SANS

Cyber Threat Intelligence

SUMMIT 2014

ARLINGTON, VA | FEBRUARY 4-11, 2014

Program Guide

Co-Chairmen: Mike Cloppert and John Pescatore

Agenda

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

All approved presentations will be available online following the Summit at ***https://files.sans.org/summits/CTI14****.*
An e-mail will be sent out as soon as the presentations are posted, typically within 5 business days of the event.

Monday, February 10

8:00 - 9:00 am

Registration & Coffee

9:00-9:15 am

Welcome & Opening Remarks

John Pescatore and Michael Cloppert, Summit Co-Chairs

9:15-10:00 am

Keynote Address:
Looking At Data: A Google Approach

For years we have been deluged with promises of "winning" with "Big Data," "Cloud," Security Analytics," "Continuous Monitoring," and so on. Yet few would argue we've been able to satisfactorily tackle the problem of predicting and detecting attacks with such strategies. Issues of scale, reliability, and disruptive technologies have crushed those dreams. Google faces all of these challenges, despite its successes in "organizing all the world's information and making it universally accessible." This talk will present some real-world scenarios where these strategies have worked, instances where it hasn't, and offer a glimpse of what the future could look like.

Heather Adkins*, Information Security Manager, Google Inc.*

10:00-10:20 am

Networking Break & Vendor Expo

10:20-11:20 am

Security Analytics: Architecture, Design, and Implementation

Threat Intelligence, Big Data, Security Analytics - these are some of the most exciting and talked-about developments in the cybersecurity industry.

But the sharing of threat intelligence is not a miracle cure. In fact, if we don't think through how such information will actually be used, we risk making the problem worse by crushing our already overloaded inboxes and operators. Yesterday's sharing models – e-mails to all of my friends, hours-long teleconferences, ALL UPPERCASE DOD MESSAGE FORMAT TEXT, proprietary verticals, meetings in nice locations once a quarter to share stories – are not fast, targeted, accurate, or actionable enough to help us.

We're never going to solve this challenge until we think of this as an Information Management problem – one where we ***design*** the total flow of information, from where it is created to where it is used, and implement it with a technical ***architecture*** that can capture, find, move, and consume the information naturally, as a way that we manage our systems.

In this panel session, we'll look at some of the most promising practices and standards that enterprises are now using to streamline and automate this information workflow, optimize their use of information, and build sharing communities.

Moderator: ***Tony Sager,*** *Director, SANS Institute*

Panelists: ***Mark G. Clancy****, Managing Director, Technology Risk Management, The Depository Trust & Clearing Corporation (DTCC)*
Phyllis Lee*, IAD Security Automation Program Manager, NSA*
Richard Struse*, Chief Advanced Technology Officer, U.S. Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC)*

11:20 am-12:15 pm

Threat Intelligence Buyer's Guide

Over the past year, the threat intelligence market has evolved almost as quickly as the hype surrounding it. It is critical for enterprises to understand this landscape so that their limited funds and operational resources can be invested in the right place. In this presentation, Forrester analyst Rick Holland will provide participants with:

- An overview of current threat intelligence trends
- An Intelligence Cycle based framework for evaluating threat intelligence
- A market overview of the threat intelligence landscape

Rick Holland, *Principal Analyst, Forrester Research*

12:15-1:30 pm

Lunch & Learn

Presented by

GENERAL DYNAMICS
Fidelis Cybersecurity Solutions

Speaker: Mike Nichols, Technical Product Manager, Fidelis Security

Yara is an excellent content identification and classification system used by malware analysts and reverse engineers to apply signatures to data-at-rest and identify or discover malicious files. A new way of discovery and detection can be harnessed by using a granular application of Yara signatures to data-in-motion as it transits your network to prevent the threat from reaching the end user.

1:30-2:15 pm

Afternoon Keynote:
Analyzing and Disrupting the Evolving Threat Landscape

Intel Security's research shows that the number of threats against that IP-enabled footprint is currently increasing at a rate of 469,000 per week. This presentation will cover analytics on the latest threat vector and techniques, drilling down into several real-world examples. It will discuss how Intel is using advanced analytics to predict, prevent, detect and respond to cyberthreats, outlining the development and use of tools and reporting capabilities to distill large amounts of data into meaningful security analysis.

