Security Operations
SUMMIT 2019

Program Guide

@SANSDefense #SOCSummit

Agenda

All Summit Sessions will be held in the Blaine Kern Ballrooms A-D (unless noted otherwise).

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

Monday, June 24

7:00-9:00 am	**Registration & Coffee** (LOCATION: BLAINE KERN PRE-FUNCTION)
9:00-9:15 am	***Welcome & Opening Remarks*** ***Chris Crowley*** *(@CCrowMontance), Summit Chair and Principal Instructor, SANS Institute*
9:15-10:00 am	***Keynote: Lessons Learned Applying ATT&CK-Based SOC Assessments*** The ATT&CK framework has seen a rise in popularity in the security community, with more and more Security Operations Centers (SOCs) wanting to ATT&CK. To help SOCs get into the game of using ATT&CK, MITRE has developed a process to quickly gauge a SOC's detective capabilities as they relate to the ATT&CK framework, producing a coverage heatmap as well as a set of recommendations the SOC can use to improve its operations. The process is low-overhead, focusing only on interviews and documentation analysis, but it provides useful results for SOCs that want to understand how their current capabilities stack up to ATT&CK. In this talk, we'll call on our practical experiences to describe some of the key lessons learned we've discovered when applying ATT&CK-based SOC assessments, ranging from the best ways to conduct the assessment to how to effectively communicate results to leadership. The lessons and tips that we present will be widely accessible, helping those who are interested in conducting third-party assessments, who want to assess their own SOCs, or who just want to learn about the assessment process in general. Attendees should walk away with a better understanding of how they can run and use ATT&CK-based SOC assessments, including tips on avoiding traps and pitfalls in the process. ***Andy Applebaum*** *(@andyplayse4), Lead Cyber Security Engineer, MITRE*
10:00-10:30 am	**Networking Break** (LOCATION: BLAINE KERN PRE-FUNCTION)

Monday, June 24

10:30-11:05 am	***Use Case Development Utilizing an ARECI Chart*** This presentation will describe use case development from the perspective of a Managed Security Service Provider (MSSP) but that is also useful for internal SOCs/CERTs. The case starts with a simple requirement statement, through scenario development, then moves on to the Analysis of Required Evidence for Correlation and Investigation (ARECI) chart to help inform engineers about alert development and system owners about detection development. The ARECI chart consists of a list of data/sources that analysts and engineers will rely on to conduct their respective work. This data/source list will be categorized, broken down into specific sources, and then analyzed for its value to alert development as well as incident response investigation. Data and sources are not limited to ingested log/event streams. Data can include data retained in the SIEM from system infrastructure, asset databases, configuration databases, org personnel data, threat intelligence, etc. Once a few team members (OPs and engineering alike), have derived what data/sources they think they need to complete their work, attention turns to the environment to ascertain if those data are available, available in the SIEMS, or not available at all. This then completes the ARECI chart and allows for conducting a feasibility assessment to determine whether the use case should move forward into an engineering phase, the environment needs to be adjusted, or new capability needs to be added to satisfy (remove gaps from) the chart requirements. Multiple ARECI charts from similar enough use cases can then be stacked to produce a compound list of gaps, which can then be ranked, prioritized, and packaged for advice to the customer. Finally, a key component to the use case development life cycle is teamwork. The fusion of security operations/analytics staff and SIEMS engineering staff at the early stage of the development life cycle helps both sides appreciate their distinctly different work and discreet goals. It creates a developer/user relationship that enhances the overall development of detection and alert presentation, and helps SOCs keep ahead of efforts to evade detection while improving their own capability and avoiding atrophy. ***Nathan Clarke*** *(@GeekNathn), APAC Advanced SOC (ASOC) Manager, Verizon Australia*
11:05-11:40 am	***Use Cases Development as a Driver for SOC Maturation*** When developing a Security Operations Center (SOC), it is important to define what you want to accomplish and to develop a road map to get there. The road map initially includes the development of policies, procedures, and process implementation to create a defined and repeatable methodology. At the highest level of maturity, a SOC identifies metrics and reports to management regularly. This leads to improvement and assures the entity that the SOC is meeting it's needs. At the heart of this is the use case. Use cases drive selection of threat intelligence feeds and frameworks. Use cases direct vulnerability management processes. Use cases bring focus to alerting and continuous monitoring. Use cases help incident responders avoid confusion. Use cases cut through all the noise information security professionals deal with. Attendees will learn how to develop desired outcomes for the SOC, identify use cases, and the understanding the how to mature use cases for long-term success. ***Eric C. Thompson*** *(@ectcyberhipaa),Director of Information Security and IT Compliance, Blue Health Intelligence*

Monday, June 24

11:40 am – 12:15 pm

A SOC Technology/Tools Taxonomy – And Some Uses for It

There are literally hundreds of different tools and technologies that are in use for monitoring and managing security operations. There is no such thing anymore as "a quick walk through the vendor expo" at any major security conference. Security managers looking to establish or evolve a SOC face a confusing array of choices when looking to justify technology funding, as well as staffing and training.

