Monday, February 19, 2018	
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 speaking 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 together 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 pply 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**
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 & 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 & responsibilities, 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**

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	**Lunch**
1:30-1:45 pm	**SANS Survey: Cloud Security** A recent survey of security practitioners find 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 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**
2:30-3:15 pm	**All Your Cloud Are Belong 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 1.59million 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**
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**

Tuesday, February 20, 2018	
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 all while 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 from the get-go. **George Gerchow, VP of Security and Compliance, Sumo Logic**
10:30-10:50 am	**Networking Break**
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**

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, Instructor, SANS Institute**
12:15-1:45 pm	**Lunch & GDPR Panel**
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**
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 & considerations for: 1. Understanding the Risk-based approach to sustainable & 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 & 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 & 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**
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**

Speaker Biographies

Toni de la Fuente, Lead of Security Operations and Senior Cloud Security Architect, Alfresco Software
Toni currently works at Alfresco Software as Lead of Security Operations. His blog is blyx.com, where he writes since more than 15 years ago. During this time, he has done some things for security and the Open Source community like phpRADmin (RADIUS Tool), Prowler (AWS Security Tool), Nagios plugin for Alfresco, Alfresco BART (backup tool), Alfresco Backup and Disaster Recovery White Paper, Alfresco Security Best Practices Guide, Alfresco data leak prevention tools, and some others. He has also co-authored or contributed to: Building a Home Security System with BeagleBone (PacktPub 2013), Icinga Network Monitoring (PacktPub 2013) and Troubleshooting CentOS 7 (PacktPub 2015).

George Gerchow, VP of Security and 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 security 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 active Board Member for several technology start upss 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/

Eric Gifford, Security Architect, Cambia Health Solutions
Eric Gifford is a Security Architect, CISSP, GWAPT, and AWS Certified Architect. He comes from a traditional InfoSec upbringing, but has recognized the inevitable trajectory of cloud computing. Eric perceives alignment to devops, cloud, and serverless principles to be a matter of organizational survival. He is helping to guide Cambia InfoSec in to a developer-centric culture where we too are agile, cloud-first, and capable of building solutions that do not exist today.

Andrew Hay (@andrewsmhay), Co-Founder & CTO at LEO Cyber Security
Andrew Hay is an information security industry veteran with close to 20 years of experience as a security practitioner, industry analyst, and executive. As the Co-Founder & CTO for LEO Cyber Security, he is responsible for the creation and driving of the strategic vision for the company.

Eric Johnson (@emjohn20), Certified Instructor, Author, & Summit Co-Chair, SANS Institute; Senior Security Consultant, Cypress Data Defense
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.

Rich Mogull, Analyst & CEO, Securosis
Rich has twenty years' experience in information security, physical security, and risk management. He specializes in data security, application security, emerging security technologies, and security management. Prior to founding Securosis, Rich was a Research Vice President at Gartner on the security team where he also served as research co-chair for the Gartner Security Summit. Prior to his seven years at Gartner, Rich worked as an independent consultant, web application developer, software development manager at the University of Colorado, and systems and network administrator. Rich is the Security Editor of TidBITS, a monthly columnist for Dark Reading, and a frequent contributor to publications ranging from Information Security Magazine to Macworld. He is a frequent industry speaker at events including the RSA Security Conference and DefCon, and has spoken on every continent except Antarctica (where he's happy to speak for free – assuming travel is covered).
Prior to his technology career, Rich also worked as a security director for major events such as football games and concerts. He was a bouncer at the age of 19, weighing about 135 lbs (wet). Rich has worked or volunteered as a paramedic, firefighter, and ski patroller at a major resort (on a snowboard); and spent over a decade with Rocky Mountain Rescue. He currently serves as a responder on a federal disaster medicine and terrorism response team, where he mostly drives a truck and lifts heavy objects. He has a black belt, but does not play golf.

John Pescatore, Director of Emerging Security Trends, SANS Institute
John Pescatore joined SANS in January 2013 with 35 years' experience in computer, network and information security. He was Gartner's Lead Security Analyst for 13 years, working with global 5000 corporations and major technology and service providers. Prior to joining Gartner Inc. in 1999, Pescatore was Senior Consultant for Entrust Technologies and Trusted Information Systems. Prior to that, Pescatore spent 11 years with GTE developing secure computing systems. Pescatore began his career at the National Security Agency, where he designed secure voice systems, and the United States Secret Service, where he developed secure communications and surveillance systems. He holds a BSEE from the University of Connecticut and is a NSA Certified Cryptologic Engineer.

Teri Radichel (@teriradichel), CEO, 2nd Sight Lab
Teri Radichel provides cyber security assessments, pen testing, and research services through her company, 2nd Sight Lab. Her career started in telecommunications and networking in 1994. She gravitated to software programming, having learned BASIC from a book in grade school. After obtaining a master of software engineering in 2000, she started a software consulting and web hosting business and served customers ranging from startups to Fortune 150. In 2011, she joined Capital One Investing and led a team working on large-scale back office systems. In 2013, she started the Seattle AWS Architects & Engineers Meetup. She moved to the cloud engineering team to help Capital One migrate production workloads to AWS and then the security operations team to help with security automation. At WatchGuard Technologies, she architected a secure CICD deployment pipeline based on her SANS white paper, *Balancing Security and Innovation With Event Driven Automation*. She has a number of SANS certifications and received the SANS 2017 Difference Makers award. You can follower her on twitter at @teriradichel.

Brad Rambur, Cloud Security Practice Leader, LEO Cyber Security
Brad Rambur's (CISA, CGEIT, CRISC) experience spans 25 years of IT Operations, Security, and Systems Integration. His current focus is building and leading organizations aligned with their

business/operational mission, developing tools, methods, and practices for secure multi-tenant public cloud computing.

Dave Shackleford @daveshackleford, 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 coauthor 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. Dave earned his MBA from Georgia State University.

Jeroen Vandeleur, Security Expert, NVISO
Jeroen Vandeleur is a Security Expert who works for the Belgian cyber security firm NVISO, which focuses on high-end cyber security services, specializing in government, defense and the financial sector. At NVISO Jeroen focuses on security architecture and during his career he had the unique opportunity to work in different environments hence building up a significant technical security experience. In total Jeroen has more than 8 years of experience in the security industry including several projects such as security design reviews, network segmentation, datacenter migration for a financial institution and implementing a security operations center for a government agency.

Nate Warfield, Senior Security Program Manager, Microsoft
By day Nate manages vulnerabilities in Windows, Hyper-V and Azure. In his spare time he hunts for emerging attack vectors and is obsessed with securing the Internet of (insecurable)Things.