SANS

The Most Trusted Source for Information Security Training, Certification, and Research

# Tactical Detection & Data Analytics

## Summit 2018

**Program Guide**

@SANSDefense #DetectionSummit

# Agenda

*All Summit Sessions will be held in the Sonora AB (unless noted).*
*All approved presentations will be available online following the Summit at* ***sans.org/detection-archive***

## Tuesday, December 4

| | |
|---|---|
| 7:00-9:00 am | **Registration & Coffee** (LOCATION: SONORA BREEZEWAY) |
| 9:00-9:15 am | ***Opening Remarks***<br>***Justin Henderson*** *(@SecurityMapper), Summit Co-Chair and Certified Instructor, SANS Institute*<br>***John Hubbard*** *(@SecHubb), Summit Co-Chair and Certified Instructor, SANS Institute* |
| 9:15-10:00 am | ***Keynote: Build it Once, Build it Right: Architecting for Detection***<br>Defensible networks are designed to prevent and detect computer attacks, and are hardened at every layer. Per Richard Bejtlich, defensible networks "can be watched" and "limit an intruder's freedom to maneuver." For example: modern malware often attempts to steal credentials and move laterally via tools such as WMIC, PSExec, and PowerShell. Most host-based firewalls can block (and log) based on applications such as PSExec. Prudent organizations use host-based firewalls to block and log network connections initiated by these tools from "regular" user desktops, and only allow authorized use from system administration drop boxes.<br>This talk focuses on designing a defensible security architecture that limits an intruder's ability to maneuver, and creates logs when it is successful in doing so. Specific examples will be provided that prevent recent malware such as Petya, NotPetya, SamSam, and others. We will provide an actionable list of techniques that prevent and detect the deadliest events that occur during virtually every successful breach.<br>***Eric Conrad*** *(@eric_conrad), Fellow, SANS Institute* |
| 10:00-10:35 am | ***Unconventional Logging and Detection***<br>Log collection and detection go hand in hand, yet both are difficult. Are you allowed to deploy a log agent or not? Can you change system settings to generate the logs you need? The problem is the answer may be no to both questions. Even if the answer is yes, some detection capabilities cannot be done with standard logging and collection.<br>All is not lost. Windows, Linux, Unix, and Mac systems all have unconventional methods of log collection and detection that augment standard processes. This talk focuses on using alternative methods such as PowerShell, Python, or built-in binaries to generate custom logs and covers multiple use cases on what detection techniques those logs provide. Example: ARP cache poisoned? How about a detection technique that produces zero logs until it happens and then generates and ships off the record directly to your platform of choice.<br>***Justin Henderson*** *(@SecurityMapper), Systems and Security Architect, GSE # 108, Cyber Guardian Red/Blue; Summit Co-Chair* |
| 10:35-11:00 am | **Networking Break** (LOCATION: SONORA BREEZEWAY) |
| 11:00-11:35 am | ***Rapid Data Analysis Thunderdome: Many Visualizations Enter; Only One Leaves Alive!***<br>We're going to virtually throw lots of models on the wall and see what sticks! All too often we forget the role of luck and happenstance in data analysis. This is a crude idea, done well-ish. Rather than spend cycles trying to develop the perfect dashboard, why not generate several dozen and pick which ones work best? Using one set of data, this tool generates dozens of visualizations, and lets you select the ones that are more meaningful to you.<br>***Mick Douglas*** *(@BetterSafetyNet), Managing Partner, InfoSec Innovations; Certified Instructor, SANS Institute* |

