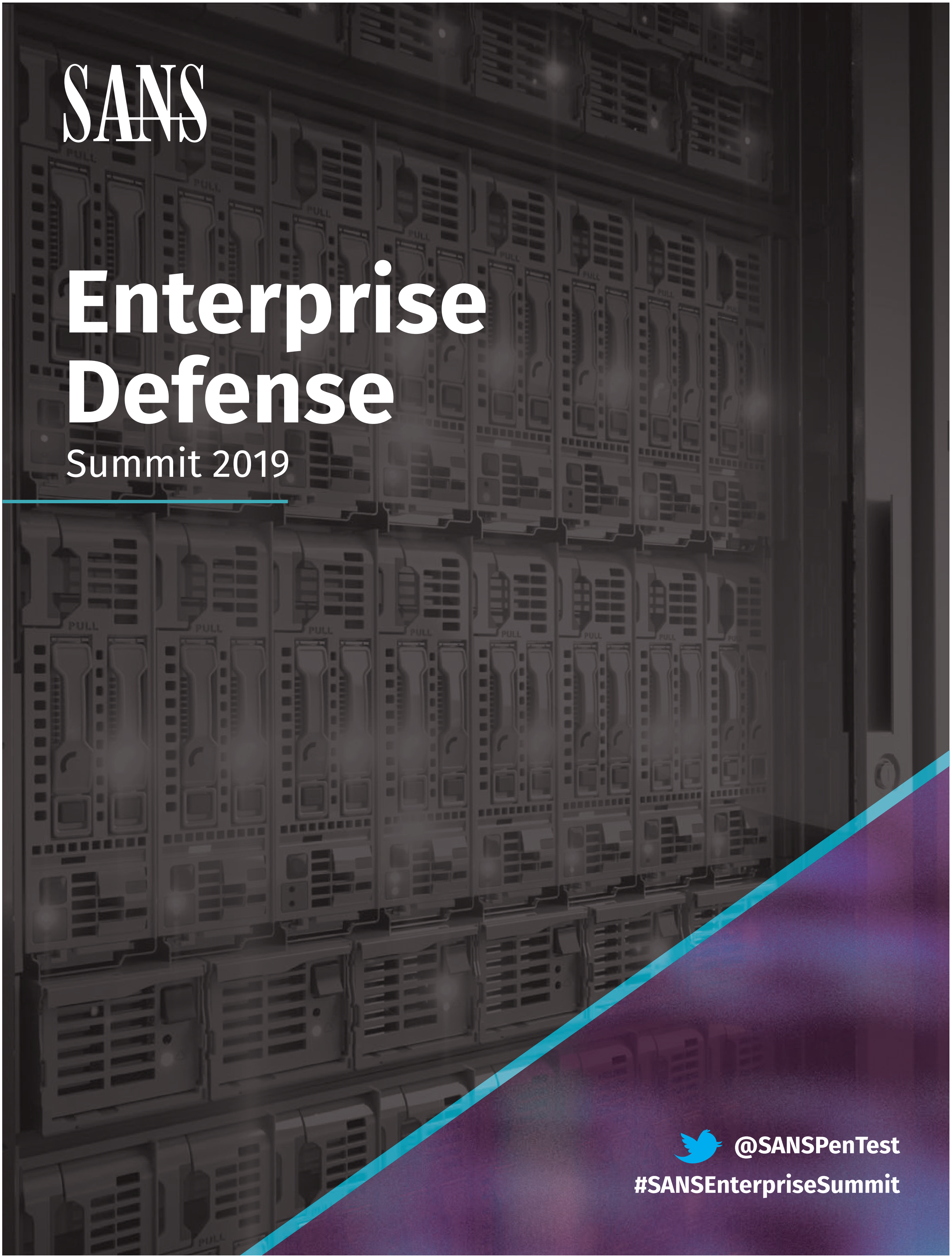

SANS

# Enterprise Defense

Summit 2019

@SANSPenTest

#SANSEnterpriseSummit

# Agenda

*All Summit Sessions will be held in the Peninsula/Pacific Ballroom (unless noted otherwise).*

