Monday, April 29	
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, need to improve. Join this emotional roller coaster to understand where we are, where we're going, and what matters right now. **Ben Hagen (@benhagen), Summit Co-Chair, SANS Institute**
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** 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 corresponded 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
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 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. **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**
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 to be named*
6:00-8:00 pm	**Get Real: Summit Night Out** 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?** 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** 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**
10:50-11:25 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, Security Engineer, Riot Games** **Zachary Pritchard, Security Engineer, Riot Games**

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 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, SIRT Manager, Box**
2:40-3:10 pm	**Networking Break**
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 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**
3:45-4:20 pm	**Cloud Security Automation: From Infrastructure to App** 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. **Frank Kim @fykim, Senior Instructor, SANS Institute**
4:20-4:30 pm	*Closing Remarks & To-Do List* **Ben Hagen (@benhagen), Summit Co-Chair, SANS Institute** **Dave Shackleford @daveshackleford, Summit Co-Chair & Senior Instructor, SANS Institute**

Speaker Biographies

Will Bengtson @__muscles, Cloud Security Tools & Operations, Netflix
Will Bengtson is a senior security engineer at Netflix, focused on security operations and tooling. Prior to Netflix, Bengtson led security at a healthcare data analytics startup, consulted across various industries in the private sector, and spent many years in the Department of Defense. Bengtson is on the BSidesSF and Bay Area OWASP leadership team. Bengtson contributes to numerous open source projects and has spoken on topics of security across the world.

Rick Correa, SIRT Manager, Box
Rick Correa is interested in creating and implementing new methods of detecting unknown and suspicious network activity and files. He works on reversing malware, tool creation for analysis, and threat intelligence. Currently a lot of his time is spent doing data exploration, tinkering with statistical analysis, machine learning, and building a SIRT Team in Austin, TX.

Tarek Dawoud, Lead Architect, Microsoft
Tarek is a lead architect in the Identity Division's Customer Success Team at Microsoft. He has 8 years' experience as an engineer in one of the world's leading and largest scale cloud identity solutions and 4 years as the technical lead of the customer success team inside the Identity Division. Tarek has worked with some of the largest Fortune 500 companies helping them design their transition to a Cloud IAM strategy and plan their solution. He has also co-authored various white papers on the Architecture of Microsoft's Cloud Identity Architecture (aka.ms/aaddatawhitepaper and aka.ms/resilientaad).

Ben Hagen (@benhagen), Summit Co-Chair, SANS Institute
Ben Hagen is likely the only security professional in the world who has won both a presidential election and an Emmy. He loves security and both building and breaking things. Ben is currently helping several organizations solve interesting security problems. Previously, he was head of Corporate Information Security at Facebook, Vice President/Principle Infrastructure Security Architect at Salesforce, and lead the Cloud Security Tools and Operations team at Netflix.

During the 2012 US Presidential Election he was in charge of security for the Obama re-election campaign's technology program. Prior to this role, he was a Security Consultant with Neohapsis, and Motorola where he had to break into, and then help fix, the computer networks of lots of organizations. He has built lots of fun tools and systems, has held many impressive sounding certifications, and enjoys pizza and cats.

Chris Farris (@jcfarris), Cloud Security Architect, Turner Broadcasting
Chris Farris is a Unix System Administrator, which basically means he herds computers. It's not as difficult as herding cats and you don't get as much fur everywhere. Usually. His areas of expertise are in Internet Applications (web, email, dns), Linux, Solaris, perl, MySQL, and most recently VoIP. He was one of the founders of the Atlanta Linux Showcase and does security-related consulting, firewall design and installation, penetration testing, network security assessment and other services. He has a blog, www.ChrisFarris.com, where he muses about life, technology, and occasionally, politics.

Nills Franssens (@nillsf), Cloud Solution Architect, Microsoft
Nills is a cloud architect at Microsoft who has spent the last 6 years working with cloud computing. With a lot of experience in IaaS and networking, he is expanding his knowledge domain into the wonderful

domain of Docker and Kubernetes. In his spare time, he enjoys the occasional beer; plays a lot a board games (never bored) and likes to run.

