SANS DFIR

CYBER THREAT INTELLIGENCE

SUMMIT & TRAINING

#CTISummit

Program Guide

@sansforensics

#CTISummit


Rick Holland

Welcome to the 5th annual Cyber Threat Intelligence Summit! Our Advisory Board has been hard at work for months to make this the most engaging CTI Summit yet, and we're delighted that you're here to share this event with us. Five years in, this Summit is more relevant than ever, and we've carefully curated the presentations and talks to provide experience-based, actionable strategies you can use to win the battle against ever-stronger adversaries.

It is a rare treat to have Cliff Stoll as our opening keynote speaker. It would not be an exaggeration to say that most of us owe our careers to his tireless efforts to track a hacker three decades ago, back when the FBI laughed at the notion of "computer crimes" being worth their time. To Cliff, it was an intellectual exercise and a matter of stubbornness, but over the course of his cat-and-mouse game, he laid the foundation for what all of us do every day. His high-energy brand of quirkiness, his persistent genius, and his rich perspective on our field promise to both entertain and inspire you.

Lastly, remember that your participation is what makes this Summit truly one-of-a kind, and attendees tell us time and again that the greatest value of our Summit is the plethora of newly forged or deepened industry connections they make during their time with us. I can tell you that over the past five years, I have built some great personal and professional relationships at this Summit. Take advantage of having a couple hundred of the sharpest minds in the threat intelligence community here with you for the next two days. Introduce yourself to those sitting around you, engage with our expert speakers during networking events, ask questions during Q&A sessions, and weigh in on twitter #CTISummit and @DFIRSummit. Join the Summit Advisory Board tonight at our "The Spy Who came in from the Cold" networking event to hear the board share insights into threat intel trends, tradecraft tips, and advice for contributing your expert knowledge at a future SANS Summit.

Let's get this party started!

Sincerely,

Rick Holland
Cyber Threat Intelligence Summit Co-Chair

Agenda

All Summit Sessions will be held in Salon 4 (unless noted).

All approved presentations will be available online following the Summit at
https://digital-forensics.sans.org/community/summits
An e-mail will be sent out as soon as the presentations are posted, typically within 5 business days of the event.

Tuesday, January 31

8:00-8:45am	**Registration & Networking Breakfast** (LOCATION: SUMMIT FOYER)
8:45-9:00am	***Welcome & Introductions***
9:00-10:00am	***(Still) Stalking the Wily Hacker: Three Decades of Computer Security in Perspective*** Before anyone thought to utter the words "cyber threat intelligence," Cliff Stoll was doing it (and chronicling it in the seminal book that led many of us to careers in the field). From his vantage point as the father of the discipline, he'll share his unique view of how far we've come (hint: he's impressed) and take a realistic look at what the future holds. He'll examine some emerging threat vectors we need to be paying attention to, and offer some words of wisdom to cyber threat intel newcomers and do-it-yourselfers. ***Clifford Stoll**, Author, The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*
10:00-10:30am	**Networking Break & Vendor Expo** (LOCATION: SUMMIT FOYER)
10:30-11:05am	***Throwback Threat Intel: How Old-School Intel Techniques Will Take Us Into the Future*** As we convene for the 5th annual SANS CTI Summit, everything old is new again. We're digging into classic, time-tested tradecraft and applying it in innovative ways to cyber threat intel. We'll look at how cyber threat intel has evolved in the years since the first CTI Summit, give ourselves a collective pat on the back as an industry for the progress we've made, and then get real about how much work we still have to do. We'll look at how borrowing from related disciplines has helped us evolve, anticipate where our threats may take us over the next five years, and note how tried-and-true tradecraft will continue to be just as important as all the shiny new tools – if not more so. ***Mike Cloppert**, **Rick Holland**, & **Robert M. Lee**, CTI Summit Co-Chairs*
11:05-11:40pm	***Inglorious Threat Intelligence*** From the depths of the Atlantic Ocean to the deserts of North Africa to the formation of the Office of Strategic Services, World War II provides countless lessons for the intelligence analyst. The talk will discuss the evolution of intelligence work at that time and how it had to evolve to address the needs of the intelligence consumer. Rick will draw conclusions from the intelligence successes and failures of the conflict that you can apply to your threat intelligence program. ***Rick Holland** (@rickhholland), Summit Co-Chair, SANS Institute*

