Agenda

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

Summit presentations will be posted via the following URL, ***https://digital-forensics.sans.org/community/summits,*** *within 5 business days. An email will be sent to all attendees once live.*

Portions of the Summit may be video-recorded. These videos may be used for marketing or other purposes, but will not be available for distribution or viewing on demand at this time.

Monday, February 2

8:00-8:45 am

Registration & Coffee

(LOCATION: DUPONT FOYER)

8:45-9:00 am

Welcome & Opening Remarks

Mike Cloppert*, CIRT Chief Research Analyst, Lockheed Martin*
Rick Holland*, Principal Analyst, Forrester Research*

9:00-10:00 am

OOPSEC: Capitalizing on OPSEC Fail

Brian Krebs*, Author, Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door*
twitter.com/briankrebs

Most cybercrooks didn't get into the game overnight, and virtually all of them make key mistakes in separating their online and offline lives. This inevitable failure of operational security provides a fascinating glimpse into the lives of today's e-thieves and n'er-do-wells, and provides a wealth of information about their identities, weaknesses and tactics. In this talk, cybercrime investigative journalist Brian Krebs will delve into some of the more interesting and entertaining opsec failures uncovered in the course of his recent reporting on the seedy underbelly of the Internet.

10:00-10:30 am

Networking Break & Vendor Showcase

(LOCATION: EXHIBIT HALL – GLOVER PARK A)

10:30-11:15 am

State of Cyber Threat Intelligence Address

Rick Holland*, Principal Analyst, Forrester Research*

Just weeks after the President's annual address to the U.S. Congress, Forrester Analyst Rick Holland will provide his State of Cyber Threat Intelligence (CTI) Address. In it, Rick will provide a macro perspective on the current state of the CTI space. Rick will discuss:

- CTI challenges and trends
- The CTI provider landscape
- The CTI platform landscape
- Threat intelligence sharing

Attendees are encouraged to stand up, sit down and applaud during the address.

11:15 am - 12:00 pm

Taming Your Indicator Consumption Pipeline

***Ryan Stillions**, Head of Detection & Response Services, Vigilant LLC*

Does your cup overflow with indicators? Sensors run hot? Analysts tired from alert fatigue? This talk is for those interested in a pragmatic model for building an indicator consumption pipeline that results in actionable, prioritized, relevant detections for your event analysts & responders. Using proven techniques from several of the world's largest environments, Ryan Stillions will discuss key steps to optimizing indicator consumption and reclaiming your alert consoles.

12:00-1:15 pm

LUNCH & LEARN
(LOCATION: FOXHALL BALLROOM)

Presented by

LogRhythm

Detecting and Responding to Log Trails from Advanced Threats and Fraud

***Timothy Papa**, Sales Engineer*

Let's face it, it's no longer a matter of 'If' your organization will be breached, but 'When', and retailers are being targeted more than ever. The key question is 'How can retailers detect and respond to breach attempts faster to minimize their impact and protect customer data?" In this presentation, David Pack, head of the LogRhythm Labs group at LogRhythm, the Security Intelligence Company, will discuss the current cyber threat landscape, the particular challenges it poses for retailers, and how security intelligence can be leveraged to protect today's retail-specific IT environments.

LUNCH & LEARN
(LOCATION: DUPONT BALLROOM)

Presented by

DOMAINTOOLS

Connect the Dots with Domain Name Intelligence from DomainTools

***Mark Kendrick**, Director of Solution Engineering*

The best incident responders know attribution can be a proxy for risk. Even when you don't know who's behind an attack, simply knowing what's linked to it can give you tremendous insight. This session will explore specific techniques for enumerating an attacker's online infrastructure and revealing patterns in the history of their domain names and IP addresses. We'll dig deep into published reports on various advanced persistent threats (APTs) and recreate the analysis which lead to their conclusions with resources you can put to immediate use.

1:15-2:00 pm

From Threat Intelligence to Defense Cleverness: A Data Science Approach

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

This session will center on a market-centric and technological exploration of commercial and open-source threat intelligence feeds that are becoming common to be offered as a way to improve the defense capabilities of organizations.

