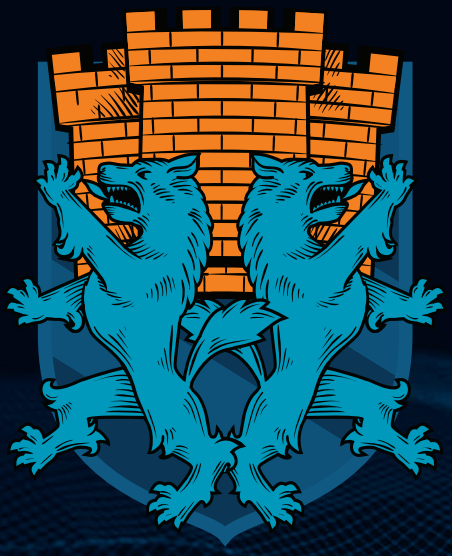
SANS



Blue Team
Summit 2019

@SANSDefense #SANSBlueTeam

Agenda

All Summit Sessions will be held in the Olmsted Ballroom (unless noted otherwise).

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

Thursday, April 11

7:00-9:00 am	**Registration & Coffee** (LOCATION: OLMSTED BALLROOM FOYER)
9:00-9:15 am	***Welcome & Opening Remarks*** ***Seth Misenar*** *(@sethmisenar), Principal Consultant, Context Security; Fellow, Co-Author SEC511, SEC542, MGT414, SANS Institute*
9:15-10:00 am	***Keynote: Threat Hunting via Sysmon*** Windows Sysinternal's Sysmon offers a wealth of information regarding processes running in a Windows environment (including malware). This talk will focus on leveraging Sysmon logs to centrally hunt malice in a Windows environment. Virtually all malware may be detected via event logs, especially after enabling Sysmon logs. Sysmon includes advanced capabilities, including logging the import hash (imphash) of each process, which fingerprints the names and order of DLLs loaded by a portable executable. This provides an excellent way of tracking families of related malware. We will also discuss updates to DeepWhite: an open source detective application whitelisting framework that relies on Microsoft Sysinternal's Sysmon and supports auto-submission of imphashes, EXE, DLL and driver hashes via a free Virustotal Community API key. ***Eric Conrad*** *(@eric_conrad), CTO, Backshore Communications; Fellow, Co-Author SEC511, SEC542, MGT414, SANS Institute*
10:00-10:30 am	**Networking Break** (LOCATION: OLMSTED BALLROOM FOYER)
10:30-11:05 am	***Azure AD Security Recommendations and the Customer Stories That Prove It*** Azure Active Directory has lots of features to help increase your organization's security posture. But which ones should you prioritize deploying? This session will discuss the key security quick wins you can go back and do immediately, best practices of deployment, and what has happened to other customers when they didn't deploy the security features they needed. ***Mark Morowczynski*** *(@markmorow) Principal Program Manager, Microsoft*
11:05-11:10 am	***Q&A***

Thursday, April 11

11:10-11:45 am	***Skill Sharpening at the CyberRange: Developing the Next-Generation Blue Team*** How do you gain defender skills? Do you know exactly how offense should inform defense? Are you learning on the job in the heat of the moment? How to you measure outcomes and ensure success? The development of blue team cyber operation skills depends on reusable, repeatable, and measurable scenarios that reflect complex networks to pit the blue team against a modern attacker. It isn't enough to take a class and run through a lab. Attackers and red teams have dozens of options (including your network), and so does the blue team. You can practice on a cyber range, but it's about much more than a few virtual machines. It's about a real outcome achieved by trained operators armed with tools, techniques, and practices that enable them to get in the hunt. This presentation will introduce you to a modern range, survey best-of-breed tools and capabilities, and highlight how a range can support skill development for the blue team operator. ***Don Murdoch*** *(@BlueTeamhb), author of* Blue Team Handbook: Incident Response *and* Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases*; Community Instructor and Courseware Developer, SANS Institute; Assistant Director, Institute for Cyber Security at Regent University*
11:45-11:50 am	***Q&A***
11:50 am – 12:25 pm	***To Blue with ATT&CK-Flavored Love*** MITRE ATT&CK was originally created by red and blue teamers working together in a giant lovefest known as the Fort Meade Experiment. Building on that history, this talk will provide a love letter rekindling that flame. The talk is more than an ATT&CK overview. The presenter will use his unique perspective from real-world red teaming experience to cover insights, lessons learned, and a general perspective of defense and the hunt in order to show how ATT&CK is a valuable tool to help red and blue teams work together to improve their defenses. Specific topics to be covered include: • Research Soap Boxes vs. the Mad, and Expensive, Real World – How the field of red team research is different from the real world and what that means for blue teamers. • Sensing and Analytics Done Right…Maybe – The sensor data blue teamers should be collecting in order to have the best chance to catch red teamers and adversaries, as well as how to write behavioral analytics to catch them. • What Does It Mean to Hunt and How Can Your Red Team Help? – Advice for blue teamers trying to undertake the mammoth task of threat hunting, and what that actually means. • How Do You Really Use ATT&CK? – ATT&CK is the new hotness. That's great and all, but how can we use it for real to make our defenses stronger? ***Jamie Williams*** *(@MITREattack), Cyber Adversarial Engineer, MITRE*
12:25-12:30 pm	***Q&A***
12:30-1:30 pm	**Lunch**