Tuesday, January 31

11:40am-12:15pm

Integrating Cyber Threat Intelligence Using Classic Intel Techniques

Service providers frequently limit the scope of CTI to the dissemination of threat feeds, third-party analysis, and indicators. As the cyber industry moves away from this limited understanding and begins to more clearly define CTI as a full-spectrum endeavor spanning tactical, operational, and strategic threat intelligence areas, it is important to illustrate how organizations can effectively incorporate actual CTI into their business models. Through integration of the intelligence cycle into the cyber domain and appropriate tradecraft, Noblis will discuss how other organizations can incorporate this model. As a result of this presentation, the audience will learn how to incorporate classic intelligence techniques into their cyber threat model to provide analysts and decision makers with actionable, predictive intelligence, and improved situational awareness. In addition, audience members will learn how integrating both tools and people (net defenders and cyber all-source analysts) within their CTI model is imperative to creating a holistic cyber-threat picture. To achieve this, we will use case studies to challenge the notion that effective CTI is purely technical – it is not. Effective CTI is the marriage between net defense and all-source analysis.

***Elias Fox**, Cyber Threat Intelligence Analyst- R&D, Noblis-NSP*
***Michael Norkus**, Cyber Threat Intelligence Analyst- R&D, Noblis-NSP*

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

1:30-2:05pm

The Threat Intel Victory Garden: Creating, Capturing, and Using Your Own Threat Intelligence Using Open Source Tools

Many threat intel programs ignore the most valuable source of intelligence: their own environment. In the battle to secure your organization, the benefits of "growing your own" threat intelligence are many. Self-sourced threat intel is quite possibly the most relevant origin of indicators when detecting and investigating actionable threats faced by your organization. Home-grown threat intel is also easy to prioritize and enrich because much of the original context is available. Unfortunately, many threat intelligence programs are hampered by manual processes and procedures. In this talk we will briefly discuss some common internal sources of threat intelligence, then present some novel collection techniques including open source tools like the stoQ framework and open source honeypot solutions. We will show through recorded demonstrations how indicators from these sources can be sourced, centrally stored, managed, and leveraged in an automated method. Pointers to usable code/resources that attendees can take advantage of immediately will be provided.

***Dave Herrald** (@daveherrald), Security Architect, Splunk*
***Ryan Kovar** (@meansec), Staff Security Strategist, Splunk*

Tuesday, January 31

2:05-2:40pm

Location-Specific Cyber Risk: Where You are Affects How Badly You'll be Hacked

Many wrongly think that because the internet is global, cyber threats are the same no matter where you are in the world. This line of thinking discounts the close-access, insider, and supply chain threat differences that exist when you change locations.

Additionally, threat actors know and believe that travelers are less protected targets than people in their homes. By compromising a business traveler overseas, it can provide an access point into the corporate network. To prevent and mitigate these scenarios, organizations must understand the location-specific threats to their information security. Organizations can do this by understanding the operational environment and the threat actors that operate in the region or country.

The threat actors include host nation governments that are monitoring in-country communications, APT-style groups, cyber-criminal groups, or hacktivists. Intelligence analysts evaluate the threat actors' intentions and capabilities to determine a threat rating. With this information, an analyst can then create viable risk scenarios through which their organization could experience information loss, operational disruption, or reputational damage. By measuring the likelihood and impact of each scenario, the analyst can determine the overall cyber risk of that location. This information informs precise decision-making to take appropriate preventive and mitigating measures.

By measuring the location-specific cyber risk and thoroughly assessing the threats in a country, intelligence analysts can identify intelligence gaps, focus collection efforts, and lay the foundation for multiple follow-on intelligence opportunities.

Lincoln Kaffenberger *(@LincolnKberger) Information Technology Officer, IMF*
John Kupcinski*, Director, KPMG*

2:40-3:10am **Networking Break & Vendor Expo** (LOCATION: SUMMIT FOYER)

3:10-3:45pm

Using CTI to Profile and Defend Against the World's Most Successful Email Scam

In this talk, we will examine the various aspects of one of the world's most successful email campaigns: The Business Email Scam. This campaign has stole nearly $3.1 billion over the past three years, and shows no signs of slowing down. This presentation will present research spanning over three years across the globe, involving multiple case studies and banks from North Carolina to Hong Kong. We will start by examining characteristics of the tools, context, and domains used by the attackers to trick companies. Using publicly-available tools, we will profile just how large this campaign is, what evidence is available, and how to extract valuable indicators from the data. The presentation will conclude with lessons on how the audience can use aforementioned publicly-accessible, free tools to build profiles on attacks such as this scam. We will discuss how to take seemingly arbitrary indicators and use them to protect our networks and business. Lastly, we will also briefly discuss open source tools that smaller teams can use to maintain and organize their indicators.

