strategic assessment needs. Attendees will leave with an understanding of which structured analytic techniques are best applied to specific scenarios within their organizations. *Rick Holland (@rickhholland), Summit Co-Chair, SANS Institute*
11:05-11:40 am	***I Can Haz Requirements?: Requirements and Cyber Threat Intelligence Program Success*** The hype around cyber threat intelligence (CTI) programs of both corporate and security companies tends to minimize the importance of the first stage of the intelligence process: the creation of requirements. Without clearly defined intelligence requirements, CTI programs can quickly flounder, without clear direction to drive such critical areas as vendor procurement and intelligence collection management, among others This talk will examine the practical application of traditional intelligence requirement management from the defense/intelligence community to private sector organizations. This includes providing the tools to successfully create, establish, and re-examine intelligence requirements that ultimately fill intelligence gaps, drive successful intelligence collection, and supply timely and relevant production of intelligence to customers and stakeholders. *Michael Rea (@ComradeCookie), Senior Security Researcher, McAfee*

Monday, January 29

11:40 am – 12:15 pm

Intelligence Preparation of the Cyber Environment

This talk will examine Intelligence Preparation for the Battlefield and for the Environment (IPB/IPE) for the cyber domain. We will look at the conventional intelligence methodologies and use our findings to answer key questions for Intelligence Preparation of the Cyber Environment (IPCE): What do I look like to my attackers, what do my attackers look like to me, how are we likely to "do battle," and thus how can I better prepare for it? The talk will provide an overview of how the conventional methodology is applied to the cyber environment and, ultimately, how it applies to the organizations of attendees themselves. We'll look at how to collect information on the attackers, how to understand your own environment, and how to visualize a likely attack and prepare for it.

Rob Dartnall (@cyberfusionteam), Director of Intelligence, Security Alliance Ltd.

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

The Importance of Your ISAC Membership and Getting Industry Relevant Intel and How Manage That Intel (LOCATION: JUDICIARY SUITE)

ANOMALI®

This session will be about the importance of being an ISAC member as it relates to intelligence. The topic covered will go into why organizations should take advantage of their ISAC both as a receiver and a contributor. Once you take the step of joining an ISAC, how to manage the intelligence they are providing you with and making use of it in an efficient manner with the goal of better awareness in mind.

***Teddy Powers**, Sr Security Engineer*

Closing the Loop: How does feedback improve CTI? (LOCATION: OLD GEORGETOWN)

NC4®

How does internally generated sensor feedback in the form of "Sighting" improve externally source CTI (Cyber Threat Intelligence)? In this presentation, we will:

- Briefly outline the purpose and power of Sighting as a STIX and CybOX construct
- Demonstrate a sensor generating a Sighting based on a Rule/Policy auto-generated from external CTI
- Outline how feedback can improve fidelity and effectiveness of an external sourced CTI, making it a more relevant/target to your real-world threats
- Show how Sightings (feedback) can add weight/score to intelligence making it more relevant to your threats in a dynamic/automated approach
- Conclude with strategies for doing this in your environment

***Michael Pepin**, Sr. Security Engineer*

2018 DNS Resolutions: Be More Proactive (LOCATION: CABINET SUITE)

DOMAINTOOLS®

Attackers borrow IP addresses, but they control domains. Learning to assess those domain names reveal intent. Unlock the power of identifying underlying domain names and using them to pivot in a way that gives you the upper hand during an investigation or response. DomainTools Sales Engineer Taylor Wilkes-Pierce as he explores using domain names and DNS information. He'll deep-dive into one of 2017's most notorious phishing attacks to show you how to use domain data and pivoting to profile threat actors and prevent future attacks.

