Monday, November 4	
9:00-9:15 am	*Welcome & Opening Remarks* **Kenneth G. Hartman @KennethGHartman,** Summit Co-Chair, SANS Institute **Eric Johnson @emjohn20,** Summit Co-Chair, SANS Institute
9:15-10:00 am	***Keynote*** **Shift RIGHT to Fix Bugs Earlier: Security in a DevOps World** **John Steven,** Chief Technology Officer, ZeroNorth Vendors and firms do a lot of DevOps 'in name only' because it gets them in the cool club. Those really changing their culture are fundamentally changing their risk management paradigm – from one of proactive governance through security assurance to one of continuous collection of security telemetry and resilient delivery pipelines. What does that mean in practice? This presentation provides a software security framework and conclusions resulting from a survey of twenty luminary organizations practicing what they preach in DevOps culture. We will explore the tools and activities people have come to rely on, the changes to staffing security and aligning them with development and the remaining challenges that impede scale. Technically, content will focus on those security activities and tools DevOps shops _actually_ use and get value from, based on data from the aforementioned survey of twenty luminary organizations. As compared to how traditional shops address vulnerabilities, survey data tends towards real-time telemetry of cloud configuration, container integrity, and user/system behavior. Vulnerabilities themselves tend away from the "OWASP Top 10" and towards account fraud, asset theft and platform abuse. The audience will walk away with a better understanding of, and ideally different perspective on, security tools and activities available to them.
10:00-10:30 am	**Networking Break**
10:30-11:05 am	**The Art of Automation: Creating A Serverless Threat Intel Bot** **Ronald Eddings** @ronaldeddings, Security Architect, Palo Alto Networks

	As organizations mature and scale their security infrastructure, it is vital that analysts, engineers, and other team members be able to query and enrich data on demand. Additionally, application features are being introduced at an increasing rate, creating the need for software-defined infrastructure. In this talk, we'll explore scaling automation efforts, with a focus on threat intelligence. We'll share practical examples for when to leverage an interactive bot, create API endpoints, employ serverless architecture, and apply actionable threat intelligence.
11:10-11:45 am	**Serverless DevSecOps: Owning Security** **Hillel Solow** **@hsolow**, Chief Technology Officer, Protego Labs The shift to cloud-native application development has ushered in a revolution in how we think about application security. For one thing, we've handed over infrastructure security to the cloud providers, letting them secure the hardware, network, operating system, and runtime. Another major change is in how we share responsibility for security within our organization. In the past, security teams worked in isolation, trying to secure applications from the outside. This paradigm is broken in cloud-native applications. Increasingly, we require a more holistic approach to securing cloud applications, where developer, DevOps, and security teams work in tandem to minimize security risks. This talk will focus on the role developers and DevOps engineers need to play in this new world. This is about technology, but more than that it's about processes and relationships, and how security needs to collaborate but not abdicate responsibility. We'll dive into how we can make the path of least resistance be the path of most security. We'll look at some practical, hands-on use cases for maximizing visibility and minimizing risk, and see how your organization can adopt a serverless DevSecOps mindset.
11:50 am – 12:30 pm	**A DevOps Approach to Security Controls** **Kenneth G. Hartman** **@KennethGHartman**, Summit Co-Chair, SANS Institute The DevOps movement has made it possible for leading companies to get their applications to market faster, with higher quality and reduced costs. DevOps is both a culture and a set of processes that enable development and operation teams to create, release, and manage applications following a Systems Development Life Cycle (SDLC) that is typically automated via Continuous Integration/Continuous Delivery (CI/CD) tooling. Today, DevOps principles have expanded beyond merely managing the application to managing the environment itself, giving rise to concepts such as software-defined networking and infrastructure as code. A security control is a testable countermeasure designed to mitigate a specific risk. Multiple, complementary controls create security capabilities. Of course, security engineers need to be baking security into applications throughout the SDLC by engaging with operations and development teams and hooking into the CI/CD toolchain. This presentation

	makes a corollary argument, advocating that security teams need to apply DevOps principles to how they implement security controls for virtually every compliance requirement, using a "security controls as code" approach. We'll present tools that can support this paradigm, but more importantly, we'll look at some fundamental principles that can be applied immediately to the development, implementation, and enforcement of security controls.
12:30-1:30 pm	***Lunch Keynote*** **Shannon Lietz,** Leader & Director – DevSecOps, Intuit
1:35-2:10 pm	**Loose Keys Bring These: Attackers + Me (Incident Responders**) **Jonathon Poling**, Managing Principal Consultant, Secureworks This presentation will walk attendees through the ever-ubiquitous Amazon Web Services Access Key Leak, showing how the lack of both proactive and reactive security integration into and by DevOps can lead to compromise. We will examine the entire chronology of the leak and ensuing attack, from initial leak through incident response and return to operations, and we'll outline how DevOps plays a critical role in building both proactive protection and incident response capabilities. In turn, the presentation will provide actionable takeaways that can be implemented immediately into DevOps to proactively help prevent such leaks, reactively monitor and alert usage of leaked keys, and build automated responses for effective mitigation, containment, and remediation.
2:15-2:50 pm	**Embedding Security in the World of DevOps: Real-World Case Studies** **Aditya K. Sood** @adityaksood, Director of Cloud Security, Symantec The scale of cloud computing is evolving at an exponential rate, and security ethics in the cloud need to be matured accordingly. Security threats in the cloud are also increasing rapidly, and thwarting them requires implementing security at early stages of development operations. There are challenges associated with that process, as organizations deal with different scenarios of DevSecOps, DevOpsSec, and SecDevOps. In this presentation, we will discuss the importance and criticality of zero trust for developmental operations and why it is needed to achieve security in the cloud for large-scale deployments. We will look at real-world case studies of issues discovered during security research associated with cloud infrastructure and the impact of not injecting security at early stages of DevOps. The talk will help attendees understand the risks and threats associated with insecure operations in cloud infrastructure, while also highlighting effective solutions to subvert those insecurities.

