SANS

Avoiding the Top 10
AWS Security Risks

Cloud INsecurity Summit 2018

Washington, DC

Program Guide

Agenda

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

All approved presentations will be available online following the Summit at
https://www.sans.org/summit-archives/cyber-defense

Friday, June 8

7:00-9:00 am	**Registration & Coffee** (LOCATION: POTOMAC BALLROOM)
9:00-9:30 am	***Keynote: The State of Security in AWS: Lessons from the Field*** Public cloud offerings have become a ubiquitous part of many organizations' technology strategies. They offer new flexibility in architecture and implementation while also offering cost savings. The programmatic nature of cloud environments has enabled the modern trends of DevOps, continuous integration and deployment, and serverless infrastructure. All of these factors represent security opportunities and risks. This keynote will dive into the top 10 security risks and challenges within cloud environments. Each of these risks represents a real-world challenge to implementing architectures in AWS securely. Throughout the day we will be coming back to these risks and learning how some innovative organizations are mitigating these problems. ***Ben Hagen*** *(@benhagen), Security Leader, Facebook*
9:30-10:15 am	***Case Study: Harvard University*** With constantly evolving threats across the Internet, Harvard University deployed a security network hardware stack to handle current and future threats and to protect our students, faculty, and staff. By using multiple geographic locations, network solutions, and homegrown automation, we now have more visibility into our cloud infrastructure and easier-to-use filtering technologies than we could on-premises. This talk will discuss the benefits, tradeoffs, and lessons learned from deploying our solution at the edge of our cloud. ***Thomas Vachon*** *(@TomVachon), Principal Cloud Architect, Harvard University*
10:15-10:45 am	***Case Study: Netflix*** At Netflix, we have committed to the cloud and have spent the last nine years understanding what it means to run a service there and the technical challenges that come along with doing so. In this talk, We will walk through the Security Through Enablement Culture that has been built at Netflix and how it enables developers to move quickly and efficiently. The talk will detail the approach Security takes as partners within Engineering, guardrails not gates, and the paved road. Attendees will walk away understanding how you can enable developers to move fast while maintaining a secure environment. ***Will Bengtson*** *(@__muscles), Senior Security Engineer, Netflix*
10:45-11:15 am	**Networking Break** (LOCATION: POTOMAC BALLROOM FOYER)
11:15-11:45 am	***Case Study: Riot Games*** Riot Games uses the cloud to provide products and services to both players and Rioters. Like many Security teams, Riot has been challenged by the move to the cloud and this new paradigm. In this talk, Mark will be discussing his five years at Riot Games, where the security team has developed a security program based on feedback and self-service. The talk will detail how the Riot security team assessed the gaps and challenges in Riot's move into the cloud before moving onto explaining how the team works with the Riot feedback culture to secure Riot's cloud presence through: internal RFCs; developer education and collaboration on solutions; receiving feedback when we don't hit the bar and acting on it; in-house tools designed and developed to provide visibility into the security posture of AWS; open-sourcing our cloud tools and contributing to other open-source cloud projects. Attendees will come away from this talk understanding how to build a feedback-driven cloud security program with a self-service approach. ***Mark Hillick*** *(@markofu), Head of Player Security, Riot Games*

