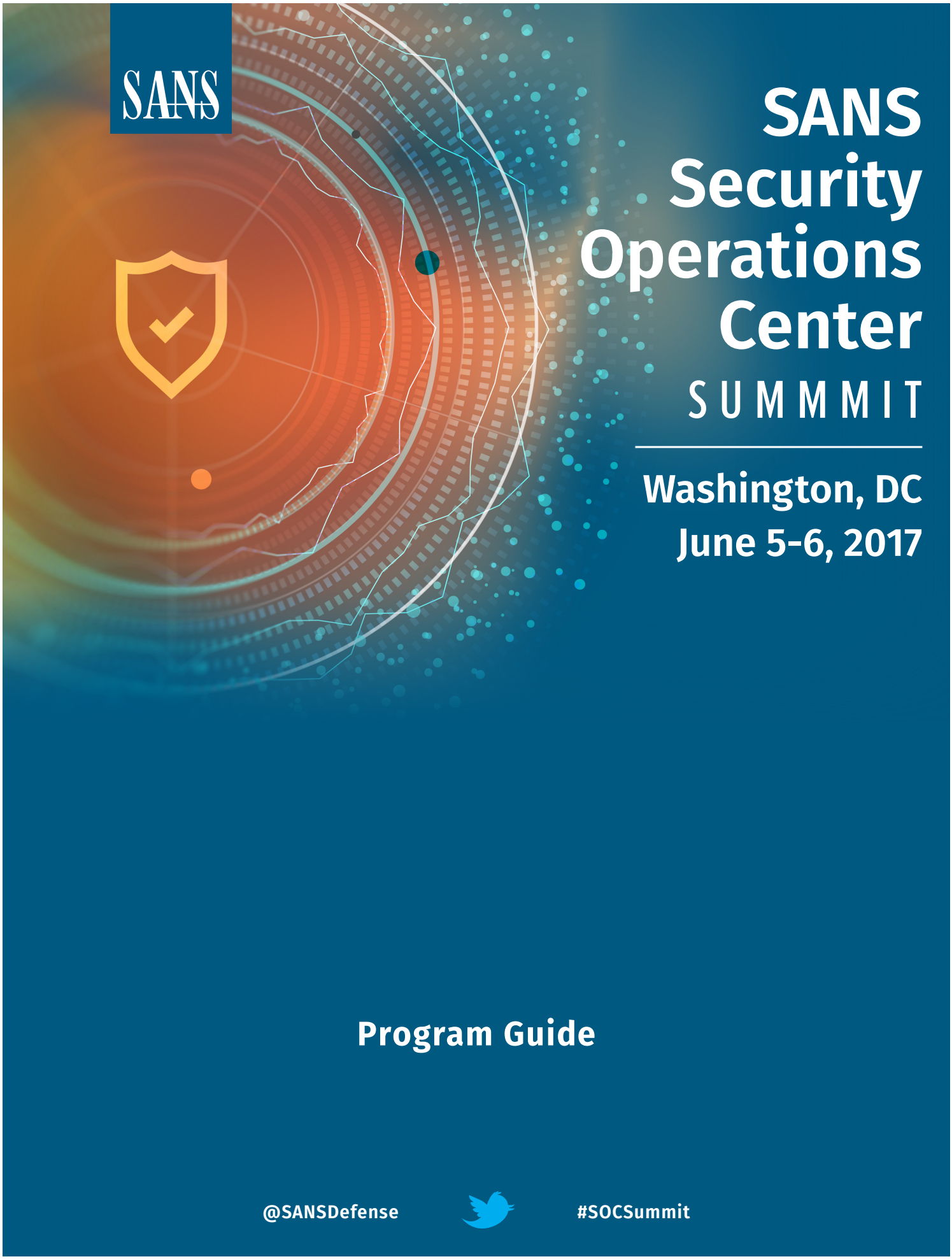

SANS Security Operations Center SUMMMIT

Washington, DC
June 5-6, 2017

Program Guide

@SANSDefense #SOCSummit

Agenda

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

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

Monday, June 5	
7:45-8:45am	**Registration & Coffee** (LOCATION: CRYSTAL BALLROOM FOYER)
8:45-9:00am	***Welcome & Introductions*** ***Eric Conrad*** *(@eric_conrad), Summit Co-Chairs, SANS Institute* ***Chris Crowley*** *(@CCrowMontance), Summit Co-Chairs, SANS Institute*
9:00-9:45am	***Good vs Evil: Winning the Age Old Battle*** The epic struggle of good versus evil has existed since time began. Throughout history, this battle has evolved to new battlefields. Today, evil is attacking good on a digital battlefield. How are you going to monitor and defend your digital assets against those who would cause you harm? How are we as a community going to work together to defeat evil? ***Doug Burks*** *(@dougburks), CEO, Security Onion Solutions LLC*
9:45-10:30am	***Stuck in the Box: A SIEM's Tale*** Organizations often spend excessive amounts of money on SIEM products only to end up with a log collection box when they thought they purchased a tactical detection system. Most organizations find themselves with a SIEM but unsure how to use its capabilities. Point solutions are quick to defend deficiencies by stating each environment is different so you, the customer, must tell them what you want the SIEM to do and then they'll help with professional services or by replacing your current SIEM with something "better and more advanced." This is complete hogwash. Organizations tend to have a lot of overlap such as the use of Windows systems or network protocols such as DNS. As such there are high fidelity detects that can be implemented in every organization. Enough is enough. If you are looking for techniques and methods to get value out of your current SIEM or are interested in seeing how a new open source big data solution such as the Elastic Stack, formerly ELK, most likely can beat what you have today then this talk is for you. Fact is that it is time to think outside the box. Come find out how one organization spent fourteen months deploying a top magic quadrant SIEM solution to have it beaten by ELK in two weeks. ***Justin Henderson*** *(@SecurityMapper), Systems and Security Architect, GSE # 108, Cyber Guardian Red/Blue*
10:30-10:50am	**Networking Break and Vendor Expo** (LOCATION: SALON CDE)

Monday, June 5

