SANS cloud security SUMMIT & TRAINING

San Francisco | Jan 17, 2017

Program Guide

@SANSInstitute #SANSCloudSummit

Agenda

All Summit Sessions will be held in the Seacliff ABCD (unless noted).

All approved presentations will be available online following the Summit at
https://cyber-defense.sans.org/resources/summit-archives
An e-mail will be sent out as soon as the presentations are posted, typically within 5 business days of the event.

Tuesday, January 17

8:00-9:00am	**Registration & Networking Breakfast** (LOCATION: SEACLIFF FOYER) SPONSORED BY F5 Networks 
9:00-9:45am	***Security as Code: The Time is Now*** The modern data center doesn't look anything like it used to, with the advent of converged and virtualized infrastructure, hybrid cloud architectures, and the steady rise of DevOps and automation/orchestration in general. Traditional security teams have been accustomed to being the people who say "no," telling business units and organizational teams that things are too risky, and so sorry, try again. Couple this with the growth of "security fatigue" and you've got a recipe for disaster. In short, people are tired of our cumbersome, tedious, and SLOW security controls and processes, and that is a terrible trend in every possible way. What to do? Security teams need to retool their skill sets, and fast. If security engineers, architects, and risk assessors aren't familiar with cloud and virtualization technologies, DevOps deployment models, and automation techniques to embed security controls into deployment pipelines, they'll just get left behind. In this presentation, Dave will talk about the need for SecDevOps (or whatever you want to call it), integration into development and operations practices for cloud, and best practices and resources that can ease the transition. ***Dave Shackleford*** *(@daveshackleford), Principal Consultant, Voodoo Security; Summit Co-Chair & Senior Instructor, SANS Institute*
9:45-10:30am	***Breaking Cloud Third-Party Risk Assessment Bad*** The presentation will focus on how the current process of performing third-party risk assessments on our cloud providers is bad and how we can break the trend. We will consider the steps necessary to properly perform third-party risk assessments on your cloud providers and what sort of transparency should or shouldn't be expected when it comes to technical security controls, vulnerability disclosure, incident response, disaster recovery and policy/procedures review. ***James Baker*** *(@ABCecurity), CISSP - ISSAP CISM, Principal Consultant, Cloud Defenders Inc.*
10:30-11:00am	**Networking Break** (LOCATION: SEACLIFF FOYER)

Tuesday, January 17

11:00-11:45am

Launching a Highly Regulated Startup in the Public Cloud

Public cloud infrastructure has been a huge enabler for the lean startup movement. Elasticity on-demand and pay-as-you-go aspects of the public cloud model have been the primary drivers for startups across all industry verticals to launch in the cloud. But, security and compliance requirements from customers and regulations can be daunting, especially when the companies are still trying build and scale product functionality.

This session presents a quick primer on bootstrapping a secure and compliant company in the public cloud. By relying on one or more public cloud providers, certain domains of security and compliance become easier by means of transferring the risk. Most cloud providers guarantee physical and environmental security compliance. In order to fully realize this benefit, it behooves for companies to minimize and eliminate local footprint of sensitive data. Similarly, rapid elasticity and broad network access made possible by the cloud providers are great for implementing a compliant disaster recovery and business continuity program.

Transferring risk to a cloud provider comes at the cost of owning the responsibility of implementing the best practices for each provider. A rigorous third party assessment machinery is required to make sure that the compliance guarantees and SLAs are being met. Data classification and clear rules about which data classes can reside where should become a part of common knowledge for personnel. With each additional provider, companies need to continually rebalance the risks by managing access control, network protections, configuration management, audit, logging, education, awareness and training, password management, information exchange, backup and recovery. Continuous monitoring, alerting and incident management plans are required for each of the distributed information assets.

The audience will learn to navigate these tradeoffs and gain practical guidance on techniques for launching a secure and compliant company using a combination of public cloud providers. The audience will also learn about a variety of open source and commercial tools to implement the security controls and automate the security and compliance operations.