While not all Threat Intelligence can be represented as "indicator feeds", this space has enough market attention that it deserves a proper scientific, evidence-based investigation so that practioners and decision makers can maximize the results they are able to get for the data they have available.

The presentation will consist of a data-driven analysis of a cross-section of threat intelligence feeds (both open-source and commercial) to measure their statistical bias, overlap, and representability of the unknown population of breaches worldwide. All the statistical code written and research data used (from the publicly available feeds) will be made available in the spirit of reproducible research. The tool itself will be able to be used by attendees to perform the same type of tests on their own data (called tiq-test).

We will provide an open-source tool for attendees to extract, normalize and export data from threat intelligence feeds to use in their internal projects and systems. It will be pre-configured with current publicly available network feeds and easily extensible for private or commercial feeds (called combine).

2:00-3:00 pm

Cyber Threat Intel Solutions For Real

MODERATOR:

***Rick Holland**, Principal Analyst, Forrester Research*

PANELISTS:

***Matt Jonkman**, CTO & Founder, Emerging Threats*
***Mark Kendrick**, Director of Solution Engineering, DomainTools*
***Adam Meyer**, Chief Security Strategist, SurfWatch Labs*
***Adam Vincent**, CEO, ThreatConnect*

In this session, leading vendors will answer tough questions about commercially-available tools and solutions that really deliver on their promise.

3:00-3:20 pm

Networking Break & Vendor Showcase

(LOCATION: EXHIBIT HALL – GLOVER PARK A)

3:20-3:35 pm

Results & Analysis of the SANS 2014 Analytics and Intelligence Survey

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

This survey, completed in December 2014, strives to understand how the IT community is consuming and using cyber threat intelligence information in order to start a dialogue about standards for production, consumption, integration and dissemination of this intelligence. Cloppert will share an overview of the findings and how they should inform your organization's CTI strategy.

3:35-4:15 pm

Tumble, Twiddle, Spin & Roll the Black Hat: Incorporating CTI into Security Assessment Programs

***Michael Willburn**, Security Assessment, Program Lead, Federal Bureau of Investigation*

Why incorporate CTI into your security assessment program? How about...to better understand your weaknesses and strengths, to discover what works in the realm of prevention and detection, to put the results into the context of a specific threat or threat category, to dispel misplaced confidence, maximize the effectiveness of limited resources, focus individuals on finding solutions to the right problems…why not?

4:15-4:30 pm

Speaking the Same Language: An Update on Standardized Information Sharing Using STIX and TAXII

***Richard J. Struse**, Chief Advanced Technology Officer, National Cybersecurity and Communications Integration Center (NCCIC) and, Stakeholder Engagement and Cyber Infrastructure Resiliency (SECIR). U.S. Department of Homeland Security*

STIX and TAXII are rapidly becoming the defacto standards for representing and exchanging cyber threat intelligence. This session will provide a concise update on STIX/TAXII developments, operational usage and a roadmap for future evolution including the transition of STIX and TAXII to formal international standards.

4:30-5:30 pm

Cyber Threat Intelligence SANS360

In one hour, multiple 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 his or her message. This format allows SANS to pack multiple experts into one fast-paced hour. The compressed format promises to deliver a clear and condensed message, eliminating the fluff. Don't blink!

Why Sharing Threat Intelligence is No Threat To Your Bottom Line
***Stephanie Scheuermann**, MSIA, CISSP, GCFA , CSC Cyber Threat Intelligence Specialist , Ford Motor Company*

Why Buy the Cow When the Milk is Free?
***Mike Green**, Sr. Manager Global Threat Intelligence, Deloitte*

Developing Threat Intel with an Automated Analysis Framework
***Don McCoy**, Incident Response Manager, Ernst & Young*

Connecting the Zero-Day Dots: Using Data Visualizations of Open Source Intelligence to Uncover Attack Patterns
***Roselle Safran**, Co-Founder/CEO, Uplevel Security*

