LOGZILLA DOCUMENTATION

Secops

LogZilla App Store application: Secops

LogZilla App Store · Generated April 27, 2026 · logzilla.ai/docs/logzilla-appstore/secops

Overview

SecOps provides unified security monitoring across all log sources. Security events from firewalls, IDS/IPS, endpoint protection, and other security tools are aggregated into a single dashboard with consistent threat levels.

App Function

- Aggregate security events from installed vendor apps
- Provide unified dashboard for cross-vendor security visibility
- Assign threat levels based on Event Type
- Alert on security threats and anomalies

Vendor Documentation

This is a LogZilla aggregate app. No external vendor documentation applies.

Device Configuration

No device configuration is required. SecOps automatically processes events from any app that sets `Event Class` containing `Security`.

Incoming Log Format

SecOps processes events tagged by vendor apps. It does not parse raw log formats directly. Vendor apps set:

- `Event Type`: Threat, Policy Violation, Access Control, Web Security
- `MitreId`, `MITRE Tactic` for threat context
- `SrcIP`, `DstIP` for network context

Parsed Metadata Fields

Tag Name	Example	Description
`SecOps Event`	`1`	Rollup tag for security events

Tag Name	Example	Description
`SecOps Threat Level`	`Critical`	Aggregated threat level based on Event Type

Threat Level Assignment

Level	Condition
Critical	Threat (IDS/IPS alerts, attacks, malware)
High	Policy Violation, Access Control
Medium	Web Security, other security events

Log Examples

IDS Alert

```
snort[5678]: [1:2001219:20] ET SCAN Potential SSH Scan
```

Firewall Block

```
%ASA-4-106023: Deny tcp src outside:192.168.1.100/12345 dst inside:10.0.0.1/22
```

Policy Violation

```
%ASA-4-733100: Drop rate-1 exceeded. Current burst rate is 100 per second
```

Dashboard

The SecOps dashboard provides:

- Key metrics: Total events, threats, policy violations, access control
- Unique hosts and source IPs counts

- EPS gauge and time chart for rate monitoring
- Event Type distribution over time
- Top source IPs, destination IPs, and hosts
- Threat level distribution and MITRE techniques
- Live event stream with security context

Triggers

Trigger	Description
`SecOps: Active Threat`	IDS/IPS alert or attack detected
`SecOps: Policy Violation`	Security policy breach
`SecOps: Access Control`	ACL permit/deny decision
`SecOps: Web Security`	WAF or web security event