

RSA®Conference2022

San Francisco & Digital | June 6 – 9

**Sumo Logic is making
the world's digital
experiences reliable
and secure**

Booth 5463 - North Expo Hall



sumo logic

Sumo Logic is making the world's digital experiences reliable and secure

Visit us at RSA Conference 2022 to learn how Sumo Logic's cloud-native security solutions can help your organization efficiently and cost effectively manage your SIEM, security investigations, compliance, and SOAR requirements across your cloud, hybrid, and on-prem environments.

Booth hours

Monday, June 6 5:00–7:00 pm	Tuesday, June 7 10:00 am–6:00 pm	Wednesday, June 8 10:00 am–6:00 pm	Thursday, June 9 10:00 am–3:00 pm
---------------------------------------	--	--	---

Booth location

The Sumo Logic booth number is **5463** and is located in the North Expo Hall.



Engage with Sumo Logic to gain deeper knowledge of our solutions by exploring any of the following activities:



RSA sponsored session

Hear how security teams are modernizing their SOC and increasing cyber resilience with Sumo Logic



Booth presentations

Learn how to secure your digital transformation and digital experiences, surface threats automatically and investigate and respond quickly to modern threats by attending our 15 minute or less booth theater presentations



Security workshops

Give us 15 minutes and we'll get you hands-on with time-saving Threat Intelligence, Security Insights, and the best in Orchestration and Automation.



Demos






Dive deeper into our technology in one of our many demos led by Sumo Logic security experts

Get the security insights you need to stay on top of your digital business.
See us in action at [Booth 5463](#) in the North Hall.

















Activity schedule

 RSA sponsored session  Booth presentation  Security workshop  Demos

Monday, June 6 | 5:00–7:00 pm [Booth 5463](#)

-  5:00–7:00 pm Demos
-  5:00–5:15 pm Modernize your security using Sumo Logic
-  5:30–5:45 pm Mini workshop: Security analytics for all your alerts
-  6:00–6:15 pm Quickly understanding the impact and context of an attack
-  6:30–6:45 pm How to automate your cybersecurity initiatives using Cloud SOAR















Tuesday, June 7 | 10:00 am–6:00 pm [Booth 5463](#)

-  10:00 am–6:00 pm Demos
-  10:00–10:15 am Modernize your security using Sumo Logic
-  10:30–10:45 am Mini workshop: Security analytics for all your alerts
-  11:00–11:15 am Introduction to Sumo Logic Threat Labs
-  11:30–11:45 am Actionable security insights with Zscaler and Sumo Logic
-  12:15–12:30 pm How to automate your cybersecurity initiatives using Cloud SOAR
-  12:45–1:00 pm Mini workshop: Automating responses with Cloud SOAR
-  1:15–1:30 pm Quickly understanding the impact and context of an attack
-  1:45–2:00 pm Mini workshop: Cloud SIEM Insights
-  2:45–3:00 pm Improving cyber defense with crowdsourced global intelligence and Cloud SIEM
-  3:15–3:30 pm Threat detection, faster investigation, and automated response for modern SOCs, with VMware and Sumo Logic
-  3:45–4:00 pm MITRE the corners of your ATT&CK surface
-  4:15–4:30 pm State of software insecurity, presented by eSentire
-  4:45–5:00 pm Quickly understanding the impact and context of an attack
-  5:15–5:30 pm Modernize your security using Sumo Logic
-  5:45–6:00 pm How to automate your cybersecurity initiatives using Cloud SOAR









Activity schedule *continued*

 RSA sponsored session  Booth presentation  Security workshop  Demos

Wednesday, June 8 | 10:00 am–6:00 pm [Booth 5463](#)

	10:00 am–6:00 pm	Demos
	10:00–10:15 am	Innovate and transform your security operations
	11:00–11:15 am	MITRE the corners of your ATT&CK surface
	11:30–11:45 am	Actionable security insights with Zscaler and Sumo Logic
	12:15–12:30 pm	How to automate your cybersecurity initiatives using Cloud SOAR
	12:45–1:00 pm	Mini workshop: Automating responses with Cloud SOAR
	1:45–2:00 pm	Mini workshop: Cloud SIEM Insights
	2:15–2:30 pm	Quickly understanding the impact and context of an attack
	2:45–3:00 pm	Threat detection, faster investigation, and automated response for modern SOCs, with VMware and Sumo Logic
	3:15–3:30 pm	Improving cyber defense with crowdsourced global intelligence and Cloud SIEM
	3:45–4:00 pm	Introduction to Sumo Logic Threat Labs
	4:15–4:30 pm	Modernize your security using Sumo Logic
	4:45–5:00 pm	Quickly understanding the impact and context of an attack
	5:15–5:30 pm	How to automate your cybersecurity initiatives using Cloud SOAR