Threat Intel: Let's Do This!
***Dominique Kilman**, Manager, KPMG, LLP*

Opportunities for the Application of Threat Intelligence: From "Actionable" to "Acted Upon"
***Michael Lotas**, Chief Cyber Security Architect , General Dynamics Fidelis Cybersecurity Solutions*

Operationalizing Self Sourced Threat Intel
***Ray Strubinger**, Security Event Response Team Lead, Ernst & Young*

Six Approaches to Creating an Enterprise Cyber Intelligence Program
***Joshua Ray,** Director, Cyber Security Intelligence, Verisign iDefense*

Cyber Intelligence FAILS
***Rob Lee**, Fellow, 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.

5:30-6:30 pm

Networking Reception & Vendor Showcase

(LOCATION: EXHIBIT HALL – GLOVER PARK A)

Join your fellow Summit attendees and vendors
for networking and refreshments in the Exhibit hall.

SANS Investigative Forensic Toolkit (SIFT) Workstation Version 3.0

The SANS Investigative Forensic Toolkit (SIFT) Workstation is a free toolkit that can match any modern forensic tool suite. SANS' SIFT is made available to the DFIR community as a public service and is frequently updated. It demonstrates that advanced investigations and responding to intrusions can be accomplished using cutting-edge open-source tools.

digital-forensics.sans.org/community/downloads

Agenda

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

Summit presentations will be posted via the following URL, ***https://digital-forensics.sans.org/community/summits,*** *within 5 business days. An email will be sent to all attendees once live.*

Portions of the Summit may be video-recorded. These videos may be used for marketing or other purposes, but will not be available for distribution or viewing on demand at this time.

Tuesday, February 3

8:00-9:00 am

Registration & Coffee

(LOCATION: DUPONT FOYER)

9:00-9:45 am

DNS As A Control Point For Cyber Risk

Dr. Paul Vixie*, CEO and Chairman, Farsight Security, Inc.*

Nothing good or bad can happen on the Internet without invoking and involving the Domain Name System (DNS). DNS offers a commanding view of both the local and global Internet, but also offers a chokepoint in cyberspace where it's possible to put a guardhouse and checkpoint. In addition, DNS is a source of risk in its own right, in terms of DDoS amplification, registrar/registry compromise, poisoning, and protocol or code vulnerabilities. In his presentation, Dr. Paul Vixie will give a whirlwind tour of cache poisoning, DNSSEC, DDoS, rate limiting, DNS Firewalls with RPZ, and passive DNS monitoring. Attendees can expect to leave with a new appreciation for DNSs risks, and new awareness of DNSs opportunities.

9:45-10:15 am

Networking Break & Vendor Showcase

(LOCATION: EXHIBIT HALL – GLOVER PARK A)

10:15-11:15 am

The Good, the Bad and the Ugly: Lessons Learned from Operation SMN and What We Would Do Differently

MODERATOR:

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

PANELISTS:

Rich Barger*, CIO/Director of Threat Intelligence, ThreatConnect, Inc.*
Brian Bartholomew*, Lead Technical Analyst, iSIGHT Partners*
Zachary Hanif*, Director of Applied Data Science, Novetta*
Nick Levay*, CSO, Bit9+CarbonBlack*

Operation SMN examines a multi-year Chinese government-sponsored cyber espionage operation which was directed against governments and the world's largest companies. The Operation was brought to light by multiple security leaders coming together to collaborate and precisely deliver an effects-based solution for their common customers and the internet as a whole. This session takes apart Operation SMN and the threat group Axiom, and examines in-depth how over 10 private industry companies banded together to take down one adversary. Whether you're familiar with Hikiti, Moudoor, Hidden Lynx, or Aurora; this family of malware's days were numbered. We'll review the strategic reasons why and the tactics of how these industry partners shared their knowledge with one another to achieve their common goal.