Matt Bromiley *(@mbromileyDFIR), Senior Managing Consultant, Kroll*

Tuesday, January 31	
3:45-4:20pm	***Reversing Threat Intelligence: Fun with Strings in Malware*** Over the years, there have been huge hacks, many of which end up in the headlines. OPM hacked, Target hacked, and <insert random company> hacked. While it's easy to get caught up in the vast scope of these attacks, we have to remember that it's just a human on the other end pushing the buttons. In this presentation, we will look at malware samples from the dark web, identify places where the attackers slipped up, and use intelligence to find other related samples. ***Ronnie Tokazowski*** *(@iHeartMalware), Senior Malware Analyst, FlashPoint*
4:20-4:55pm	***Hunting Cyber Threat Actors with TLS Certificates*** This presentation will go over how net defenders and threat intel analysts can use TLS/SSL data from open source sites like scans.io and censys.io to defend their networks and track threat actors that use TLS/SSL to encrypt their command and control, perform credential harvesting or even manage their command and control infrastructure. Most analysts know and use Whois registrant info to track domains threat actors create. However, a lot of threat actors have learned to use Domain Privacy Registration which mitigates that tracking ability. Analysts also like to use passive DNS sources to track domains and ip's as actors move their infrastructure. Others analysts use things like VirusTotal to track threat actors based off their malware but not everyone has access to VirusTotal. Using this technique that I will be discussing, defenders and analysts can easily track malware command and control infrastructure as it moves and put the appropriate defense mitigations in place as needed. ***Mark Parsons****, DevOps/ThreatIntel, Punch Cyber Analytics*
4:55-5:00pm	***Day 1 Wrap-Up***
5:00-6:00pm	**Networking Reception & Vendor Expo** (LOCATION: SUMMIT FOYER)
6:00-7:30pm	NETWORKING RECEPTION: ***The Spy Who Came in from the Cold*** (LOCATION: SALON 5, 6, & 7) We're getting cozy with the Summit advisory board in the CTI Ski Chalet. Cuddle up with a cup of cocoa and some gooey s'mores, de-brief day 1 of the Summit with other attendees, and hear the board share insights into cyber threat intel trends, tradecraft tips, and advice on how to get your expertise on the program at a future SANS Summit.

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.

Wednesday, February 1	
8:00-9:00am	**Registration & Networking Breakfast** (LOCATION: SUMMIT FOYER)
9:00-9:15am	***Day 2 Welcome & Overview***
9:15-10:00am	***Knowing When to Consume Intelligence and When to Generate It*** In the threat intelligence community there are consumers and there are generators. Many organizations only know that they want "threat intel." However, the difference between consuming and generating intel is vast and will structure intelligence requirements, goals, and measurements of success completely differently. In this presentation, the differences between threat intelligence generation and threat intelligence consumption will be covered as well as how to determine when your organization is ready for one or both. Additionally, intelligence requirements will be covered to help ensure that your program is on track regardless of your choice. Many organizations should consume intelligence, some organizations should generate intelligence, and all organizations should know the difference. ***Robert M. Lee*** *(@RobertMLee), CEO & Founder, Dragos, Inc.*
10:00-10:30am	**Networking Break & Vendor Expo** (LOCATION: SUMMIT FOYER)
10:30-11:05am	***Pen-To-Paper and The Finished Report: The (Often Overlooked) Key To Generating Threat Intelligence*** Generating meaningful intelligence is a challenge, even with the right people and technology. Analysts maintain extensive personal "databases" of notes and indicators, but typically do not memorialize their insights in a finished form. The result is that intelligence—our knowledge of threats, and the TI team's core value proposition within the security organization—falls into a state of limbo. Indicators may make it to the SIEM, but incident responders and other stakeholders still lack a complete, coherent picture of the threats they face. To realize the full value of threat intelligence, organizations must embrace and institutionalize a process of creating the quintessential intelligence product: the finished report. Classic intelligence approaches champion the finished report and—if it is correctly executed—praise its value. This talk will argue that the finished report is the only way to truly codify knowledge in way that benefits both tactical and strategic customers. This talk will explore decades-worth of US intelligence community (IC) best practices for generating finished reports and adapt them to threat intelligence. Attendees will gain a new perspective on the importance of writing (and writing well!), and they will learn simple approaches that they can immediately apply in their day-to-day operations to put their intelligence in a finished form. ***Christian Paredes*** *(@cyint_dude), Threat Intelligence Analyst, Booz Allen Hamilton*