Friday, June 8

11:45 am - 12:30 pm	***Case Study: Lyft*** Lyft has been using cloud technologies since day one to connect passengers and drivers and to help people get where they're going. The ability to automate and scale cloud resources elastically has enabled us to move quickly and grow our business rapidly, which has been crucial to Lyft's success. However, our extensive use of the cloud and rapid growth have also posed security challenges that we've needed to solve in new or different ways. In this talk, Steve will describe how Lyft thinks about security for its cloud infrastructure while supporting a DevOps-oriented culture. This will be followed by a deeper dive into several areas where we've automated and leveraged AWS infrastructure to implement security controls: cloud orchestration, identity and access control, network controls, monitoring and alerting, and application lifecycle management. Steve will also cover lessons we've learned about running and securing our AWS presence, including some AntiPatterns that you may wish to avoid as you build and secure your cloud infrastructure. ***Stephen Woodrow**, Security Engineering Manager, Lyft*
12:30 -12:45 pm	***Morning Wrap-Up*** ***Ben Hagen** (@benhagen), Security Leader, Global Social Media Outlet*
12:45-1:30 pm	**Networking Lunch** (LOCATION: POTOMAC BALLROOM)
1:30-3:30 pm	***Training, Part 1*** In the first training section, we will do a broad summary of AWS services and security controls and summarize strategies to mitigate the Top 10 issues we've been talking about throughout the day. You will leave this portion of the training understanding many of the puzzle pieces necessary to secure any AWS environment. The agenda will include: · Core AWS Services · Core AWS Security Controls · Applying Security Controls to the Top 10 Risks
3:30-3:45 pm	**Networking Break** (LOCATION: POTOMAC BALLROOM FOYER)
3:45-5:15 pm	***Training, Part 2*** The remainder of the training will focus on understanding how to interact with the AWS API to collect information, deploy some common sense controls to monitor your environment, and establish a CloudTrail logging pipeline. You will leave this portion of the training understanding the fundamentals of how to use the AWS API via Python to build and automate repeatable and scalable security controls. The agenda will include: · API Fundamentals · Authentication · Python basics · Lambda and Events · Exercise: S3 bucket monitoring · Exercise: Takeover Protection
5:15-5:30 pm	***Closing Remarks/Next Steps*** ***Ben Hagen** (@benhagen), Security Leader, Global Social Media Outlet*
5:30-6:30 pm	**Networking Reception** (LOCATION: POTOMAC BALLROOM FOYER)

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.

SPEAKERS

***Will Bengtson** (@__muscles), Senior Security Engineer, Netflix*
Will Bengtson is senior security engineer at Netflix focused on securing the cloud as a member of the security operations and tooling team. He loves tackling hard problems that have high impact from both a success and failure standpoint. Prior to Netflix, Will led security at a healthcare data analytics startup, consulted across various industries in the private sector, and spent many years as a Department of Defense contractor. Will is highly active in the security community and is on the BSidesSF and Bay Area OWASP leadership team. When not working, Will can be found working out, appreciating fine whiskey, or doing research/side projects.

***Ben Hagen** (@benhagen), Security Leader, Facebook*
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 the head of Corporate Information Security at Facebook and has been a Vice President/Principle Infrastructure Security Architect at Salesforce. He led the Cloud Security Tools and Operations Team at Netflix. During the 2012 U.S. 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.

***Mark Hillick** (@markofu), Head of Player Security, Riot Games*
Mark leads Player Security at Riot Games, makers of League Legends. Prior to moving to the US, Mark built and led Riot's InfoSec team in Europe. At Riot, he has done everything from building a team from scratch, engineering cool solutions, levelling up the security program, dealing with DDoS attacks and providing a secure cloud for Riot's developers. Before Riot, Mark worked in the financial industry, Citrix and MongoDB, architecting secure solutions and first coming across the cloud in early 2010. He has done numerous SANS courses and has held the GIAC GSE for several years. In his spare time, now that he lives somewhere sunny, Mark can usually be found in the water, on the slopes or struggling to keep up with his kids.

***Thomas Vachon** (@TomVachon), Principal Cloud Architect, Harvard University*
Tom Vachon is a self-described "Cloud Gray Beard" who has been consuming and advocating for the use of Public Cloud since 2008. He has a passion for both the technical as well as the cultural challenges resulting from enterprise use of the Cloud. Tom is currently the Principal Cloud Architect at Harvard University and has previously worked at SessionM, KAYAK.com, and other mid-sized enterprises.In his previous roles, he has architected numerous high security financially significant systems both on-premises and in the Cloud. Currently his focus is architecting multi-cloud solutions to provide equivalent controls and availability regardless of the workload's location. When he isn't working in the Cloud, he is flying near the clouds through his hobby of drone photography.

***Stephen Woodrow**, Security Engineering Manager, Lyft*
Stephen works on infrastructure security engineering at Lyft. As Lyft's first security hire, he built out and led Lyft's security engineering team and program, and is now focused on supporting Lyft's growth with safe and scalable engineering practices. Prior to joining Lyft, Stephen was an early engineer at Stripe where he worked on fraud and infrastructure, and later co-founded Stripe's security team. He also spent time building research infrastructure for measuring Internet performance at Georgia Tech.