10:50-11:35am	***How to Measure Anything in the SOC*** No matter the size or sophistication level of your SOC, you need analytics not only for your SOC to be effective, but also to justify all the resources you pour into it. Drawing on research from How to Measure Anything in Cybersecurity Risk (Wiley 2016), we'll delve into how to develop meaningful metrics that give you the edge over the adversary. ***Rich Seiersen**, Former General Manager – Cyber Security & Privacy, GE Healthcare*
11:45am-12:30pm	**Solutions Sessions**

The Silver Bullet vs. "The 5-Point-Palm Exploding Heart Technique"

ARBOR NETWORKS

In the world of Security analysis and incident response you have so many choices. Please join Arbor's Paul Bowen for a discussion and presentation on Point Solutions to help with this or Centralized Security monitoring, and find out why he feels that building a security practice is the better way to go. Don't just choose a solution, have a plan for the future and build upon your past.

***Paul Bowen**, Principal Security Technologist, Arbor Networks*

LOCATION: JACKSON ROOM, MEZZANINE LEVEL

Get More From Your SOC With Open Source

Recorded Future

Security operation centers (SOC) are typically pressed for time due to the immense amount of data being monitored. Threat feeds assist SOCs in surfacing relevant events to the forefront for analysis. During this talk, we will focus on creating your own unique custom threat feed with high fidelity indicators from existing open source data. More specifically, threat feeds pertaining to the following:

- File hashes of samples submitted to websites like VirusTotal, but not distributed to antivirus vendors or sold to security researchers. These are typically used by malicious actors to test their malware before distributing.
- Command and control (C2) servers in malware configuration files posted on paste sites and code repository sites.

***Daniel Hatheway**, Senior Technical Analyst at Recorded Future*

LOCATION: HARRISON ROOM, MEZZANINE LEVEL

Case Study: Tripling Incident Response Capacity with SOC Automation and Orchestration

CYBERBIT
PROTECTING A NEW DIMENSION

This case study was developed in collaboration with the SOC manager of one of Israel's top 3 banks. It is intended for SOC managers, SOC teams and security executives interested in optimizing SOC performance and incident response capacity. The session will review the strategy by which the bank's SOC manager substantially improved his primary KPI's over a period of 9 months. These included: reducing time to response by 70%, and increasing the number of incidents closed within 6 hours from 30% of the incidents to 80%. The session will provide live demonstrations of SOC automation and orchestration tactics that were used to achieve these results.

