SESSION TITLE	Cloud Security: Automate or Die
SESSION QUICK ABSTRACT	This session will walk through a number of different case examples for cloud security automation, including forensics, incident response, vulnerability management, and network security.
SESSION ABSTRACT	Much has been said about DevOps, and SecDevOps for security automation and integration. However, to many in the security community, this is still a buzzword. There are many practical applications of automation in cloud security controls, however, across all security-related disciplines. This talk will delve into concrete examples of security automation in the cloud, with metrics examples, as well.
SESSION DETAIL	This talk will begin with a mock architecture that actually exists in AWS for demonstration purposes, and the talk will then proceed into different subject matter areas of security operations, with concrete examples of how to develop automation workflows, explicit discussion of tools and functions needed, APIs required or advantageous to employ, and code discussion. Each case study will then have active screenshots provided for demonstration (or a live demonstration in the session, TBD depending on time requirements). The following categories and examples will be included: 1. Security event management and monitoring: Automated log collection will be performed from numerous running instances and cloud admin activity, stored to a defined container, secured with access controls and defined permissions, and loaded into an event management platform for analysis. 2. Identity and Access Management: Automated provisioning of new users into defined roles will be discussed, as will federation using SAML-based IDaaS providers. 3. Network access control and scaling: DNS, load balancing, and auto scaling will be demonstrated in automated workflow models for ensuring reliable and durable infrastructure. This will also include accommodation for resilience to some Denial-of-Service. 4. Endpoint configuration and monitoring: Automated agent deployment using host-based tools that deploy in image builds, “phone home” for policy, and report back on configuration status will be developed, along with monitoring and alerting controls that can be automated as well. 5. Vulnerability scanning: Vulnerability scanning within a cloud environment will be scheduled and automated, with reports automatically generated and stored for review.