2:50-3:15 pm	**Networking Break**
3:20-3:55 pm	**Lessons from Developing Microsegmentation for Container Environment Networks** **Thomas Kaiser**, Principal Kernel Developer, Edgewise Traditional microsegmentation has become too complex to implement, beyond human cognitive capacity to manage, and nearly impossible to update proactively. Treating computer resources as a dynamically scaled substrate onto which workloads can be automatically and dynamically assigned is at odds with the requirement of microsegmentation to lay out subnets as security domains. Kubernetes presents new authorization problems, raising questions about the efficacy of distributed firewalls – there is little point in enforcing via Linux IPTables or nftables firewalls when rule sets are not evaluated for loopback interfaces shared between containers within the same pod. While these problems were traditionally approached from the network perspective, this presentation examines them through the lens of applications. Risk management, after all, is best conducted from the application point of view, as it is the application which must ultimately be the arbiter of whom/what shall have access to its data and services. In this talk we'll examine lessons learned while implementing a zero-trust microsegmentation solution. We will answer such questions as: Is wrapping all communications in TLS sufficient? How much effort is required to implement distributed firewalls versus a syscall-layer (e.g., Linux LSM-based) security solution? How can we discover topology in complex networks?
4:00-4:35 pm	**Infrastructure as Code is Real! Using the Cloud to Provision Infrastructure with Software** **Shaun McCullough @TheCybergoof,** Software Engineer; Community Instructor, SANS Institute Infrastructure as Code (IaC) is the dream that sounds good in practice but can be complicated to implement. Cloud providers give us new tools to realize this dream in ways that could change business operations, only if we let it. This talk will explore the goal of IaC, where it works, and where it falls short. Then, we dive into specific capabilities in Amazon Web Services cloud provisions that make IaC a reality. We will also discuss the skills needed to implement IaC and how to get started.
4:40-5:15 pm	**Add Continuous Compliance to Your Continuous Integration/Continuous Deployment Pipelines**

	Eric Gerling, CTO, Trility Consulting Software development teams have long been able to take advantage of unit, integration, and functional testing as an integral part of a robust, test and behavior-driven development environment. Infrastructure as Code (IaC) provides new capabilities for DevOps teams to utilize new frameworks to build ephemeral environments with integrated compliance testing before, during, and after deployment. We will discuss ways to enhance your team's CI/CD pipelines with Continuous Compliance for Amazon Web Services based environments. Specific examples will include integration and functional testing of machine images and network and security group configuration validation.
6:00 – 8:00 pm	**Summit Night Out** Everyone is invited to chat and relax! Details to come.
Tuesday, November 5	
9:15-10:00 am	***Keynote*** **Building Zero Trust: A Cloud-Native Perspective** **Kathy Wang**, Sr. Director of Security, GitLab Although the concept of zero trust is not new, very few cloud-native companies have successfully implemented it. This keynote will discuss GitLab's approach to and implementation of zero trust on GitLab.com and will highlight the benefits and challenges the organization has encountered along the way. Takeaways will include a deeper understanding of how GitLab built its roadmap to achieve zero trust.
10:00-10:30 am	**Networking Break**
10:30-11:05 am	*Session to be announced* **Tim Anderson**, Sr. Technical Industry Specialist, AWS Security
11:10-11:45 am	**CloudSec Rules Everything Around Me** **Kyle Dickinson**, Cloud Security Architect, Koch Industries When a company moves to the cloud, the security team will need to figure out how to adjust in order to go about day-to-day operations in cloud environments. This presentation will go over how to accomplish the different

