Experience Sumo Logic at AWS re:Invent

sumo logic

Certification Offerings:

Level 1 Pro Certification
Monday, November 26
9:00am–12:30pm
Mirage Hotel–Portofino Room–Lunch Following

Sumo Pro Users have a broad knowledge around analyzing logs and metrics. They can get up and running with their familiarity with services related to simple data searching, filtering, parsing, and analyze.

Register

Security Certification
1:00pm–4:30pm
Mirage Hotel–Portofino Room–Lunch Prior

Sumo Security Power Users exhibit deep technical knowledge on how to analyze and correlate their logs to secure their organizations. Using Sumo Logic's Threat Intelligence, they can build content to increase velocity and accuracy of threat detection.

Register

Lunch provided to all certification attendees from 12:00pm – 1:30pm

AWS Hosted Sessions with Sumo Logic

AWS Programs

Breakout Session

Security Challenges and Use Cases in the Modern Application Build and Deploy Pipeline
Dave Frampton, VP of Security Solutions, Sumo Logic
Olaf Stein, Security Solutions Architect, Sumo Logic
Brad Segobiano, Sr. Software Engineer, Genesys

Tuesday, November 27
5:30pm–6:30pm | *Venetian, Level 4, Delfino 4005*

Modern application build and deploy workflows are creating new challenges for traditional security models. Traditional workflows need to be recast in new data sets, and new workflows need to be added to cover the expanding threat surface area. This session will explore the security challenges created by modern application build/deploy pipelines, basic considerations for the security defense, example use cases, and a customer case study to illustrate the concepts.

AWS Theater Session

Learn How Sumo Logic's Global Intel Drives Better DevSecOps
Bruno Kurtic, Founding VP, Product & Strategy

Tuesday, November 27
5:10 PM–5:30 PM | *Venetian, Level 2, Pavilion Theater–Expo Hall*

Sumo Logic Booth #840 Engagements and Experiences

Sumo Logic Demos

DevOps - Monitoring & Troubleshooting a Modern App
Minimize downtime and improve system availability to deliver a world-class customer experience.

A DevOps engineer is alerted to a spike in latency breaking the payment service in their travel booking app, causing massive revenue loss. Using Sumo he quickly correlates between logs and metrics to quickly identify the root cause and take action.

Sumo Logic helps with:
- Aggregating Across All Data Sources
- Visibility via Unified Logs & Metrics Dashboards
- Resolving Issues Faster with Machine Learning

DevSecOps - Continuous Security at Scale
Minimize risk by fusing security best practices with your DevOps process.

A DevSecOps engineer is alerted to a sudden increase in threats detected by Crowdstrike and log ingest rate into Sumo. She quickly triages the threat using Sumo's consolidated logs & metrics from CI/CD pipeline tools, security logs, and infrastructure logs.

Sumo Logic helps with:
- Anomaly Detection
- User Misconfiguration
- Identifying Malicious Behavior

Security Analytics - Detecting & Investigating Threats
Correlate across your entire IT infrastructure to solidify your security and compliance posture.

A Security engineer utilizes Sumo to monitor and detect threats and abnormal behaviors in his company's IT ecosystem. See him leverage Sumo's powerful analytics capabilities to correlate and prioritize incidents so he can focus on identifying the root cause of his most critical threat within minutes.

Sumo Logic helps with:
- Threat Detection
- Event Correlation & Prioritization
- Investigation & Response

Presentation Theater Schedule

Time	Monday–11/26 Booth Hours: 4pm–7pm	Tuesday–11/27 Booth Hours: 8am–6pm	Wednesday–11/28 Booth Hours: 10am–6pm	Thursday–11/29 Booth Hours: 10am–4pm
10:00am				
10:30am		Customer Session– NordCloud	AWS Security	
11:00am				Pagerduty & Sumo Logic
11:30am		New Relic & Sumo Logic	Palo Alto Networks & Sumo Logic	
12:00pm				
12:30pm				
1:00pm		Customer Presentation Informatica	Customer Presentation Wag!	
1:30pm				
2:00pm		eSentire & Sumo Logic		
2:30pm				
3:00pm		Serverless Monitoring		
3:30pm				
4:00pm	DevSec Ops	DevSecOps	DevSecOps	
4:30pm	AWS Security	AWS Security	Okta & Sumo Logic	
5:00pm	Killer Queen & Sumo Logic	Killer Queen & Sumo Logic		
5:30pm	Kubernetes & AWS	Kubernetes & AWS	Kubernetes & AWS	
6:00pm	Modern App Report			
6:30pm				
7:00pm				

Presentation Abstracts

Achieving DevSecOps with Sumo Logic
While it is hard to settle on a definition of DevSecOps, at a high level it is the philosophy of integrating security practices within the DevOps process and making every team member responsible for security. This includes monitoring all of your environment- from your Github repository, through your Continuous Integration (CI)/Continuous Delivery (CD) pipeline, into your development environment, and finally into your production environment- for both operational and security issues. In this demo we will show how Sumo can be used to practice DevSecOps, giving you visibility into your entire environment and increasing the scope of your awareness across the security landscape.

Best Practices for Monitoring Microservices With Sumo Logic
Adoption of container technologies such as Docker and Kubernetes is leading the rapid expansion of ephemeral entities that teams must manage. Teams not only collect, correlate, and dashboard telemetry, but leverage intelligence from those streams for the optimization of IT operations and security event management. Join our team for a breakdown of common challenges and monitoring best practices for microservices environments with Sumo Logic.