***Taylor Wilkes-Pierce**, Sales Engineer*

Monday, January 29

1:30-2:05 pm	***Event Threat Assessments: G20 as a Case Study for Using Strategic Cyber Threat Intelligence to Improve Security*** Large events pose unique cyber risks to organizations that have employees attending them. As the technology and threat landscape evolves, organizations need to understand the full extent of the cyber risks to which their personnel are exposed while attending such events. This presentation will use the G20 meetings as a case study to see how strategic cyber threat intelligence (CTI) illuminated the threat landscape for the organization's attendees, used timeline analysis to come to surprising conclusions, and utilized Analysis of Competing Hypotheses (ACH) to evaluate adversary courses of action. This information allowed the organization to implement custom-tailored security guidance to improve security. In covering everything from intelligence requirements to product dissemination, the presentation will walk the audience through the story of how a cyber intelligence analyst used available intelligence resources and service providers to collect information, drew on internal resources to conduct analysis, and then partnered with the organization's risk professionals to disseminate security guidance to event attendees. Attendees will see an example of an intelligence "success" that can be modeled and replicated, as well as learn about the cyber threats facing G20 meeting attendees and, ultimately, all of us. *Lincoln Kaffenberger (@LincolnKberger), Threat Intelligence Officer, International Monetary Fund*
2:05-2:40 pm	***Hunting Hidden Empires with TLS-Certified Hypotheses*** The "threat hunting" landscape has drastically changed due to the increase in encrypted transport layer security (TLS) Internet traffic. The days of adversaries registering domains with their given names are gone, and malicious actors increasingly use malware that takes advantage of TLS encryption to hide their tracks. Yet, even in this brave new world of altered tactics, techniques, and procedures, adversaries leave clues that can expose their infrastructure. To find these clues, however, blue teams need to learn some new tricks. This talk focuses on expanding on techniques that have been researched and presented at various conferences by Mark Parsons, and specifically on his methods for using TLS certificates to find malicious malware infrastructure. We will build on Parsons' body of work and show how his approach to malware certificate hunting can be expanded to detect instances of PowerShell Empire servers that have self-generated SSL certifications on port 443 and 8080. These certificates have a unique fingerprint that can be detected by leveraging tools like zmap/zgrep, python, and statistics/machine learning. The results of this research will show how network defenders can find previously unknown instances of malicious infrastructure communicating with their network and prevent them in the future. Finally, we will discuss our creation of hypotheses, codes and techniques, and methods of validation for verification. We'll then release our tools and methodologies for use by the community to explore other potential "hidden empires" of malware. *Dave Herrald (@daveherrald), Staff Security Strategist, Splunk* *Ryan Kovar (@meansec) (@splunk), Senior Security Architect, Splunk*
2:40-3:10 pm	**Networking Break** (LOCATION: REGENCY FOYER)

Monday, January 29

3:10-3:45 pm	***Intelligent Hunting: Using Threat Intelligence to Guide Your Hunts*** More modern organizations are now developing and maintaining threat intelligence functions to improve their defensive posture. However, for many organizations, implementation of detection methods is still limited to low levels of the "pyramid of pain." The end result is that the threat intelligence function is not producing as much value as it could. This presentation will provide practical examples of applying higher-level "pyramid of pain" detection taken from open-source reporting to hunting activities. Applying similar techniques also provides additional benefits to the organization, as it enables the organization to operationalize and collect feedback on more aspects of its threat intelligence functions. Lastly, we'll present one possible classification and prioritization framework using the Lockheed Martin Cyber Kill Chain. *Keith Gilbert (@Digital4rensics), Security Technologist, Sqrrl/Malformity Labs*
3:45-4:20 pm	***Homemade Ramen & Threat Intelligence: A Recipe for Both*** Julia Child said "No one is born a great cook; one learns by doing." The same thing could easily be said of threat intelligence analysis. In this talk, you'll learn the recipe and techniques for building an in-house threat intelligence capability (as well as a great bowl of ramen). The focus will be on what you can do today, now, regardless of budget, fancy feeds, or background. Chef's knife not required. *Scott J. Roberts, Bad Guy Catcher, GitHub; Summit Advisor, SANS Institute*
5:30-7:30 pm	**CTI Summit Night Out in Bethesda** (LOCATION: 7940 NORFOLK AVE. BETHESDA, MD 20814) Enjoy food and drinks as you network with fellow Summit attendees at Tommy Joe's in Downtown Bethesda.