***Ofir Barzilay**, VP R&D, Cyberbit*

LOCATION: WILSON ROOM, MEZZANINE LEVEL

12:30-1:30pm	**Vendor Expo & Lunch** (LOCATION: SALON CDE)

Monday, June 5

1:30-2:00pm	***Metrics for Justifying SOC Investment to the CEO and Board*** The SOC paradox: A mature, effective and efficient Security Operations Center can often provide the answers to cybersecurity status and risk questions that CEOs and Boards of Directors are asking. However, to implement, staff and enhance real SOC processes and capabilities, security managers often need to get resources for security technology, hiring and training. Making sure your SOC collects the right data and produces meaningful metrics that can satisfy both operational cybersecurity demands and answer those questions from the Board is key to solving that paradox. In this session John Pescatore will take a What Works look at how Boards of Directors think about cybersecurity, what answers they are looking for and show examples of SOC-centric data and metrics that are key to convincing management to fund SOC establishment, evolution and operation. ***John Pescatore**, Director of Emerging Security Trends, SANS Institute*
2:00-2:45pm	***Debunked: Traditional IR Calls*** It's Friday night "IR Night," 5pm and you get the call. After some initial information is collected, inevitably the next first step is to spin up an IR bridge. Rapidly the various teams join; incident managers, server and network, application analysts and the incident response lead. 90%+ of IR teams will convene on a conference line – and that method negatively constrains communication and synergy. Leveraging visual techniques in training is proven to increase speed of understanding and depth of retention by an additional 80%. So why don't IR teams everywhere do this? In this presentation, attendees will learn why they should – for every IR event. Attendees will learn about the "Storyboard" Incident Response Methodology, a simple, effective, repeatable, and extremely visual methodology. And did we mention no cost? ***Gregory Braunton**, National Director, Threat Management, Incident Response and Forensics, Catholic Health Initiatives*
2:45-3:30pm	***Siri for SOC: How an Intelligent Assistant can Augment the SOC Team*** Security operation center (SOC) teams are burdened with a deluge of alerts, repetitive processes for data analysis, and lack of skills and tools to stop advanced threats. To address these challenges, it is crucial to empower junior analysts to stop advanced threats, before damage and loss occurs. Digital assistants like Siri or Alexa have proved their ability to give time back to our day by tackling tasks, a security chatbot can streamline workflows, perform complex tasks, and make recommendations to the SOC analyst to alleviate alert fatigue. Using a combination of subject matter expertise from SOC analysts and the power of machine learning, Chatbots can help teams overcome resource shortcomings by using conversation to offload data collection and guide analysts through recommended courses of action. This process provides an intuitive interface to remediation/investigation workflows and complex storage structures so the analyst can spend less time on collection efforts and more on analysis and response. ***Bobby Filar** (@filar), Sr. Data Scientist, Endgame* ***Rich Seymour** (@rseymour), Sr. Data Scientist, Endgame*
3:30-3:45pm	**Networking Break and Vendor Expo** (LOCATION: SALON CDE)

Monday, June 5

3:45-4:30pm	***Recipe for Continuous Security Improvement*** When it comes to security, the problem is getting worse by a factor of 4x. Recent data shows that organizations will allocate 80% of their security spend on better point-based solutions and disregard best practice processes that can create an ultimate back-stop for security threats. This is evident by the average security spending per year vs security breaches per year. Security breaches are now outpacing security spending by a factor of 4:1 and the DHS recently indicated that 85% of organizations today have been breached and they just don't know it yet. IP Services and IT Process Institute will review and share best practices for, among other things, managing change/configurations, inventorying assets, implementing effective release management, and deploying controls that are both visible and auditable. By implementing these processes, organizations can install a system of continuous improvement that meets today's security and compliance challenges while ensuring that business objectives are met. ***Scott Alldridge**, CEO, IP Services*
4:30-5:15pm	***The Need for Investigation Playbooks at the SOC*** As SOCs mature and start to formalize their operations, they typically focus on preparedness, escalation process and incident response plans. However, even with these plans in place, SOCs report that 25% of the alerts are not triaged and that investigations take too long. Why so? In many cases, this can be attributed to the lack of a standardized investigation process and community wide tools that can be applied consistently & repeatedly over time, preventing less experienced analysts and incident responders from doing their job effectively. In this talk, Ismael Valenzuela (Certified SANS Instructor, GSE #132 and Global Director of Foundstone Consulting Services), and Matias Cuenca-Acuna, (Principal Engineer at McAfee), will showcase how SOC investigations can be presented as an iterative process of postulating hypotheses and answering questions in the pursuit of an outcome. Using this approach, they will show how to use Markdown to capture investigation playbooks and how they should be structured so they can be effectively used by SOC analysts and incident responders. ***Matias Cuenca-Acuna**, Principal Engineer, McAfee* ***Ismael Valenzuela**, SANS Certified Instructor, GSE #132; Global Director - Foundstone Consulting Services*
5:15-6:15pm	**Networking Reception & Vendor Expo** (LOCATION: SALON CDE)

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.