11:15 am - 12:00 pm

Maltego Kung-Fu: Exploiting Open Source Threat Intelligence (OSINT) To Gain Strategic Advantage Over Your Adversary

***Matt Kodama**, VP, Recorded Future*

There exists on the open web, an entire universe of valuable open source intelligence (OSINT) containing Analysis on malicious code and infrastructure as well as key indicators of compromise (IOCs) and techniques tactics and procedures (TTPs) associated with specific threat actors or groups of actors, be they organized gangs of underground cyber criminals, terrorist organizations or foreign nation-state sponsored espionage campaigns. In the world of Cyber Threat intelligence, misattribution, confusion, false information and collusion, inadequate collection tools and techniques are often the adversary's greatest strength in their persistent attempt to successfully conduct malicious attacks and campaigns targeting private companies, government organizations and the general public at large.

Discovering and validating new and relevant IOCs and TTPs to strengthen your cyber threat intelligence operation can be a daunting and time consuming task, especially in a world where such gems are often closed source, isolated to specific data sets and costly to consume and maintain.

In this talk, Matt will demonstrate and provide a step-by-step walkthrough of how threat analysts can use Maltego and other tools in an optimal way to reduce the time it takes to extract, correlate and make insightful, valuable cyber OSINT data living on the open web. Additionally the talk will focus on how data collected can be used to enhance detection and monitoring content on the internal network so Security Operations can gain leverage on the adversary who seeks to do you harm.

12:00-1:10 pm

LUNCH & LEARN
(LOCATION: DUPONT BALLROOM)

Presented by

Controlled Collaboration for Large Enterprises

***Trish Cagliostro**, Senior Cybersecurity Architect*

In the war for information, the adversary has one key advantage…collaboration. There's no barrier preventing cyber criminals from joining forces to attack organizations. With bot army's and sophisticated malware RATs, the enemies resources are limitless. It's time to take control and turn the tables by enabling our own community. Real-time threat indicator sharing is now a possibility. Join other like-minded security professionals to create a collective defense grid by sharing threat intelligence.

LUNCH & LEARN
(LOCATION: FOXHALL BALLROOM)

Presented by

Do More with Less: Winning the War with Open Source Threat Intelligence

***Matt Jonkman**, Founder and CTO*

Increasingly sophisticated and targeted malware-based attacks bypass traditional detection methods. The bad guys are always on the move, dramatically reducing the shelf life of threat intelligence. Security solutions vendors are not delivering timely threat intelligence for the most crucial attack vectors. Good news: it's relatively straightforward to build a state of the art network based detection system with open source tools and cyber threat intelligence feeds.

In this talk we will explore the latest in open source network based intrusion detection and a new generation of cyber threat intelligence feeds that you can cost-effectively deploy in your environment today. You will leave this session with a new set of tips and tricks that you can immediately use to bolster your defensive posture.

1:10-2:00 pm

The Most Dangerous Game: Hunting Adversaries Across the Internet

***Scott Roberts**, Bad Guy Catcher, GitHub*
***Kyle Maxwell**, Senior Researcher, Verisign iDefense*

Threat intelligence analysis seems like something of a black art to many people. We intend to demystify it a bit and show how hackers can uncover international criminal conspiracies and cyber spy rings from the comfort of their own caffeine delivery systems & electronic display pods. We discuss targeting based on existing intelligence and verticals. This leads naturally to a discussion of hunting via OSINT, forensics, and reverse engineering as well as tools and systems to enhance hunting effectiveness. We also discuss appropriate response efforts in terms of internal incident response and external sharing with other organizations. Open source tools and methodologies will be discussed so that attendees can begin implementing these techniques immediately.

2:00-3:00 pm

SOLUTIONS SESSION
(LOCATION: DUPONT BALLROOM)

Presented by

iSIGHTPARTNERS TANIUM™

Making Cyber Threat Intelligence Automated and Actionable in the Enterprise

***Christian Hunt**, Senior Director, Product Engineering and Technical Account Management. Tanium Inc.*
***Allan Liska**, Director of Technology Alliance Program, iSIGHT Partners*

So an alarm fires off an indicator. Now what? Who was behind the attack? What is their motivation? What are they targeting and why? In this session Tanium and iSIGHT Partners will discuss how to leverage cyber threat intelligence to find and remediate impacted systems in seconds. We will share two separate case studies in the Cyber Crime and Cyber Espionage arenas using recent attacks. You will learn how to gain situational awareness into an attack and how to pivot and hunt for additional indicators to ensure you find and remediate everything.

