SANS

Cloud Security

Summit 2019

@SANSDefense #SANSCloudSummit

Agenda

All Summit Sessions will be held in the Fir/Oak Ballroom (unless noted otherwise).

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

Monday, April 29

7:00-9:00 am	**Registration & Coffee** (LOCATION: GATEWAY FOYER)
9:00-9:15 am	***Welcome & Opening Remarks*** ***Ben Hagen*** *(@benhagen), Summit Co-Chair, SANS Institute* ***Dave Shackleford*** *(@daveshackleford), Summit Co-Chair & Senior Instructor, SANS Institute*
9:15-10:00 am	***Cloud Security at its Finest*** This talk will explore the best and sparkliest cloud security has to offer; focusing on new techniques, ideas, and defenses in use at organizations across industries. The thrill of discovering new techniques for sanity, however, will quickly be quelled with the harsh reality of where we, the security community, and the need to improve. Join this emotional roller coaster to understand where we are, where we are going, and what matters right now. ***Ben Hagen*** *(@benhagen), Summit Co-Chair, SANS Institute*
10:00-10:30 am	**Networking Break** (LOCATION: GATEWAY FOYER)
10:30-11:05 am	***Secrets for All the Things: The Injection of Secrets for Every Application in Your Cloud-Agnostic Environment*** In this presentation we'll discuss why a centralized location for the management of secrets is important, and how to leverage this to retrieve secrets for applications and micro-services across multiple cloud environments. These environments include Amazon Web Services, Google Cloud Platform, and container orchestration platforms like Kubernetes, EKS, and GKE. We'll provide examples of each platform using secrets management solutions like Hashicorp Vault, and we'll look at how to reduce friction for application owners by automating this process with the help of custom-tailored sidecar containers. ***Brian Nuszkowski****, Staff Security Engineer, Cruise Automation* ***Mike Ruth*** *(@MF_Ruth), Staff Security Engineer, Cruise Automation*
11:05-11:40 am	***Keep it Flexible: How Cloud Makes it Easier and Harder to Detect Bad Stuff*** It's a new world—a cloud world. Everyone is moving to AWS because of its ease and scalability. However, with that flexibility comes security challenges. To actively monitor and secure their networks, AWS cloud customers need to understand what cloud services our on-premises technologies correspond to, what data is security-relevant, where and how to get that data, and then how that data can be used to detect malicious activity. This talk will focus on great places to start collecting data and then how to make use of it. ***Lily Lee****, Staff Security Specialist, Splunk*

Monday, April 29

11:40 am – 12:15 pm

Automating Cloud Security Monitoring at Scale

The big three cloud providers innovate at a pace that security teams have a hard time keeping up with. New architectural patterns for cloud security and governance call for each team or application to get its own account to limit blast radius and provide for better financial accountability. The depth of services and the breadth of accounts across multiple different cloud providers prevent many security organizations from detecting issues before they become a data breach. Most vendor-based solutions either lack the ability to scale to hundreds of accounts or ignore the misconfiguration risks of the newer, more advanced offerings from the cloud providers. Cloud providers innovate faster than the security vendor community, and the security team shouldn't have to slow the adoption of new services because our vendor community cannot keep up. Turner Broadcasting is a cloud-first organization with a variety of brands ranging from CNN to the Cartoon Network and Adult Swim, in addition to broadcast and streaming partnerships with organizations such as the National Basketball Association and the National Collegiate Athletic Association. Turner operates in all three public cloud providers. In this talk, we will touch on the history of our cloud migration and dive deep into how we blended a set of policies with a swarm of Amazon Web Services lambda to deliver customized compliance reports to all of our business stakeholders for all three public clouds. Attendees will come away with a strategy and actionable set of tasks to kick-start their cloud security programs, along with guidance on how to find and select tools they can use to automate configuration checking at scale.

***Chris Farris** (@jcfarris), Cloud Security Architect, Turner Broadcasting*

12:15-1:30 pm

Lunch

1:30-2:05 pm

Who Done It? Gaining Visibility and Accountability in the Cloud

Every day more enterprises are incorporating cloud services and workflows. Moving data to the public cloud has many advantages, but it also brings new risks and challenges for the security team. While traditional techniques and controls can be applied in many cases, there are also new areas involving cloud-native services and APIs unique to this environment. In this presentation, we will explore several use cases, techniques, and tools that can be applied to resolve the challenges associated with moving data to the cloud.