Thursday, June 9 | 10:00 am –3:00 pm [Booth 5463](#)

	10:00 am–3:00 pm	Demos
	10:00–10:15 am	Threat detection, faster investigation, and automated response for modern SOCs, with VMware and Sumo Logic
	10:30–10:45 am	MITRE the corners of your ATT&CK surface
	11:00–11:15 am	Moving the SOC needle: from reactive triage to a data-driven scientific approach
	11:30–11:45 am	Mini workshop: Cloud SIEM Insights
	12:15–12:30 pm	How to automate your cybersecurity initiatives using Cloud SOAR
	12:40–1:10 pm	Modernize your SOC and increase cyber resilience with Sumo Logic
	12:45–1:00 pm	Mini workshop: Automating responses with Cloud SOAR
	1:15–1:30 pm	Actionable security insights with Zscaler and Sumo Logic
	1:45–2:00 pm	Improving cyber defense with crowdsourced global intelligence and Cloud SIEM
	2:15–2:30 pm	Modernize your security using Sumo Logic
	2:45–3:00 pm	Mini workshop: Security analytics for all your alerts

Activity descriptions

RSA sponsored session

Modernize your SOC and increase cyber resilience with Sumo Logic

Speaker: Dana Torgersen, Director, Security, Sumo Logic

Sumo Logic is making the world's digital experiences reliable and secure with our SaaS analytics platform that helps you secure and protect against modern threats. This presentation highlights how Sumo Logic's security solutions can help secure your digital transformation initiatives, solve security complexity, and automate your threat investigation and response workflows.

Date/Time: Thurs, June 9 | 12:40–1:10 pm

Location: North Expo briefing center

Demos Booth 5463

Visit Sumo Logic's booth in the North Hall where you can speak with one of our security experts and see any of the following solution demonstrations

- Getting started quickly with AWS to transform your security data
- Enriching security alerts with user context using Cloud SIEM
- Quickly selecting & customizing SOAR playbooks in App Central
- Automating responses to a phishing attack
- Stepping into the War Room
- Monitoring Lambda and automatically responding when threatened

Booth presentations Booth 5463

Innovate and Transform your Security Operations

Speakers: Abby Pagliaro, Director of Security Platforms and Endpoint Security, MassMutual
Lynne Doherty, President of Worldwide Field Operations, Sumo Logic

The ever-increasing sophistication of attacks, abundance of disparate security tools, and limited security talent poses increasing challenges for security leaders looking to improve their cyber defenses, mitigate risk and increase resiliency. In this fireside conversation you will hear how MassMutual, a Fortune 500 company, innovates and modernizes its security operations to handle the rapidly evolving threat landscape through cloud-native security solutions and on the future state of security.

Modernize your security using Sumo Logic

Presenter: Jason Dunne, Product Marketing Manager, Sumo Logic

Learn how Sumo Logic's cloud-native security solutions support the entire spectrum of security use cases—from logging compliance data, to monitoring and securing hybrid clouds, to delivering market-leading SIEM and SOAR capabilities. Example: Monitor, prioritize and investigate security insights within your AWS infrastructure.

Quickly understanding the impact and context of an attack

Presenter: Dana Torgersen, Director of Product Marketing, Security, Sumo Logic

Security operations teams need to rapidly detect, analyze, and respond to cybersecurity threats and attacks. Unfortunately, legacy SOC tools and slow, manual workflows lead to lengthy investigation and response times. Learn how Sumo Logic automatically detects and correlates real-time threats and incidents across your on-prem, cloud, and hybrid data sources.

This session will also:

- Demonstrate the benefits of Sumo Logic Cloud SIEM
- Experience a day in the life of a SOC analyst using Sumo Logic

Activity descriptions *continued*

Booth presentations [Booth 5463](#)

How to automate your cybersecurity initiatives using Cloud SOAR

Presenter: Enrico Benzoni, Marketing & Technical Alliance Manager, Orchestration & Automation, Sumo Logic

Enterprise security teams face several challenges that impede efforts to modernize their security operations. Sumo Logic's Cloud Security Orchestration Automation Response (SOAR) solution augments and empowers modern SOC tools, technologies, and teams by offering automated real-time incident management, threat, and response capabilities. In this session, you will learn:

- Why use a SOAR
- Benefits of a modern SOAR
- Walkthrough of our Cloud SOAR

Introduction to Sumo Logic Threat Labs

Presenter: Paul Tobia, Sr. Product Manager, Sumo Logic

Come learn about the team at Sumo Logic who safeguard Sumo customer organizations from emerging threats, inject security DNA throughout Sumo Logic, and contribute to the broader security community. Our Threat Labs team is monitoring threat activity to produce and distribute actionable intelligence, detection content, and timely guidance. We'll also highlight some of our latest blogs and research.

