SANS

Cyber Threat Intelligence

SUMMIT & TRAINING

Program Guide

Summit Co-Chairs: Mike Cloppert and Rick Holland

@sansforensics #CTISummit #ThreatIntel @SANSDefense

Agenda

All Summit Sessions will be held in the Virginia Ballroom (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.

Wednesday, February 3	
8:00-9:00am	**Registration & Coffee** (LOCATION: VIRGINIA HALL)
9:00-9:20am	***The Levels of Threat Intelligence*** Classifying threat intelligence and capabilities at tactical, operational, and strategic levels enables more nuanced thinking in our increasingly-complex discipline. In this presentation, the levels of intelligence, their history, and application to our domain will be discussed. ***Mike Cloppert**, CIRT Chief Research Analyst, Lockheed Martin & Summit Co-Chair*
9:20-10:00am	***An End User's Perspective on the Threat Intelligence Industry (Hint: We Have Work to Do)*** Cyber Threat Intelligence has matured over the past few years. We now have people who specialize in cyber threat intelligence, entire companies focused on threat intelligence as a flagship product offering, and even global regulators who measure organizations' maturity in threat intelligence. This talk will describe how threat intelligence is used at some of the world's largest financial institutions, highlight the regulatory and other requirements being levied, and share some constructive feedback on what is needed from industry. ***Rohan Amin**, Ph.D., Global Chief Information Security Officer, JPMorgan Chase & Co.*
10:00-10:30am	**Networking Break and Vendor Expo** (LOCATION: VIRGINIA PREFUNCTION)
10:30-11:15am	***Threat Intelligence Awakens*** There's been an awakening. Have you felt it? Threat intelligence: it's calling to you. Just let it in. Join Forrester analyst Rick Holland as he describes the awakening of the cyber threat intelligence market. Rick will discuss the current state of the CTI market, the need to produce organic intelligence, and indicators of exhaustion (IOEs). This presentation will include Star Wars: The Force Awakens spoilers. ***Rick Holland**, Summit Co-Chair, SANS Institute*

Wednesday, February 3

11:15-12:05pm	***Plumbing's Done! Now What Do We Do With All This Water?*** With the explosive growth in the adoption of the STIX™ and TAXII™ Cyber Threat Intelligence standards we are well on our way to having the "plumbing" of CTI established globally. This talk will explore successful existing applications of CTI (i.e. "the water") and where the cybersecurity community is heading based on this new ecosystem. Promising new uses of CTI will be highlighted and the audience will gain insights into emerging focus areas including: • Prevention at the scale of millions of endpoints simultaneously • Rapid correction of false positives through automated feedback loops • Advanced analysis and meaningful data-driven visuals ***Richard Struse**, Chief Advanced Technology Officer, U.S. Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC)*
12:05-1:15pm	**Lunch & Learn Presentation** (LOCATION: CARTER ROOM) ***Turning Malicious VBA into a Source of Threat Intelligence*** Malicious VBA continues to be a favored tactic by a wide range of threat actors and a thorn in the side of many security platforms and defenders. In this session, we'll explore the basics of the challenges presented by this tactic, look at some simple tools and techniques for decomposing and understanding VBA, and discuss potential approaches for operationalizing newly gained intelligence using the file intrusion detection system (FIDS) LaikaBOSS. ***Kurt Silberberg, Cyber Intel Analyst, Lockheed Martin*** LOCKHEED MARTIN
1:15-2:05pm	***Multivariate Solutions to Emerging Passive DNS Challenges*** These days, most threat intelligence analysts know how to use passive DNS to pivot on initial indicators: given one bad domain, analysts will routinely use passive DNS to identify other domains using the same IP address or name servers, etc. Less discussed are the corner cases that make simple passive DNS methods hard to successfully employ. For example, if a domain's name servers are shared with 100,000 other domains (including many legitimate domains!), "guilt by association" based solely on name server commonality can becomes difficult. Fortunately, it is still possible to identify related bad domain by employing passive DNS along with various other attributes rather than just focusing on a single screening factor such as shared name servers. Audience members will learn about the emerging challenges to using Passive DNS and specifics steps they can take to successfully overcome them. ***Dr. Paul Vixie**, CEO/Co-Founder, Farsight Security*