@SANSDefense **#SOCSummit**

Tuesday, June 6

9:00-9:45am	***Survey Says: Actionable Insights from the SANS SOC Survey*** SOCs need to provide active defense against live, often unknown threats, while measuring their security success with metrics. Just how satisfied are organizations with their SOCs in these areas? Do they experience better service with cloud-based managed providers or are in-house SOCs most effective? And what did respondents to the new SANS SOC survey indicate that they'd like to see in their future SOCs? Chris will share actionable insights and recommendations based on the findings from this survey so you can capitalize on the wisdom of the hive mind and learn from others' mistakes without having to repeat them. ***Chris Crowley*** *(@CCrowMontance), SANS Institute*
9:45-10:30am	***SIEMple Simon Met a WMIman*** While a SIEM is primarily designed to gather logs and events from network devices such as servers, routers, firewalls, IDS and Anti-Virus, the truth is a SIEM will accept and process just about any type of data you can throw at it. Therefore, you can greatly enhance the data you are collecting live on the network by comparing it to static (or semi-static) data you can gather directly from the enterprise via PowerShell scripts or WMI commands. The data you manually gather (or schedule on a periodic basis) is used as a baseline or a reference to make sure the live data remains within a certain boundary. My talk will provide several examples of the scripts used, the data captured and how the comparison to live traffic enables SOC personnel to have better situational awareness of the security posture of their network by detecting possible suspicious behavior. This presentation will demonstrate how to use simple PowerShell scripts and WMI commands to gather information about your enterprise, feed that information into your SIEM and produce valuable reports, alerts, and dashboards to enhance the ability of your security and operations personnel to monitor and respond to issues on your network. ***Craig L. Bowser****, Sr. Security Engineer, Dept. of Energy*
10:30-11:00am	**Networking Break and Vendor Expo** (LOCATION: SALON CDE)
11:00-11:45am	***Inattentional Blindness (IB) & Security Monitoring*** Inattentional blindness (IB), also known as perceptual blindness, is a psychological lack of attention that is not associated with any vision defects or deficits. In my experience, security analysts fall prey to this phenomenon as part of the security event triage process. This talk will examine the phenomenon of IB is and provide examples of how we tend to laser focus on the obvious (IPs, URLs , ports), causing us to miss potential threats. This presentation will include screen shots of packet captures and events to illustrate and drive home the notion that IB can be a cognitive enemy of security analysis. ***Ismail Cattaneo****, Sr. Manager of Security Operations & Engineering, Verizon Enterprise Solutions*

Tuesday, June 6

11:45am-12:15pm	***Hunting Adversaries with "rastrea2r" and Machine Learning*** Usually, hunting requires a lot of digging in enormous amounts of data, sometimes these data has to be gathered from endpoints and then analyzed. The type of analysis, the tools and the methodology that are used change among analysts. Such variability make reusability harder as each analyst uses its own scripts with its own abstractions. In order to avoid such duplicability of efforts, we present a simple set of tools consisting of 1. a simple client/server architecture based on rastrea2r to gather endpoint snapshots from the endpoint, 2. a python SDK that provides a layer of abstraction over the data that has been gathered, 3. a ML library that will mine that data and 4. a reporting tools that generates a report of all the findings. At this phase, the ML library contains algorithms for detecting visual spoofing on process names. ***Gabriel Infante-Lopez**, Principal Engineer, McAfee* ***Ismael Valenzuela**, SANS Certified Instructor, GSE #132; Global Director - Foundstone Consulting Services*
12:15-1:30pm	**Lunch & Learn**

The Agile SOC: Applying the Scrum Framework to Your Security Operations

cybereason

Using an Agile methodology can empower SOC managers and their teams to move at the speed of modern business and become enablers of innovation and growth. The Scrum/Kanban methodologies can put your SOC in a position to embrace the elastic nature of information security and better align with business objectives. Join Justin Erdman, Cybereason Senior Security Specialist, as he discusses how you can get the best from your SOC:

- Learn the principles of two Agile methodologies and why they are well-suited for InfoSec
- Hear a brief case study on his experience adopting Scrum/Kanban and how it continuously provides a system for facilitating rapid change
- See how Scrum/Kandan can work in your SOC and how it can advance your team by changing attitudes toward teamwork and collaboration

***Justin Erdman**, Security Incident Response/Research*

***Chris Bush**, Senior Director, Security Services*

LOCATION: JACKSON, MEZZANINE LEVEL

Tuesday, June 6

Cover Your In-Memory Blind Spots: Stop Fileless, Malwareless attacks

ENDGAME.

