Recorded Future and Sumo Logic

PRODUCT OVERVIEW

Sumo Logic provides best-in-class cloud monitoring, log management, Cloud SIEM tools, and real-time insights for web and SaaS-based apps. The Sumo Logic platform helps analysts make data-driven decisions and reduce the time to investigate security and operational issues so you can free up resources for more important activities. Sumo Logic collects and centralizes more than 150 applications and integrations make it easy to aggregate data across your stack and down your pipeline. Searches and investigations use real-time analytics to help analysts rapidly identify and resolve potential cyber-attacks, detect and prevent breaches, and reduce compliance costs.

JOINT INTEGRATION DESCRIPTION

Recorded Future for Sumo Logic allows organizations to quickly resolve security threats using external threat intelligence and rich context from Recorded Future directly on top of Sumo Logic's Cloud SIEM Enterprise (CSE) and Continuous Intelligence Platform (CIP).

CSE provides security analysts with enhanced visibility to seamlessly monitor their on-premises, hybrid, and multi-cloud infrastructures and thoroughly understand the impact and context of an attack. CSE parses, maps, and creates normalized records upon ingestion from your structured and unstructured data, giving analysts full access to rapidly drill down into a record during threat investigations without needing to learn a query language.

Now with Recorded Future for CSE, analysts are able to view related external risk and evidence assigned to IPs, Domains, Hashes, and URLs on CSE Insights for greater context as they investigate and respond to incidents. Full transparency is provided on the evidence applicable to any given IOC (indicator of compromise).

In addition to an integration with CSE, Recorded Future's data is brought directly integrated into CIP, to correlate internal telemetry data against high fidelity datasets from Recorded Future to detect threats faster. The integration makes use of the Recorded Future IP, Domain, Hash, URL, and CVE risk lists. As a result, security and threat analysts can make quick and effective decisions at critical moments.

CHALLENGES OVERCOME THROUGH INTEGRATION

Security operations center (SOC) teams are inundated with alerts and events. By joining forces through seamless integration, security event management from Sumo Logic and security intelligence from Recorded Future helps analysts reduce manual research time and make informed verdicts. SOC analysts can efficiently dismiss false positives and capture threat context for true incidents.

The joint solution enables analysts to instantly integrate prioritized and actionable threat intelligence with your existing security controls inside CSE and CIP.

USE CASES

The integration between Sumo Logic's CSE and CIP and Recorded Future allows security responders to:

- Detect and gain context on CSE Insights with real-time external intelligence to identify true incidents and dismiss false positives
- Proactively block threats before they impact the business using the Recorded Future risk lists in CIP
- Reduce time for threat detection, remediation, and response

BENEFITS:

- Detect and gain context on CSE Insights with real-time external intelligence to identify true incidents and dismiss false positives
- Proactively block threats before they impact the business using the Recorded Future risk lists in CIP
- Reduce time for threat detection, remediation, and response
### About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.

© Recorded Future, Inc. All rights reserved. All trademarks remain property of their respective owners.

---

### About Sumo Logic

We’re putting the power of machine data analytics in the hands of everyone by unifying all data types, enabling universal access, and leveraging cloud economics—all from a single, cloud-native, continuous intelligence platform delivered and consumed as a true SaaS.