SANS

SIEM Summit

Weaponize Your Data

Program Guide

@SANSDefense #SIEMSummit

Agenda

All Summit Sessions will be held in the Rosemont C/D (unless noted otherwise).

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

Monday, October 7

7:00-9:00 am

Registration & Coffee (LOCATION: ROSEMONT C/D FOYER)

9:00-9:50 am

Keynote: Untapped Potential: Getting the Most out of Your SIEM

SIEMs are not a tool we can afford to under-utilize, yet many organizations still have sub-par, underperforming deployments that analysts don't enjoy using. While many of us do a decent job of the basics, we still often miss both low-hanging fruit and many simple to implement but non-traditional sources we could harness to greatly increase our detection capabilities. This talk will cover some of the most important data sources and use cases that are often missed, as well some commonly overlooked data sources that can add tremendous value. The goal will be to help illuminate gaps you may have, give you some new clever detection ideas, and point to the tools that will help you fix the problems.

Justin Henderson*, @SecurityMapper, Summit Co-Chair*

John Hubbard*, @SecHubb, Summit Co-Chair*

9:55-10:30 am

Get the Basics Right!

Most organizations deploy SIEM to serve two main purposes: achieve compliance and improve their security posture. Although there are multiple compliance-related frameworks specific to each industry, assessing existing security posture is a challenge. Hence, organizations leverage SIEM solutions for this purpose, but they fail to tap its true potential due to high volumes of data, lack of proper detection rules, and high false-positive rates. In most cases, SIEM solutions are deployed by third parties, and we need to ask those parties the right questions in order to have a high degree of confidence on detection capabilities and further improve security posture. This talk focuses on identifying the blind spots where the necessary data are not available; baselining rules and mapping them to threat categories; identifying areas where a SIEM solution is not enough for investigation; and examining automation strategies to reduce the mean time to detect and respond to incidents. We will provide a checklist that helps an organization go through all the phases from risk assessment to post-SIEM deployment maintenance. This checklist is neither industry- nor vendor-specific but serves as a holistic reference guide for any organization.

Balaji Nakkella*, Senior Consultant, Deloitte Canada*

Rakesh Kumar Narsingoju *@Rakeshwill, Solution Delivery Advisor, Deloitte US-India*

10:30-11:00 am

Networking Break (LOCATION: ROSEMONT FOYER)

11:00-11:35 am

We Need to Talk about the Elephant in the SOC

Why have we accepted alert fatigue as a normal occurrence in the Security Operations Center (SOC)? And why are we compounding the problem by whitelisting and suppressing the noise to the point where we have essentially created a situational security numbness within the enterprise? Our data are trying to tell us a story. The MITRE ATT&CK framework helps us figure out where we are in terms of our ability to tease the story from the data while simultaneously providing guidance for building out our own threat models. In this talk, we will go into detail to describe a trend we are seeing that introduces a layer of abstraction between detection analytics and the alerting process; both align nicely with ATT&CK and also account for user/system-specific context when scoring anomalous or interesting behavior. Attendees will learn how an organization of any size can transform its SOC quickly by reducing the alert overload, improving its false positive rates, adding data/analytics without scaling up the number of analysts, and aligning against a framework of its choice.

Jim Apger *@JimApger, Security Specialist, Splunk*

Monday, October 7

11:40 am – 12:25 pm

Custom Application Behavioral Security Monitoring Using SIEM

Welcome to the Application Security Monitoring session. This presentation will take you through the roller coaster ride that is setting up security monitoring for custom applications and devices. Limited communication between business owners and security teams can leave a gap in security monitoring, which poses a threat to your company's security. This session will focus on the detailed process of setting up security monitoring for crown jewels, including the identification of business risks and relevant applications; how to define technical-use cases to cover business risks and the onboarding of data to your SIEM platform. We will also discuss the implementation of SIEM content and best practices for setting up, alerting, and follow-up.

Prithvi Bhat*, Junior Manager, Deloitte Nederland*

Himanshu Tonk *@tonkhimanshu2, Junior Manager, Cyber Risk Services, Deloitte Risk Advisory*

12:30-1:30 pm

Lunch (LOCATION: ROSEMONT FOYER)

1:30-2:15 pm

Panel: Automate All the Things

Automation and orchestration tools are clearly a new trend for integrating with your SIEM. But what is commonly automated compared to what should be automated are not always the same thing. Join us for a discussion on automation and the SIEM during which our panel of experts will be sharing their experiences on what works and what does not work when it comes to automation, as well as the major benefits and risks automation can bring to security operations. Audience participation and questions are encouraged!