Wednesday, February 1

11:05-11:40pm

The Use of Conventional Intelligence Analysis Methodologies in Cyber Threat Intelligence

We need to stop re-inventing the wheel. Intelligence collection, analysis and dissemination methodologies have existed for hundreds, in-fact thousands of years. Designed, honed and perfected by some brilliant analysts and operators, the cyber intelligence industry needs to embrace conventional analysis methodologies to better understand and predict the threat landscape in which they operate. Predominately focused on methods used by British and US agencies and Militaries the talk looks to identify various methods used to help better understand the intelligence picture. From back-casting to cones of plausibility; from analysis of competing hypothesis to breaking the mirror, there are methods that exist to better help us understand what happened, what is happening and what is likely to happen.

***Rob Dartnall**, Director of Cyber Intelligence, Security Alliance Ltd.*

11:40am-12:15pm

Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks

So, you're a threat intel shop? You want to have the beat on that 'sophisticated' group attacking your clients? Good luck with that. The days of lifting a couple of relevant IOCs, googling around, and writing a fancy report with solid attribution are long gone. Today's APT actors are well aware of compilation timestamps and command-and-control infrastructure reuse and some of them value nothing more than to lead researchers astray. Investigators have had an increasingly difficult time finding reliable and agreed upon metrics for attributing attacks. Recent debates over the accuracy and usefulness of attribution keep touching upon the possibility that attackers may be manipulating indicators. Rather than continue to discuss the 'theoretical' possibility of false flags, we will present never before revealed, real-world examples of these operations. APT groups have in fact been following published research and are using the information they glean to throw researchers off their trail. The final aim is to discuss the relevancy of attribution in the commercial and government sectors and to insist on curbing the appeal of 'sexy attribution claims' in the threat intelligence space in favor of actionable intelligence.

***Brian Bartholomew** (@Mao_Ware), Senior Security Researcher, Kaspersky Lab – GreAT*
***Juan Andrés Guerrero-Saade** (@juanandres_gs), Senior Security Researcher, Kaspersky Lab – GreAT*

12:15-1:30pm **Lunch & Learns**

Sponsor: DomainTools

Enrich All the Things: Turning Threat Data into Threat Intelligence

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 help you profile threat actors for the prevention of phishing, data exfiltration, and brand compromise.

Presenter: Mark Kendrick, Director of Business Development, DomainTools

Location: Studio E

Sponsor: Flashpoint

Over the Endpoint Horizon: Evolving Network-centric Cyber Threat Intelligence Into Enterprise Applied Business Risk Intelligence (BRI)

In order to provide comprehensive risk assessments and knowledgeable security advice to business decision makers, we must move beyond classic network and endpoint threat intelligence. Current operating and application models of cyber threat intelligence does not fully provide the elevated vantage points to reveal enterprise-wide risks. Mapping threats to critical business functions and assets can only be done by drawing on intelligence curated from multiple sources and applied to reveal the whole threat picture, beyond just technical aspects. In this presentation, we examine the principles of shifting upward to gain visibility dominance of the threat landscape.

Presenter: Tom Hofmann, VP Intelligence, Flashpoint

Location: Studio B

Sponsor: Anomali

Looking Beyond Your 4 Walls: Periphery Threat intelligence

Over 63% of the breaches in the past year involved compromised credentials and phishing scams. What this means is despite using threat intel that is integrated into the network solutions, such as a SIEM, organizations need to strongly consider the importance of looking beyond their four walls so that they are aware of potentially harmful threats like credential exposures and suspicious domain registrations. Understanding tools and techniques, such as automation of exposure monitoring for yourselves and third-party contractors are all vital to protecting your organization. This presentation will teach you about the various ways that bad actors can and will use these techniques against you what you can do to proactively protect yourselves again them.

