



Event Log Analytics

Actionable Insights Without Information Overload

From Logs to Intelligence — See, Correlate, and Act in Real Time

Redefining Security Visibility Through Intelligence and Automation

In today's hyper-connected threat landscape, reactive monitoring is no longer enough. Underscore's Event Log Analytics is an advanced, AI-driven Security Information and Event Management solution that transforms disparate, unstructured log data into actionable intelligence — enabling faster detection, profound analysis, and automated response actions.

Underscore Event Log Analytics empowers security teams to see, correlate, and act on events in real time, combining the scalability of traditional log management with the intelligence of modern analytics. It's designed for organisations that demand clarity without complexity, offering high-speed data ingestion, automated event correlation, and AI-enhanced threat detection — now extended with automated threat intelligence exchange, policy-based message routing, and a fully customizable alerting engine.

The solution comes optionally bundled with a Network Time Protocol (NTP) appliance, which is perfectly suited for air gapped or isolated environment running in separate silos.

Benefits

- **Meet Regulatory Requirements**
Comply with laws-of-the-land or regulatory mandates pertaining to tamper-resistant retention and retrieval
- **Automate Intelligence Sharing**
Enhance effectiveness of security solutions by eliminating interoperability complexities
- **Support Legacy Devices & Applications**
Fetch event data when no native forwarding capability exists. Support multi-protocol event receiving mechanisms
- **Transforms Data Feeds**
Make sense of unstructured data, apply transformation logic and, improve quality of outcome for downstream peers
- **Data Masking**
Hide sensitive data while preserving data format and type

Core Capabilities

Unified Data Ingestion

- Collects logs from applications, network devices, endpoints, cloud, and IoT.
- Supports both agent-based and agentless data collection.
- Normalizes multi-format data into a unified schema for consistency.
- Broad protocol support out of the box — Syslog (TCP/UDP/AMQP/Kafka), GELF, NetFlow, SNMP, AWS CloudTrail & Flow Logs, JSON over HTTP, and firewall/VPN/IPS event feeds.

Intelligent Correlation & Analytics

- Real-time event correlation across multiple sources to detect hidden patterns.
- AI engine helps simplify inferences.
- Improved stream-aware modelling techniques for predictive analytics.

Detect Threat & Future Risks

- Built-in Models detect anomalies, threats, and advanced attacker behavior.
- Heuristic profiling automatically baselines user and system activity.
- Uses Threat Intelligence feeds to enrich detections with context and relevance.
- Text-free live search across streaming logs delivers instant visibility with no predefined queries required.

Secure, Compliant Data Retention

- Supports tamper-proof storage and regulatory compliance for log retention.
- Immutable, write-once-read-many (WORM) storage prevents modification or deletion of stored logs.
- Built-in compression (50–90%) reduces storage cost and bandwidth, with faster retrieval for downstream tools.
- Replication across DC and DR ensures high availability and continuity.
- ELA logs its own operational activity, providing a complete internal audit trail for the logging platform itself.
- Aligned with CERT-In log-retention and clock-synchronization directives (IT Act 2000, Section 70B) alongside ISO 27001, NIST, and GDPR.

Scalable Architecture

- Handles up to 500,000 Events Per Second (EPS) with distributed architecture.
- Storage-centric scaling model — capacity grows with storage, not EPS, enabling true horizontal and vertical scale without artificial limits.
- High Availability (HA) and Disaster Recovery (DR) ready.
- Flexible deployment — on-premises, cloud, or hybrid environments.

Policy-Based Message Routing

- Routes specific events to the right destination — SIEM, compliance archive, backup, or specialized analysis tools — based on custom rules.
- Optimizes infrastructure by directing data only where it’s needed.
- Reduces downstream tool load and cost by pre-filtering at the source.

Threat Information Exchange

- Automatically shares malicious and suspicious Indicators of Compromise (IOCs) across connected security tools.
- Pushes IOCs to firewalls, endpoints, and network devices for immediate blocking and containment.
- Notifies security teams automatically, accelerating coordinated response to emerging threats.

Advanced Alert System

- Custom, rule-based alerting tailored to organization-specific security and compliance requirements.
- Complex rule logic — pattern matching, threshold-based triggers, and multi-source correlation — adapts to evolving threats.
- Multi-channel delivery via Email, SMS, Webhook, and SIEM ensures alerts reach the right team, every time.

Key Advantages

Feature	Value Delivered
AI-Augmented Analysis	Detects emerging threats and behavioral anomalies automatically.
Real-Time Correlation	Links related events across sources to uncover attack chains.
Compliance Ready	Aligns with ISO 27001, NIST, CERT-In, and GDPR mandates.
Lower TCO	Simple GB/day licensing model reduces operational overhead.
Cloud & Edge Flexibility	Deploy across hybrid workloads securely.
Actionable Insights	Converts raw data into contextual intelligence for decisive response.
Automated Threat Exchange	Shares IOCs across firewalls, endpoints, and security tools without manual effort.
Policy-Based Routing	Delivers the right data to the right destination automatically, cutting noise and cost.
Massive Scale	Handles up to 500,000 events per second with storage-centric, near-unlimited growth.

About Underscore:

Contact Us: