SANS

SIEM & Tactical Analytics SUMMIT

Scottsdale, AZ
Nov 28-29, 2017

Program Guide

@SANSDefense #SIEMSummit

Agenda

All Summit Sessions will be held in Sonora A+B (unless noted).

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

Tuesday, November 28

8:00-9:00 am	**Registration & Coffee** **(Location: Sonora Breezeway)**
9:00-9:15 am	***Opening Remarks & Introductions*** *Justin Henderson (@SecurityMapper), Systems and Security Architect, GSE # 108, Cyber Guardian Red/Blue; Summit Co-Chair* *Ismael Valenzuela (@aboutsecurity), SANS Certified Instructor, GSE #132; Global Director of Foundstone Consulting Services*
9:15-10:00 am	***Keynote: Tactical Acceleration*** Adversaries are running throughout your network. Your job is to chase them down. Sometimes it feels like we can't run quite fast enough to catch them. Maybe this is because we don't have the right data at our fingertips, or perhaps we're overwhelmed by the amount of data and can't analyze it efficiently. Let's discuss ways to accelerate our daily analysis so we can run down our adversaries! *Doug Burks (@dougburks), CEO, Security Onion Solutions LLC*
10:00-10:35 am	***Lesser-Used Logs: Why You *NEED* To Be Looking at Them*** Attendees of this talk will learn some of the more commonly overlooked log sources in their environment. These lesser used logs can have a HUGE impact on your overall security posture. *Mick Douglas (@BetterSafetyNet), DFIR Practice Lead, Binary Defense Systems; SANS Instructor, SEC504*
10:35-11:00 am	**Networking Break** **(Location: Sonora Breezeway)**
11:00-11:35 am	***Modern Phishing Defeated by Plain Old Logs*** Today, phishing and ransomware attacks are prevalent, and getting ever-more advanced. Signature based detection cannot keep up. New security technologies are helpful, but expensive. Instead, organizations should consider a low-cost solution that they already have: plain old logs. This talk demonstrates how to catch some of the most modern attacks using key log sources you already have or can easily enable. Better yet, it is easy to setup and maintain. If your organization could use a quick win in this area, this talk is for you. *Art Azarenko, Security Analyst, TDS Inc.*

Tuesday, November 28

11:35 am – 12:10 pm

Actionable Detects: Blue Team Cyber Defense Tactics

Organizations relying on third parties to detect breaches can go almost a full year before finding out they have been compromised. Detect the breach yourself, and on average you will find it within about a month of the initial occurrence. Considering detection and defense against modern adversaries too costly to perform yourself can be a very expensive miscalculation considering the substantially increased price of response and recovery with breach duration.

Seth Misenar's ever-evolving Actionable Detects offer tactics, techniques, and procedures to once again take pride in your Blue Team Cyber capabilities. Not applying these lessons learned could prove costly in the face of adapting threat actors. Dig in and learn to hold your head high when talking about your defensive cyber operations capabilities.

Seth Misenar (@sethmisenar), Principal Consultant, Context Security; Senior Instructor, Author, SEC511 and SEC542, SANS Institute

12:10-1:30 pm

Lunch Panel: Go, Blue!: Trends and Opportunities in Detection **(Location: Sonora Breezeway)**

Enjoy lunch on us and get some bonus insight from experts in detection from various industries. The informal panel discussion will touch on industry trends – both the ones that are promising, and the ones that you can safely ignore. We'll look at the active detection techniques that really work, no matter the size of your organization or the industry you're in. After all, in the SIEM space, we all bleed blue!

Moderator:

Justin Henderson (@SecurityMapper), Systems and Security Architect, GSE # 108, Cyber Guardian Red/Blue; Summit Co-Chair

Panelists:

Stefan Hazenbroek, Cyber Defense Analyst, Shell

John Hubbard, SOC Manager, GlaxoSmithKline

Kevin Wilcox (@kmwilcox_), Information Security Specialist, Appalachian State University

1:30-2:05 pm

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

Tuesday, November 28

2:05-2:40 pm

Deploying Windows Advanced Auditing: Deploying One Incident Responder’s Wish List of Events

As an incident responder, I’ve found it to be rare that the victim organization has taken advantage of Windows Advanced Auditing. This functionality was introduced by Microsoft with Server 2008 R2 and Windows 7, and increased the security auditing policy settings from nine to 53. Deploying this policy provides immediate insight into such useful information at process creation and termination, outbound connections to IP addresses by process, targeted monitoring of sensitive files, and command line logging. This presentation will cover a brief history of Windows security auditing, how to take advantage of Windows Advanced Auditing, event ID’s of particular interest, and sample group policy objects (GPO’s) for deployment to client workstations, member servers and domain controllers.