	requirements for a Security Operations Center. We'll present war stories of solutions that were implemented and worked very well, as well as solutions that blew up, ranging from native services to open-source tools and some commercial tools (no, this isn't an advertisement). We will go over the pros and cons of each option so that you can accelerate your decisions on how you secure your cloud.
11:50 am – 12:30 pm	**Continuous Security Buddy – OpenShift Kubernetes/OpenStack Platform** **Mahesh Bang**, Information Security Architect, Cisco Systems This presentation will provide attendees with insights into lessons learned about managing continuous security assurance in a shared responsibility model. We will look at developing the tools and capabilities to automate the validation of security guardrails for a private cloud on OpenStack, OpenShift, and Kubernetes. Attendees will learn about the experience of driving an enterprise culture change from a traditional security mindset to the new DevSecOps world.
1230-1:30 pm	**Lunch**
1:35-2:10 pm	*Talk to be announced*
2:15-2:50 pm	*Talk to be announced*
2:50-3:15 pm	**Networking Break**
3:20-3:55 pm	*Talk to be announced*
4:00-4:45 pm	**DevSecOps To Go: Your Takeaways and To Do List** **Eric Johnson @emjohn20,** Summit Co-Chair, SANS Institute Hopefully after two days of talks, fortified by informal learning through networking with your peers, you're fired up to get back to the office and put these ideas to work. Eric will help you distill the key themes and advice from the Summit and organize them into manageable, actionable tasks that yield real results.

Speaker Biographies

Ronald Eddings

Ronald Eddings is a cybersecurity expert, blogger, and digital nomad based in Silicon Valley whose ingenuity, dedication, and ambition have earned him a reputation as a trusted industry leader. Over the course of his career, he has worked at various Fortune 500 companies and mentored a multitude of fellow professionals along the way. In addition to cybersecurity, he is well-versed in software development, DevOps, and artificial intelligence.

Kenneth G. Hartman

Kenneth G. Hartman is a security engineering leader in Silicon Valley. He teaches the SANS SEC545: Cloud Security Operations course and has worked for a variety of cloud service providers in security architecture, engineering, compliance, and security product management roles. From 2002–2011, Ken helped launch and develop a company called Visonex into a profitable, nationwide dialysis-specific electronic medical record firm using a software-as-a-service business model. Ken holds a BS in electrical engineering from Michigan Technological University and a master's in information security engineering from the SANS Technology Institute. Ken has earned the CISSP® and multiple GIAC security certifications, including the GIAC Security Expert.

Jonathon Poling

Jonathon Poling is a Managing Principal Consultant at Secureworks. With 11+ years of experience spanning government, contracting, and the private sector, he is a Digital Forensics and Incident Response subject-matter expert in all major Operating Systems (Windows, Linux, Mac), including the cloud (Amazon Web Services), currently focusing on SOAR. He is most at home on the *nix command line, using FOSS like a BOSS.

Liz Rice

Liz Rice is the Technology Evangelist at the container security specialist firm Aqua Security and coauthor of the book *Operating Kubernetes Clusters and Applications Safely* published by O'Reilly. She has a wealth of software development, team, and product management experience from years spent working on network protocols and distributed systems, and in digital technology sectors such as video on demand, music, and voiceover Internet protocol. When not building startups and writing code, Liz loves riding bikes in places with better weather than her native London or racing in virtual reality on Zwift.

Hillel Solow

Hillel Solow is the Chief Technology Officer and co-founder of Protego Labs, a developer of pioneering application security for the rapidly emerging serverless landscape. Passionate about security innovation, Hillel drives product innovation and security at Protego. Prior to co-founding Protego, he was Chief Technology Officer of Cisco's IoT Security Group, where he worked on innovative security solutions for new technology markets, and frequently spoke at the firm's internal SecCons.

Aditya K. Sood

Aditya K. Sood is the Director of Cloud Security for Symantec. He has presented at a number of conferences such as BlackHat, DEFCON, HackInTheBox, RSA, and Toorcon. He is also the coauthor of the book *Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware* published by Syngress.

John Steven

For two decades, John Steven led technical direction at Cigital, where he rose to the position of co-Chief Technology Officer. He founded spin-off Codiscope as Chief Technology Officer in 2015. When both firms were acquired by Synopsys in 2016, John transitioned to the role of Senior Director of Security Technology and Applied Research. His expertise runs the gamut of software security—from threat modeling and architectural risk analysis to static analysis and security testing. John is keenly interested in using orchestration and automation to provide security governance at the cadence of modern development. As a trusted adviser to security executives, he uses his unparalleled experience with a broad range of security tools to build and mature security programs. He has served as a co-editor at IEEE Security & Privacy magazine and as the leader of the Northern Virginia OWASP chapter. John is regularly invited to speak, including keynotes at AppSecUSA and BSIMM.

Kathy Wang

Kathy Wang leads the security team at GitLab and is a recognized thought leader in information security with a strong background in project management, research, and business development. She has worked in government, commercial, and technology startup environments, and currently advises security services/products startup companies. Kathy is also an internationally recognized malware expert who has researched, developed, evaluated, and operationalized various solutions for detecting and preventing client-side attacks used by advanced persistent threats targeting common platforms (e.g., browser, email, mobile phones). She have spoken internationally at many conferences and on many panels, including RSA, DEFCON, AusCERT, and REcon. She is co-author of the book *Beautiful Security*, and holds a BS and MS in electrical engineering from the University of Michigan.