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

## Monday, June 3

| | |
|---|---|
| **7:00-9:00 am** | **Registration & Coffee** (LOCATION: CORAL FOYER) |
| **9:00-9:15 am** | ***Welcome & Opening Remarks***<br>***Jeff McJunkin*** *(@jeffmcjunkin), Certified Instructor, SANS Institute*<br>***Alissa Torres*** *(@sibertor), Principal Instructor & Author, SANS Institute* |
| **9:15-10:00 am** | ***Keynote: Practical Detection Engineering at Scale***<br>Have you ever found yourself reviewing an automated alert, but no matter how hard you try you can't seem to answer simple questions about what is happening? What type of activity might have caused this alert to occur? What are the first steps an analyst should take to determine if this alert is real or is a false positive? Detection is just one of the components of a healthy defensive progam. However, it is often the component that most organizations struggle with the most. I will demystify the concept of Detection Engineering and provide guidance for how you can integrate it into your day to day operations. This talk will provide a practical Detection Engineering use case and demonstrate steps that can convert your effort from yet another ignored alert to a robust detection with the tools and context analysts need to successfully track it down.<br>***Jared Atkinson*** *(@jaredcatkinson), Adversary Detection Technical Lead, SpectreOps* |
| **10:00-10:30 am** | **Networking Break** (LOCATION: CORAL FOYER) |
| **10:30-11:10 am** | ***Legacy Authentication and Password Spray, Understanding and Stopping Attackers' Favorite TTPs in Azure AD***<br>One of attackers' favorite techniques today is password spraying. And it should be: in August 2018, 200,000 accounts were compromised using this method. Nearly all password spray attacks are targeting legacy authentication protocols. The good news is there are several steps you can take to prevent this type of attack. In this session we will focus on what legacy authentication is, how to look for it in your environment and what you need to do to prevent it from compromising your accounts.<br>***Ramiro Calderon*** *(@ramirocld), Principal Program Manager – Azure AD, Microsoft*<br>***Mark Morowczynski*** *(@markmorow), Principal Program Manager, Microsoft* |
| **11:10-11:50 am** | ***Assumed Breach: A Better Model for Penetration Testing***<br>The current model for penetration testing is broken. The typical scan and exploit model doesn't reflect how real attackers operate after establishing a foothold. At the same time, most organizations aren't mature enough to need a proper Red Team assessment. It's time to start adopting the assumed breach model. In this talk, I'll discuss techniques for assumed breach assessments that provide a better model for emulating the techniques attackers use once they've established a foothold inside a typical network.<br>***Mike Saunders****, Principal Consultant, Red Siege* |
| **11:50 am – 1:00 pm** | **Lunch** (LOCATION: CORAL FOYER) |

## Monday, June 3

**1:00-1:45 pm**

### *Five Mistakes We Wish Users Would Stop Making*

Despite the carrots and sticks, admonishments, and reward gift cards, enterprise users continue to make critical missteps. This talk presents the top five mistakes that users continue to make, despite seemingly obvious (to us!) consequences. Why are organizations, even those with impressive technology stacks and defensive layers, still vulnerable to user misbehavior? What can security teams do to shape user behavior to eliminate or at least mitigate these risks? Bring your best enterprise user awareness solutions as Chelle and Lee share what works based on their professional experiences. They'll also collect feedback from participants, and give everyone actionable ideas to take home.

***Chelle Clements***, *Web Mistress, OMP*

***Lee Neely***, *Senior Cyber Analyst, Lawrence Livermore National Laboratory*

**1:45-2:25 pm**

### *Realigning from Chaotic Evil*

Organizations, especially at the enterprise level, often fail to align the goals and incentives of offensive and defensive teams. This can lead to those teams working to satisfy metrics that don't actually help the organization close security gaps. In the worst cases, the teams can actually be working against each other. This talk explores the basics of Purple Team strategies that can allow both sides to benefit from each other's skills and knowledge. We'll also look at some common organizational issues that both teams can attempt to address to ensure that their performance reviews reflect bringing real security to their organization rather than meeting arbitrary numbers.

***Joe Schottman*** *(@JoeSchottman), Senior Security Analyst, BB&T*

**2:25-3:00 pm**

### *Sky-High Incident Response at Cloud Scale*

Does your organization plan ahead for Incident Response (IR) events? Have you accounted for the unique challenges that diverse cloud environments pose for incident responders? In this talk, we'll explore the tactical, strategic, and even legal implications of conducting IR operations in public, private, and hybrid cloud environments. We'll look at supporting architecture, scenarios, and industry trends as well, with the goal of arming you with information and knowledge to conduct IR in the cloud. Finally, we will look at critical components, tools, and some crown jewels to discuss how they could be compromised and thus derail your (or your client's) IR processes.