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 30

9:00-9:15 am	***Day 2 Welcome and Overview***
9:15-10:00 am	***Keynote: Attributing Active Measures, Then and Now*** Security breaches, intrusions, exfiltration of information, and subsequent surfacing and "leaking" of compromised (and compromising) material for targeted effect is an old phenomenon. How has the internet changed this classic spy game? And how has the attribution of hack-and-leak operations evolved? Rid will present a small number of case studies to illustrate larger trends and conclusions. *Thomas Rid (@RidT), Professor of Strategic Studies, Johns Hopkins University's School of Advanced International Studies; Author, Rise of the Machines*
10:00-10:30 am	**Networking Break & Vendor Expo** (LOCATION: REGENCY FOYER)
10:30-11:05 am	***The Challenge of Adversary Intent and Deriving Value Out of It*** One of the most challenging intelligence requirements is determining adversary intent, yet many executives leverage this as an early expectation. Understanding why the challenge exists, how to move towards understanding perceived intent, and the role it plays in satisfying intelligence requirements is vastly important to helping our intelligence customers succeed. This presentation will focus on presenting the challenges and successes in this area through use cases and case studies that show the value of going through this process correctly and helping others become more successful. *Robert M. Lee (@RobertMLee), CEO, Dragos Inc.; Summit Co-Chair, Author, Certified Instructor, SANS Institute*
11:05-11:40 am	***Legal Implications of Threat Intelligence Sharing*** In order to stem the tide of cyber attacks, many organizations have bought into the notion of threat intelligence sharing. While the benefits are clear to security pros, the legal risks are not. In protecting your organization from attack, are you actually making it more vulnerable to legal action? This session will explore the pros and cons of threat intelligence sharing through the eyes of the law. Attendees will walk away with a better understanding of the legal implications of intelligence sharing, and receive tips on how to maximize shared threat intelligence to avoid wasting resources. We'll also spotlight other security methods that are as equally effective as shared intelligence, such as encrypting data, tightening access controls, and minimizing sensitive data collection. *Jason Straight (@UnitedLex), Chief Privacy Officer/SVP, Cyber Risk Solutions, UnitedLex*

Tuesday, January 30

11:40 am – 12:15 pm

Leveraging Curiosity to Enhance Analytic Technique

Investigations are centered on bridging the gap between perception and reality. The narrower the gap, the more likely you are to build quality intelligence, make sound judgements, and come to the correct conclusion about events that have transpired. Curiosity is what stimulates our ability to learn and close information gaps in a way that is critical for our day-to-day success as well as our career development. Simply put, security practitioners who are insatiably curious will generally be more successful than their less curious peers. This presentation will examine curiosity in-depth so that you may better understand how it affects your daily work and broader career development. We'll look at information gap theory and the components that constitute curiosity where security, threat intelligence, and cognitive psychology intersect. We'll also introduce rapid gap awareness and how the sudden onset of stress from realizing what you don't know can limit your ability to learn. Finally, we'll present original research and the results of a study that attempts to measure and understand the development of curiosity in security and intelligence practitioners. The presentation will tie these concepts into a series of practical takeaways you can use to stimulate your curiosity and enhance your analytical techniques. You should walk away from this talk with a greater appreciation of curiosity and with effective strategies to apply it in the right places.

Chris Sanders (@chrissanders88), Founder, Applied Network Defense

12:15-1:30 pm **Networking Lunch & Vendor Expo** (LOCATION: REGENCY FOYER)

1:30-2:05 pm

AlphaBay Market: Lessons From Underground Intelligence Analysis

AlphaBay Market was by far the largest and most prolific provider of cyber crime and fraudulent services in the world prior to its seizure by the FBI on July 4, 2017. While the Tor-based marketplace was most famous for the sale of narcotics, firearms, and stolen goods, AlphaBay's forum was the epicenter of the English-speaking cyber criminal community. During the site's tenure, it provided a rich source of intelligence on the tactics, techniques, and operations of cyber criminal groups targeting a wide range of corporations and selling exfiltrated data through the marketplace securely and anonymously. This included visibility into the attack cycle, AlphaBay operating as a bridge between the English and Russian language cyber criminal communities, and the likely role of AlphaBay's administrators in cryptocurrency market manipulation on a large scale. This presentation will discuss iDefense's research into AlphaBay Market as a case study on how in-depth analysis of underground communities can contribute to an organization's security posture. It will provide a detailed discussion of the tradecraft and methodologies used for underground intelligence, such as the use of undercover personas and how to apply social engineering techniques to gain additional intelligence. It will also discuss the strengths and weaknesses of such an approach and the risks associated with cyber underground collection. Finally, the case study will present lessons learned from engagement and analysis of criminal underground communities and how attendees can integrate cyber underground intelligence into their threat intelligence program.

Christy Quinn (@ChristyQuinn), Security Specialist – Cyber Threat Intelligence, iDefense – Accenture Security