Poornaprajna Udupi *(@poornaudupi), CISO, LyraHealth Inc.*

Tuesday, January 17

11:45am-12:15pm	***Virtualization-Based Security: Hardware-Enforced Protection for the Internet of Everything*** Mobility, consumerization, adoption of cloud services, and ready access to the web lead inexorably toward a stark reality: IT is out of control. Sophisticated attackers penetrate enterprise infrastructure with ease. Even organizations with the most sophisticated security products cannot prevent breaches. Security vendors offer an endless succession of fancily named technologies that aspire to greater protection, but they gloss over a fatal flaw, namely the undeniable fact that the "detect to protect" paradigm has passed its sell-by date. There is a silver lining to this cloud. Thanks to the relentless progress of Moore's Law, every device (client and cloud) has CPU features that can enable it to protect itself by design, on untrusted networks and in the hands of unreliable users. Virtualization is poised to deliver its third and most important benefit – hardware enforced protection via micro-segmentation and micro-virtualization. Endpoints stay gold, automatically self-remediate, and can safely run legacy code. Hardware isolation enables us to track the execution of malware, eliminating false alarms and providing accurate, real-time forensic insights when an organization is attacked. This talk will introduce the concepts of virtualization based security, micro-virtualization and micro-segmentation. It will use live-malware to demonstrate the benefits of hardware-isolation to protect endpoints and applications "by design," while delivering real-time forensic insights for each attacker. ***Simon Crosby*** *(@simoncrosby), Co-Founder & CTO, Bromium*
12:15-1:30pm	**Networking Luncheon** (LOCATION: SEACLIFF ABCD)
1:30-2:15pm	***Barbarians at the Gate(way)*** This talk will examine the tools, methods and data behind the DDoS and web attacks that are prevalent in the news headlines. Using information collected, I will demonstrate what the attackers are using to cause their mischief and mayhem and examine the timeline and progression of attackers as they move from the historical page defacers to the motivated attacker. I will look at the motivations and rationale that they have and try to share some sort of understanding as to what patterns to be aware of for their own protection. ***Dave Lewis*** *(@gattaca), Global Security Advocate, Akamai Technologies*
2:15-3:00pm	***Taking Control: Making Sense of the Cloud with the Critical Security Controls*** Is cloud security feeling a bit nebulous? A solid framework can help get you on stable footing. The CIS Critical Security Controls are publicly available (and free), and offer just such a framework. This talk will offer an in-depth examination of three of the Critical Security Controls and how they can be applied to Amazon Web Service (AWS) products and tools. ***Eric Johnson*** *(@emjohn20), CISSP, GWAPT, GSSP-NET, GSSP-Java AppSec Curriculum Product Manager, SANS Institute*
3:00-3:30pm	**Networking Break and Vendor Expo** (LOCATION: SEACLIFF FOYER)

Tuesday, January 17	
3:30-4:15pm	***Implementing and Maintaining a DevSecOps Approach in the Cloud*** Our organization has been in the public cloud for six years and we have a highly regulated environment. We are protecting against major attacks on a daily basis such as DDoS, malware and insider threats while going through many audits to maintain certifications and attestation like PCI 3.2, ISO27001/CSA Star and EU Privacy Shield. Like many other organizations, all of our IT operations folks are deploying a cloud strategy leveraging DEV/OPS, Containerization and Saas-based business applications and they have to give non-IT users access to systems beyond the control of the internal Ops organization. Typically, security is the last to know and the first to say no as these users are going beyond the traditional boundaries of IT and putting potentially sensitive data into cloud systems. We believe the cloud can be more secure and compliant with the right components in place, but it takes a new way of thinking and a cloud-native approach such as the one we have in place. ***George Gerchow*** *(@georgegerchow), VP – Security & Compliance, Sumo Logic*
4:15-5:00pm	***Are You Raising Your Internet Assets in a Bad Neighborhood?*** We don't scrutinize our cloud or hosting-provider selections like we do apartments, neighborhoods, or cities we wish to live in – but maybe we should. Common questions like "What is my tolerance for crime in the neighborhood versus really affordable rent?" and "How unsafe would a neighborhood really have to get before the low rent just wasn't worth it?" are never asked of our providers before we decide to "move in." Most individuals would not go out of their way to live in an apartment complex that was overrun with crime and unsavory tenants. In fact, most would likely avoid the neighborhood entirely and base their decision, in part, on word of mouth, crime studies for the area, and the condition of the apartment, complex, and neighborhood. Unfortunately, most select the provider with the right combination of marketing visibility and price – with the emphasis on the latter. Since most providers compete on rock-bottom pricing to draw new customers into their respective clouds, the question of "is $0.06 per compute hour on 'X' provider a less risky choice than $0.065 per compute hour on provider 'Y'?" is rarely, if ever, asked by the customer. This is because the required information has not been made available to them until now. This research will determine if there is truly a link between the valuation of hosting "properties" and the occurrence of poorly-maintained guest instances. ***Andrew Hay*** *(@andrewsmhay), CISO, DataGravity; Summit Co-Chair, SANS Institute*
5:00-6:00pm	**Networking Reception** (LOCATION: SEACLIFF ABCD)

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

James Baker (@ABCecurity), CISSP - ISSAP CISM, Principal Consultant, Cloud Defenders Inc.
James has seven years of cloud security experience to include spending four years as the security lead of a software-as-a-service provider. James has been on both sides of the third-party risk assessment, guiding a team to fill out hundreds of assessment questionnaires and performing assessments of his own.

