SANS

Secure DevOps SUMMIT

DENVER, CO | OCT 10-11, 2017

Program Guide

@sansappsec #SecDevOpsSummit

Agenda

All Summit Sessions will be held in Harvard/Princeton (unless noted).

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

Tuesday, October 10

8:00-8:50 am	**Registration & Coffee** (LOCATION: PRINCETON FOYER)
8:50-9:00 am	***Welcome*** *Eric Johnson (@emjohn20), Certified Instructor, Author, & Summit Co-Chair, SANS Institute; Senior Security Consultant, Cypress Data Defense* *Frank Kim (@fykim), Curriculum Lead & Summit Co-Chair, SANS Institute; Founder, ThinkSec*
9:00-9:45 am	***Keynote: Demystified DevSecOps*** In the spirit of Software Safer Sooner, you're hearing about DevSecOps everywhere...but seriously, what is it and how do you really grab on and do it? Are there ways to make a big leap quickly and switch processes to dive in and do it better? Demystified DevSecOps provides mechanics and ideas to evolve your security practice so that it meets the needs of everyone making security decisions. More importantly, we'll explore what works and doesn't work from insights deep inside the trenches. *Shannon Lietz (@devsecops), Leader & Director – DevSecOps, Intuit*
9:45-10:30 am	***Scaling Trust with Millions of Containers: Microsegmentation Strategies for Authorization*** Traditional approaches to security and segmentation break down at scale. Specifically, firewalls and SDNs either become overwhelmingly tedious to manage or require such coarse granularity that they cannot reliably contain breaches. This challenge only increases with microservices and loose coupling. In this presentation, we'll deploy a capability-based security model for client-to-service and service-to-service integrations, allowing us to safely nest microservices while avoiding duplicated, complex authorization code and widespread dependencies on querying RBAC data stores. We'll also explore how this approach mitigates attack patterns like the Confused Deputy. *David Strauss (@DavidStrauss), CTO, Pantheon*
10:30-11:00 am	**Networking Break** (LOCATION: PRINCETON FOYER)

Tuesday, October 10

11:00-11:45 am	***Automating Security in DevOps Pipelines*** One of the big challenges facing organizations today is how to automate security controls inside of continuous delivery pipelines. Traditionally, organizations have used waterfall or agile methodologies where applications are pushed to production less than a dozen times per year. With the advent of DevOps, applications can be pushed multiple times a day – or even multiple times per hour – into a production environment. With this kind of velocity, it can often be difficult to apply security controls without adversely impacting the production pipeline. This session will focus on some of techniques used by Aetna's global security team as they automate security controls in their DevOps pipelines. DJ will also cover his experience of designing solutions across a rapidly changing and diverse application ecosystem; and how continuous integration and continuous monitoring can go hand in hand in delivering application agility, security vigilance, and competency at the same time. *DJ Schleen (@dschleen), Security Architect and DevSecOps Evangelist, Aetna*
11:45 am-12:20 pm	***Forging Forensic Fortifications*** Most organizations are aware of the benefits of leveraging tools such as Puppet, Chef, and SaltStack to rapidly deploy systems. Many organizations are also becoming aware of the potential security risks. The majority of organizations, however, don't realize the numerous challenges of conducting incident response (IR) activities and forensic investigations across their environments. Digital forensics and incident response (DFIR) is usually a "oh, I wish we had done 'x' before this happened" regret. This session will discuss the forensic and IR challenges of investigating servers and applications in different platform architectures. Harnessing the power of Puppet, this session will show you how to prepare your workstations, servers, cloud instances, and containers to enable effective incident response in your environment. Scenarios such as preparing for ransomware, unauthorized access detection, and remote forensic acquisition will be discussed with associated modules for Windows and Linux-based operating systems. *Andrew Hay (@andrewsmhay), Co-Founder & CTO at LEO Cyber Security*
12:20-1:30 pm	**Lunch**
1:30-2:15 pm	***The Future of SecDevOps: Containers, Clouds, and Creating Change*** Hear from our expert panel on the foundational building blocks that are transforming the way organizations develop applications and deploy products and learn how security can be a leader of positive change in this transformation. MODERATOR: *Frank Kim (@fykim), Curriculum Lead & Summit Co-Chair, SANS Institute; Founder, ThinkSec* PANELISTS: *Shannon Lietz (@devsecops), Leader & Director – DevSecOps, Intuit* *Justin Smith (@justinjsmith), Chief Security Officer, Pivotal* *David Strauss (@DavidStrauss), CTO, Pantheon* *Nir Valtman (@ValtmaNir), Head of Application Security, NCR Corporation*