Kenneth G. Hartman (@KennethGHartman), Security Consultant; Community Instructor, SANS Institute
Kenneth G. Hartman is a security engineering leader in Silicon Valley. Ken's motto is "I help my company earn and maintain the trust of our customers in our products and services." Toward this end, Ken drives a comprehensive program portfolio of technical security initiatives focused on securing customers' data in the AWS Cloud. Ken has worked for a variety of Cloud Service Providers in Architecture, Engineering, Compliance, and Security Product Management roles. From 2002-2011, Ken helped launch and lead a company called Visonex into a profitable, nation-wide dialysis-specific electronic medical record using a software-as-a-service (SaaS) business model. Ken holds a BS Electrical Engineering from Michigan Technological University and a Masters Degree in Information Security Engineering from SANS Technology Institute. Ken has earned the CISSP, as well as multiple GIAC security certifications, including the GIAC Security Expert. Ken is also a Licensed PI in Michigan as required by law to consult on criminal cases involving digital forensics.

Frank Kim @fykim, Senior Instructor, SANS Institute
Founder of ThinkSec, a security consulting and CISO advisory firm. Previously, as CISO at the SANS Institute, Frank led the information risk function for the most trusted source of computer security training and certification in the world. With the SANS Institute, Frank continues to lead the management and software security curricula, helping to develop the next generation of security leaders.

Frank was also executive director of cybersecurity at Kaiser Permanente where he built an innovative security program to meet the unique needs of the nation's largest not-for-profit health plan and integrated health care provider with annual revenue of $60 billion, 10 million members, and 175,000 employees.

Frank holds degrees from the University of California at Berkeley and is the author and instructor of popular courses on strategic planning, leadership, application security, and DevOps. For more, visit frankkim.net

Lily Lee, GCIH Staff Security Specialist, Splunk
Lily Lee is currently a Security Specialist at Splunk. She has also held a Sales Engineering role at Splunk. Lily has 15+ years of experience working with Fortune 500 companies and government agencies, operationalizing their IT and security data sources to gain insight and mitigate threats. Lily has experience in application development, security, networking, and IT operations. She is focused on training and enabling global security teams through workshops and adversary simulation and helping customers solve interesting cyber security problems. Lily holds a B.S. in Computer Science, as well as numerous security and IT certifications and has presented at several industry conferences.

Reza Nikoopour, Security Engineer, Riot Games
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.

Ryan Nolette (@sonofagl1tch), Security Engineer, Independent Researcher
Ryan is Amazon's primary AWS security technologist and expert. He has previously held a variety of roles including threat research, incident response consulting, and every level of security operations. With over

a decade in the infosec field, Ryan has been on the product and operations side of companies such as Sqrrl, Carbon Black, Crossbeam Systems, SecureWorks and Fidelity Investments. Ryan has been an active speaker and writer on threat hunting and endpoint security. https://github.com/sonofagl1tch

Brian Nuszkowski, Staff Security Engineer, Cruise Automation
Brian likes to design and build systems using industry best practices and holistic principles. He held previous roles as a Security Engineer for Uber, a Cloud Services Engineer for AHEAD, and a DevOps Engineer for Stratos Card and Duo Security.

Alexander Pavlovsky, Lead Program Manager, Microsoft
Alex is a lead program manager in the Identity Division's Customer Success Team at Microsoft. Over his 22 year career, he led architecture, design and implementation of identity solutions in enterprises, including 2 years as a member of the Identity product team at Microsoft.

Zachary Pritchard, Security Engineer, Riot Games
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.

Mike Ruth (@MF_Ruth), Staff Security Engineer, Cruise Automation
Mike is a Staff Security Engineer at Cruise Automation, where he helps in securing one of the world's best autonomous vehicle platforms. Previously a security lead in VMware's cloud management division, Mike has a decade of experience securing, designing, and deploying cloud infrastructure and enterprise storage systems.

Ory Segal (@orysegal), CTO, PureSec
Ory is a world-renowned expert and veteran in application security with 20 years of experience. A leading authority in serverless security.

Dave Shackleford @daveshackleford, Summit Co-Chair & Senior Instructor, SANS Institute
Dave Shackleford is the owner and principal consultant of Voodoo Security and a SANS analyst, senior instructor, and course author. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering, and is a VMware vExpert with extensive experience designing and configuring secure virtualized infrastructures. He has previously worked as CSO for Configuresoft, CTO for the Center for Internet Security, and as a security architect, analyst, and manager for several Fortune 500 companies. Dave is the author of the Sybex book Virtualization Security: Protecting Virtualized Environments, as well as the coauthor of Hands-On Information Security from Course Technology. Recently Dave coauthored the first published course on virtualization security for the SANS Institute. Dave currently serves on the board of directors at the SANS Technology Institute and helps lead the Atlanta chapter of the Cloud Security Alliance. Dave earned his MBA from Georgia State University.