Scott Montgomery*, CTO and VP of Public Sector, INTEL Security (formerly McAfee)*

2:15-3:15 pm

Panel:
Moving from SIEM to Security Analytics: Evolution or Starting Over?

Security Information and Event Management (SIEM) products are a $2B per year market and many organizations already use them for log monitoring and reporting. Many SIEM vendors have added event handling and analytics tools and position SIEM as the foundation for Security Analytics. However, others argue that the complexity of security events and the sheer volume of events that need to be analyzed to spot advanced targeted threats required performance and capabilities that are well beyond traditional SIEM products. This panel will argue both sides of this debate, with an emphasis on using case studies of real implementations to prove their points.

Moderator: ***John Pescatore****, Director – Emerging Security Trends, SANS Institute*

Panelists: ***Salo Fajer****, Senior Director Product Management – Risk, Compliance and Analytics, McAfee*
Adam Meyers*, Director of Intelligence, CrowdStrike*

3:15-3:30 pm

Networking Break & Vendor Expo

3:30-4:15 pm

Building an Effective Corporate Cyber Threat Intelligence Practice

Threat intelligence has become a critical component to enterprise security and a strong resource for understanding cyber risk in a corporate environment. This presentation provides insight to lessons learned in implementing operationally-focused threat intelligence capabilities and developing the security team capability to ensure continuous use of the intelligence for managing tactical threats and strategic risks. A corporate threat intelligence program must focus on specific needs of the corporate environment, threats, and critical assets driving increasing maturity across a range of core functions. The audience will be exposed to best practices associated with implementing a full spectrum threat intelligence capability to deal and the requirements to maintain and mature a threat intelligence capability.

Greg Rattray*, Chief Executive Officer, Delta Risk LLC*

4:15-5:15 pm

Cyber Threat Intelligence SANS360

In one hour, 10 experts will discuss Cyber Threat Intelligence and how they use it in their organizations. If you have never been to a lightning talk it is an eye opening experience. Each speaker has 360 seconds (6 minutes) to deliver their message. This format allows SANS to present 10 experts within one hour, instead of the standard one Speaker per hour. The compressed format gives you a clear and condensed message eliminating the fluff. If the topic isn't engaging, a new topic is just 6 minutes away.

APT Sans Malware
Harlan Carvey, Dell SecureWorks

Re-thinking our Approach to Threat Intel Sharing
Douglas Wilson, Mandiant

The Business Side of Threat Intelligence
Adam Vincent, Cyber Squared Inc.

Employing Enterprise-Wide Data to Mitigate the Insider Threat
Dr. Michael Gelles, Deloitte Consulting LLP

Indicators: Not just IP Addresses Anymore
Dean De Beer, ThreatGRID

Intelligence-Driven Security
Adam Meyers, Crowdstrike

Distinguishing Cyber Espionage Activity to Prioritize Threats
John Hultquist, iSIGHT Partners

Insights for Executives: Cyber Media Analysis
Stephen Cottle, Deloitte

Placing a $ Value on Cyber Risk
Dr. James Ulrich, CyberPoint LLC

Introducing the Concept of a Core IDS
Bob DeWolfe, DB Networks

Pragmatic Intelligence
Curt Shaffer, Symbiotic Network Technologies, LLC

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, February 11

8:00 - 9:00 am

Registration & Coffee

9:00-10:00 am

Keynote Address:
The Defenders' Asymmetric Advantage

It is often said that offensive actors have an asymmetric advantage – they only need to find one flaw to get into a system/network while the defender needs to protect all avenues in. While oversimplified, there is a kernel of truth. At a campaign level, however, the asymmetry may work for the defenders – a defender needs to identify one aspect of an offensive actor to discover and undermine a multi-victim campaign… or at least that could be true with the right analysis, threat intelligence, sharing, and ability to operationalize information across multiple domain. This talk will discuss where we could be going over the next few years in threat intelligence and explore some of the major factors that may limit our threat intelligence as well as some emerging capabilities and opportunities to drive threat intelligence into new and interesting places.