***Aaron Lancaster*** *(@aarondlancaster), Senior Security Engineer, BB&T*

**3:00-3:30 pm** **Networking Break** (LOCATION: CORAL FOYER)

**3:30-4:10 pm**

### *The Offensive Defender: Cyberspace Trapping*

The attackers always win because they have the advantage. Wrong! Any seasoned Red Teamer knows that while attackers need to succeed at each stage of their compromise to achieve their objective, we as defenders only need to stop them along one point in the intrusion. By leveraging our "home field advantage" and weaponizing our networks with traps and snares, we have the opportunity to take the initiative and bring the fight to the intrusion set. Attackers may have an untold and ever-growing number of tools and techniques to use during the attack, but they have a limited set of tried-and-true tactics. Targeting the adversary and poisoning those tactics enable us to weaponize our environments and transform attackers' own decision-making into their undoing. When attackers can never be certain if their own, unique tools are safe for them to use, their decision-making gets disrupted and we've already won the fight. This talk is about the strategy of cyberspace trapping and includes a library of scripts and demonstrations for attendees to take with them and apply on day 0.

***Matthew Toussain*** *(@0sm0s1z), CTO, Open Security; Certified Instructor, SANS Institute*

## Monday, June 3

4:10-4:45 pm

### *LOLBin Detection Methods: Seven Common Attacks Revealed*

Primary objectives of survivability and evasion have shaped the tactics employed by today's threat actors in victim environments. Attackers utilize fileless methods of payload download, persistence, reconnaissance and exfiltration to blend into the white noise of normal operations. By actioning native Windows utilities and minimizing creation of file-system artifacts, malicious activity can exist undetected and evade sophisticated host intrusion detection strategies. In the absence of common indicators of compromise, how can analysts detect these living off the land threats such as fileless persistence, dual-use tools and memory-only malicious execution? This presentation will walk through detection methods for seven common LOLbins and fileless attacks and returns the upperhand to the Blue Team.

***Alissa Torres*** *(@sibertor), Principal Instructor & Author, SANS Institute*

5:30-8:00 pm

### Sittin' on the Dock of the Bay

179 N. Harbor Drive, Redondo Beach, CA 90277

Soak up the SoCal sea breezes (and possibly spot some harbor seals) at **R/10 Social House**. This waterfront gastropub is just a 5-minute walk from the hotel and offers panoramic views of King Harbor Marina. Food, drinks, and relaxing salt air are included.

**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, June 4

7:00-9:00 am

**Coffee & Tea** (LOCATION: CORAL FOYER)

9:00-9:45 am

***Keynote: With Great Scale Comes Great Responsibility***

Enterprise Incident Responders are heavily involved in a variety of incidents: some straightforward, some critical, some complex, some even overwhelming for large and mature teams. To succeed in this environment, we need scalable tools and processes that are both flexible and powerful. James will talk through the peculiarities, complexities and opportunities that come with responding at scale, while also outlining the responsibilities that come along with that.

***James Nettesheim*** *(@JamesNettesheim), Security Engineer, Google*

9:45-10:15 am

***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, which is, 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 to make a simple detection of a suspicious IP and add 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*

10:15-10:45 am

**Networking Break** (LOCATION: CORAL FOYER)

10:45-11:25 am

***Do-It-Yourself ATT&CK™ Evaluations to Improve YOUR Security Posture***

This talk will enable defenders to improve their security posture through the use of adversary emulation by performing their very own ATT&CK Evaluations. MITRE ATT&CK evaluations use an open methodology based on the ATT&CK framework to evaluate cybersecurity products and then publicly release all evaluation results. This provides transparency around the true detection capabilities of security products and services, and it drives the security vendor community to enhance its capabilities to detect known adversary behaviors. Do-It-Yourself ATT&CK Evaluations will provide you with that same level of transparency surrounding detection capabilities. By using a few different open-source projects and the ATT&CK Evaluation methodology, you can evaluate your personalized defensive setup no matter the tooling and respective configurations within your environment. The ATT&CK Evaluations have given vendors an objective platform to demonstrate to the community and their own customers the unique ways that their tool presented detection capabilities given the techniques and procedures tested. So why not empower your Blue Teams to do the same?