***Marta Gomez-Macias** (@Mrs_DarkDonato), IT Security Developer, Wazuh*

***Ryan Nolette** (@sonofagl1tch), Security Engineer, Independent Researcher*

2:05-2:40 pm

Automating the Creation of Network Firewall Rules Using PowerShell and CI/CD

Managing firewall rules is a complex task. During this talk, we'll discuss one way to automate the creation and management of those firewall rules using PowerShell and a continuous integration and deployment (CI/CD) pipeline. The basis of the presentation is an actual customer implementation of this end-to-end process. We will discuss the requirements for the solution and how this solution was developed and has grown from proof of concept to production. Although the implementation is Azure-specific, the talk will be abstracted to showcase the feasibility of this approach across multiple clouds. Demos presented during the talk will showcase the PowerShell script and then the end-to-end workflow using Azure DevOps.

***Nills Franssens** (@nillsf), Cloud Solution Architect, Microsoft*

2:40-3:10 pm

Networking Break (LOCATION: GATEWAY FOYER)

Monday, April 29

3:10-3:45 pm

Locking Them Out of Their Own House: Access Control to Cloud at Startups

As a security engineer, when you join a startup or smaller company, it's likely there isn't going to be gold standard access control to services, especially cloud services. When you don't even know who works on what, or what works on which, how do you navigate determining who gets access? On top of that, how they get access? We'll run through some of my experiences setting up cloud access control as well as pitfalls and tips I've learned along the way.

Jackie Bow*, Security Operations Engineer, Patreon*

3:45-4:30 pm

Panel: Cloud Security as Culture

This panel will focus on the wins and failures experienced by panel participants in promoting cloud security initiatives within their organizations. We will also explore the culture and mind shifts necessary to adapt to new security models and mentalities.

MODERATOR:
Ben Hagen *(@benhagen), Summit Co-Chair, SANS Institute*

PANELISTS:
Will Bengtson *(@_muscles), Cloud Security Tools & Operations, Netflix*
Jackie Bow*, Security Operations Engineer, Patreon*
Mike Ruth *(@MF_Ruth), Staff Security Engineer, Cruise Automation*

5:15-7:15 pm

Get Real: Summit Night Out

The 6th Floor Orchid Room at the Casino M8trix | 1887 Matrix Boulevard, San Jose, CA 95110

After a long day of learning, get out of the hotel and shake it off with virtual reality games in a private event space overlooking Silicon Valley. We'll have food, drinks, and lots of fun. The Orchid Room is a quick walk from the hotel, and everyone is invited. Just wear your Summit badge.

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, April 30

7:00-9:00 am

Coffee & Tea (LOCATION: GATEWAY FOYER)

9:00-9:45 am

The State of Cloud Security: How Does Your Organization Compare?

Be the first to hear highlights from the SANS 2019 Cloud Security Survey, conducted in cooperation with the Cloud Security Alliance, concerning organizations' use of the public cloud. The survey, and Shack's commentary and insights, will provide actionable advice for attendees to improve their cloud security. Topics include: types of applications that are implemented most frequently through the cloud; Concerns organizations have about use of the public cloud and the frequency of those concerns becoming realities; issues associated with public cloud breaches; technologies used to secure sensitive data in the cloud and integrate with in-house environments; challenges organizations face in adapting incident response and forensics to a cloud environment.

Dave Shackleford *(@daveshackleford), Summit Co-Chair & Senior Instructor, SANS Institute*

9:45-10:20 am

Serverless Security: Attackers and Defenders

In serverless applications, the cloud provider is responsible for securing the underlying infrastructure, from the data centers all the way up to the container and run-time environment. This relieves much of the security burden from the application owner, but it also poses many unique challenges when it comes to securing the application layer. In this presentation, we will discuss the most critical challenges related to securing serverless applications, from development to deployment. We will also walk through a live demo of a realistic serverless application that contains several common vulnerabilities, and see how they can be exploited by attackers and how to secure them. We will also use examples from a recent story published in Dark-Reading magazine on how we hacked a real-world serverless application and won the $1,000 bounty!