Thursday, April 11

1:30-2:05 pm	***Seriously, I Can Still See You*** Last year in Deadwood, South Dakota, strangers broke into my hotel (i.e., my network) and thought no one would notice the sound of the crashing front door. And no one did. Then they broke into an empty room (i.e., a desktop) and thought no one would notice that sound either. Again, no one did. Then they started to crack the locks between adjoining rooms and moving between them, thinking no one would notice. But I did, because my room was occupied, and I can show you how easy it was to see them. Silly thieves! I was there and my lights were on! And who uses the side doors anyhow?! This year the same thing happened, and it started the same way, but the attackers were smarter. Instead of breaking into the rooms one by one, they just slid notices under each door that said: "When you're ready to check out, don't dial zero as that extension is currently out of service. Instead, dial extension 666, and confirm your payment details there. Sorry for the inconvenience, and we hope you had a nice stay! – Management." Again, the attackers thought this would work nicely because guests wouldn't think anything of it, and because the real hotel management wouldn't notice until it was too late. Normally that would have worked, as it almost always does. But I watched them do it because, again, I was paying attention. When the room party at extension 666 was raging, I was standing outside the door. Imagine their surprise! Abuse of the Link Local Multicast Name Resolution (LLMNR) and Web Proxy Auto Detection (WPAD) protocols are probably the easiest way for an attacker to hijack your entire fleet's credentials and web traffic from right under your nose, LAN by LAN. Pay attention. I'll show you how easy it is to see. [Caveat venditor: no commercial tools are required!] ***Jonathan Ham*** *(@jhamcorp), Principal Systems & Security Architect, Rendition Infosec*
2:05-2:10 pm	***Q&A***
2:10-2:45 pm	***Using Statistical Analysis to Reduce Noise and Improve Efficacy*** Security analysts and engineers in Security Operations Centers all around the world are treading water. They come to work and respond to alerts. But there's a queue of alerts when they get to work, and the queue is still there when they leave. A few of the alerts may be legitimate indicators of malicious activity, but many are false positives, and still others are impossible to classify as either malicious or benign. This talk will demonstrate how to track the amount of time your blue team is spending on alerts and analyze relevant statistics to "tune" or even get rid of those alerts that are unnecessarily bogging you down. You'll learn what to measure and how to calculate useful data points, handle outliers, and build a security scoreboard. You'll also see when to take action, what "tuning" means for you, and how to track the impact of the decisions you end up making. Also included are specific examples in Splunk and Python and lessons learned along the way. Ultimately, this talk will empower you to optimize team resources, allowing your analysts to spend more time on fulfilling, proactive work. In other words, they can spend more time swimming and less time treading water or drowning. ***Keshia Levan*** *(@redcanaryco) Detection Engineering Lead, Red Canary* ***Kyle Rainey*** *(@verri3r), Detection Engineering Lead, Red Canary*
2:45-2:50 pm	***Q&A***
2:50-3:15 pm	**Networking Break** (LOCATION: OLMSTED BALLROOM FOYER)