## Tuesday, December 4

| | |
|---|---|
| 11:35 am - 12:10 pm | ***Wreck SIEM Noise: How to Build and Measure Effective Alerting***<br>Security Incident Event Managers are prone to intense noise and alert fatigue. Focusing our limited resources on prioritized alerts is a key to success. This talk will share successful tactical concepts including initial approach, simple analysis techniques anyone can do, use case life-cycle and effective metrics to maintain success. While stepping through real life experiences, the talk will also discuss how these techniques convert information into intelligence and how these operations weave into engineering, content development, and architecture.<br>***Frank Angiolelli*** *(@fnksec), Strategic Consultant, Foundstone* |
| 12:10-1:30 pm | **Lunch & Learn** (LOCATION: SONORA BREEZEWAY)<br>Grab your lunch and settle in for a bonus talk.<br>***BGP Hijacking by Example*** (LOCATION: SONORA A/B)<br>BGP Hijacking is no longer the exclusive domain of nation state adversaries. Attacks on the control plane of the internet are now within reach of spammers and fraudsters. This talk will use the 2018 MyEtherWallet hijacking attack to illustrate how a BGP Hijack works. We will also cover how you can start the conversation within your organization about BGP hijacking defense and practical steps you can take to protect yourself.<br>***Kevin Tyers****, Technologist, LKDM* |
| 1:30-2:05 pm | ***The Tools of Tactical Detection: The toolchain and Techniques That Power Modern SOC***<br>Each SOC may have a different battle rhythm, a different methodology that makes them tick, but all security defenders rely on some set of tools to achieve success. Those tools may be all commercial or all free open source, or some mixture of the two. Should we have a tool for everything? If not, how should the tools be used? Does one size fit all? How early should we adopt the next generation of tools? Which tools are critical, which are nice to have, and which are pure luxuries? The panel will weigh in on these and other questions offered up by the audience that concern tools important to building, maintaining, and improving a security defense team.<br>MODERATOR:<br>***John Hubbard*** *(@SecHubb), Summit Co-Chair, SANS Institute*<br>PANELISTS:<br>***Craig L. Bowser*** *(@reswob10), Senior Security Engineer, Dept. of Energy*<br>***Justin Henderson*** *(@SecurityMapper), Systems and Security Architect, GSE # 108, Cyber Guardian Red/Blue; Summit Co-Chair*<br>***Dave Herrald*** *(@daveherrald), Staff Security Strategist, Splunk* |
| 2:05-2:40 pm | ***Machine Learning in Cybersecurity: Fact, Fantasy, and Moving Forward***<br>In the last several years we have seen personal assistants like Alexa, self-driving cars, and automated foreign language translation all made possible by machine learning. Looking for new investment opportunities, the venture capital community has turned its attention to machine learning in cyber and is investing millions of dollars into the sector. Now, nearly every product advertises machine learning, which has led to confusion between what's real and what's marketing. This talk will demystify machine learning in cyber, separating fact from fantasy. We will discuss what machine learning is, why it is particularly challenging in cyber, and how to design machine learning applications that will have the biggest impact for your business.<br>***Dan Liebermann****, Senior Associate – Advanced Analytics, Booz Allen* |
| 2:40-3:00 pm | **Networking Break** (LOCATION: SONORA BREEZEWAY) |

## Tuesday, December 4

| | |
|---|---|
| 3:00-3:35 pm | ***Case Study: Detection with MITRE ATT&CK in the Energy Sector***<br>The time before an adversary is detected continues to be excessive, averaging 6-12 months. Are you comfortable with an adversary having 180 days to pillage your data and have free reign? The MITRE ATT&CK framework was created to help aid defenders and significantly reduce dwell time (the time an adversary is on the network before being detected). The framework takes an "Assume Breach" stance, meaning you've already been compromised you just haven't discovered it yet, and introduces detection methods to detect post-compromise tactics and techniques. This talk will focus on an introduction to the MITRE ATT&CK Framework and integration of open-source tools to increase cyber defenses and ensure your Blue Team can detect post-compromise techniques.<br>***Christian Kopacsi*** *(@1nf0s3cp1mp), Director - Cyber Threat, Response and Adversary Operations, Consumers Energy* |
| 3:35-4:10 pm | ***What's In a (User) Name, That Which We Call a Kevin?***<br>I know, "kevin logged in from klaptop" is, well, boring. Why do we still give those useless logs to our analysts and admins? In a world with Active Directory, LDAP, and management databases, why should an analyst have to query five different systems to find out that "kevin" is in human resources but logging into a computer from payroll? The answer is: we should not!<br>Gather round as we talk about one of my favorite types of log enrichment, where we key on user names and machine names to save analysts time and make searching, alerting, and reporting faster and more useful for everyone. There may even be a bit of Python provided for those wanting to play at home.<br>***Kevin Wilcox*** *(@kmwilcox_), Information Security Specialist, Appalachian State University* |
| 4:10-4:45 pm | ***Top 5 Things To Know About Azure Active Directory Logs***<br>If you aren't leveraging your Azure Active Directory logs, you are missing a large part of your organization's picture. This session will cover the fundamentals of the Azure AD logs, how to integrate these into your existing SIEM systems, and key events to look for that may indicate a compromise in your environment.<br>***Mark Morowczynski*** *(@markmorow), Principal Program Manager, Microsoft* |
| 4:45-5:00 pm | ***Day 1 Wrap-Up and Closing Remarks***<br>***Justin Henderson*** *(@SecurityMapper), Summit Co-Chair and Certified Instructor, SANS Institute*<br>***John Hubbard*** *(@SecHubb), Summit Co-Chair and Certified Instructor, SANS Institute* |
| 6:00-8:00 pm | ***Tactical Networking and Poolside Analytics***<br>Enjoy live music while debriefing on the day's talks and get to know Summit attendees and speakers at this informal poolside reception. Drinks and snacks will be served. |