MITRE the corners of your ATT&CK surface

Presenter: Paul Tobia, Sr. Product Manager, Sumo Logic

MITRE ATT&CK is a great framework for categorization of attack tactics, techniques, and processes. In this session we'll talk a little about the evolution of ATT&CK and offer tips for molding the framework to practical use in your regular security operations.

Improving cyber defense with crowdsourced global intelligence and Cloud SIEM

Presenter: David Andrzejewski, Director of Engineering, Sumo Logic

You're not a data scientist? Want to learn how 'non-experts' can leverage and benefit from using machine learning (ML) for security use cases? Join this session to find out how Sumo Logic can help you solve the data challenge by pooling, or crowdsourcing, across our customer base to help address current and emerging threats.

State of software insecurity, presented by eSentire

Presenters: Tia Hopkins, Field CTO & Chief Cyber Risk Strategist, eSentire
Dana Torgersen, Director of Product Marketing, Security, Sumo Logic

Insights from software supply chain threat intel research, observed attacks in customer environments, dissections of threat detection and response investigations driven by Threat Research and key recommendations.

Moving the SOC needle: from reactive triage to a data-driven scientific approach

Presenters: Yaron Levi, CISO, Dolby Laboratories
Dave Frampton, VP/GM Cloud SIEM & Security Analytics, Sumo Logic

For many, an effective SOC feels like magic and great analysts as sorcerers but in fact moving the SOC needle requires science not magic. Catch this special session to learn more from Yaron Levi, CISO for Dolby Laboratories and Dave Frampton, VP/GM for Sumo Logic's Cloud SIEM and Security Analytics.

Threat detection, faster investigation, and automated response for modern SOCs, with VMware and Sumo Logic

Presenters: Kendra Kendall, Technical Marketing Manager, VMware Carbon Black BU
Drew Horn, Sr. Director, Technology Alliances, Sumo Logic

The most sought-after capabilities to fend off attackers in a modern SOC are high-fidelity alerts, endpoint telemetry, attack technique insights, and coordinated containment across multiple domains. This session showcases VMware Carbon Black and Sumo Logic's new suite of integrations for EDR, SIEM, and SOAR to enhance threat detection, accelerate investigations, and reduce response times with holistic threat visibility, automated correlation and remediation.

Activity descriptions *continued*

Booth presentations [Booth 5463](#)

Actionable security insights with Zscaler and Sumo Logic

Presenters: Rahim Ibrahim, Business Development & Technology Alliances Manager, Zscaler
Jason Dunne, Product Marketing Manager, Sumo Logic

Zscaler and Sumo Logic have partnered to integrate rich web, social, and mobile user and security event data to provide actionable, single views across all elements in an environment. Zscaler provides security and policy enforcement through the Zero Trust Exchange while Sumo Logic provides analytics and visibility—all delivered 100% in the cloud. Join this session to learn how to automatically discover useful security information embedded in your data across heterogeneous environments.

Security workshops [Booth 5463](#)

Mini workshop: Security analytics for all your alerts

Presenters: John Merideth, Technical Trainer, Sumo Logic
Stacy Kornluebke, Director of Education and Digital Nurture, Sumo Logic

Monitor for malicious activities with Sumo Logic's threat intelligence dashboards and queries. Engage in hands-on labs using advanced operators and features that can rapidly assist you in threat investigation.

Mini workshop: Cloud SIEM Insights

Presenters: John Merideth, Technical Trainer, Sumo Logic
Stacy Kornluebke, Director of Education and Digital Nurture, Sumo Logic

Monitor your systems and investigate threats through Sumo Logic's out-of-the-box Insights. Engage in hands-on labs in our Cloud SIEM environment and triage issues in real-time.

Mini workshop: Automating responses with Cloud SOAR

Presenters: John Merideth, Technical Trainer, Sumo Logic
Stacy Kornluebke, Director of Education and Digital Nurture, Sumo Logic

Harness the power of playbooks to increase your security readiness and decrease response times for your team. Engage in hands-on labs in our Cloud SOAR environment.



sumo logic