Tuesday, October 10

2:15-3:00 pm	***Secure DevOps in Regulated Environments: Balancing Speed, Cost, Feedback and Control*** DevOps teams pushing changes to production several times a day is cool for online Lean Startups. But it won't work in regulated environments that enforce clear separation of duties, rigorous change management and extensive activity auditing... or can it? We'll look at how Agile and DevOps teams can succeed in highly regulated industries, and how DevOps can be used to achieve continuous compliance - at speed, and at scale. The presentation will cover: • Different types of regulatory frameworks: prescriptive and outcome-based • Data Privacy for Agile and DevOps teams • Handling Separation of Duties in DevOps and NoOps • Risk Management for Agile and DevOps teams • Compliance in the Cloud • Continuous Compliance and Compliance as Code - wiring compliance into Continuous Delivery • Keeping auditors and developers happy *Jim Bird (@jimrbird), Analyst and Co-Author - DEV534 Secure DevOps, SANS Institute*
3:00-3:30 pm	**Networking Break** (LOCATION: PRINCETON FOYER)
3:30-4:15 pm	***The Art of Securing 100 Products*** How many times you heard people stating "it's best practice"? How many times you successfully implemented ALL best practices for a large scale of products? This presentation takes you out of the comfort zone of the best practices and guides you through the day to day challenges to secure 100 products, while considering the procedural and technological challenges, as working with diverse software architectures, multiple development languages/platforms, variety of development lifecycles, injecting security into continuous integration/delivery etc. This presentation introduces solid approaches to cope with these challenges, by scaling out the application security team's capabilities, putting the right security tools in place, and following newly introduced thumb rules to build a successful application security program. As result of this talk, you will be armed with the practical execution approach for securing a massive scale of products. Takeaways: • Learn how to gain quick wins while scaling out the application security program and team. • Being able to understand how to implement product security in diverse software organization. • Get a solid approach to get the buy-in from the most parties in the company. *Nir Valtman (@ValtmaNir), Head of Application Security, NCR Corporation*

Tuesday, October 10

4:15-5:00 pm	***Security in the Cloud: AWS & Cloud Custodian*** A deep dive into critical aspects of public cloud security using the open source Cloud Custodian tool. The rise in adoption of public cloud infrastructure has brought significant productivity and efficiency gains to organizations, however as numerous incidents have highlighted it also comes with risks if an organizations infrastructure is improperly managed. Cloud Custodian is an open source rules engine that allows for organization-wide management of security, compliance, and cost optimization. We'll look at using Custodian to address key topics in cloud security, including enforcement of access control, encryption, and DDoS protection across a variety of resources. ***Kapil Thangavelu*** *(@kapilvt), Technical Fellow, Capital One*
5:00-6:15 pm	**Networking Reception**
6:15-7:00 pm	BONUS SESSION: ***Secure DevOps: A Puma's Tail*** DevOps is changing the way that organizations design, build, deploy, and operate online systems. Engineering teams are making hundreds or even thousands of changes per day, and traditional approaches to security are struggling to keep up. Security must be reinvented in a DevOps world to take advantage of the opportunities provided by continuous integration and delivery pipelines. In this talk, we start with a case study of an organization trying to leverage the power of Continuous Integration (CI) and Continuous Delivery (CD) to improve their security posture. After identifying the key security checkpoints in the pre-commit, commit, acceptance, and deployment lifecycle phases, we will explore how unit testing and static analysis fit into SecDevOps. Live demonstrations will show how to identify vulnerabilities pre-commit inside the Visual Studio development environment, and how to enforce security unit tests and static analysis in a Jenkins continuous integration (CI) build pipeline. Attendees will walk away with a better understanding of how security fits into DevOps, and an open source .NET static analysis engine to help secure your organization's applications. ***Eric Johnson*** *(@emjohn20), Certified Instructor, Author, & Summit Co-Chair, SANS Institute; Senior Security Consultant, Cypress Data Defense*

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.

Wednesday, October 11

8:00-9:00 am	**Registration & Coffee** (LOCATION: PRINCETON FOYER)
9:00-9:45 am	***Continuous Security and DevOps: Three Keys for Modern Security Success*** Learn three things that security teams can do to get to "yes" with DevOps teams that are striving to move at an even more rapid pace. *Frank Kim (@fykim) , Curriculum Lead & Summit Co-Chair, SANS Institute; Founder, ThinkSec*
9:45-10:30 am	***API Security: The Past, Present, and Future*** API Security has moved from being an afterthought to being a critical component of API deployments. Organizations are now evaluating many security services to meet business needs. Foundational security services, such as data encryption, rate limiting, and access control are now available across a range of on-premise, CDN, and SAAS offerings to provide organizations the flexibility of aligning API security with overall security needs. Advanced attacks, including bot detection, API data and control system attacks, and API DDoS attacks are a big data problem which requires large-scale processing techniques to reliably identify and remediate attacks. Once again, multiple security platform choices are becoming available. Moving forward, one can envision the availability of a security services menu that supports automated deployment and delivers the desired API security to protect an organization's critical assets. *Bernard Harguindeguy (@bernardh_), Founder & CEO, Elastic Beam*
10:30-11:00 am	**Networking Break** (LOCATION: PRINCETON FOYER)
11:00-11:45 am	***Anatomy of a Technological and Cultural Transformation*** Matt will share candid insights into how Allstate has created a brand around the Allstate transformation initiative. Recognizing the need to modernize its developer experience, Allstate took on an impressive transformation project with major cultural and technical implications. Matt will explain how his team successfully implemented such an undertaking by balancing the dramatic shifts in culture & technology that go along with it. His talk underscores the cultural importance of enabling cloud consumers to identify with a branded experience when grappling with the idea dramatic cultural and technological change in a large enterprise. *Matt Curry (@mattjcurry), Director of Cloud Engineering, Allstate Insurance Company*