Chris Crowley will present a taxonomy of SOC tools and technologies he has developed, taking a portfolio view and mapping across moderate/advanced budget levels and showing typical owned by/used by patterns. John Pescatore will share a decision methodology for using that information to optimize your strategy for increasing your SOC capabilities and maturity level based on common business drivers and security operations patterns.

Chris Crowley *(@CCrowMontance), Summit Chair and Principal Instructor, SANS Institute*

John Pescatore*, Director of Emerging Technologies, SANS Institute*

12:15-1:15 pm

Lunch & Learn Sessions

Practical Application of Network Intel for Analysts and Threat Hunters (LOCATION: BLAINE KERN E)

Threat Intelligence and hunting hold great potential for helping network defenders block adversaries who have not yet breached them, and find evidence of those who may have. And while external threat intel feeds can be great, most organizations also are sitting on a potential gold mine of useful forensic data. However, making practical and impactful use of the data can be tricky. It doesn't have to be. Tim Helming of DomainTools will demonstrate straightforward methods and data sources to strengthen your security posture without breaking the bank, using real-world examples of network and DNS-based threat hunts that exposed attack campaign infrastructure. The talk concludes with a simple 5-point checklist you can apply immediately to begin your organization's threat intel evolution.

Tim Helming*, Director of Product Management*

Using Security Orchestration and Automation to respond to Insider Threats (LOCATION: BLAINE KERN F)

Insider threats to your organization are one of the most common type of security incident and can be the most damaging. This session will look at how to leverage security orchestration and automation to work through an insider threat playbook. This session will feature a technology demonstration of the escalation of an incident from the SIEM to a SOAR platform, the creation of a playbook and the incident remediation process, leveraging third-party integrations.

John Avendano*, Technical Consultant, IBM Security*

1:15-1:50 pm

Mental Models for Effective Searching

One of the most intimidating challenges many analysts face is a blank search bar. That search bar is the only thing standing between you and a mountain of data containing the answers you need to determine if a compromise has occurred on your network. It's for this reason that effective searching is a core competency for investigators. This presentation will provide a conceptual framework for effective searching, show how to master any search tool faster, and offer strategies to combat the biases and limitations of the mind that can negatively affect your ability to process search results.

Chris Sanders *(@chrissanders88), Founder, Applied Network Defense; and Founder, Rural Technology Fund (@RuralTechFund)*

Monday, June 24

1:50-2:25 pm	***Managing Security Operations in the Cloud*** Our goal is to prevent unexpected access to cloud resources. To do this we must maintain strong identity and access policies (IAM) and effectively detect and react to changes. In this session we will discuss tools within the cloud for managing IAM in order to control access to cloud resources. We will also cover how to deploy and control cloud infrastructures using code templates that include change management policies. ***Marc Baker**, Online Training Subject-Matter Expert, SANS Institute*
2:25-2:55 pm	**Networking Break** (LOCATION: BLAINE KERN PRE-FUNCTION)
2:55-3:35 pm	***Virtuous Cycles: Rethinking the SOC for Long-Term Success*** Many Security Operations Centers (SOCs) have a burnout problem that leads to negativity and constant turnover. With the increasing cybersecurity talent shortage, keeping the people we have will only become increasingly important. The problem is that "Tier 1" and other SOC roles seem destined to burn people out. So what do we do? While the field of psychology understands the factors that cause burnout, many SOCs do not take the time to do the research and create an environment to fight it. Though meticulously defined process and tiering may be the norm, does it lead to sacrificing quality in the long term? Using science-backed research on intrinsic motivation and studies on SOC burnout factors, this talk will make the case that it's time to reconsider how we structure SOCs in order to create long-term success that benefits both the individual and the organization. ***John Hubbard** (@SecHubb), Author and Certified Instructor, SANS Institute*
3:35-4:30 pm	***2019 SANS SOC Survey Preview: Live Simulcast*** The 2019 SANS SOC Survey will be released in early July. Join Chris Crowley live or via simulcast for a discussion of what's new in this year's survey, and a sneak peek into topics and responses from this year's results. He will talk about the detailed interviews included this year, and highlight the methodology used to develop the results that many organizations use to direct SOC activities for the following year. If you can't attend the 2019 SANS Security Operations Summit in New Orleans, attend the simulcast! Registration details to be announced. ***Chris Crowley** (@CCrowMontance), Senior Instructor, SANS Institute*
4:30-4:45 pm	***Day 1 Wrap-Up and Action Items***
6:00-8:00 pm	**Let's Roll!** Fulton Alley | 600 Fulton Street Head down the street just a few blocks to Fulton Alley. Food, drinks, bowling lanes, and shoe rentals are on us. Bragging rights up for grabs. Wear your attendee badge for access to the event. ***Sponsored by:*** IBM Intelligent Security SIEMPLIFY