MODERATOR:

Justin Henderson *@SecurityMapper, Summit Co-Chair*

PANELISTS:

Rob Gresham *@socologize, Security Solutions Architect, Splunk*

John Hubbard *@SecHubb, Summit Co-Chair*

John Stoner *@stonerpsu, Principal Security Strategist, Splunk*

2:20-2:55 pm

Company Phishing Trip: Analysis of Brand Phishing Kits and Campaigns

Individuals and companies lose hundreds of millions of dollars every year to phishing. Fast detection of phishing pages and the harvested credentials is an ever-challenging task, but all hope is not lost. Using free and open-source tools we can detect sites targeting our customers and track compromised credential use by using active defense techniques. This talk will look at how common phishing campaigns are put together; the anatomy of a phishing kit, including detailed code analysis of samples; and detection of brand phishing pages (open-source, paid, and home-grown detection). Takeaways will include how phishing campaigns work, how common phishing kits operate, and how to use active defense to detect phishing kits targeting your brand.

Jared Peck *@medic642, Cyber Threat Intelligence Analyst, Fortune 500 Financial Company*

2:55-3:20 am

Networking Break (LOCATION: ROSEMONT FOYER)

Monday, October 7

3:25-4:00 pm

The Right Data at the Right Time

Analysts and incident responders have so many tools and data sources to choose from that it can be daunting to understand what is necessary versus what is simply nice to have. When putting together a monitoring playbook, it's essential to understand what data is available to you and how it can be used for security monitoring and incident response. Enterprise analysts may have different data preferences than analysts at smaller organizations. How can detection and incident response (IR) teams effectively protect their organizations with the right data sources? How can you deliver context with raw machine data? This presentation will draw from years of experience in designing and operating world-class network security operations to help you understand the "ideal" set of data sources for security monitoring and IR for any environment; consider data sources depending on your size or threat profile; operationalize event data (extract, transform, load); and understand the evolution of your security event data. We'll look at real-world incidents involving data perceived to be undervalued, and at clever ways to use other data sources.

Jeff Bollinger *@jeffbollinger, CSIRT Investigations and Analysis Manager, Cisco*

Matthew Valites *@matthewvalites, US West Outreach Lead, Cisco Talos*

4:05-4:40 pm

A SIEM Engineer's Guide to Threat Modeling

Since becoming the center of gravity for security operations teams over a decade ago, security information and event management (SIEM) platforms have grown exponentially in terms of complexity and capability. Unfortunately, many teams have failed to grow with the technology. Content development – implementing use cases to escalate events of interest – is the best way to get more value out of a SIEM, but these efforts are often subjective and heavily reliant on the skills, experience, and biases of the content developers. How can we maximize the value of the SIEM for our home organizations in a consistent and scalable way? Threat modeling is a great starting point.

Historically focused on reducing risk in application development, threat modeling at the organizational level can help identify and prioritize defensive measures for the most critical parts of your business. Visibility gaps, key users and assets, and other critical variables are outputs of this process, which compliment knowledge bases and detection frameworks like MITRE ATT&CK and the Diamond Model. In this talk, I'll identify reasons why most ad hoc content engineering ultimately fails, and discuss more effective, repeatable approaches to threat modeling that will drive continuous use case development and help your organization get maximum return on its SIEM investments.

Mark Orlando *@markaorlando, CTO, Raytheon Cyber Protection Solutions*

5:30-7:30 pm

Summit Night Out (LOCATION: BUB CITY ROSEMONT, 5441 PARK PL, ROSEMONT, IL 60018)

After a long day of learning, join speakers and fellow attendees at Bub City Rosemont, a Chicago staple for food, music and fun. Complimentary BBQ and drinks will be provided.

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.

Tuesday, October 8

7:00-9:00 am **Registration & Coffee** (LOCATION: ROSEMONT FOYER)

9:00-9:45 am ***Keynote: How I Learned to Stop Worrying and Love TLS***

Encryption has been the security tool most disliked by security people charged with monitoring networks. While it hides secrets from attackers, it also hides malicious activity and exfiltrated secrets from network monitoring. While the fight against encryption may seem lost (or the fight to encrypt all data may seem won), there is more that you can do than turn your IDS into a crypto coin miner. Think outside of the traditional IDS box, and before you despair, remember that it didn’t do much for you anyway except to produce false positives. Networks change and so need your skills and approaches to finding evil. In this talk, you will learn about all the useful things you can do once you leave the superficial glamour of analyzing payloads behind and focus on the data that matters. Become one with your network and understand its needs and desires to identify the new evil your IDS never told you about.

Dr. Johannes Ullrich *@johullrich, Fellow, SANS Institute*

9:45-10:15 am **Networking Break** (LOCATION: ROSEMONT FOYER)

10:15-10:50 am ***Techniques to Reduce Alert Fatigue in Security Analysts***

Alert fatigue is real. Security analysts face a huge burden of triage because they not only have to sift through a sea of alerts, but also correlate them from different products manually or by using a traditional correlation engine. This talk describes the flagship machine learning system embedded within Azure Sentinel, Microsoft’s Cloud SIEM, to tackle alert fatigue. It will describe how to obtain a 90 percent reduction in alert fatigue for internal and external customers. Attendees will learn about three techniques used to reduce alert fatigue (probabilistic kill chain, iterative attack simulation, and graphical inference); a framework to combine alerts from multiple cloud services; and a design pattern to scale detection systems. We’ll then walk through the series of steps in the ML system within Azure Sentinel that go from low-fidelity alerts to security alerts, and we’ll demo this system in action combining O365 logs with Azure Active Directory alerts. The talk will wrap up with a look at a framework to combine the system, sharing how to normalize events across different products and presenting an engineering pattern design for others to build on.

Ram Shankar Siva Kumar *@ram_ssk, Data Cowboy, Azure Security Data Science, Microsoft*

Sharon Xia *@sharonxia, Principal PM Manager, Microsoft*

10:55-11:30 am ***Don’t Be a SIEMingly SOAR Loser***

This title is so perfect for this discussion. Security operations, automation, and response constitute an awesome path for security teams, whether it’s automation attached to the SIEM or a stand-alone orchestration tool. We love innovation, yet it seemingly creates such a SOAR on our seating devices. Where is the value in our SOAR products, and how long will it take until we are rewarded? Is it measured by your detection or response time? Containment, reimage, or resolution times? Is it a ticketing tool, case management, or neither? What is the difference between ticketing and case management tools? There are generally two approaches to the SOAR implementation models. One is as infinite as the ocean and the other is how you “really” work. We will explore these areas, offer suggestions, and provide some definitive truths (IMHO). We’ll use the TTP0 fractal to define our flows and I2A2 to collect that SOEL, and if you don’t SOAR after implementing those. We will demonstrate how your existing use cases or tribal knowledge can be exploited to deliver powerful automation and response, and how the human-machine team can be taken up a notch and work immediate automation into your processes that will lead to true orchestration. SOARing isn’t an easy task (even though some make it look so easy, right?) and yet all of us want to fly or be flown.

Rob Gresham *@socologize, Security Solutions Architect, Splunk*

Tuesday, October 8

11:35 am – 12:10 pm

That SIEM ~~Won't~~ Will Hunt

Hunting is not the first thought that comes to mind when someone says SIEM, is it? But do you know that SIEM can be another tool that threat hunters on the security operations team can leverage effectively as part of their hunt? This talk uses the fictional advanced persistent threat group Taedonggang to demonstrate how SIEM can be used to aid our hunt activities. We will talk about MITRE ATT&CK and the intersection of threat hunting and security operations, and how threat hunt findings should be operationalized into SIEM for the security operations team. Operationalizing refers to more than just a blacklist of IP addresses and file hashes! John Stoner will show how we can tie our findings to adversary tactics and techniques that can then have automated responses built to address these techniques as they are identified in the future. Attendees will come away with an understanding how SIEM can be used during threat hunting; knowledge of how MITRE ATT&CK can serve as a common taxonomy in SIEM for both security operations and threat hunters; ideas for how to create SIEM alerts and views based on threat hunts; and a data set and instructional application that they can take home and play with!