***Daniel Weiss*** *(@d4weiss), Cyber Security Engineer, MITRE*

## Tuesday, June 4

11:25 am – 12:00 pm

### *Finding Evil with Skadi*

Security teams and those trying to get into Digital Forensics and Incident Response (DFIR) share a common problem: how to find a DFIR platform that enables the quick and easy collection, processing, and analysis of data from MacOS, Linux, and Windows endpoints. The platform needs to be one where all of the components work together out of the box, that requires little training to set up, and that can run on either a student's laptop, a server, or in the Cloud. The open-source community is full of fantastic tools, but getting them to work together requires a very high level of systems administration skill and experience. What if you could solve this problem with an open-source DFIR solution that includes CDQR, CyberChef, CyLR, Plaso, and TimeSketch? It would be a platform where all of the dependencies have been installed and configured to a point where everything works! That's where the Skadi project comes in. Skadi is a DFIR solution that can be deployed on either a laptop, server, or cloud instance via a turnkey OVA or a Vagrant box, or as a digitally signed installation script. It enables anyone to easily collect data from MacOS, Linux, or Windows endpoints, process that data into CSV, ElasticSearch, and TimeSketch formats, and review the results in a web UI using either Kibana (using over 45 custom searches/visualizations/dashboards) or TimeSketch. This talk provides guidance on how to effectively deploy and use Skadi for data collection, processing, and analysis. It covers what to consider for quick and easy deployment for various use cases. Skadi works just as well for the student trying to learn and practice DFIR as it does for the professional team looking for a solid foundation to build upon. The primary goal of this talk is to share best practices and lessons learned about how to quickly and effectively use Skadi to practice DFIR fundamentals and find evil in any environment.

***Alan Orlikoski** (@AlanOrlikoski), Security Engineer*

12:00-1:15 pm

### Lunch (LOCATION: CORAL FOYER)

1:15-1:55 pm

### *Finding a Domain's Worth of Malware*

Are you tired of demonstrations of products that take months or years to get effective data from? How many products have you seen half-implemented (but fully paid for!) that didn't ever deliver any real value to your organization? Here, I'll discuss multiple free products that you can use next week to find evil inside your organization. Some techniques will find less advanced adversaries, and some will trip up even some of the most advanced ones - but they'll all deliver value in less than a week of implementation, and I'll discuss how you can integrate them and find the malware you already have in your environment. "Assume breach"...then find it!

***Jeff McJunkin** (@jeffmcjunkin), Certified Instructor, SANS Institute*

1:55-2:30 pm

### *Hide and Seek: Where Your Business Does Business*

Most organizations use the cloud in some form or another. But do you know all the software-as-a-service (SaaS) applications configured for your domain? This session will provide an overview of the free CloudSeeker tool and how you can use it to help your organization gain insight into which apps are in use, uncover applications provisioned without IT knowledge, and identify risks to your organization. We will also walk through how threat actors can use this information to target your organization with credential phishing.

***Tonia Dudley** (@_tdudley), Security Solutions Advisor, Cofense*

2:30-2:50 pm

### Networking Break (LOCATION: CORAL FOYER)

| Tuesday, June 4 | |
|---|---|
| **2:50-3:30 pm** | ***The Best of Both Worlds: Blending Tactics from the Public and Private Sectors***<br>Public and private enterprises face the same threats, and yet often have different approaches to defense. What if you could take some of the best tactics from each and blend them together? What if I told you this is already happening in small pockets around the US? Enhance your defenses by studying the strengths and weaknesses of each sector and blending tactics from both.<br>***Josh Bryant*** *(@FixtheExchange), Director of Technical Account Management, Tanium* |
| **3:30-4:10 pm** | ***Creating Incident Response Playbooks***<br>Incident Response is a lot like fighting fires. While your house is burning down is not the best time to try to come up with a plan for how to properly put out a fire. By developing a series of plans for the most common types of incidents, the response steps can be laid out ahead of time and then followed when needed. Following a pre-planned playbook ensures actions occur quickly, no steps are missed, incidents are responded to consistently, and new incident responders can easily fall into the team's way of responding. In this presentation we will discuss how to develop your own incident response playbooks customized specifically to your environment.<br>***Chris Taylor****, Incident Response Consultant, Taksati Consulting* |
| **4:10-4:50 pm** | ***Analyst Unknown Cyber Range (AUCR): A Standardized Open Source Web Framework***<br>Problem:<br>The open-source tools community has a large number of issues when it comes to web UIs. Often tools lack critical security features like 2fa, oauth tokens for APIs, or even more simple the use of LDAP as a back-end, etc. We can take examples from MISP to the Hive to cuckoo. All these tools have amazing capabilities and handle sensitive data for most organizations. However, when it comes to security features, they are, in some cases, non-existent. Even some of the most basic functions, such as password resets are not supported.<br>Solution:<br>I created a framework the Analyst Unknown Cyber Range that by itself does all this while doing nothing else. It's a micro web service that has an extendable plugin system to manage any possible need an analyst can have. I created this base framework to solve these issues and give basic functions as easy as argparse to use, so developers can easily convert code into a plugin.<br>***Wyatt Roersma*** *(@WyattRoersma), Senior Cyber Defense Operator, SimSpace* |
| **4:50-5:00 pm** | ***Closing Remarks***<br>***Jeff McJunkin*** *(@jeffmcjunkin), Certified Instructor, SANS Institute*<br>***Alissa Torres*** *(@sibertor), Principal Instructor & Author, 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.*

**@SANSPenTest** **#SANSEnterpriseSummit**