SOLUTIONS SESSION
(LOCATION: FOXHALL BALLROOM)

Presented by

WEBROOT®

Smarter Intelligence: Real Time, Contextual, and Predictive

***Patrick Kennedy**, Vice President and Security Evangelist, Webroot*

Identifying unknown threats before they cause damage has been virtually impossible, until now. Predictive Threat Intelligence combines big data architecture and advanced data science to capture and analyze massive amounts of real-world data in real-time and apply deep data correlation across multiple threat vectors. Learn how you can more accurately identify active threats that go undetected today, as well as objects that represent a higher than normal risk of a future attack.

3:00-3:20 pm

Networking Break & Vendor Showcase
LOCATION: EXHIBIT HALL – GLOVER PARK A

3:20-4:00 pm

Reconciling Objective Data with Analytical Uncertainty

***Ruth Cuddyer**, Lockheed Martin CIRT*

This talk will focus on the different sources of analytical uncertainty in traditional and cyber intelligence, where to draw lines between known data and assessed conclusions, and discuss how similar methods can be used to address analytical uncertainty within both traditional and cyber intelligence analysis. Examples will be pulled from current geopolitical events and cyber security blog posts and whitepapers.

4:00-5:00 pm

A Case Study in Competing Hypotheses

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

The discipline of strategic intelligence analysis leverages a process known as Analysis of Competing Hypothesis to structure, qualify, and ensure the best possible conclusions. This process is what is behind many of the assessments provided to high-level US decision-makers from the intelligence community, and adds an element of science to what is otherwise very much an art form. We will discuss when this process is applicable to CTI analysis, and as a group (including the audience) come to a conclusion about a disputed, relevant news item based on publicly-available evidence. Participants should take away the fundamental tenets of ACH, their applicability, and a more nuanced position on recent news impacting the domain of Cyber Threat Intelligence.

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

Core Security Technologies
Core Security provides the industry's first comprehensive attack intelligence platform offering advanced analytics to prioritize, validate and ultimately eliminate security threats. With Core Security, enterprises and security professionals focus on the most likely threats to their business by modeling, simulating and testing the actions of an actual attacker. Core Security helps more than 1,400 customers worldwide identify the most vulnerable areas of their IT environments in order to improve their remediation efforts and better secure their business. The Company's patented, proven, award-winning enterprise products and solutions are backed by more than 15 years of applied expertise from CoreLabs research and Core Security Consulting Services.

DomainTools
DomainTools cyber threat intelligence solutions give organizations the ability to assess threats, map of criminal activity and prevent future attacks. DomainTools' 12 years of domain name, DNS and related 'cyber fingerprint' data across the entire Internet is why Fortune 500 security teams and online fraud investigators use DomainTools for threat investigation and mitigation work.

Digital Shadows
Digital Shadows is a UK-based cyber intelligence company that helps clients discover sensitive data exposed through social media, cloud services and mobile devices. It also identifies which hostile groups are targeting its client base. From its Canary Wharf headquarters, Digital Shadows serves clients around the world, including some of the world's largest banks.

Emerging Threats
Over 500 organizations in more than 40 countries trust cyber threat intelligence products from Emerging Threats to protect them from today's advanced cyber attacks. Emerging Threats is committed to providing our customers with the most timely, accurate and meaningful cyber threat intelligence available. For more information, visit www.EmergingThreats.net.

Farsight Security
Founded in 2013 by Internet pioneer Dr. Paul Vixie, Farsight Security, Inc. delivers real-time, contextual Threat Intelligence enrichment solutions for faster, more precise detection and response to today's cyberthreats. Farsight solutions include DNSDB™, SIE™, WHOIS Domain and NOD™. The company is headquartered in San Mateo, California.

iSIGHT Partners
iSIGHT Partners is the leading global provider of cyber threat intelligence. With 200+ experts in 16 countries and expertise in 24 languages, only iSIGHT can deliver the full context and intent of the most damaging threats, allowing security organizations to respond faster, defend proactively, and invest smarter.