Simon Crosby (@simoncrosby), Co-Founder & CTO, Bromium
Simon Crosby is the co–founder and CTO of Bromium. Previously, he was the co-founder and CTO of XenSource prior to its acquisition by Citrix. He then served as the CTO of the Virtualization and Management Division at Citrix. Previously, Simon was a principal engineer at Intel, where he led strategic research in distributed autonomic computing, platform security and trust. He was also the founder of CPlane, a network-optimization software vendor. Prior to CPlane, Simon was a tenured faculty member at the University of Cambridge, where he led research on network performance and control, and multimedia operating systems. In 2007, Simon was awarded a coveted spot as one of InfoWorld's Top 25 CTOs.

George Gerchow (@georgegerchow), VP – Security & Compliance, Sumo Logic
As Sumo Logic's Vice President of Security and Compliance, George Gerchow brings 18 years of information technology and systems management expertise to the application of IT processes and disciplines. His expertise impacts the security, compliance, and operational status of complex, heterogeneous, virtual and cloud computing environments. Mr. Gerchow's practical experience and insight from managing the infrastructures of some of the world's largest corporate and government institutions, make him a highly regarded speaker and invited panelist on topics including cloud secure architecture design, virtualization, configuration management, operational and compliance. George was one of the original founders of the VMware Center for Policy and Compliance and he holds CISSP, ITIL, Cisco, and Microsoft Certifications. Mr. Gerchow is also an acvtive Board Member for several technology start-ups and the co-author of Center for Internet Security – Quick Start Cloud Infrastructure Benchmark v1.0.0 and is a Faculty Member for IANS – Institute of Applied Network Security https://www.iansresearch.com and an instructor for MISTI http://misti.com.

Andrew Hay (@andrewsmhay), CISO, DataGravity; Summit Co-Chair, SANS Institute
Andrew Hay is the CISO at DataGravity where he advocates for the company's total information security needs and is responsible for the development and delivery of the company's comprehensive information security strategy. Prior to that, Andrew was the Director of Research at OpenDNS (acquired by Cisco) and was the Director of Applied Security Research and Chief Evangelist at CloudPassage, Inc.

SPEAKERS

Eric Johnson (@emjohn20), CISSP, GWAPT, GSSP-NET, GSSP-Java AppSec Curriculum Product Manager, SANS Institute

Eric Johnson is a Senior Security Consultant at Cypress Data Defense and the Application Security Curriculum Product Manager at SANS. He is the lead author and instructor for DEV544: Secure Coding in .NET, as well as an instructor for DEV541: Secure Coding in Java/JEE. Eric serves on the advisory board for the SANS Securing the Human Developer awareness training program and is a contributing author for the developer security awareness modules. His experience includes web and mobile application penetration testing, secure code review, risk assessment, static source code analysis, security research, and developing security tools. Eric completed a bachelor of science in computer engineering and a master of science in information assurance at Iowa State University, and currently holds the CISSP, GWAPT, GSSP-.NET, and GSSP-Java certifications. He is located in West Des Moines, IA and outside the office enjoys spending time with his wife and daughter, attending Iowa State athletic events, and golfing on the weekends.

Dave Lewis (@gattaca), Global Security Advocate, Akamai Technologies

Dave has over two decades of industry experience. He has extensive experience in IT operations and management. Currently, Dave is a Global Security Advocate for Akamai Technologies. He is the founder of the security site Liquidmatrix Security Digest and co-host of the Liquidmatrix podcast. Dave writes a column for CSO Online and Forbes.

Dave Shackleford (@daveshackleford), Principal Consultant, Voodoo Security; 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 co-author 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.

Poornaprajna Udupi (@poornaudupi), CISO, LyraHealth Inc.

Poornaprajna is currently the CISO at LyraHealth, bootstrapping a sound security and compliance program. Previously, he managed product and application security at Netflix, developed scalable, multi-tier, web systems for cloud security and API development. Poornaprajna holds an MS (Computer Science) from UCSD and an Advanced Computer Security Professional Certificate from Stanford.