Mike Lombardi, President, Vertigrate

2:40-3:00 pm **Networking Break** **(Location: Sonora Breezeway)**

3:00-3:35 pm

Exit Night, Enter Light

This presentation will present a case study of the implementation of security monitoring in a non-profit environment. In a budget and personnel constrained environment, what were the most effective and valuable actions that were taken to ramp up security operations? What is the outcome if you implement and use the techniques that are taught in the various SANS courses? How do these techniques measure up to or complement commercial options? In a nutshell, “I went to a SANS class and they said do these things, so this is what it looks like if you actually do them”. The details of collection and analysis of security events will be the primary focus along with examining other potentially useful event sources. There will also be a discussion of the evolution of security control implementation in the environment, looking at the starting point, the current state, and the envisioned future state.

David Mashburn (@d_mashburn), IT Security Manager

3:35-4:10 pm

Ten Holiday Gift Ideas for the SOC Who Has Everything

Automating your organization’s security operations is no longer optional. It’s essential. Increasing analyst productivity and decreasing response time can mean the difference between successfully containing an attack, and suffering a devastating breach. This talk will focus on ten practical automation techniques—each implemented in either Python or PowerShell—that extend the functionality of a popular commercial SIEM. Each technique will demonstrate how to automatically gather additional context on an alert, make configuration changes in an operational environment, or retrieve and analyze forensic evidence. Proof of concept code samples and live/recorded demonstrations will be provided.

Dave Herrald (@daveherrald), GSE #79, Senior Security Architect, Splunk

Ryan Kovar (@meansec), Staff Security Strategist, Splunk

4:10-4:45 pm

Taking Your SIEM to the Next Level with 3rd Party Tools and Scripts

Accelerate your SOC workflow and provide meaningful and context-rich information to your analysts using free open-source scripting frameworks like Flare and VulnWhisperer. You will learn advanced SIEM techniques such as identifying periodic communication, critical asset tagging, custom risk scores, compartmentalized vulnerability scans, and automated risk tracking over time.

Austin Taylor (@HuntOperator), Senior Security Researcher, IronNet Cybersecurity;
Mentor, SANS Institute

Tuesday, November 28

4:45-5:00 pm

Day 1 Wrap-Up & Closing Remarks

Justin Henderson (@SecurityMapper), Systems and Security Architect, GSE # 108, Cyber Guardian Red/Blue; Summit Co-Chair

Ismael Valenzuela (@aboutsecurity), SANS Certified Instructor, GSE #132; Global Director of Foundstone Consulting Services

6:30-9:30 pm

SIEM NetWars (Location: Sonora Breezeway)

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.

Topics Include:

- SIEM Design & Architecture
- Advanced Endpoint Analytics
- Log Analysis & Enrichment
- PowerShell Monitoring
- Post-Mortem Analysis

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.

Wednesday, November 29

8:00-9:00 am	**Registration & Coffee** **(Location: Sonora Breezeway)**
9:00-9:45 am	***Keynote: This Is Not Your Grandfather's SIEM*** For many CSOCs, there was a simpler time, when their security event collection and monitoring problems could, in theory, be solved by buying, installing, and optimizing one core product-- a commercial SIEM. Today, life is not so simple. The SIEM marketspace started with many startups, consolidated to a handful of leaders, and has diversified again. Acquiring and operating an analytic platform for large and mature CSOCs is a major investment of time, money and effort. The best approach to common tasks - normalization, near-real-time correlation, analyst triage, pivot, and workflow - is not always cut and dried. In this talk, Carson will provide an overview of major design considerations and opportunities in implementing, and evolving the modern CSOC analytic platform. *Carson Zimmerman, Cyber Security Operations Center (CSOC) Engineering Team Lead, Microsoft*
9:45-10:20 am	***Stashing the SIEM*** Whether you use ELK, Splunk with Enterprise Security, ArcSight, QRadar or something else, the basis for all of our SIEMs is log data. After we spend tens (or hundreds) of thousands of dollars every year for our SIEM, why do we pump them full of "dumb" data and then act surprised when they fail to produce? We'll examine some of the data we feed our SIEMs, why it's critical we turn that into "smart" data, and show examples of how to do that using logstash from the ELK/Elastic stack. *Kevin Wilcox (@kmwilcox_), Information Security Specialist, Appalachian State University*
10:20-10:40 am	**Networking Break** **(Location: Sonora Breezeway)**
10:40-11:15 am	***Defeating Advanced Attacks with Simple Detects*** Tired of the bad guys breaking in and using your own systems against you? PowerShell in particular is the loaded weapon everyone is afraid of, but it doesn't have to be. This talk focuses on applying simple detection and enrichment techniques with PowerShell logs that can catch even the most sophisticated attacks. We'll use PowerShell as a use case to demonstrate how you can view, enrich, and use logs in simple yet highly effective ways. The old saying is "bad guys only need to find one way in," but the new saying needs to be "defenders only have to find attacks with one good detection technique." Focus is on high-fidelity techniques because…. we only need one to trigger to win. Detection in depth is the future. *Justin Henderson (@SecurityMapper), Systems and Security Architect, GSE # 108, Cyber Guardian Red/Blue; Summit Co-Chair*