Thursday, April 11

3:15-3:50 pm	***Cloud Security Challenges for the Blue Team*** It seems like we are being bombarded by reports of exposed data due to misconfigurations in cloud services. Gartner estimates that up to 95 percent of cloud security failures will be "the customer's fault" by 2020. There are many security benefits for the blue team, but it seems we are lacking the skills necessary to take advantage of these. This talk will focus on the security benefits provided by the cloud and the necessary skill sets that the blue team must focus on developing in order to ensure that our organizations do not become another cloud security failure. ***Marc Baker**, Online Training Subject-Matter Expert, SANS Institute*
3:50-3:55 pm	***Q&A***
3:55-4:30 pm	***Zero-Trust Networks: The Future Is Here*** The traditional perimeter-based security architecture used in sectors ranging from education to government and communications has basically failed to protect internal assets. New technologies such as the Internet of Things and mobile devices will force a new approach to network security architecture. Zero-trust networks (ZTNs) assume that the network is hostile, attackers are already inside the net, and segmentation isn't sufficient to determine trust, among other characteristics. This talk will describe zero-trust network properties and how we are integrating this architecture with existing cybersecurity defense strategies. We believe all sectors will have to adopt this strategy in the near future. In this talk, we'll explore ZTN components and their relationships, determine what off-the-shelf software can be used to build a ZTN, and help you improve your overall security posture by integrating ZTN concepts into your existing network architecture. ***Randy Marchany** (@randymarchany), CISO, Virginia Tech; Instructor, SANS Institute*
4:30-4:35 pm	***Q&A***
4:35-5:10 pm	***Suspiciously Inconspicuous*** One of the most challenging aspects of working for a security vendor is attempting to "catch everything" while simultaneously not inundating SOC teams with more alerts than they can realistically handle. It's a delicate balance of striving toward high-efficacy detections and reducing false positives. Even with high fidelity alerting, attackers are consistently developing new ways to subvert security controls, and remain hidden – oftein plain sight. This talk derives from the techniques that I've seen in the wild and have used in our internal testing to subvert various security technology stacks, such as Next Gen Firewalls, SIEM, Anti Virus, and EDR. More importantly, learn what you can do to close those gaps, and how the industry is shifting focus to better protect our shared customer base. We're all in this fight together, and separating the noise from the critical data is imperative to our shared success. ***Greg Foss** (@Heinzarelli), Senior Threat Researcher, Carbon Black*
5:10-5:15 pm	***Q&A***
6:00-9:00 pm	**Blue Team Summit Night Out!** Batter Up! It's a walk in the (ball)park as the Louisville Bats (AAA affiliate of the Cincinnati Reds) take on the Gwinnett Stripers (AAA affiliate of the Atlanta Braves), in their 2019 season home opener! Join us for food, drinks, networking and America's favorite pastime. We'll get you there and back, and even if you're not a baseball fan, this outing is sure to be a home run.

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.

Friday, April 12

7:00-9:00 am	**Coffee & Tea** (LOCATION: OLMSTED BALLROOM FOYER)
9:00-9:15 am	***Opening Remarks*** ***Eric Conrad*** *(@eric_conrad), CTO, Backshore Communications; Senior Instructor, Co-Author SEC511 and SEC542, Author MGT514, SANS Institute* ***Seth Misenar*** *(@sethmisenar), Principal Consultant, Context Security; Senior Instructor, Co-Author SEC511 and SEC542, SANS Institute*
9:15-10:00 am	***Network Flow Data: A Cornucopia of Value*** Did you realize that many network devices, such as routers, offer a treasure trove of data that can be analyzed to find unusual traffic patterns and intrusion activities on your network? Sure, most diligent companies have intrusion detection systems and sensors but even the best tuned solutions miss malicious behavior due to blind spots like sensor placement and encrypted payloads. Network flow data is a feature available on almost all networking products but is often overlooked as part of a defensible architecture. Need to hunt for lateral movement on a user segment that doesn't have a sensor? Flow data can provide visibility where other solutions fail. Come join me to learn tips for taking advantage of already available data. ***Andrew Laman*** *(@andylaman), Founder & Principal Consultant, A4 InfoSec; Instructor, SANS Institute*
10:00-10:30 am	**Networking Break** (LOCATION: OLMSTED BALLROOM FOYER)
10:30-11:05 am	***Forgotten But Not Gone: Gathering NTFS Artifacts of Deletion*** 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. ***Mari DeGrazia*** *(@MariDeGrazia), Senior Director, Incident Response, Kroll* ***Scott Hanson****, Senior Director- Cyber Risk, Kroll*
11:05-11:10 am	***Q&A***
11:10-11:45 am	***Mental Models for Effective Searching*** One of the most intimidating challenges many analysts encounter 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 you 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; Founder, Rural Technology Fund (@RuralTechFund)*
11:45-11:50 am	***Q&A***