Chris Betz*, Senior Director, Microsoft Security Response Center, Trustworthy Computing, Microsoft Corp.*

10:00-10:20 am

Networking Break & Vendor Expo

10:20-11:15 am

Leveraging File Artifacts for Threat Intelligence

Threat Intelligence isn't just IP addresses and domain names. In fact, since adversaries can quickly transition to different domain names and IP addresses, the usefulness of that intelligence diminishes very fast with respect to time. File artifact intelligence is generally longer lasting, but it can be difficult to use effectively and in a timely manner. File artifacts includes things such as hashes of PE File import tables, JavaScript from PDF files, and even specific shellcode techniques.

This talk will discuss ArtifactR, a scalable static file analysis platform, and how it can be used to both create and leverage this kind of intelligence. I will show how ArtifactR can be used to extract very detailed artifacts from a file. Then we will discuss several real world scenarios where we can use this capability to leverage intelligence from blog posts and white papers that we haven't been able to use before and even intelligence you didn't know you could use.

David Dorsey*, Lead Security Researcher, Click Security*

11:15 am-12:15 pm

Diamond Model for Intrusion Analysis

Any good Threat Intelligence analyst's overarching goal is to provide actionable intelligence to aid in the defense of the network and larger business processes of the organization. To do this, the analyst needs to correlate data from several sources internal and external, make associations between disparate events, recommend or take courses of action from their analysis, and likely write reports for management describing the nature and intent of the threats they are dealing with.

The Diamond Model for Intrusion Analysis lays a foundation for analysts to begin to address these challenges by applying scientific rigor to what has long been considered an art. It accurately details the fundamental aspects of all malicious activity as well as the core analytic concepts used to discover, develop, track, group, and ultimately counter both the activity and the adversary.

In this talk, we'll go over the basics of the Diamond and demonstrate how analysts can start using it today to begin making better informed analytic pivots walking through several Diamond pivot scenarios within ThreatConnect, creating activity threads, and identifying intelligence gaps. We'll also lead into more advanced Diamond usage for generating hypothesis and creating activity-attack graphs for mitigation scenarios.

Andy Pendergast*, Threat Intelligence Analyst, Cyber Squared Inc.*

12:15-1:30 pm

Lunch

1:30-2:15 pm

Threat Intelligence for Incident Response

Let's talk threat intelligence without marketing buzzwords, FUD, or politics. Defending modern infrastructure requires an aggressive, active approach to watch the bad guys and hunt them down in your network. Simply trying to prevent attacks and reacting to incidents late in the kill chain has proven ineffective.

You'll learn about different types of threat intel based on type, source, and usefulness, plus some thoughts about how to organize, analyze, and share what you learn. We will also discuss various tools and frameworks like indicator management, threat actor databases, and event/incident vocabularies - all of which you can start implementing immediately.

Kyle Maxwell*, Senior Analyst, Verizon Business*

2:15-3:00 pm

Agile Defensive Technologies

In order to proactively defend an enterprise network, the security team must employ a strategy that is technically precise, agile, and versatile to change. The ability to mold with the evolving adversary will be critical in successfully defending an enterprise network. Open IOCs are an industry standard developed by Mandiant Corporation. They are a flexible concatenation of forensic elements that can be reviewed to identify intrusions on your enterprise network. IOCs can be developed to identify a multitude of threat activity, everything from a specific malware family to a broad scoped adversary methodology. In order to conduct full-spectrum cyber defense, organizations must use organic intelligence collection capabilities as well as open source collection capabilities to fuel IOC development. The built and shared repository of indicators will catalyze a stronger industrial base and decrease reaction time to respond to a threat.

Captain Robert S. Johnston*, Director, Marine Corps Information Assurance Red Team*
Nathan McBride*, IOC Bucket, LLC*
Heather Ward*, IOC Bucket, LLC*

3:00-3:20 pm

Networking Break & Vendor Expo

3:20-4:00 pm

The Dollars and "Sense" Behind Threat Intelligence Sharing

Within the ThreatConnect Intelligence Research Team (TCIRT), we feel that sharing what we know, whether publicly or privately, helps to grow our organization. We recognize that Threat Intelligence is not a one-size-fits-all solution, but rather a series of tailored processes. We also see significant benefits to organizations that implement even the most modest Threat Intelligence sharing processes. As a resource-constrained organization ourselves, we understand how limited budgets, thin staffing rosters, and busy schedules can impact an organization's ability to consume, produce, and share fully analyzed Threat Intelligence.