Wednesday, November 29

11:15-11:50 am

Active Defense via a Labyrinth of Deception

A network baseline allows for the identification of malicious activity in real time. However, maintenance and organization presents a significant challenge in false positive free alarming. To surmount these hurdles, network architects need to design a network free from continuous change. This includes, changing company requirements, untested systems or application updates, and the presence of unpredictable users. The creation of a static, never-changing environment is the goal. But wait, that breaks everything we do with networks? A Labyrinth is the definition of a real, but fake (static) world. A network labyrinth would be capable of detecting changes in its environment, i.e. to real systems, and still remain static in nature. A SIEM's capabilities take center stage as the Labyrinth can add changing values to a block list, protecting the production network lying behind.

Nathanial Quist, Incident Response Engineer, LogRhythm

11:50-1:15 pm **Lunch & Learn Session (Location: Sonora Breezeway)**

Hunting or Monitoring: Machine Learning in Threat Detection

Speakers: Kevin Keeney & Michael Paquette, Elastic

Machine learning in cybersecurity can be thought of as an arsenal of "algorithmic assistants" to help the security expert automate the analysis of data by looking for interesting anomalies and patterns. In this presentation, we introduce a set of "recipes" that describe how to apply machine learning, in the form of automated anomaly detection, to detect a set of elementary attack behaviors that are often difficult to detect using other means. In a live demonstration of one such detection recipe, we'll configure machine learning software to detect DNS tunneling activity by analyzing DNS requests coming from client workstations within a small environment, instructing the machine learning algorithms to create baselines of normal DNS request activity sent from each client, and to detect anomalous behavior associated with DNS tunneling.

1:15-1:50 pm

Sinkhole all the Things!: Using a (DNS) Sinkhole to Detect and Respond to Malicious Activity

All computers can get infected, and relying on security suites to catch compromise is not enough. Simple techniques like sinkholing provide a method to catch compromised systems while also providing extra benefits such as prevention and response. This presentation will outline real-world success using a DNS sinkhole to detect and respond to malicious activity and offer pointers for implementation in any organization.

Stefan Hazenbroek, Cyber Defense Analyst, Shell

1:50-2:25 pm

Panel: SIEMtervention

Come and join us for a SIEM intervention! This interactive discussion focuses on the sins and flaws our SIEM solutions have or that we, the security community, have created. Sometimes the truth is uncomfortable, but constructive conflict breathes new life and purpose. Our SIEMs can and should be better. If you want to know how join the intervention.

Moderator:

Justin Henderson (@SecurityMapper), Systems and Security Architect, GSE # 108, Cyber Guardian Red/Blue; Summit Co-Chair

Panelists:

Mick Douglas (@BetterSafetyNet), DFIR Practice Lead, Binary Defense Systems; SANS Instructor, SEC504

John Hubbard, SOC Manager, GlaxoSmithKline

Ismael Valenzuela (@aboutsecurity), SANS Certified Instructor, GSE #132; Global Director of Foundstone Consulting Services

Wednesday, November 29

2:25-3:00 pm

Cracking the Upper Management Code

Every security analyst knows the feeling all too well. You open your beloved SIEM dashboard when you first get into the office and witness a sea of alerts. From experience, you know that many of these alerts may be false positives, but as any good security analyst going through their SIEM would do, you investigate every one of them. Logs and event are coming from every direction, even after all your expert tuning. Events from your IDS/IPS, VPN devices, Active Directory, Web Servers and all other integral devices to the bottom line of the company are correlating their events correctly. Your SIEM is in top working condition and it took you a long time to get to this point.