Wednesday, February 3	
2:05-2:50pm	***Data Mining Malware for Fun and Profit: Building a Historical Encyclopedia of Adversary Information*** According to VirusTotal, almost 500,000 unique malware samples are seen by them every day. That doesn't include all the malware VirusTotal doesn't see. The shear deluge of unique malware samples makes it difficult for incident responders to keep up to protect their networks. Even more difficult is the task to investigators and law enforcement to keep up with the size and number of command-and-control networks and criminal operations. The size and scope of malware may seem daunting, but these repositories can be mined for intelligence in a programmatic way to build not only threat intelligence feeds for current threats, but a historical encyclopedia for attacks seen in previous months and years. The ability to correlate attacks and malicious infrastructure historically has opened up new methods to attribute attackers and to support long-term disruptive activity. This talk will discuss how a massive historical intelligence database can be used to correlate historical attacks and what the possibilities hold for this kind of analysis. The audience will come away with the knowledge in how to build a system of their own, what open source tools and repositories are available for defenders and the basics in how to apply threat intelligence techniques to automated threat data collection of this type. ***John Bambenek**, Sr. Threat Analyst, Fidelis Cybersecurity; Incident Handler, Internet Storm Center*
2:50-3:10pm	***Community Intelligence & Open Source Tools: Building an Actionable Pipeline*** Every vendor will tell you the solution to stopping the most basic to the most advanced threats is simple: buy their offering. While vendor services can be useful, and sometimes COTS tools are efficent, there are alternatives. Free or almost free threat intelligence services are popping up constantly and seemingly every day there's a new promising open source tool. So what does it take to build intelligence-driven incident response with open source tools and community threat information? We'll walk through the process of integrating community threat information with Facebook's osquery in the detection and investigation phases of an incident as well as a few important open source projects. Additionally we'll talk about contributing back to the community, both tools and information, and how we can build a sustainable ecosystem. ***Scott J. Roberts**, Director of Bad Guy Catching, GitHub*
3:10-3:40pm	**Networking Break and Vendor Expo** (LOCATION: VIRGINIA PREFUNCTION)

Wednesday, February 3

3:40-4:00pm

Six Years of Threat Intel: Have We Learned Nothing?

The modern era of open threat reporting began in 2010, when Google first broke the news that it and several other large companies had been the target of an APT campaign which came to be known as "Operation Aurora." Security companies around the world rushed to be the first to provide reports on the threat actors, their activities and their toolset. Six years later, security companies still race to publish reports on the hottest new actors or malware families. With all this practice, the industry should be very good at communicating actionable threat intelligence, and organizations should have mature processes in place for consuming and using it. So why is this still so hard?

In this presentation, we'll take a look back at the last six years of open threat reporting. Using models like the Pyramid of Pain and the Detection Maturity Model, we'll examine the types of intel these reports contain and how that has (or has not!) changed over time. If you are a creator of threat reports, we'll give you some recommendations for improving your offerings to make them more useful to enterprise defenders. If you are a consumer of threat reports, we'll cover our best tips for gathering and making use of the intel they contain. No matter your role, though, learning from our threat intel past can help us all be more successful at making life harder for the attackers.

***David J. Bianco**, Security Technologist, Sqrrl Data, Inc.*

4:00-4:45pm

Data-Driven Threat Intelligence: Metrics on Indicator Dissemination and Sharing

For the last 18 months, MLSec Project and Niddel collected threat intelligence indicator data from multiple sources in order to make sense of the ecosystem and try to find a measure of efficiency or quality in these feeds. This initiative culminated in the creation of Combine and TIQ-test, two of the open source projects from MLSec Project. These projects have been improved upon for the last year, and are able to gather and compare data from multiple Threat Intelligence sources on the Internet. This research culminated on a talk on SANS CTI Summit 2015 and a contribution to the Verizon DBIR on the same year.

In this talk, we have gathered aggregated usage information from intelligence sharing communities in order to determine if the added interest and "push" towards sharing is really being followed by the companies and if its adoption is putting us in the right track to close these gaps. We propose a new set of metrics on the same vein as TIQ-test to help you understand what does a "healthy" threat intelligence sharing community looks like.

To better illustrate the points and metrics, we will be conducting part of this analysis using usage data from some high-profile threat intelligence platforms and sharing communities, that have been kind enough to contribute with usage data for this research.

Join us in an data-driven analysis of threat intelligence sharing communities and their impact on operational usage of indicators!

***Alex Pinto**, Chief Data Scientist, Niddel*

Wednesday, February 3

4:45-5:30pm	***You Got 99 Problems and a Budget's One*** Threat Intelligence programs have earned a reputation for being budget-breakers – including million dollar feeds, custom-built platforms, and hiring personnel straight out of black ops-inspired action movies (balaclavas optional). Some organizations have the money and resources for this – most do not. That doesn't mean that they should give up on threat intelligence, there is a wealth of openly available information for an organization who is just starting out or has limited resources. This talk will discuss how to identify the best open source or no-cost intelligence resources for your organization, how to integrate them into operations, and how to show value and build a business case for future investment in your threat intelligence program. ***Rebekah Brown**, Threat Intelligence Lead, Rapid7*

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.