***John Stoner** @stonerpsu, Principal Security Strategist, Splunk*

12:10-1:15 pm

Lunch

1:30-2:05 pm

Panel: Modern Detection Despite Limitations

Many organizations are entering the SIEM arena with their hands tied behind their backs in one way or another. Uncollected endpoint data, encryption, lack of network sensors, and cloud logs all contribute to the problem. This panel will be a group discussion on what, if anything, can be done to maintain detection when business, political, and technical challenges necessitate less-than-perfect data.

MODERATOR:

***Justin Henderson** @SecurityMapper, Summit Co-Chair*

PANELISTS:

***Tim Garcia** @tbg911, Certified Instructor, SANS Institute*

***Scott Lynch**, Cyber Security Operations Manager, SSC Space U.S.*

***Dr. Johannes Ullrich** @johullrich, Fellow, SANS Institute*

2:00-2:35 pm

Hunting with Sysmon to Unveil the Evil

System Monitor (Sysmon) is a Windows system service and device driver that, once installed, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. These logs provide investigators with a wealth of information that can be analyzed in many different ways. By splitting analysis in each field of a Sysmon event alert, you can create a deeper analysis of the event itself and create a hunting view that could point you towards certain processes or behaviors in order to better analyze or find uncommon processes in your endpoints. By correlating these alerts with your network and business requirements, you can make detection more accurate and generate less noise, thereby helping your staff prioritize which events to handle first. This presentation will discuss methods to analyze and score each field from those events, ideas for implementation, projects, and results based on deployment. We'll also show how you can improve your hunting capabilities by using Sysmon as a more powerful detection vector to identify specific user behaviors and activity patterns.

***Felipe Esposito**, Senior Instructor at Blue Team Operations, BlueOps Consulting and Training*

***Rodrigo Montoro** @spookerlabs, Head of Research and Development, Apura Cyber Intelligence*

2:35-3:00 pm

Networking Break (LOCATION: ROSEMONT FOYER)

Tuesday, October 8

3:05-3:40 pm	***Rapid Recognition and Response to Rogues*** The need to detect rogue devices on a network is part of the first control listed in the CIS Top 20 Critical Security Controls, Actively Manage Inventory and Control of all Hardware Assets. There are many solutions to monitor, detect, and respond to rogue devices on enterprise networks. These include commercial, open-source, and home-grown capabilities. Each solution uses different methods to determine what is a rogue. This talk will cover several of those methods and their strengths and weaknesses, as well as the pros and cons of the different responses available to enterprises when rogues are found. The focus will be on using different techniques to show how a simple detection, which is usually just an IP address, can be enhanced to provide enough details to the analyst to speed up response decisions and even automate some responses based on business logic. We'll demonstrate this by using one rogue detection tool detect and analyze suspicious IPs by adding information to the event to make analysis easier. Then we'll look at how that enhanced event can used for automated responses. ***Craig Bowser*** *@reswob10, Senior Security Engineer, U.S. Department of Energy*
3:45-4:20 pm	***Did You Do Your Homework? Use Case-Driven SIEM Deployments*** Benjamin Franklin once said, "If you *fail to plan*, you are *planning to fail*." We have all been taught that we need to have a plan before working on the project yet how many times did you actually sit down and make one. Did you identify any requirements? Did you ask anyone else if they had requirements? Usually, the answer is, sort of. In the case of a SIEM, you need to identify the purpose and use cases behind the SIEM to be successful and minimize rework while saving money and time. We will discuss ways to identify detection techniques and how you can use various use cases such as business, compliance, customer and even post-incident/breach to help not only identify what your SIEM needs to be doing, but also how to test and validate that it is meeting your requirements successfully. ***Scott Lynch*** *@packetengineer, Cyber Security Operations Manager, SSC Space U.S.*
4:20-4:30 pm	***Wrap-Up and Takeaways***
6:30-9:30 pm	**SIEM NetWars** (LOCATION: ROSEMONT C/D) SIEM NetWars is a hands-on, interactive learning scenario that enables security professionals to develop and master real-world, in-depth skills they need to efficiently and effectively leverage their SIEM to gain actionable intelligence and defend their organization. Participants learn in a cyber range while working through various challenge levels with a focus on mastering the skills information security professionals can use in their jobs every day. All Summit and training attendees are welcome to participate. SIEM NETWARS EXPERIENCE

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.