**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**  **#DetectionSummit**

## Wednesday, December 5

| | |
|---|---|
| 8:00-9:00 am | **Registration & Coffee** (LOCATION: SONORA BREEZEWAY) |
| 9:00-9:45 am | ***From Automation to Analytics: Simulating the Adversary to Create Better Detections***<br>Security teams have more detection tools at their disposal than ever before, yet most are still struggling to find even the most basic malicious activity occurring in their environments. Building effective detection analytics requires realistic data and the ability to iterate quickly in a rapid analytic development cycle. In this talk, we will introduce a full lifecycle attack simulation and analytics development environment featuring the MITRE ATT&CK framework and the Atomic Red Team project using Splunk and Splunk Phantom mapped to an imaginary APT group, Taedonggang. We will focus on how security teams can use such a system to rapidly develop and share new detection analytics. Links to all components referenced in the talk will be provided, including a cloud-based dataset that can act as a playground for users who want to see the results of the activity. All use of the commercial software will be limited to free/Enterprise trial/ Community editions.<br>***Dave Herrald*** *(@daveherrald), Staff Security Strategist, Splunk*<br>***Ryan Kovar*** *(@meansec) (@splunk), Senior Security Architect, Splunk* |
| 9:45-10:20 am | ***Using Open-Source Tools for Data Analytics: Learning from a Corpus of Endpoint Snapshots***<br>It is a common practice among security analysts to take snapshots from different systems for further analysis. To that purpose, there are few tools that work in a similar manner: they work as proxies of a set of operating system calls that are executed, whose logs and outputs are captured, then parsed and, finally, transferred to a central location. An example of such tool is rastrea2r, an open-source tool that executes around 20 windows commands, captures their output, and stores those logs on a central repository. Usually, snapshot tools capture the processes a system is currently running, all cached DNS queries, part of the web history, etc. The resulting information is usually referred as endpoint snapshot.<br>One endpoint snapshot contains information particular to one machine, but a few hundred is in fact a powerful source of friendly intelligence. Defining a notion of similarity among snapshots and using it for clustering them can answer many key questions.<br>***Gabriel Infante-Lopez****, Principal Engineer, McAfee* |
| 10:20-10:40 am | **Networking Break** (LOCATION: SONORA BREEZEWAY) |
| 10:40-11:15 am | ***Forgotten But Not Gone: Gathering NTFS Artifacts of Deletion***<br>While endpoint threat monitoring tools are powerful, many lack ways to quickly and efficiently recover evidence of deleted information. This deleted information may include evidence of staging tools, exfiltration files and malware that attackers clean up as they go. How can you track an attacker through your environment if they are cleaning up after themselves? Learn how to pull back and leverage two files on the system, the MFT and the NTFS Index Attribute, to discover evidence of deleted files. Once an attacker's favorite staging location is known, this technique can be scaled up and automated to sweep an environment to locate and analyze evidence of deleted files.<br>***Mari DeGrazia*** *(@MariDeGrazia), Director, Incident Response, Kroll*<br>***Scott Hanson****, Director, Kroll* |

