SANS

Secure DevOps

Summit 2018

Program Guide

@SANSappsec  #SecDevOpsSummit

Agenda

All Summit Sessions will be held in the Silverton 2/3 Room (unless noted).
All approved presentations will be available online following the Summit at
sans.org/DevOps-Archive

Monday, October 22

7:00-9:00 am	**Registration & Coffee** (LOCATION: SILVERTON FOYER)
9:00-10:00 am	***Opening Keynote: Fast Forward: Reflecting on a Life Watching Movies and a Career in Security*** Things change, and people and industries adapt. Individuals and businesses that can spot the trends and adjust quickly are likely to be more successful. With this as an underlying thesis, we'll talk about some trends in the movie industry that relate well to similar changes in technology and security. We'll also run through some tips and lessons learned to help security teams stay ahead as they navigate technical and operational changes. ***Jason Chan*** *(@chanjbs), VP – Cloud Security, Netflix*
10:00-10:30 am	**Networking Break** (LOCATION: SILVERTON FOYER)
10:30-11:15 am	***Serverless Security: Your Code, Your Responsibility*** In serverless, the cloud provider is responsible for securing the underlying infrastructure, from the data centers all the way up to the container and runtime environment. This relieves much of the security burden from the application owner, however 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. ***Ory Segal*** *(@PureSecTeam) (@orysegal), CTO, PureSec*
11:15 am - 12:00 pm	***Moving Fast & Securing Things*** "Process" is often seen as an antithetical to the fast-moving nature of startups. Security processes, in particular, can be regarded as a direct impediment to shipping cool features. On the other hand, the security of an organization and its users shouldn't be disregarded for the sake of speed. Striking a balance between security and nimble development is a vital aspect of an application security team. At Slack, we have implemented a secure development process which has both accelerated development and allowed us to scale our small team to cover the features of a rapidly growing engineering organization. In this presentation we will discuss both our Secure Development Lifecycle (SDL) process and tooling, as well as view metrics and provide analysis of how the process has worked thus far. We'll discuss our deployment of a flexible framework for security reviews, including a lightweight self-service assessment tool, a checklist generator, and most importantly a messaging process that meets people where they are already working. We'll show how it's possible to encourage a security mindset among developers, while avoiding an adversarial relationship. By tracking data from multiple sources, we can also view the quantified success of such an approach and show how it can be applied in other organizations. ***Kelly Ann****, Security Engineer – Product Security, Slack* ***Nikki Brandt****, Senior Security Engineer – Product Security, Slack*
12:00-1:15 pm	**Lunch** (LOCATION: SILVERTON FOYER)

Monday, October 22

1:15-2:00 pm	***Unify DevOps and SecOps: Security Without Friction*** In a world of change, how do you balance the speed and agility of DevOps with the security and compliance of SecOps? In this session, Matt will focus on the challenges facing both DevOps and SecOps when it comes to security. Only by understanding each team's objections, can a frictionless approach to security be achieved. Next, Matt will highlight the security challenges of container applications. Here, we must first understand the three primary approaches: Kernel Plug-ins, Privileged Containers, and Embedded Security. The pros and cons of each approach will be presented. And finally, Matt will explain how to integrate security within the DevOps process without impacting development but also providing security the visibility and control needed to secure containers. This frictionless approach is the only one that unifies DevOps and SecOps. ***Matt Alderman*** *(@maldermania), Chief Strategy Officer, Layered Insight*
2:00-2:45 pm	***Security Change Through Feedback at Riot*** 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. Riot Games' 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 on to explain how the team works within the Riot feedback culture to secure Riot's cloud presence through: • Internal RFCs • Developer education & 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 ***Zach Pritchard****, Security Engineer, Riot Games*
2:45-3:15 pm	**Networking Break** (LOCATION: SILVERTON FOYER)
3:15-4:00 pm	***Threat Model-as-Code: A Framework to Go from Codified Threat Modeling to Automated Application Security Testing*** Threat Modeling is critical for Product Engineering Team. Yet, even in the rare event that it's performed, it's performed without actionable outputs emerging from the exercise. It is erroneously relegated to the status of a "Policy/Best Practice Document." But Threat Models are – or should be – the playbooks of Product Security Engineering, and the best way to do threat modeling is to integrate it into the Software Development Lifecycle (SDL). Threat Models should produce outputs that are actionable across the organization. This session with explain and share the "ThreatPlaybook," an open-source framework that allows product teams to capture User Stories, Abuser Stories, Threat Models and Security Test Cases. ***Nithin Jois*** *(@bondijois), Solutions Engineer, we45*