Ory Segal *(@orysegal), CTO, PureSec*

10:20-10:50 am

Networking Break (LOCATION: GATEWAY FOYER)

10:50-11:25 am

Secure by Default: Enabling Developers to Focus on Their Mission by Providing Cloud Security for Free

Riot Games aims to deliver security for free to our developers to enable them to focus on making games. From a tooling perspective, we do this by leveraging both our in-house skills and off-the-shelf tech to create developer-focused, maintainable and scalable solutions. This talk will cover how we:

- Built security into our "AWS account creation" process such that security is there for free and the process is easy and repeatable with AWS Lambda and Step Functions
- Developed our own temporal auth solution for AWS, leveraging AWS STS and proprietary solutions resulting in both a more secure method of auth and a vastly reduced permanent AWS credential footprint
- Are moving forward with security in the cloud with some discussion on our future direction as new products get rolled out

Reza Nikoopour *(@RNikoopour), Security Engineer, Riot Games*

Zachary Pritchard*, Security Engineer, Riot Games*

Tuesday, April 30

11:25 am-12:10 pm

Demonstration of Typical Forensic Techniques for AWS EC2 Instances

This demo is a step-by-step walk-through of techniques that can be used to perform forensics on Amazon Web Services (AWS) Elastic Cloud Compute (EC2) instances. During the demonstration we'll use a cloud-based SIFT Workstation and a systematic methodology to find malware and Indicators of Compromise (IOC) on an compromised Elastic Block Storage (EBS) Volume. For more info, see https://forensicate.cloud

***Kenneth G. Hartman** (@KennethGHartman), Security Consultant;*
Community Instructor, SANS Institute

12:10-1:30 pm

Lunch

1:30-2:05 pm

Cloud, the Hard Way

This talk will focus on understanding what it takes to deploy in the cloud and some concepts/techniques to make living in the cloud easier in the long term. We will discuss approaches to deployments with immutable infrastructure, identify building blocks, add some chaos to your life, and coast home on the paved road for your organization.

***Will Bengtson** (@__muscles), Cloud Security Tools & Operations, Netflix*

2:05-2:40 pm

Cloud DFIR: Why so Cirrus?

As companies move to cloud-based methods of collaboration, the days of looking thru MFT files for digital artifacts are quickly becoming thin and wispy. This talk will examine a real case study of tracking an advanced adversary through a modern cloud environment by following various breadcrumbs involving logs, emails, infrastructure and files. Additionally, we will provide recommendations to help practitioners answer the "5Ws and H" surrounding attacks involving cloud infrastructure. At the end of this talk, practitioners will be able to take our techniques and apply them to various cloud environments, and guide understand what they should be capturing for proper visibility.

***Rick Correa**, Senior Operations Security Manager, Box*

2:40-3:10 pm

Networking Break (LOCATION: GATEWAY FOYER)

3:10-3:45 pm

Securing your Application Identities

As organizations are modernizing their applications and moving them to the cloud, the challenge of securing your application identities, the way your applications authenticate themselves to access secrets/data necessary to run, becomes very important. The old paradigms of service accounts are shifting to newer technologies that help your applications to become more secure by default. Come learn how you can secure your application identities in Azure Active Directory and in the Azure Eco System and avoid common anti-patterns as you move more and more of your IaaS and PaaS components to the cloud.

***Tarek Dawoud**, Lead Architect, Microsoft*

***Alexander Pavlovsky**, Lead Program Manager, Microsoft*

Tuesday, April 30

3:45-4:00 pm	***Closing Remarks & To-Do List*** Learn how to leverage security automation in your cloud infrastructure, DevOps pipeline, and applications. Using the open source Cloud Custodian tool, you'll see how AWS CloudTrail, CloudWatch, and Lambda are used to implement automated infrastructure monitoring and remediation. Then you'll see how DevOps security automation and Infrastructure as Code is used to build a Blue/Green deployment infrastructure to quickly patch critical security vulnerabilities. Finally, using the open source AWS WAF Security Automations project you'll see how it can be automatically deployed via your Jenkins CI/CD pipeline, how the WAF leverages Lambda for automation, and how it automatically blocks critical application vulnerabilities. ***Ben Hagen*** *(@benhagen), Summit Co-Chair, SANS Institute* ***Dave Shackleford*** *(@daveshackleford), Summit Co-Chair & Senior 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.