## Wednesday, December 5

| | |
|---|---|
| 11:15-11:50 am | ***Keeping Up with the Joneses: SIEM Rules Edition***<br>Keeping up with the evolving landscape of threats and attacker techniques can feel like an uphill battle. Many environments leverage a SIEM to perform log correlation and analysis, and keeping rules current is a challenge. To combat the burden of "keeping up with the Joneses" SIEM rules, this presentation will detail a new initiative to develop, share, and assess the latest and greatest in alerting logic—the Threat Alert Logic Repository (TALR). TALR is a repository of approved SIEM rules, designed for quick and easy translation into the SIEM tool of your choice. This repository will be publicly hosted and serve to keep SIEM engineers and analysts up-to-date on alert logic.<br>Attendees will gain a comprehensive overview of TALR and understand how to incorporate it into their cyber environments as a way to remain on the cutting edge of alerting logic.<br>***Nick Ascoli**, Consultant, Security Risk Advisors*<br>***Kevin Foster**, Manager, Security Risk Advisors* |
| 11:50 am - 1:15 pm | **Lunch and Lightning Talks** (LOCATION: SONORA BREEZEWAY)<br>Enjoying the Summit talks? Think you've got something to add? Here's your chance. Sign up for a 5-minute slot and show us what you've got. |
| 1:15-2:00 pm | ***Data Science and Domain Expertise***<br>Data science is the capability to automatically find needles in a haystack. Yet some needles are good, some are evil, and others are just plain confusing. This panel is a discussion on the impact of applying domain expertise to data science and whether one can exist without the other.<br>MODERATOR:<br>***Justin Henderson** (@SecurityMapper), Systems and Security Architect, GSE # 108, Cyber Guardian Red/Blue; Summit Co-Chair*<br>PANELISTS:<br>***Gabriel Infante-Lopez**, Principal Engineer, McAfee*<br>***Kristen Quade** (@BlueTeamQuade), Data Scientist, NERC's E-ISAC*<br>***Austin Taylor** (@HuntOperator), Director of Cybersecurity R&D, IronNet Cybersecurity; Community Instructor, SANS Institute* |
| 2:00-2:35 pm | ***Sharing is Caring: Improving Your Detection Capability with the Sigma Framework***<br>To succeed in cyber defense, the blue team needs to start sharing, the problem is our tools aren't doing us any favors. Vendor lock-in and incompatible signature storage formats make import and export of SIEM rules across products difficult, hindering our ability to share with the community. What if there was another way? The Sigma framework is a new effort from Florian Roth and Tomas Patzke that aims to solve this problem. It works by defining a new, generic signature format that is easy to use and allows anyone to convert rules to work with their own SIEM, and it could be a major step forward in solving this problem. This talk will discuss how Sigma works, how it can help you write better and more maintainable detection rules, and why I think it is an important step forward for the blue team.<br>***John Hubbard** (@SecHubb), Summit Co-Chair and Certified Instructor, SANS Institute* |
| 2:35-3:00 pm | **Networking Break** (LOCATION: SONORA BREEZEWAY) |

## Wednesday, December 5

| | |
|---|---|
| 3:00-3:35 pm | ***Measure Your Bad Self: The SIEMquel***<br>Here's an obvious statement: Without logs, a SIEM is practically useless.<br>But unhealthy logs are worse than no logs at all. Sick logs lead to false feelings of security (because alerts don't fire due to missing logs from some machines), longer investigations (because critical logs were not collected), and misleading reports (because missing data skews calculations). A previous talk by Carson Zimmerman discussed the importance of measuring your data ("Measure your bad self" SANS SOC Summit 2018). In this talk I am going to build on his talk by showing how to apply the concepts and theories he lays out to your SIEM. This talk will cover the definition of healthy logs and sick logs, the four areas we need to measure our logs, and practical methods for measuring and monitoring.<br>***Craig L. Bowser*** *(@reswob10), Senior Security Engineer, Dept. of Energy* |
| 3:35-4:10 pm | ***Users as a Data Source: Are You Leveraging Security-Aware Employees in Your Detection Strategy?***<br>After years of users being trained to report phishing emails, they are now providing great intel that you didn't even have to pay for. Are you using it to search for badness in your environment – sending it to your SIEM – or to your data lake? Are you sharing those free IOCs with your Threat Intel teams that are trying to protect your brand? Pushing the IOCs to your endpoints to protect your assets when they're off your network?<br>***Tonia Dudley****, Director, Cofense* |
| 4:10-4:45 pm | ***Applied Data Science and Machine Learning for Cybersecurity***<br>Determining which machine learning algorithm to use and where to use it can be difficult. This talk will discuss various machine learning classifiers that you can use for popular attack techniques and provide steps to operationalize the results in your investigation.<br>***Austin Taylor*** *(@HuntOperator), Director of Cybersecurity R&D, IronNet Cybersecurity; Community Instructor, 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.***