Monday, October 22

4:00-4:45 pm	***Building Cloud Apps Using the Secure DevOps Kit for Azure*** At Microsoft, we've adopted agile methodologies for our internal cloud app development. Traditional SDLC processes proved slow, ineffective, and created long queues of applications awaiting security reviews by centralized teams. To build security into our agile development process and provide a baseline for security in cloud apps, we created the Secure DevOps Kit for Azure. The kit contains automation, extensions, plugins, templates, modules, and other tools that seamlessly add security to cloud applications during the development process. Additionally, the kit helps our engineering teams save time and money, increase security awareness in Azure, and create a simpler, more structured, and consistent security environment. This talk will detail the security challenges faced by Microsoft's security teams with the adoption of DevOps processes at scale and discuss the capabilities of the Azure Secure DevOps Kit, which was built to help overcome these challenges. We will walk through and demonstrate the capabilities of the Kit, which was open sourced and made available externally via Github at http://aka.ms/azsdkossdocs. ***Jonathan Trull*** *(@jonathantrull), Global Director – Cybersecurity Strategy & Compliance, Microsoft*
6:00-8:00 pm	***Summit Night Out: Let It Roll!*** We're all heading out to Lucky Strike, located in the Denver Pavilions at 500 16th Street Mall, for bowling and billiards, food and drinks, networking and fun. Head over (it's about a 10-minute walk) and wear your Summit badge to get in on the fun.

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, October 23

8:00-9:00 am	**Registration & Coffee** (LOCATION: SILVERTON FOYER)
9:00-9:45 am	***Keynote: Everything New is Old Again*** Security, as a field and as an industry, demands constant change and understanding. New technologies rarely introduce novel risks, but do require some ingenuity when applying old lessons to new problems. In this talk we'll cover some of the most common risks to modern cloud computing while highlighting some great security opportunities. Also, everything Jason Chan tells you is a lie. ***Ben Hagen*** *(@benhagen), Security Enthusiast*
10:00-10:30 am	**Networking Break** (LOCATION: SILVERTON FOYER)
10:30-11:15 am	***SANS Secure DevOps Survey: Sneak Peek*** To be truly effective in today's on-premise, cloud and hybrid environments, integrating security and DevOps requires new mindsets, processes, and tools. The latest survey of industry practitioners examines how security and risk management leaders approach the collaborative, agile nature of DevOps. Be the first to hear the survey results - before the whitepaper is published – to find out how your organization stacks up and be inspired to make your DevOps even more secure. ***Frank Kim*** *(@fykim), Summit Chair, SANS Institute*
11:15 am - 12:00 pm	***Ship of Fools: Shoring Up Kubernetes Security*** Hackers gonna hack. They have their own motivations, and they don't care about your constraints. As attackers, they want to find vulnerabilities and exploit them. As a defender, your mission is to stop them. Mistakes can be easy to make, but with the right configuration and attention to security best practices many attacks can be prevented. This talk will give you practical advice about securing your Kubernetes clusters, from an attacker's perspective. We'll walk through the attack process from discovery to post-exploitation, and you'll walk away with tools and techniques that can be used for prevention along the way. Learn how to keep your infrastructure safer by making a hacker's job harder. ***Ian Coldwater*** *(@IanColdwater), DevOps Engineer, Jamf Software*
12:00-1:15 pm	**Lunch Panel** (LOCATION: SILVERTON FOYER) ***The Future of DevOps & AppSec*** Enjoy lunch and listen in as some of the Summit speakers have an off-the-cuff and off-the-record conversation on what we're doing, what we should be doing, and what we'll be doing in the future. MODERATOR: ***Frank Kim*** *(@fykim), Summit Chair, SANS Institute* PANELISTS: ***Kelly Ann****, Security Engineer – Product Security, Slack* ***Jason Chan*** *(@chanjbs), VP – Cloud Security, Netflix* ***Ian Coldwater*** *(@IanColdwater), DevOps Engineer, Jamf Software* ***Ben Hagen*** *(@benhagen), Security Enthusiast* ***Aaron Rinehart****, Chief Enterprise Security Architect, UnitedHealth Group*