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 25

7:00-9:00 am	**Coffee & Tea** (LOCATION: BLAINE KERN PRE-FUNCTION)
9:00-9:45 am	***Keynote: How to Disrupt an Advanced Cyber Adversary*** The number of cyber actors that utilize a high degree of tool sophistication and tradecraft techniques has skyrocketed in the last few years. We usually refer to them as "advanced persistent threats." As the number of capable threat actors grows, it is imperative for organizations to have a clear picture and good understanding of actions they can take to disrupt, deny or even prevent cyber-attacks. Whether the actors are nation states, organized cyber-criminal groups or cyber mercenaries, this talk will share lessons learned from actual cyber activities, investigations and best practices that can help you improve your own cyber defenses. ***Manny Castillo*** *(@cyberwarrior777) Senior Information Security Technical Executive, Federal Bureau of Investigation*
9:45-10:15 am	**Networking Break** (LOCATION: BLAINE KERN PRE-FUNCTION)
10:15-10:50 am	***Breach -> ATT&CK -> Osquery: Learning from Breach Reports to Improve Cross-platform Endpoint Monitoring*** There's plenty of news about breaches, but the reporting is usually so vague that as defenders we don't get good enough useful information about what actually happened to help us improve our defenses. However, in 2018, both the SingHealth (Singapore) and Equifax (United States) breaches resulted in significant, detailed reports. In this talk, we will look at significant findings from these reports and map them to the MITRE ATT&CK framework in order to understand if our defenses are effective. We will then look to see how we can monitor our systems with the open-source and cross-platform tool Osquery in order to detect such breaches on Windows, Mac, and Linux. ***Guillaume Ross****, Lead Security Researcher, Uptycs*
10:50-11:25 am	***Shared Security Services: How to Adjust to an Ever-growing Landscape of Security Operations Center Responsibilities*** As organizations have grown to understand the importance of growing their Security Operations Centers (SOCs) to support the needs of their business units, security teams have also had to take on greater workloads and demands. SOCs are forced to accommodate to the growth of the business at the expense of the quality of their own work. This talk will help you realize the full potential of your SOC and consolidate its success for years to come. Topics of takeaway will include metrics that can be used to track a SOC that is being overworked; how to approach upper management to ask for resources to help grow and strengthen a shared SOC; how using threat intelligence can make more informed and smarter alerts to help reduce workloads; how to grow SOCs using a risk-based approach; and how growth spurs the need for a SOAR-based approach, and how to implement such an approach. ***Kevin Garvey*** *(@TheKevinGarvey), US IT Security Manager for CLS International Bank*

Tuesday, June 25

11:25 am – 12:10 pm

The Call Is Coming from Inside the House: How Does Your SOC Respond When Attackers Are On-Site?

Many of the most agile and well-trained blue teams rehearse response procedures and conduct tabletop scenarios to better prepare for incidents as overt as targeted phishing campaigns by outsiders, as subtle as illicit data exfiltration by a data breach, and as innocuous as unauthorized network activity by over-zealous employees. And while you may think you've prepared and practiced for a wide range of threats, have you ever considered how your Security Operations Centers (SOC) would react during a physical compromise? My team engages in physical security penetration, inserting ourselves within your perimeter and proceeding on-site through corporate campuses, office buildings, and data centers. During the course of such operations, we engage in a wide range of tactics specifically geared to frustrate and confuse SOC teams. This talk will walk attendees through a series of case studies of what can happen if attackers have direct access to doors, compromise your communication system, or don your own company uniforms. How would your SOC react to attackers who don't simply show up on network maps, but rather show up at the front door?

Deviant Ollam *(@deviantollam), Director of Education, CORE Group*

12:10-1:30 pm

Lunch & Learn Sessions

Modelling Advanced Playbooks with Siemplify
(LOCATION: BLAINE KERN E)

Intelligent Security SIEMPLIFY

SOC playbooks range from the general guideline to precise step-by-step procedures, and everything in between. Given this variability, many organizations considering a SOAR technology are concerned that their specific playbooks may not translate well from tribal knowledge/pen and paper to digital. If this is your situation, you are not alone. Working with enterprise organizations and MSSPs around the world, we have seen just about every playbook you can imagine and have developed our technology to make this transitioning them into the platform easy.