Wednesday, October 11

11:45 am-12:30 pm	***Preparing for Disaster by Integrating BCDR Principles into your DevOps Practice*** Embracing DevOps, microservices, and cloud-centric environments can provide high velocity innovation and highly scalable services. However, these DevOps methodologies diverge from traditional business continuity and disaster recovery practices. As a service running entirely in the cloud, Netflix is keenly aware of such challenges, and a great deal of time is spent building services and automation to tie into the DevOps pipeline and DevSecOps methodologies that match up with the traditional ERM and BCDR practices and procedures. Through modernizing the BCDR exercises, we were able to focus in on and mitigate some key areas of concern within both the cloud and with microservices based architectures. This session will provide a brief review of core disaster recovery best practices and how they can be better applied to services deployed to cloud environments, as well as micro-services based architectures. We will review some significant failures of note within the cloud ecosystem over the past few years and discuss how these disasters could have been averted or mitigated. We will review some of the services and systems built at Netflix to augment existing practices by building new services and automating BCDR exercises. ***Jeremy Heffner**, Senior Software Security Engineer, Netflix (former)*
12:30-1:30 pm	**Lunch**
1:30-2:15 pm	***Pacing Security in the Surging World of Containers*** The enterprise workloads of the future are container-based. Container platforms present a tremendous challenge to security teams. It's critically important for security teams to understand platform architecture, what to monitor, and when and how to take action. The rate of change in a container platform tends to be higher than what most security teams are used to. Features, architecture, and dependencies are changing faster than ever before. In this talk, Justin will offer concrete, experienced-based advice on how to think about security in a container platform. Specific topics include: where to focus log monitoring resources, key metrics to track, dealing with patch and version velocity, and departmental policy ideas. ***Justin Smith** (@justinjsmith), Chief Security Officer, Pivotal*
2:15-3:00 pm	***SDL Unicorns or Thoroughbreds: Application Security in DevOps*** With a combination of agile development, DevOps, and cloud technologies, companies deliver services more rapidly than ever. To ensure these services are delivered securely, security practices need to adapt to this fast-paced environment. In this talk, we'll see how the secure development lifecycle (SDL) can evolve to ensure services are delivered not just quickly, but also securely. We'll examine some benefits and challenges to this transition, as well the changes in culture, methods, and technologies needed to overcome them. ***Hemanth Srinivasan**, Manager – Secure Development, Autodesk*
3:00-3:20 pm	**Networking Break** (LOCATION: PRINCETON FOYER)

Wednesday, October 11

3:20-4:05 pm	***Practical Tips for Defending Web Applications in the Age of Agile/DevOps*** The standard approach for web application security over the last decade and beyond has focused heavily on slow gatekeeping controls like static analysis and dynamic scanning. However, these controls was originally designed in a world of Waterfall development and their heavy weight nature often cause more problems than they solve in today's world of agile, DevOps, and CI/CD. This talk will share practical lessons learned at Etsy on the most effective application security techniques in today's increasingly rapid world of application creation and delivery. Specifically, it will cover how to: • Adapt traditionally heavyweight controls, like static analysis and dynamic scanning, to lightweight efforts that work in modern development and deployment practices • Obtain visibility to enable, rather than hinder, development and DevOps teams ability to iterate quickly • Measure maturity of your organizations security efforts in a non-theoretical way ***Zane Lackey*** *(@ZaneLackey), CSO & Co-Founder of Signal Sciences; Former Head of Security Engineering, Etsy*
4:05-4:30 pm	***Closing Remarks*** ***Eric Johnson*** *(@emjohn20), Certified Instructor, Author, & Summit Co-Chair, SANS Institute; Senior Security Consultant, Cypress Data Defense* ***Frank Kim*** *(@fykim) , Curriculum Lead & Summit Co-Chair, SANS Institute; Founder, ThinkSec*

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.