Thursday, February 4

8:00-9:00am	**Registration & Coffee** (LOCATION: VIRGINIA HALL)
9:00-9:45am	***The Revolution in Private Sector Intelligence*** Threat intelligence is a hot topic, but the hype obscures a revolution which extends beyond the latest Silicon Valley venture-backed tech unicorn. This movement is powered by the combination of social media, ubiquitous cameras, low-cost digital satellite imagery, and a mix of former intelligence professionals and enthusiastic hobbyists. Together these forces are driving a revolution in private sector intelligence, exposing actors, motives, and capabilities. Whether one looks at the physical conflicts in Ukraine or Syria, or untrusted regimes in North Korea or Iran, or in the supposedly murky online world, the signs of this movement are present. This talk will present examples of the revolution, discuss its costs and benefits, and offer insights into its future. ***Richard Bejtlich**, Chief Security Strategist, FireEye & Nonresident Senior Fellow, The Brookings Institution*

Thursday, February 4

9:45-10:30am

Hide and Seek: How Threat Actors Respond in the Face of Public Exposure

This presentation explores how threat groups respond when their operations are publicly exposed. We'll evaluate how public reporting impacts threat groups' decision making, and how public exposure influences threat actors' tactics, targets, timing, and the resources they apply to their operations. Through case studies, we'll demonstrate that threat groups are keenly aware of public reporting on their operations, but the ways they respond differ – sometimes quite dramatically. By the end of the presentation, it will be clear that threat groups' response to exposure often reveals new context about the groups themselves, their capabilities, and their planning cycles.

***Kristen Dennesen**, Senior Threat Analyst, FireEye*

10:30-11:00am — **Networking Break and Vendor Expo** (LOCATION: VIRGINIA PREFUNCTION)

11:00-11:45am

There Can Be Only One!: Last CTI Vendor Standing Pitch

You have very limited resources and don't have the ability to invest in multiple threat intelligence offerings. You're overwhelmed by "actionable intelligence" and need vendors to concisely present their value proposition. In this unique session, four vendors will each have 10 minutes to convince you, the SANS CTI Summit attendees, why their offering should be your top priority.

Moderator: ***John Pescatore**, Director, SANS Institute*

Panelists: ***Mark Kendrick**, Director of Business Development, DomainTools*
***Matt Kodama**, VP, RecordedFuture*
***Jess Parnell**, Director of Information Security, Centripetal Networks*
***Roselle Safran**, Co-Founder/CEO, UpLevel Security*

11:45am-12:05pm

Analysis of the Cyber Attack on the Ukrainian Power Grid

On December 23rd a power outage occurred in Ukraine. The Ukrainian government shortly thereafter claimed that it was a cyber attack by the Russian government. Robert M. Lee, Michael Assante, and Tim Conway on the SANS ICS team began analyzing the incident and were first to reveal that there was a sample of malware uncovered from the network. This presentation will discuss the findings to date of the Ukrainian outage and the lessons learned for cyber threat intelligence.

***Robert M. Lee**, Author & Instructor, SANS Institute*

12:05-1:15pm — **Lunch & Learn Presentation** (LOCATION: CARTER ROOM)

Best Practices For Operationalizing Threat Intelligence In Your Environment

If I told you a storm was coming tomorrow, but it took 5 days to get to the shelter, is there any value to knowing about it in the first place? The same concept applies to cyber intelligence. If you cannot operationalize at scale and speed, then it has no value. There is an overwhelming amount of threat intelligence and industry has struggled to see value because they do not have a way to consume, prioritize and operationalize it.

