Sumo Logic Introduces Threat Labs Unit for Advanced Detection and Expanded Security Community Contribution

June 7, 2022

Establishes Sumo Logic Threat Labs Unit to deliver accelerated detection for modern threats at cloud scale

SAN FRANCISCO, June 07, 2022 (GLOBE NEWSWIRE) -- **RSA Conference –** Sumo Logic (NASDAQ: SUMO), the SaaS analytics platform to enable reliable and secure cloud-native applications, today unveiled Sumo Logic Threat Labs, a threat research and security detection unit. The Threat Labs unit is among the expanded services and tools from Sumo Logic to help customers modernize security operations and achieve greater cyber-resilience. Sumo Logic will showcase the functionality of its security intelligence solutions from Booth #5463 at the RSA Conference 2022 this week in San Francisco.

Threat Labs

Sumo Logic Introduces Threat Labs Unit for Advanced Detection and Expanded Security Community Contribution

The Sumo Logic Threat Labs Unit is built to deliver a continuous stream of deep detection content, rapid response guidance, and actionable best practices to Sumo Logic security customers. The team is staffed with domain experts with backgrounds in forensics, incident response, and red/blue teaming, as well as offensive and defensive cyber operations in the United States military and intelligence services. Informed by deep human expertise, the Threat Labs Unit will also play a larger role in contributing advanced detection logic and best practices to the security community to help collectivize the defense.

Dave Frampton, VP/GM, Sumo Logic Security Business Unit:
"Our Threat Labs Unit will contribute actionable insights to our customers from leading-edge threat research, we will also share insight with the community to improve the industry's collective defense. Our deep and diverse practitioner expertise translates into advanced detection coverage delivered in a unique SaaS model which combines real-time global updates with deployment customization for individual customers."

Translating Threat Research into Proactive Defense
Modern threat surfaces also encompass application security at every layer of the stack. Customers need end-to-end workflows coordinated across detection, investigation and response efforts. Threat Labs insights are delivered across the Sumo Logic security portfolio, ranging from detection and investigation in Cloud SIEM to automated threat response in Cloud SOAR. In its SaaS delivery platform, Sumo Logic updates detection content for all customers at least twice weekly, to shorten the cycle time from research to concrete defense adaption in environments where every minute counts.

Sumo Logic Threat Labs in Action
As first reported in the media in April, the very first malware exploiting serverless computing was found in the wild creating crypto-miner instances in AWS Lambda. Called Denonia, this cutting-edge malware requires a holistic approach to detection, investigation, and response. The Threat Labs Unit performed research and detection engineering on the Sumo Logic platform. The team then generated content for detection in Cloud SIEM, delivered analysis and hunting across the platform, and orchestrated the response in Cloud SOAR all in one workflow.

Learn about the latest contributions from the Sumo Logic Threat Labs Unit:

- Learn about Denonia: Security in a Serverless World
- Contribution from Threat Labs for Customers: Log4Shell CVE-2021-44228
- Contribution from Threat Labs for the Community: Mind your Single Sign-On (SSO) logs
- Proactive Contribution for the Community: Weaponizing paranoia: developing a threat detection strategy
- Report with eSentire: Strengthening the Detection of Software Supply Chain Attacks

About Sumo Logic
Sumo Logic, Inc. (NASDAQ: SUMO) empowers the people who power modern, digital business. Through its SaaS analytics platform, Sumo Logic enables customers to deliver reliable and secure cloud-native applications. The Sumo Logic Continuous Intelligence Platform™ helps practitioners and developers ensure application reliability, secure and protect against modern security threats, and gain insights into their cloud infrastructures. Customers around the world rely on Sumo Logic to get powerful real-time analytics and insights across observability and security solutions for their cloud-native applications. For more information, visit www.sumologic.com.

Media Contact
Carmen Harris, Sumo Logic

charris@sumologic.com
(469) 534-3069

Jenna Shikoff
RH Strategic
SumoLogicPR@RHStrategic.com
(267) 300-7190

A photo accompanying this announcement is available at https://www.globenewswire.com/NewsRoom/AttachmentNg/9d6c55f8-3c74-4166-b2c6-4a7fd91be42a