Friday, April 12

11:50 am – 12:25 pm	***OSINT: Not Just Offensive*** Open-source intelligence (OSINT) is often considered an offensive tactic, as attackers seek to leverage publicly available information to tailor attacks to a specific environment. However, savvy defenders can use OSINT techniques and data to enhance security operations. We'll dig into some specifics for using open source intel as a defensive tool. ***David Mashburn*** *(@d_mashburn), Certified Instructor, SANS Institute, IT Security Manager, U.S. Pharmacopeia*
12:25-12:30 pm	***Q&A***
12:30-1:30 pm	**Lunch & Lightning Talks** (LOCATION: OLMSTED BALLROOM FOYER) Feeling inspired by all the great talks so far? Have something to add? Sign up here to give a lightning talk! The talks are five minutes each (slides not required). This session will not be recorded.
1:30-2:05 pm	***Relentless Team Building*** Given the current demand for highly skilled InfoSec professionals, it's easy to overlook how one achieves that level of proficiency. Drive, aptitude, and devotion all contribute to an individual's skillset, but one critical factor may often be disregarded: The importance of the team. Not everyone transitions from layperson to professional overnight. Some people need constructive mentoring to realize their growth potential. Others may simply need the opportunity to break into the field at large to find their niche before progressing on to future endeavors. If a key asset to professional growth is being part of a great team, who is supposed to build the team and how? This presentation focuses on the positive aspects of building, coaching, managing, and cultivating healthy teams. It covers the importance of maintaining ethical group and individual standards, effective measurements of success, and the value of investing in human capital. We will also cover the need for continual team enrichment through training and situational exercises. "The only thing worse than training your employees and having them leave is not training them and having them stay." –Henry Ford ***Dustin Lee*** *(@_dustinlee), Principal Engineer, Security Onion Solutions LLC*
2:05-2:10 pm	***Q&A***
2:10-2:45 pm	***One Phish, Two Phish, Red Phish, Green Phish*** Every single organization has an incredible amount of distributed horsepower just sitting around and doing nothing in their building. We are, of course, talking about your users! Many, if not hopefully all, orgs have some sort of "Phishing@acme.com" account that users can send suspicious emails for analysis by the information security team. However, without immediate gratification or response, they often become disenchanted with the process. Imagine if your user base was able to send emails in and have an automated process give a green/yellow/red response. This talk discusses how to use the tools stoQ and Splunk to automate analysis and defense while simultaneously improving user satisfaction. ***Dave Herrald*** *(@daveherrald), Staff Security Strategist, Splunk* ***Ryan Kovar*** *(@meansec), Principal Security Strategist, Splunk*
2:45-2:50 pm	***Q&A***
2:50-3:15 pm	**Networking Break** (LOCATION: OLMSTED BALLROOM FOYER)

Friday, April 12

3:15-3:50 pm	***Statically Analyzing Infrastructure as Code*** As more and more companies move towards a DevOps philosophy, infrastructure as code is gaining popularity. Tools like terraform, CloudFormation, puppet, and Ansible, now allow us to define our security controls as code. The upside of this is we can now apply application security methodologies to our infrastructure. At Wayfair, we have developed tooling to statically analyze terraform plans within our CI/CD pipeline for this purpose. It is currently used within our production environment to detect issues before deployment. This approach can easily translate to other orchestration frameworks and configuration management solutions. This talk details how we solved some our challenges and provides a sampling of tools you can use in your own build processes to improve your organization's security posture. ***Mike Siegel*** *(@ml_siegel), Red Team Lead, Wayfair LLC*
3:50-3:55 pm	***Q&A***
3:55-4:30 pm	***Spend Less Time Being a Data Janitor and More Time Doing Data Analysis*** Most analysts' time is spent figuring how to work with well-known data structures (CSV, JSON, XML). This process usually involves a combination of using Linux command line kung-fu or investing time to get data ingested into a SIEM. Furthermore, the pre-processor to machine learning is data normalization. This talk will show powerful ways to normalize, manipulate, visualize, and gain valuable insights from network security data using python programming and the Pandas framework. ***Austin Taylor*** *(@HuntOperator), Director of Cybersecurity R&D, IronNet Cybersecurity; Community Instructor, SANS Institute*
4:30-4:35 pm	***Q&A***
4:35-4:45 pm	***Closing Remarks*** ***Eric Conrad*** *(@eric_conrad), CTO, Backshore Communications; Senior Instructor, Co-Author SEC511 and SEC542, Author MGT514, SANS Institute* ***Seth Misenar*** *(@sethmisenar), Principal Consultant, Context Security; Senior Instructor, Co-Author SEC511 and SEC542, 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.