SANS

cloud security

SUMMIT

Program Guide

@SANSDefense #SANSCloudSummit

Agenda

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

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

Monday, February 19

9:00-9:45 am	***DevSecOps: Getting There From Here*** As a professional consultant, I've worked with many organizations on cloud design and deployment strategies. In many cases, I've discovered that security teams and development/operations teams are not just misaligned, but speak entirely different languages. In order for cloud initiatives to proceed smoothly and securely, these teams need to get on the same page, and fast. This talk will discuss many areas where security and DevOps often have disconnects, and we'll break down what those are and why they exist. In addition, we'll talk about how we can better reconcile the differences these teams often have, all while aligning to adhere to security policies, meet best practices and internal standards, and keep moving forward with cloud business initiatives. *Dave Shackleford @daveshackleford, Senior Instructor, SANS Institute*
9:45-10:30 am	***Build, Don't Buy: Enable Analytics, ML, and Forensics with a Security Data Lake on AWS*** This talk will dive deep into some of the challenges and opportunities in cloud security. We'll examine how to ingest and store security logs in their native formats on cheap, durable cloud storage; how to apply schema-on-read and enrich the data "just in time" so that it is more actionable; and how to use enriched security logs data to rapidly evaluate promising ML technologies and surface "insights." Source code for an AWS-based, multi-protocol log aggregation pipeline will be shared. *Eric Gifford, Security Architect, Cambia Health Solutions*
10:30-10:50 am	**Networking Break** (LOCATION: BEL AIRE FOYER)
10:50-11:25 am	***Stay in Control: How Moving to the Cloud Really Changes Your Security Requirements*** Moving towards cloud services poses some unique security challenges as we move from an on-premise security model towards a more abstract and distributed cloud-based model. Shifting between these models implies that conventional security products are no longer always effective; a transformation from on-premise security controls to controls that are designed to support your cloud environment is necessary. This presentation offers a case study of our migration to the cloud. Starting from the initial analysis and pre-requirements, this talk will guide you through the common pitfalls, roles and responsibilities, an operational model with different trust levels, selected cloud controls, and solutions to minimize risk exposure and remain in control over your own IT environment. *Jeroen Vandeleur, Security Expert, NVISO*

Monday, February 19

11:25 am - 12:10 pm	***Locking Down Your Cloud*** Some companies have stated that they can be more secure in the cloud. "Can" is the key word in that sentence. To be more secure in the cloud, companies need to understand and use the new security controls available in a cloud environment to create fine grained access, detailed monitoring, segregation of duties, and automated remediation of security problems. Security teams that try to use traditional security controls without an understanding of cloud architectures and services will end up breaking cloud environments, having performance problems, and cost overruns. By not understanding and leveraging cloud security controls correctly, companies may end up with more, instead of less, security problems. Hear some stories from the trenches – both from a large company moving legacy systems to the cloud, a smaller greenfield project, and personal experimentation to design networks and capture traffic in the cloud. *Teri Radichel @teriradichel, CEO, 2nd Sight Lab*
12:10-1:30 pm	**Networking Lunch** (LOCATION: BEL AIRE BALLROOM & FOYER)
1:30-1:45 pm	***SANS Survey: Cloud Security*** A recent survey of security practitioners found that organizations are putting more sensitive customer-related data, particularly personally identifiable information (PII) and healthcare records in the cloud than ever, but that they continue to have major concerns about sensitive data. More than 60% worry about unauthorized access by outsiders, followed by insecure, unmanaged devices accessing sensitive info from the cloud, followed by breach of sensitive data by cloud personnel. So what? We all have the same worries, but what are the solutions? Learn how your organization compares to survey respondents', and get recommendations for these common challenges. *Dave Shackleford @daveshackleford, Senior Instructor, SANS Institute*
1:45-2:30 pm	***Pragmatic Cloud Security Patterns*** By now you, your children, and possibly your goldfish all know and understand that traditional security patterns don't tend to hold up well when copied and pasted into the cloud. In this dynamic session, Rich will demonstrate cloud-native security patterns for managing both traditional security issues and some of the new challenges in Infrastructure as a Service (IaaS). You will learn practical approaches from leveraging auto scale groups and immutable laws for security, to handling real-time event-driven alerting and automated remediation, to enterprise-scale, multiple account security monitoring and alerting infrastructure. Most demonstrations will be in AWS with discussion of the differences in Azure and GCP. *Rich Mogull, Analyst & CEO, Securosis*

