
| Monday, April 29 | |
|---|---|
| 9:00-9:15 am | *Welcome & Opening Remarks*<br>**Ben Hagen (@benhagen), Summit Co-Chair, SANS Institute**<br>**Dave Shackleford @daveshackleford, Summit Co-Chair & Senior Instructor, SANS Institute** |
| 9:15-10:00 am | *Keynote to be announced* |
| 10:00-10:30 am | Networking Break |
| 10:30-11:05 am | **Secrets for All the Things: The Injection of Secrets for Every Application in Your Cloud-Agnostic Environment**<br>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.<br>**Brian Nuszkowski, Staff Security Engineer, Cruise Automation**<br>**Mike Ruth (@MF_Ruth), Staff Security Engineer, Cruise Automation** |
| 11:05-11:40 am | **Demonstration of Typical Forensic Techniques for AWS EC2 Instances**<br>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 various tools such as LiME, Magarita Shotgun, AWS-IR, SIFT, Rekall, and Volatility. For more information, see bit.ly/cloud_dfir_demo and bit.ly/2NwmBVH.<br>**Kenneth G. Hartman (@KennethGHartman), Security Consultant; Community Instructor, SANS Institute** |
| 11:40 am – 12:15 pm | **Automating Cloud Security Monitoring at Scale**<br>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 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 program, along with guidance on how to find and select tools they can use to automate configuration checking at scale.<br>**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**<br>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.<br>**Marta Gomez-Macias (@Mrs_DarkDonato), IT Security Developer, Wazuh**<br>**Ryan Nolette (@sonofagl1tch), Security Engineer, Independent Researcher** |
| 2:05-2:40 pm | **Automating the Creation of Network Firewall Rules Using PowerShell and CI/CD**<br>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.<br>**Nills Franssens (@nillsf), Cloud Solution Architect, Microsoft** |

| | |
|---|---|
| 2:40-3:10 pm | **Networking Break** |
| 3:10-3:45 pm | **Locking Them out of Their Own House: Access Control to Cloud at Startups**<br>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.<br>**Jackie Bow, Security Operations Engineer, Patreon** |
| 3:45-4:30 pm | *Panel*<br>**Cloud Security as Culture**<br>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.<br>**Moderator**: **Ben Hagen (@benhagen), Summit Co-Chair, SANS Institute**<br>*Panelists to be named* |
| 6:00-8:00 pm | **Get Real: Summit Night Out**<br>After a long day of learning, get out of the hotel and shake it off with virtual reality games in a private space overlooking Silicon Valley. We'll have food, drinks, and lots of fun. The space is a quick walk from the hotel, and everyone is invited. Just wear your Summit badge. |
| **Tuesday, April 30** | |
| 9:00-9:45 am | **The State of Cloud Security: How Does Your Organization Compare?**<br>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** |
| 9:45-10:15 am | **Networking Break** |
| 10:15-10:50 am | **Serverless Security: Attackers and Defenders**<br>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!<br>**Ory Segal (@orysegal), CTO, PureSec** |
| 10:50-11:25 am | **Secure by Default - Enabling developers to focus on their mission by providing cloud security for free**<br>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:<br>• 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<br>• 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<br>• Are moving forward with security in the cloud with some discussion on our future direction as new products get rolled out<br>**Reza Nikoopour, Security Engineer, Riot Games**<br>**Zachary Pritchard, Security Engineer, Riot Games** |
| 11:25 am-12:10 pm | *Talk to be announced* |
| 12:10-1:30 pm | **Lunch** |
| 1:30-2:05 pm | |

| | |
|---|---|
| | *Talk to be announced* |
| 2:05-2:40 pm | *Talk to be announced* |
| 2:40-3:00 pm | **Networking Break** |
| 3:00-3:35 pm | *Talk to be announced* |
| 3:35-4:10 pm | *Talk to be announced*<br>**Frank Kim @fykim, Senior Instructor, SANS Institute** |
| 4:10-4:45 pm | *Talk to be announced* |

Reza Nikoopour works as a Security Engineer at Riot Games on the Platform Security team. He began his career as a penetration tester then shifted over to focusing on cloud security.

Zachary Pritchard works as a Security Engineer at Riot Games on the Platform Security team. He is a security enthusiast and has worked in many fields in the industry, but specializes in cloud security.