During this session, we will cover the following:

- The basics of SOAR playbooks
- How to model different types of playbooks
- Examples of putting playbooks to use
- Best practices in playbook creation

Meny Har, *VP Products*

Operationalizing Response to Close the "Breakout" Window
(LOCATION: BLAINE KERN F)

ENDGAME.

Nobody knows an organization's environment better than its IT security team. Software deployment tools, networking and routing nuances, threat models, operational IT tasks, change controls, and more, prove that there are many things that make one infrastructure infinitely unique compared with another. Yet security vendors try to solve the same problems for every organization in the same way. The most aggressive of preventions are disabled and often hidden, to avoid the deluge of false positives. Detections are suppressed until cloud services can analyze the stream of events and identify an attack, stopping potential alert fatigue and hiding inaccuracy, yet opening a threat window for adversaries to exploit. In this presentation, you will learn how you can prepare to respond to threats in real-time, closing the 'breakout window' between detection and response, and hear about Endgame's recently announced technology, Reflex, that was built with customized protection in mind.

Keith Weisman, *VP- Solutions Engineering, Endgame*

Tuesday, June 25

1:30-2:05 pm	***How to Literally Think Like an Attacker to Become a Better Defender*** For years, defenders have been educating themselves on the tradecraft being used by adversaries. At the same time, defenders continue to lose the battle, even when armed with some of the greatest talent and technologies in the world. Why is this? This talk will examine why technology alone is not helping close the gap and will explain the importance that our own minds play in the role of defense. Attendees will learn: • Key similarities between defenders and attackers • How to avoid counterfactual thinking that focuses on past negative events • The role our thoughts play in behavior and outcomes • Strategies for adopting a new forward-looking mindset that instills ownership, pride, and confidence ***Eric Groce**, Incident Handler, Red Canary*
2:05-2:40 pm	***Arming SecOps with a Special Forces Targeting Process*** In the face of high demand and limited resources, it is critical for security operations programs to work smarter, not harder. Using the F3EAD targeting process, we maximize our small unit resources to hunt and respond to threats in a large and highly complex environment. Find, Fix, Finish, Exploit, Analyze, Disseminate or F3EAD, is a methodology originating from military special forces doctrine that fuses the operations and intelligence cycles. F3EAD uses intelligence and targeting to increase the effectiveness and efficiency of hunt and response activities. This talk will provide key lessons learned from our experience using F3EAD and MITRE ATT&CK to protect high-value people and assets at a tier-one research institution. ***Andrew Stokes** (@_andrewstokes), Information Security Officer, Texas A&M Engineering*
2:40-3:00 pm	**Networking Break** (LOCATION: BLAINE KERN PRE-FUNCTION)
3:00-3:35 pm	***The Case for Building Your Own SOC Automations*** Security Orchestration, Automation and Response (SOAR) platforms are promising easy automation of security operations center (SOC) tasks, but can it be as easy as the product vendors say it is? Is there still a case to be made for learning how to automate SOC processes for yourself? Is all hope lost for those that do not have the latest SOAR products? What can be done when you ask your product vendor if they have compatibility with an existing network device and they respond with "We have an API"? Attendees will be given examples of how to automate security operations and intelligence gathering that they can use to mature their security operations. ***Nathanael Kenyon**, Mentor, SANS Institute*

Tuesday, June 25

3:35-4:10 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 of determining what a rogue device is. In this talk we will cover several of those methods along with their strengths and weaknesses. We'll also discuss the pros and cons of different responses that enterprises can take when rogues are found. But we will focus 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 to tackle a simple detection of a suspicious IP, add information to the event to make analysis easier, and show how that enhanced event can be used for automated responses. ***Craig Bowser*** *(@reswob10), Senior Security Engineer, U.S. Department of Energy*
4:10-4:45 pm	***This Will Never Work: Tales from Disappointingly Successful Pen Tests*** The deck is stacked against cyber defenders. Budget and responsibility scope seem to obey the inverse square law, budget shrinking exponentially as scope grows. Worse yet, internal breakdowns can be much more useful to an adversary than the latest zero day. Lapses in communication, unclear delineations of ownership, and neglecting to time-box security exceptions can cause far reaching blind spots. Over the years I've had the privilege of participating in engagements working closely with the SOC and forensic analysts, witnessing some forehead slapping, groan inducing moments that have made the words "This will never work" just as infamous as "Hold my beer" on my teams. Enjoy my cautionary tales, but learn from our previous blunders so you don't have to learn from your own! ***Derek Rook*** *(@_r00k_), Senior Manager – Offensive Security, Teradata; Instructor, SANS Institute*
4:45-5:00 pm	***Wrap-Up and To Do List***

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.