After looking at all the alerts coming from the SIEM, numerous things come popping into your mind. How are you going to actively take care of these alerts and adhere to your SLAs your company has based on the severity of alerts? How are you going to be able to keep up with the influx of new devices in your environment? Can your SIEM grow along with the growth of the company? Is the backend architected to scale with the number of alerts and events being ingested? Will you need more resources to help you investigate and triage all the alerts? Many of the solutions to these problems start and end with upper management and their signature on the dotted line to augment your existing SIEM capabilities.

Many of us in this room have made the mistake before of thinking the large number of alerts being generated from a SIEM or any of the currently deployed security solutions would be enough to convince upper management to give you an infinite budget to fight evil. Sadly, we all know this is not the case. Upper management always has questions you were not expecting when shown the console for the first time, such as:

1) “Why are we alerting on these occurrences?”

2) “Are there ways we can utilize other tools to assist us in covering our gaps?”

3) “Why do you need to add more capabilities to the SIEM? Everything looks just fine to me.”

As frustrating as some of these questions and the lack of extra funding can be, upper management is asking legitimate questions to protect their budgets and the rest of the security program. Secretly, behind the scenes, the issue was not their budget but it may be with the data presented to them. Graphs included in traditional SIEMs try to bridge the gap between security analysts and upper management but many times it is not enough. Upper management needs to be wowed and compelled to make the move you want. Luckily, all the data is already at your fingertips and you can present it in a way that will not only benefit you but your whole group. Today we will talk about the ways you can present to upper management to win the budget you so desperately need.

Kevin Garvey, Senior Analyst IT Security Operations, Corporate Information Security, Time Warner

3:00-3:20 pm **Networking Break** (Location: Sonora Breezeway)

3:20-3:55 pm

The Most Dangerous Game: Hunting for Post-Exploitation Stage Attacks with Elastic Stack and the MITRE ATT&CK Framework

Modern cyber defense requires the mindset of “assume breach”, but with so much data generated by our networks and endpoints, how can we collect the information needed to identify attacks in an affordable way, let alone sort through it all? This talk will discuss the unique challenges of finding post-exploitation activity in our mountains of data and walk through using the open source Elastic Stack to identify the techniques enumerated in MITRE’s ATT&CK framework. Attendees will be given an overview of how to leverage the ATT&CK body of knowledge, options for data collection, and suggested rules and dashboards that specifically target finding post-exploitation activity. The goal of this talk is to arm defenders with industry validated attack knowledge, and demonstrate how late stage compromises can be identified and stopped before significant damage is caused.

John Hubbard, SOC Manager, GlaxoSmithKline

Wednesday, November 29

3:55-4:30 pm

Open CNA (Collection, Normalization and Analysis) using rastrea2r and Machine Learning

Hunting for the presence of the adversary usually involves digging, sifting and analyzing vast amounts of data gathered from endpoints and network traffic logs. The type of analysis, the tools and the methodologies used for this purpose varies among analysts though, making reusability harder as each analyst uses its own scripts with its own algorithms and abstractions.

To assist with this challenge, Ismael Valenzuela (Certified SANS Instructor, GSE #132 and Principal Engineer at McAfee) will introduce Open CNA, a new strategy based on open standards for Collection, Normalization and Analysis, together with a new open source toolset consisting of (1) a simple client/server architecture based on the "rastrea2r" project (presented at BlackHat Arsenal 2016), which allows analysts to gather valuable data from endpoint snapshots, (2) a python SDK that provides a layer of abstraction over the data that has been gathered, (3) a powerful Machine Learning library containing algorithms that will assist detecting the adversary's presence in the data mined and (4) a set of reporting tools that can present all the findings in an actionable way.

Ismael Valenzuela (@aboutsecurity), SANS Certified Instructor, GSE #132; Global Director of Foundstone Consulting Services

4:30-4:45 pm

Closing Remarks

Justin Henderson (@SecurityMapper), Systems and Security Architect, GSE # 108, Cyber Guardian Red/Blue; Summit Co-Chair

Ismael Valenzuela (@aboutsecurity), SANS Certified Instructor, GSE #132; Global Director of Foundstone Consulting Services

6:30-9:30 pm

SIEM NetWars (Location: Sonora A/B)

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.

Topics Include:

- SIEM Design & Architecture
- Advanced Endpoint Analytics
- Log Analysis & Enrichment
- PowerShell Monitoring
- Post-Mortem Analysis

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.