EXHIBITORS

LogRhythm
LogRhythm, the leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company's patented and award-winning platform uniquely unifies next-generation SIEM, log management, network and endpoint forensics, and advanced security analytics.

Lookingglass Cyber Solutions
Lookingglass Cyber Solutions is the world leader in threat intelligence management combining global network situational awareness with automated Internet intelligence to support threat, security and risk operations. Lookingglass enables security professionals to navigate, investigate, analyze and research relevant, context-enriched threat information through a single platform. The Lookingglass Scout platform provides aggregated access to Lookingglass' industry-leading, extensive and diverse threat sources alerting organizations to impending risk while maximizing effectiveness and efficiency. For more information, visit www.LGScout.com

OPSWAT
OPSWAT's innovative solutions for secure data workflow deliver advanced threat protection through scanning data with many anti-malware engines and sanitizing documents to prevent unknown threats. We enable customers to easily adapt our solutions to their existing infrastructure to add control over the flow of data into and out of secure networks.

RecordedFuture
RecordedFuture arms you with real-time threat intelligence to proactively defend your organization from cyber attacks. Our patented Web Intelligence Engine indexes and analyzes the open web to provide you full context into emerging threats. Four of the top five companies in the world rely on Recorded Future to understand and mitigate threats.

SenseCy
SenseCy, a unique, proactive cyber threat intelligence company, serves as a one-stop shop for all cyber intelligence needs. SenseCy offers a unique blend of technical and linguistic experts who provide tailored, actionable intelligence, in real-time. SenseCy clients receive regular alerts and cyber threat assessments for their specific areas of interest.

SentinelOne
SentinelOne is reinventing endpoint security to protect organizations against advanced threats and nation state malware. The company uses predictive execution modeling to detect and protect all devices against targeted, zero day threats in real time. SentinelOne was formed by an elite team of cyber security and defense experts from Intel, McAfee, Symantec, Checkpoint, IBM and the Israel Defense Force

EXHIBITORS

SurfWatch Labs

SurfWatch Labs delivers powerful cyber risk intelligence analytics and applications through a business intelligence approach that helps organizations improve their long-term cyber resiliency. Created in 2013 by former US Government intelligence analysts, SurfWatch Labs solutions go beyond the low-level threat data and security tactics that organizations can drown in, by providing insights into cyber risks and their impact on key business operations. SurfWatch Labs: Cyber In Sight. For more information, visit **www.surfwatchlabs.com**.

Tanium

Tanium provides the unique power to secure, control and manage endpoints across the enterprise within seconds. Serving as the "central nervous system" for enterprises, Tanium empowers security and IT operations teams to ask questions about the state of every endpoint, retrieve data on their current state, and execute change all within seconds.

ThreatConnect

ThreatConnect® is the most comprehensive Threat Intelligence Platform (TIP) on the market. ThreatConnect delivers a single platform in the cloud and on-premises to aggregate, analyze, and act to counter sophisticated cyber-attacks. Leveraging advanced analytics capabilities, ThreatConnect offers superior understanding of relevant cyber threats. To learn more, visit: **www.threatconnect.com**.

ThreatStream

ThreatStream offers the first-ever community-vetted cyber security intelligence platform that aggregates millions of threat indicators from around the internet and integrates them directly to an organization's existing security infrastructure. ThreatStream provides businesses and governments visibility into newly discovered security threats so they can proactively defend against malicious attacks.

Webroot

Webroot leverages the power of an intelligent cloud architecture to deliver real-time predictive threat detection and endpoint security to 27+ million consumers, businesses and enterprises worldwide. Our BrightCloud® Security Services are embedded in leading security vendors' offerings, and our SecureAnywhere® endpoint security provides advanced threat forensics, blocking and auto-remediation of threats in <1MB agent. It's time for smarter security.