Monday, February 19

2:30-3:15 pm	***All Your Cloud Belongs To Us: Hunting Compromise in Azure*** MongoDB, Redis, Elastic, Hadoop, SMBv1, IIS6.0, Samba. What do they all have in common? Thousands of them were pwned. In Azure. In 2017. Attackers have shifted tactics, incorporated nation-state leaked tools and are leveraging ransomware to monetize their attacks. Cloud networks are prime targets; the DMZ is gone, the firewall doesn't exist and customers may not realize they've exposed insecure services to the Internet until it's too late. In this talk I'll discuss hunting, finding and remediating compromised customer systems in Azure – a non-trivial task with 1.59 million exposed hosts and counting. Remediating system compromise is only the first stage so we'll also cover how we applied the lessons learned to proactively secure Azure Marketplace. Finally, I will present research I've done into the default security configuration of Azure Marketplace images and present a call to action for teams working on Azure security offerings. *Nate Warfield, Senior Security Program Manager, Microsoft*
3:15-3:35 pm	**Networking Break** (LOCATION: BEL AIRE FOYER)
3:35-4:00 pm	***What Would FedRAMP Do?*** The GSA FedRAMP cloud services certification program now has 88 cloud services authorized for government use and 75 more in various stages of the pipeline. This presentation will provide attendees with an approach for taking advantage of the testing done by FedRAMP and the documentation produced by cloud service providers as a first step in driving business units to select secure cloud services. Then we will go through additional steps to determine where gaps may still remain and how to add additional visibility and control functions to use of external cloud services. *John Pescatore, Director of Emerging Security Trends, SANS Institute*
4:00-4:45 pm	***Forensics as a Service: IRDF in the Cloud*** What was hardware, now is software; it is just an API call. We deploy infrastructure the same way we deploy applications. That fact has many implications in security and automation. We can automate recon, attacks and lateral movement but also automate many incident response processes along with hardening. This talk will cover concepts and challenges doing forensics in cloud vendors and it will go deeper to show some attack vectors and hardening for AWS in particular. *Toni de la Fuente, Lead of Security Operations and Senior Cloud Security Architect, Alfresco Software*
4:45-6:00 pm	**Networking Reception** (LOCATION: BEL AIRE 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.

Tuesday, February 20

9:00-9:45 am	***Addressing the Mismatch Between IT and Security in a Cloud-First World*** The race to the cloud is putting security professionals on their heels. CIOs are moving to the cloud at a staggering rate, often with little regard for security protocols, thus putting their security teams at a disadvantage. Determining who has responsibility for the protection of applications, services, and data once cloud has become part of an enterprise stack is a major challenge for enterprise landscapes. Enterprises not only need to understand the risks of the cloud, but also the shared responsibility model that most cloud providers operate under. Most cloud providers are not managing data so much as providing a platform or infrastructure, leaving the protection of the data up to the internal security team. While the cloud offers more availability and uptime, it could also be making data more accessible and vulnerable to an attack. There is elevated risk when it comes to convenience. Every copy of data is a potential liability. Enterprises need to own the responsibility of securing their own data and make sure they are maintaining access control lists properly, performing quality-assurance on configurations and policies, and auditing who has access to what. In this session, we will explore how security professionals can take ownership of their organization's security and gain a clearer understanding of where responsibility lies. We'll offer steps they can take to make the cloud more secure for their enterprise. *Ben Johnson, Co-Founder & CTO, Obsidian Security*
9:45-10:30 am	***We Can't Hold on a Sec: Why We Need DevSecOps from Day 1*** DevSecOps means everyone is responsible for security from Day 1. In this day and age, a "live and learn" mentality when it comes to security is not going to cut it. Teams need to be on guard against major attacks, while simultaneously building their apps in compliance with regulations. This session will dive into the issues of DevSecOps implementation, and how we can bake it all in from the get-go. *George Gerchow, VP of Security and Compliance, Sumo Logic*
10:30-10:50 am	**Networking Break** (LOCATION: BEL AIRE FOYER)
10:50-11:25 am	***Reference Architecture for Identity and Access Management: Role Data Pattern Distribution in AWS*** Attendees can expect to learn how to apply AWS IAM Roles consistently across a fleet of AWS Accounts. Attendees can also explore the use of AWS Account boundaries to limit damage (blast radius containment) in the event of an attack. Attendees can begin to think about how use of multiple AWS Accounts in an enterprise cloud environment. This use pattern can segment data and computing streams as needed. *Brad Rambur, Cloud Security Practice Leader, Leo Cyber Security*

Tuesday, February 20

11:25 am - 12:10 pm

The Top 3 Risks of Migrating to Cloud

Most organizations are aware of the benefits of embracing cloud architectures, but the majority fail to realize the risks of migrating existing servers and applications into a public cloud environment.

Cloud computing enables the rapid deployment of servers and applications, dynamic scalability of system resources, and helps businesses get products to market faster than ever before. What's lacking, however, are many of the standard compensating controls that organizations lean on to protect their datacenter-hosted assets.