***Trish Cagliostro**,*
Principal Security Architect, ThreatStream

Thursday, February 4

1:15-1:35pm	***Anticipating Novel Cyber Espionage Threats*** When assessing cyber espionage threats to your enterprise, it's wise to focus on adversaries you've already encountered, and known threats to your sector should provide excellent insights as well. Nonetheless, it's easy to miss intelligence opportunities when you're overly focused on the proximate and the immediate. The threat actors who ruin your day tomorrow may not even know the name of your organization today, but you can still prepare for and learn from them. Cyber espionage is a global problem carried out by actors organized against a variety of problems and who respond to a variety of taskings. Some operators are laser-focused on limited objectives, but many change their interests regularly. Many major threats have inauspicious beginnings – a cyber espionage campaign focused on regional dissidents, a group of defacers, or an advertisement for services in a cybercrime forum. It is impossible, and even undesirable, to track every emerging threat, but it is possible to isolate and focus on those threats that are mostly likely to affect your enterprise in the long-term by evaluating them on the basis of several historic trends. This talk will focus on those historic trends, and how to use them in effective forecasting. ***John Hultquist**, Director of Cyber Espionage Analysis, iSIGHT Partners*
1:35-2:20pm	***Cyber Threat Intel: Maturity and Metrics*** What are the characteristics of a mature cyber threat intelligence program, and how do you develop meaningful metrics? Traditionally, intelligence has been about providing decision support to executives whilst the field of cyber threat intelligence supports this customer, and network defenders, who have different requirements. By using the intelligence cycle, this talk will seek to help attendees understand how they can identify what a mature intelligence program looks like and the steps to take their program to the next level. ***Mark Arena**, CEO, Intel471*
2:20-3:05pm	***Borderless Threat Intelligence: Proactive Monitoring your Supply chain and Customers for Signs of Compromise*** This past year was the year of the data breach. Large and small organizations across every industry vertical were impacted by compromises that ranged from theft of PII, intellectual property, and financial information to publication of entire backend databases and email spools. The data from these breaches often wound up being exposed publicly, exchanged or sold on underground markets, or simply leveraged to breach other organizations. Many of these breaches have cascading effects due to the transitive nature of security that exists across many companies. Many companies rely on critical business partners, subsidiaries, and other organizations whose services are trusted. Also, due to password reuse, customers' accounts included in a third-party data dump could enable unauthorized access to another business's assets. This talk will outline through case studies several ways that Threat Intelligence is being used today to improve the security and awareness of organizations by monitoring "supply chain" partners, customers, and trusted third parties, specifically focusing on brand monitoring, mass credential compromises, signs of infection/compromise, and signs of targeting and social networking data-mining. Learn how organizations can effectively integrate this practice into their existing security programs. ***Nicholas Albright**, VP of Security and Intelligence, ThreatStream, Inc.* ***Jason Trost**, VP of Threat Research, ThreatStream, Inc.*
3:05-3:30pm	**Networking Break and Vendor Expo** (LOCATION: VIRGINIA PREFUNCTION)

Thursday, February 4

3:30-4:15pm	***We Can Rebuild Him; We Have the Technology*** A decade ago manual analytics were all the rage: all you needed were Excel, i2's Analyst NoteBook and Windows XP to do a semi-decent job of Cyber Threat Intelligence analysis. Unfortunately, yesterday's processes can no longer scale to the threats of today. Our talk discusses how to identify and tackle organizational inefficiencies through process and platform. For example many organizations are still convinced the answer to CTI is a SEIM and vendor feeds - yet they do not memorialize or organize freely available knowledge. They are complacent in allowing analysts to conduct highly repetitive and manual tasks versus enabling them to do what they do best, analyze threats. Organizations must allocate analysts' time and effort where they can provide the most impact and be as efficient as possible. Together, Rich and Rob will demonstrate how process and platform are key enablers in automating resource intensive aspects of Cyber Threat Intelligence. Understanding what you are trying to achieve and building processes around it is more efficient and effective in the long run - allowing the organization to save time and money. ***Rich Barger**, CIO, ThreatConnect* ***Rob Simmons**, Sr. Threat Researcher, ThreatConnect*
4:15-4:35pm	***From the Cyber Nerdery to the Board Room*** Intelligence is generated for a variety of consumers, in the enterprise the typical consumer is the operator. As businesses begin to recognize that the impact of incursions into their enterprise have real consequences, they will need to elevate the implications into their business decisions. Intelligence in a traditional context is meant to allow the decision maker whether that is a battlefield commander, a political, diplomatic, or economic officer make effective decisions. That is they need as much information to make the best possible decision they can. As information security continues to encroach into the board room, practitioners need to know what to deliver and how in order to meet the growing needs of the business decision maker. This presentation will explore a variety of issues from traditional intelligence disciplines and apply them to the information security needs to the modern business. ***Adam Meyers**, VP of Intelligence, CrowdStrike*
4:35-4:45pm	***Closing Remarks*** ***Mike Cloppert**, CIRT Chief Research Analyst, Lockheed Martin & Summit Co-Chair* ***Rick Holland**, 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** **#ThreatIntel** **@SANSDefense**