Tuesday, October 23

1:15-2:00 pm	***Detection as Code: Applying the Software Development Lifecycle to Blue Team Operations*** The modern software development lifecycle (SDLC) is the result of decades of evolution to the processes software engineers use to launch and maintain high quality systems While hunting and detection capabilities of a typical blue team are in their relative infancy compared to the SDLC, important software lessons can be ported to the security operations world to drive a generational leap forward for daily blue team activities. In this talk, attendees will learn how the SDLC can be brought to the blue team for operationalization to improve the predictability, reliability, and effectiveness of hunting and detection through: • Treating detection as code • Source controlling detection techniques and alerts with Git • Unit testing detection techniques and alerts • Using pull requests and peer reviews as change control • Continuous integration and continuous delivery to get tested changes into production systems ***Chris Rothe**, Chief Product Officer & Co-Founder, Red Canary*
2:00-2:45 pm	***Total Chaos: How Experimenting with Chaos Leads to More Control*** Chaos Engineering takes an approach to injecting controlled objective failure into complex systems. In this presentation, you will learn how to do this in real life. We'll start small with game day exercises, develop chaos experiments, and eventually mature to production level testing. After all, production systems are always different at that stage. Your attacker is not going to be instrumenting your systems in stages and neither should you. Aaron Rinehart, the innovation leader behind the open-source software tool, ChaoSlingr, will show you why this is important and how security automation and chaos experimentation can help you to understand how your security really works. Security is changing and this talk gets you ready for what's just around the corner. ***Aaron Rinehart**, Chief Enterprise Security Architect, UnitedHealth Group* ***Mike Zhou**, Software Engineer, UnitedHealth Group*
2:45-3:15 pm	**Networking Break** (LOCATION: SILVERTON FOYER)
3:15-4:00 pm	***Lessons Learned From Illumina's SecDevOps Transition*** Illumina is a leading developer, manufacturer, and marketer of life science tools and integrated systems for large-scale analysis of genetic variation and function. Ninety percent of all genetic sequencing world-wide is performed on Illumina equipment. The BaseSpace Suite consists of multiple SaaS and PaaS solutions that allow customers to store, analyze, and share the large genetic data sets generated. This talk will share the lessons that Illumina has learned as the company adopts SecDevOps principles while integrating acquisitions and scaling out to serve new geographies. ***Kenneth G. Hartman** (@KennethGHartman), Associate Director, Cloud Security, Illumina; Community Instructor, SANS Institute*

Tuesday, October 23

4:00-4:45 pm	***Oh, You Got This? Practical Attacks on Modern Infrastructure*** Have you ever been on a Web Assessment, Bug Bounty, Pen Test, or Red Team and encountered a component using the latest frameworks, languages, libraries, or on the infrastructure? This presentation will provide a practical guide to approach these types of scenarios. Many of these technologies are strikingly new, probably visually stunning, but are they entirely secure? This talk will explore concepts like Modernized languages, Exposed In-Memory Databases, Proxies, Breaking Microservices, and more. We will show demos of how to abuse the latest architectures and frameworks. Follow me as we break the stuff that everyone else is just riding by, or discovering accidentally. Let's go attack the cloud people! This talk walks through the land of the cloud in a fun and storybook way. Let's also figure out along the way how to break, attack, and pillage, for good. ***Moses Frost*** *(@mosesrenegade), Security Architect, Cisco Systems; 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.