In this session, we will review the top 3 risks of migrating servers and applications out of the datacenter and into the most popular public cloud environments. Topics that will be discussed include:

- Cloud security fundamentals
- The new perimeter (and the tools available)
- Data protection and proliferation

***Andrew Hay**, Co-Founder and CTO, LEO Cyber Security; Certified Instructor, SANS Institute*

12:15-1:45 pm

Lunch & SkyBox Lunch & Learn (LOCATION: BEL AIRE BALLROOM & FOYER)

You Can't Secure What You Can't See — The Importance of Visibility in the Cloud

It goes without saying, you can't secure what you can't see. However, as organizations continue to migrate workloads to virtual and cloud environments, many are challenged with gaining the visibility they need to truly understand their security posture. What is the best approach to ensuring that visibility? What should be included? What are the unique challenges posed by these environments? And, how does visibility impact CIS critical security controls, such as continuous vulnerability assessment and remediation or maintaining secure configurations? In session, SANS Director John Pescatore and Skybox Security Director of Professional Services Delivery Tony Turner discuss the importance of gaining comprehensive visibility of virtual and cloud networks. They will cover best practices and examples of how to quickly understand what IT assets exist in your cloud environment. And, how that understanding informs your overall security program, managing physical, virtual and cloud environments holistically.

***John Pescatore**, Director, SANS Institute*

***Tony Turner**, Director of Professional Services Delivery, Skybox Security*

1:45-2:30 pm

Building a Defense Strategy for Your Cloud Workloads

Learn how to use modern cloud technologies and OSS to start building a defense strategy for your cloud workloads. We will discuss areas ranging from DDoS protection to access management to automatic IR – even down to instance-based memory captures. We will start with overarching strategy design decisions and work our way to practical code samples and explicit OSS tools and projects. This session is very tech/code/OSS heavy and expert level but can still accommodate intermediate to advanced users to show what can be accomplished by using a combination of native cloud controls and OSS tooling. 1) Understand how to use cloud technologies to improve your IR strategy. 2) Learn about various Cloud specific OSS projects available for defense strategies. 3) Understand the difference in cloud vs on-prem defense strategies

***Henrik Johansson**, Principal SA Content PM, AWS*

Tuesday, February 20

2:30-3:15 pm

Planning For Success - Strategies for Architecting, Implementing, and Migrating PCI-DSS Compliant Cloud-Based Solutions

This session will address strategies for architecting, implementing, and migrating to cloud-based solutions where one or more components has some level of PCI DSS applicability, including partial and complete cardholder data environments (CDE). Attendees will leave this session with a basic and actionable understanding of general strategies and considerations for: 1) Understanding the risk-based approach to sustainable and effective PCI-DSS compliance management; 2) Determining what, if any, cloud-based systems or resources may be in-scope for PCI DSS compliance; 3) Strategies for designing defensible cloud-based infrastructure and connectivity to support PCI DSS compliance; 4) Strategies for streamlining compliance management tasks and driving down the cost of audit; 5) Strategies for establishing and demonstrating a complete chain-of-trust for all cloud-based resources with PCI scope applicability; 6) Strategies for migrating PCI systems, data, or workloads to new cloud-based infrastructure or platforms while reducing risk of compliance or security control deficiencies; 7) Strategies for managing and delegating responsibilities for managing PCI DSS controls in a cloud-based solution, including both internal teams and service providers Primary focus will be largely conceptual, but generally aligned to AWS and Azure design concepts.

Noah Weisberger, VP & CISO, LEO Cyber Security

3:15-3:30 pm **Networking Break** (LOCATION: BEL AIRE FOYER)

3:30-4:15 pm

Continuous Security: Monitoring & Active Defense in the Cloud

Monitoring and feedback loops from production is a critical tenant in DevOps for measuring performance, runtime errors, statistics, and changes. In the SecDevOps world, security teams can take advantage of DevOps monitoring tools to increase security visibility, identify anomalies, and respond swiftly to real time attacks.

Cloud providers are offering powerful infrastructure, development, and application continuous monitoring services that generate a wealth of data. But, building continuous security monitoring on top of the data can be challenging. Where are the log files? What is the log file format? What security events are captured? How do we display meaningful metrics? Can we detect and defend in real time?

This talk will introduce attendees to a realistic AWS environment's monitoring and active defense system and discuss real data collected during a war game exercise. Afterwards, we will walk through the postmortem, review the alerts raised during the incident, determine if there were any surprises, and identify opportunities to improve the system. Attendees will walk away with actionable techniques for building an active defense framework to help protect your organization's cloud resources.

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.