Enterprises are constantly targeted by cybercriminals stealing millions of dollars, often causing damage and destruction. These targeted attacks are 100% successful and are not just malware. Targeted attacks, such as Dridex, Shamoon2 and Odinaff, use sophisticated techniques once available to nation state actors, like evading defenses by hiding in memory. These attacks have proliferated and are now in the hands of criminal groups and hacktivists, bypassing existing enterprise security defense stack.

With the rise of fileless and malwareless attacks, security analysts must protect endpoint memory to stop adversaries from gaining foothold on endpoints. In this session, we will discuss real-world targeted attacks and their sophisticated techniques often used by attackers to hide their presence within enterprise networks. Join our lunch and learn session and learn how a SOC analyst can stop targeted attacks, before damage and loss occurs.

***Braden Preston**, Principal Product Manager*

LOCATION: HARRISON, MEZZANINE LEVEL

Advanced Threat Protection: DDos to Endpoint

STRATEGIC INTEGRATORS

Today's cyber attacks are bigger, last longer and are more sophisticated than ever before. Strategic Integrators and their partners will discuss how to anticipate threats like ransomware and end-point vulnerability and intelligently apply powerful technologies to stop them.

***Brian Lahoue**, VP of Technology and Sales, Strategic Integrators*

***John Fahey**, Senior Security Architect, Comodo*

***James Willett**, VP of Product Management, Neustar*

LOCATION: WILSON, MEZZANINE LEVEL

1:30-2:15pm	***Color My Logs: Understanding the Internet Storm Center***

The Internet Storm Center is a global collaborative information security community. Founded originally in 1999 as incidents.org, the Internet Strom Center in collaboration with DShield is a unique open resource to explore global threats, understand the attack "background radiation" and find more context for events you may be investigating. The Internet Storm Center offers several data feeds, APIs and tools to help you add "color" to your events, and to allow you to share data easily. You will learn how to use these data feeds and how to integrate them into your tools. You will also learn how to collaborate and contribute to the Internet Storm Center's data collection and how to give back to our global information security community.

***Johannes Ullrich, PhD**, Dean of Research, SANS Technology Institute*

Tuesday, June 6

2:15-3:00pm	***SOCs for the Rest of Us*** In this talk we will discuss key traits of some of the largest and most successful security operations centers we've visited over the last two years. From automating tier-1 to integrating investigations into Slack channels, from curating toolchains to cutting out threat feeds, we'll cover what's working well and what challenges remain. Many industry verticals will be represented including financial services, multi-national conglomerates, entertainment, healthcare, energy, defense, technology, and dynamic internet startups. ***Dave Herrald*** *(@daveherrald), GSE #79, Senior Security Architect, Splunk* ***Ryan Kovar*** *(@meansec), Staff Security Strategist, Splunk*
3:00-3:15pm	**Networking Break and Vendor Expo** (LOCATION: SALON CDE)
3:15-3:45pm	***Building the Cybersecurity Workforce We Need: Creating Pipelines and Pathways Without Poaching*** While cybersecurity has become a focal point of media and public attention in recent years due to a series of high-profile hacks (e.g. OPM, Sony), the real crisis often goes ignored – the cybersecurity talent shortage. There simply are not enough qualified candidates to fill the available positions across the public and private sectors in the United States, much less around the world. In response, HR and hiring managers continue to recruit from the same pools of existing professionals, poaching from one another but acting surprised about the shortage of talent and constantly rising salaries. Innovative approaches and strategies are needed to develop new sources for talent that are time-to-market sensitive and will help employers in both the short- and long-run. ***Arlin Halstead****, Strategic HR Business Partner, NTT Security* ***Maxwell Shuftan*** *(@SANSCyberTalent), Director of CyberTalent Solutions, SANS Institute*
3:45-4:30pm	***DDoS Attacks in Action*** This session will explore active DDoS attacks in the SOC of a victim through a live demonstration. We'll share the current trends we're seeing in the wild, predictions for the next round of threats, and pointers for developing effective defense strategies. ***Ben Herzberg****, Security Research Group Manager, Imperva Incapsula*
4:30-4:45pm	***Closing Remarks*** ***Eric Conrad*** *(@eric_conrad), Summit Co-Chairs, SANS Institute* ***Chris Crowley*** *(@CCrowMontance), Summit Co-Chairs, 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.

@SANSDefense **#SOCSummit**