Tuesday, January 30

2:05-2:40 pm	***Determining the Fit and Impact of Cyber Threat Intelligence Indicators on Your Monitoring Pipeline (TIQ-Test 2.0)*** The challenge to implement an appropriate data processing pipeline to make good use of your indicators of compromise has been successfully addressed over the last few years. Even with all the push for automation and orchestration, a fundamental question remains: which data should you be ingesting in your detection pipelines? There is no lack of data available, shared or not, paid or not. But how do you keep your cyber threat intelligence (CTI) incident response team from spinning its wheels on a pile of CTI mud? This presentation will discuss statistical analysis you can undertake using the CTI indicators that you collect and your own network telemetry. *Alex Pinto (@alexcpsec), Chief Data Scientist, Niddel*
2:40-3:10 pm	**Networking Break & Vendor Expo** (LOCATION: REGENCY FOYER)
3:10-3:45 pm	***Upgrading Your Cyber Threat Intelligence to Track Down Criminal Hosting Infrastructures*** Ransomware, trojans, cybercrime forums, and stolen credentials shops are commonly hosted on bulletproof hosting servers. Even though defenders are spending billions of dollars to mitigate these threats by reactively collecting and pushing convicted domains, IPs, and signatures into enforcement products, cyber crime continues to increase and cause more damage. In this talk, we'll present proven approaches to upgrade your threat intelligence from being IOC-driven to being more proactive with a longer-lasting advantage. We'll show how to extract behaviors of criminal-hosting infrastructures used for malware, phishing, crimeware forums, and various toxic content, and how to track evolving evasion patterns used by adversaries. We correlate findings using different threat intelligence collection, and analysis techniques applied to large-scale network data and OSINT. This talk will be useful to security practitioners, threat analysts, and law enforcement personnel, and it will provide actionable best practices to improve security controls in protecting organizations. *Dhia Mahjoub (@DhiaLite), Head of Security Research, Cisco Umbrella (OpenDNS)*
3:45-4:20 pm	***ElasticIntel: Building an Open-Source, Low-Cost, Scalable, and Performant Threat Intel Aggregation Platform*** In this talk we will present a new platform, built on Amazon Web Services and backed by ElasticSearch, that allows organizations to easily collect large amounts of open-source threat intelligence and make this data available for consumption by both analysts and machine-based tools via application programming interface (API). Orchestrated with Terraform, this platform can be spun up with a single command and be up and running in less than 30 minutes. No technical expertise is required. The goal of the platform is to provide an open-source alternative to expensive and often inflexible threat intelligence aggregation platforms. This will allow an organization to start using external threat intelligence without the high cost barrier to entry. Highly configurable and scalable from a few megabytes of data to many terabytes, the platform enables an organization to collect threat intel data from any number of sources. Sources can be easily configured by adding a few lines to a Json configuration file and data can be easily queried via the Kibana search interface or the query API, which can scale to tens of thousands of queries per second. We'll also go over the reasons that prompted me to create this platform, the challenges I faced, the problems the platform solves, and the architecture behind it. Finally, we'll go over how to get started with the platform and how it can be easily integrated into an organization's daily workflow. *Matt Jane (@PansyMcCoward), Principal Security Engineer, Okta*

Tuesday, January 30

4:20-5:00 pm	***Information Anarchy: A Survival Guide for the Misinformation Age*** We are surrounded by information – data on every topic, from any angle, in every shape and size. All of this data should provide us with more understanding and insight than ever before. But there is just one problem. The information isn't always accurate. We are living in the misinformation age. How can threat intelligence analysts survive in an age of information anarchy? We need information to form the basis of our analysis, but how can we pick out the truth from the overwhelming piles of data and ensure that our analysis is sound? This talk will discuss how we got to the state we are in, and how to identify accurate information versus intentional misinformation and misinformation born of confusion. Finally, we'll look at some steps we can take as a community to eliminate unintentional misinformation and get to ground truth sooner, including ways to calculate mean time to accurate information on Twitter and how to identify IOC-outliers that require more scrutiny. *Rebekah Brown (@PDXbek), Threat Intelligence Lead, Rapid7; Summit Advisor, SANS Institute*
5:00-6:15 pm	**Networking Reception** (LOCATION: REGENCY FOYER)
6:15-7:00 pm	***Getting on the Same Page: Leveraging a Common Framework for Enhanced Intel Sharing*** The proliferation of threat models has made it difficult for information to be accurately and easily shared between organizations and with consumers of cyber intelligence. The development of a common Cyber Threat Framework (CTF) and a lexicon of malicious cyber activity has helped create standard definitions and a methodology for characterizing and describing cyber threat activity for senior leaders and cyber technicians alike. *Jim Richberg, National Intelligence Manager for Cyber, Office of the Director of National Intelligence*
7:00-8:00 pm	***Pass the Popcorn: Cyber Threat Intel Pros Get Real*** Summit Co-Chair Robert M. Lee and a group of cyber threat intel professionals will host a candid after-hours panel discussion. Ask them anything you were too afraid to ask during the Summit and get a chance to pick the brains of some of the best in the business. Get your popcorn ready; this session is sure to be as entertaining as it is educational. Snacks will be served! The session is open to all Summit and training course registrants.

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.