Presenter: Josh Fu, Sr. Sales Engineer, Anomali

Location: Studio D

Wednesday, February 1

1:30-2:05pm	***Beyond Matching: Applying Data Science Techniques to IOC-Based Detection*** There is no doubt that indicators of compromise (IOCs) are here to stay. However, even the most mature incident response (IR) teams are currently mainly focused on matching known indicators to their captured traffic or logs. The real "eureka" moments of using threat intelligence mostly come out of analyst intuition. You know, the ones that are almost impossible to hire. In this session, we show you how you can apply descriptive statistics, graph theory, and non-linear scoring techniques on the relationships of known network IOCs to log data. Learn how to use those techniques to empower IR teams to encode analyst intuition into repeatable data techniques that can be used to simplify the triage stage and get actionable information with minimal human interaction. With these results, we can make IR teams more productive as soon as the initial triage stages, by providing them data products that provide a "sixth sense" on what events are the ones worth analyst time. They also make painfully evident which IOC feeds an organization consume that are being helpful to their detection process and which ones are not. This presentation will showcase open-source tools that will be able to demonstrate the concepts form the talk on freely available IOC feeds and enrichment sources, and that can be easily expandable to paid or private sources an organization might have access to. ***Alex Pinto*** *(@alexcpsec), Chief Data Scientist, Niddel*
2:05-2:40pm	***Threat Intelligence At Microsoft: A Look Inside*** Sergio Caltagirone will dive deep into the operations, processes, and tools of the threat intelligence practice at one of the largest companies in the world, Microsoft. He will share how they do what they do to protect billions of customers worldwide while at the same time protecting their own multi-national organization from threats. This presentation will include their core philosophies which influence decisions around threat intelligence and some lessons and perspective for others building and managing their own threat intelligence practice. ***Sergio Caltagirone*** *(@cnoanalysis), Director – Threat Intelligence & Analystics, Dragos, Inc.*
2:40-3:10am	**Networking Break & Vendor Expo** (LOCATION: SUMMIT FOYER)
3:10-3:45pm	***Using Intelligence to Heighten Your Defense*** When people think of threat intelligence, they think tracking groups outside of an organization. There is an often overlooked and equally (if not more) important function threat intelligence teams can serve. By focusing inwards first, teams can understand what the organization deems important, and prioritize detection efforts. Likewise, understanding what assets are at a higher risk of being compromised can help lead efforts in detection and remediation. Coming up with lists of High Value Assets and High Risk targets will allow intel teams to inform various stakeholder groups about risk they face. Heightened monitoring becomes possible as well, which can cause lower fidelity indicators to become useful. This presentation will cover defining High Value and High Risk Assets, while discussing methods and ideas for providing heightened monitoring for those assets. By knowing ourselves, we can better understand the adversary and their objectives. ***Jeremy Johnson*** *(@agnu), Cyber Threat Intelligence Analyst, Ford Motor Company*

Wednesday, February 1

3:45-4:20pm	***Effective Threat Intel Management*** Threat Intelligence cells, once constrained to military circles, the financials and the largest corporations, have become a common component of mainstream information security practices. Many organizations are struggling to reap the full value of threat intelligence functions. This is commonly caused by a handful of approaches including: Squirrel Chasing - chasing vendor marketing threats Pure Count based metrics (pure number indicators, signatures, and threats) Focusing more time on less-valuable, more-transient indicator types. By focusing analysis towards the intelligence found within the organization's own data, Threat Intelligence analysts can help their organizations improve their security posture and reach measurable goals. Orienting away from headline-threats and towards realized threats Measuring Collection Time, Collection Coverage, Detection Rates, Dwell Time, and Response Time Focusing on generalized and strategic detections that detect entire classes of activity with auto-enrichment services. Measuring Contextual Enrichment and Data Quality over pure counts. ***Aaron Shelmire*** *(@ashelmire), Principal Threat Researcher, Anomali*
4:20-4:55pm	***Accurate Thinking: Analytic Pitfalls and How to Avoid Them*** Proper forensic investigation requires more than log review and image examination. To provide useful information, analysis must be approached with an appropriate level of intellectual rigor. This talk examines specific methodologies drawn from fields as widely varied as mathematics and political science, such as falsification and compensation for cognitive bias. Attendees will learn how to apply several frameworks and techniques they can apply immediately to improve the accuracy and reliability of all types of analysis within their organizations. ***Kyle Maxwell*** *(@kylemaxwell), Senior Researcher, Verisign iDefense*
4:55-5:00pm	***Closing Remarks***

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.