The very lack of resources is one of the strongest arguments an organization can make for adopting more comprehensive Threat Intelligence processes. This is especially true for those who are new to Threat Intelligence consumption, development and sharing discussions. Many newcomers struggle with identifying their specific intelligence requirements and key data points needed to conduct a broader cost-benefit analysis. This analysis is critical when evaluating new business investment decisions, and Threat Intelligence programs are no different. This presentation will discuss observations and metrics associated with the TCIRT's Threat Intelligence sharing for the third quarter (Q3) 2013 and beyond.

Rich Barger, *Chief Intelligence Officer, Cyber Squared; Director, ThreatConnect Intelligence Research Team*

4:00-5:00 pm

Valuing Intelligence: Emergent Techniques for Measuring the Value of Intelligence and Maturity of CTI Organizations

Organizations seeking to leverage intelligence in furtherance of Computer Network Defense face many challenges in this new domain. In this one-hour session, two of these challenges representing each pole of this spectrum will be explored: the value of indicators themselves, and how organizations using CTI can measure their maturity and guide it forward. Pulling from work done towards his PhD at George Washington University, as well as models developed within Lockheed Martin CIRT throughout its maturation as a CTI-proficient organization, this presentation will leave analysts and managers alike with ideas on how to progress their understanding and use of threat indicators, and forward evolutionary progress of their network defense organization.

Michael Cloppert*, Chief Research Analyst, Lockheed Martin CIRT*

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.

EXHIBITORS

LOOKINGGLASS

Lookingglass

Lookingglass Cyber Solutions is the world leader in threat intelligence monitoring and management enabling cyber threat visibility and risk decision support. With an outside-in approach, Lookingglass accounts for its client's entire cyber ecosystem and leverages all-source intelligence to provide context to threats far and near. For more information, visit **www.LGScout.com**.

GENERAL DYNAMICS
Fidelis Cybersecurity Solutions

General Dynamics Fidelis Cybersecurity Solutions

General Dynamics Fidelis Cybersecurity Solutions provides organizations with a robust, comprehensive portfolio of products, services, and expertise to combat today's sophisticated advanced threats and prevent data breaches. Our customers can face advanced threats with confidence through use of our Network Defense and Forensics Services and Fidelis XPS™ Advanced Threat Defense Products.

GENERAL DYNAMICS
Fidelis Cybersecurity Solutions

Face Advanced Threats with Confidence

A powerful combination of Products, Services, and Expertise to combat today's sophisticated advanced threats

Network Defense & Forensic Services:

- Proactive Defense
- Continuous Assurance
- Incident Response and Forensics

Fidelis XPS™ Advanced Threat Defense:

- Discover & eradicate threats in real-time
- Broad visibility & control over all phases of threat lifecycle
- All network ports & protocols, at multi-gigabit speeds

FIDELIS XPS

ADAPT AT THE **SPEED** OF ADVERSARY
CYBER THREAT INTELLIGENCE MANAGEMENT
LOOKINGGLASS
www.lgscout.com

UPCOMING SUMMITS & TRAINING EVENTS

2014

Industrial Control Systems Security Summit & Training
Orlando, FL | March 12-18

Security Leadership Summit & Training
Boston, MA | April 29-May 7

Digital Forensics & Incident Response Summit & Training
Austin, TX | June 3-10

Industrial Control Systems Security Training
Houston, TX | July 21-25

Cyber Defense Summit & Training
Washington, DC | August 2014

Pen Test Hackfest Summit & Training
Washington, DC | November 2014

For more information on speaking at an upcoming summit or sponsorship opportunities, e-mail SANS at **summit@sans.org**.

Visit **www.sans.org/summit** for detailed summit agendas as they become available.