Solution brief

sumo logic

Sumo Logic Threat Intelligence

Visibility into the threats that matter most to you

Migrating to the cloud doesn't mean compromising visibility or losing sight of adversaries targeting your organization. With Sumo Logic Threat Intelligence, you can take back control. This solution provides real-time security intelligence to counter sophisticated attacks from cybercriminals, corporate spies, spammers, nation-states, and hacktivists alike.

You've invested heavily in your security infrastructure to prevent, detect, and respond to cyber threats. Yet, it can feel like you're constantly fighting fires and struggling to understand your cybersecurity posture clearly.

You need a way to:

- Be more proactive and effective.
- Gain strategic insights into your defenses.
- Enhance your capabilities without disrupting your current

Sumo Logic's Threat Intelligence delivers precisely what you need—actionable intelligence at the right time and in the right format—to stop breaches before they occur. This capability, included with Sumo Logic Cloud SIEM and the Sumo Logic Log Analytics Platform at no extra cost, empowers your security team by matching Indicators of Compromise (IOCs) like IP addresses, domain names, URLs, email addresses, and MD5 hashes.

Sumo Logic Threat Intelligence key capabilities

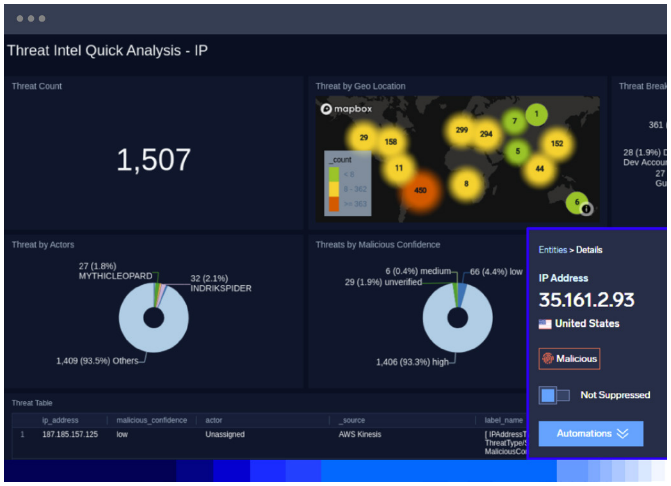
Feature	Customer benefits
Diverse feed support	Supports ingestion from STIX/TAXII (1.1, 2.0, 2.1), MISP, OpenIOC, and proprietary formats.
Advanced data filtering	Enables attribute-based filtering during ingestion, such as confidence levels or indicator types.
Cross-platform integration	Unified access to threat intelligence via a centralized data store.
Scalable indicator storage	It supports up to five million indicators per organization and can be increased to ten million, with configurable retention policies for expired indicators.
Real-time enrichment	Automatically normalizes and enriches logs and alerts with metadata from multiple threat intelligence sources.
Custom rule operators	Provides operators like threatlookup and hasThreatMatch for fine-grained, rule-based detection leveraging threat attributes.

Benefits of Sumo Logic Threat Intelligence

1. **Supercharge your threat defenses**
   Integrate real-time threat intelligence directly into your enterprise systems. Enhance the speed and accuracy of your threat detection capabilities to stay ahead of adversaries.

2. **Be informed, not overwhelmed**
   Gain real-time visualizations of IOCs in your environment, which are searchable through an intuitive web interface. Simplify the flood of information into actionable insights.

3. **Achieve proactive security**
   Understand which adversaries may target your organization through strategic, operational, and technical reporting. Leverage timely alerts to strengthen your defenses.



	ip_address	malicious_confidence	actor	_source	label_name
1	187.185.157.125	low	Unassigned	AWS Kinesis	[IPAddressT ThreatType/ MaliciousCo

About Sumo Logic

Sumo Logic, Inc. unifies and analyzes enterprise data, translating it into actionable insights through one AI-powered cloud-native log analytics platform. This single source of truth enables Dev, Sec and Ops teams to simplify complexity, collaborate efficiently and accelerate data-driven decisions that drive business value. More than 2,400 customers around the world rely on the Sumo Logic SaaS Log Analytics Platform for trusted insights to ensure application reliability, secure and protect against modern security threats, and gain insights into their cloud infrastructures.

For more information, visit www.sumologic.com.

Toll-Free: 1.855.LOG.SUMO | **Int'l:** 1.650.810.8700
855 Main Street, Redwood City, CA 94603

www.sumologic.com