Leveraging Sumo Logic for Security Insights Across AWS
The Sumo Logic AWS Security apps provide security professionals with a comprehensive set of pre-built dashboards to provide the analytics and visibility they need to fully leverage the AWS environment. In this session we will highlight the wide range of pre-built options available from the Sumo Logic platform for the AWS environment including pre-built support for GuardDuty, VPC Flow Logs, CloudTrail and ELB dashboards that facilitate deep visibility into trends, anomalies, in real-time and with actionable intelligence into AWS and hybrid environments. We also show how you can customize alerts and alarms associated with critical events to perform automated actions, responses and notifications to accelerate rapid identification and response to potential threats to security and compliance standards.

The Authoritative Guide on AWS Trends
Do you ever ask yourself, "how do the cloud savvy companies like Twitter, Airbnb, Adobe, SalesForce, etc., build and manage their modern applications on AWS?" If so, this is the session for you. Get data-driven insights, best practices and trends from enterprises who run massive mission-critical modern applications on AWS. Sumo Logic provides this data by anonymously analyzing technology adoption among more than 1,600 Sumo Logic customers.

Monitoring Lambda with Sumo Logic
Are you ready for serverless? AWS Lamba has moved from the fringe of the discussion to being a key consideration for application architectures on AWS. How do you integrate AWS Lambda into your monitoring strategy? How do you use CloudWatch metrics and CloudTrail auditing along with logging to get a full picture? How do you detect security threats to AWS Lambda and fold it into your security operations? Come hear how Sumo Logic can help and how Sumo Logic customers are doing this with success today.

Sumo Logic + AWS Overbridge = Awesome Security Analtyics
AWS has enlisted Sumo Logic to be one of its early design partners to participate in the beta for its upcoming Overbridge security service. In this session, we will cover AWS Overbridge fundamentals and show you how Sumo Logic and Overbridge work together can improve your security analytics effectiveness and reduce the risk of security breaches.

Building Cloud-Native Security Operations with Sumo Logic
Customer: NordCloud - Ilja Summala

Today's Cloud based applications and infrastructures and the inherent gaps in legacy security tools for this new environment, is driving the need for better tools and a new approach to managing modern security operations. By combining these concepts organizations can not only deliver better security operations, but at a fraction of the cost. In this session we will review best practices for Security Operations Centers (SOCs) in the cloud and for the cloud.

Effective Incident Management with Sumo Logic
Customer: Informatica - Lior Mechlovich - Principal Software Engineer and Architect

The Informatica cloud platform is a collection of dozens of microservices that spans across 10+ teams and 5+ countries. When a production incident happens we primarily use sumologic for managing the incident. Lior will walk you through the dashboard templates his team developed for each service as well as cross service key transactions that help them to manage those incidents and minimize to time to fix it.

Logs for Dogs
Customer: Wag — Dave Bullock, Director of Engineering

Over the past six months, Wag has radically improved their infrastructure and visibility into our systems and application with a combination of Terraform and Sumo Logic. Dave Bullock will walk through their journey with hopes of helping others on the same path - and show you how to use Sumo Logic Logs and Metrics to ensure excellent app performance.

A New Approach to Monitoring Complex Modern Systems in the Cloud

Partner - New Relic - Mark Weitzel, Sr. Director, Platform & Ecosystem
New Relic and Sumo Logic work together to jointly help clients uncover and solve issues faster, while being able to effortlessly move between products. In this session, we will outline key use

cases by which joint customers can get complete visibility into application performance and error logs with our products.

How to Do Incident Response in the Cloud
Partner – Palo Alto Networks - Hermann Hesse, Manager, Systems Engineering Public Cloud

In this session with Palo Alto Networks, we will discuss how the cloud and modern applications are changing security teams and incident response. We will also discuss our joint integrations giving SOC teams advanced insight into their security and compliance posture.

Empowering Security Ownership with PagerDuty and Sumologic
Partner – Pager Duty – Dave Cliffe: Head of Strategy, New Use Cases

Sumo Logic and PagerDuty have teamed up in this session to discuss how the ownership of security operations have changed from traditional SOC teams to a DevSecOps model and how customers can benefit from the strengths of each platform via existing integrations between the two products.

Eliminate cybersecurity blind spots in cloud and hybrid IT environments
Partner – eSentire – Chris Braden, VP Global Channel & Alliances

Traditional SIEM platforms require continuous costly investment while leaving blind spots in evolving hybrid IT environments. Learn how the game-changing esLOG+ combines critical visibility with threat hunting to enable rapid response by integrating eSentire's Managed Detection and Response (MDR) platform with Sumo Logic's cloud-native solution. In this session you'll also learn how:

- The new esLOG+ provides full spectrum visibility and eliminates blind spots exploited by threat actors.
- eSentire's expert security analysts leverage Sumo Logic's log and metric data from on-premises and cloud assets to quickly identify and contain suspicious activities and disrupt threats before they impact your business.
- esLog+ evolves as your on-prem, hybrid or cloud environment evolves and the threat landscape expands.
- Managed Detection and Response (MDR) keeps organizations safe from advancing cyberattacks that technology alone can't prevent via elite security analysts who hunt, investigate, and respond in real-time to known and unknown threats.

Gaming

KILLER QUEEN

Engage in an exciting multi-player challenge of the popular game, Killer Queen in Sumo Logic's booth 840. See a modern app in action displaying real time analytics through Sumo Logic to help the gamer understand the value and impact of leveraging continuous intelligence using Sumo, while playing the game in real-time.

Game challenges will be offered continuously during booth hours. We expect this to be very popular, so tickets will be provided if needed to save you a spot and alleviate waiting in line.

Not familiar with the game? No problem! Learn how to play in one of two ways before arriving.

Read How to Play
Video: How to Play