LOGZILLA DOCUMENTATION

Complianceops

LogZilla App Store application: Complianceops

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

Overview

ComplianceOps provides unified compliance monitoring across all log sources. Events tagged with compliance frameworks (PCI-DSS, HIPAA, SOX, GDPR, etc.) from firewalls, identity systems, and applications are aggregated into a single dashboard for audit readiness.

App Function

- Aggregate events with Compliance Framework tags from installed vendor apps
- Provide unified dashboard for cross-vendor compliance visibility
- Assign severity levels based on Event Type (Threat, Privilege Escalation, etc.)
- Alert on high-priority compliance events

Vendor Documentation

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

Device Configuration

No device configuration is required. ComplianceOps automatically processes events from installed vendor apps that call `apply_compliance_frameworks()`.

Incoming Log Format

ComplianceOps processes events tagged by vendor apps. It does not parse raw log formats directly. Vendor apps set the `Compliance Framework` tag when they call `TAXONOMY.apply_compliance_frameworks(event, event_type)`.

Parsed Metadata Fields

Tag Name	Example	Description
`ComplianceOps Event`	`1`	Rollup tag for compliance-relevant events

Tag Name	Example	Description
`ComplianceOps Severity Level`	`High`	Aggregated severity based on Event Type

Severity Level Assignment

Severity	Event Types
Critical	Threat, Policy Violation
High	Privilege Escalation, Access Control, Failed Authentication
Medium	Configuration, Account Management
Low	Session (successful), Service

Log Examples

Privilege Escalation (sudo)

```
sudo: admin : TTY=pts/0 ; PWD=/home/admin ; USER=root ; COMMAND=/bin/bash
```

Failed Authentication

```
sshd[5678]: Failed password for admin from 192.168.1.100 port 22 ssh2
```

Successful Login

```
sshd[5678]: Accepted publickey for admin from 192.168.1.100 port 22
```

Dashboard

The ComplianceOps dashboard provides:

- Key metrics: Total events, unique frameworks, hosts, users
- Failed authentication and privilege escalation counts
- EPS gauge and time chart for rate monitoring
- Top compliance frameworks distribution
- Event Type and severity distribution
- Top hosts, users, and vendors
- Live event stream with compliance context

Triggers

Trigger	Description
`ComplianceOps: Security Threat`	Threat or policy violation detected
`ComplianceOps: Failed Authentication`	Authentication failure in compliance context
`ComplianceOps: Privilege Escalation`	Sudo/su/dzdo privilege escalation
`ComplianceOps: Account Management`	User/group account changes
`ComplianceOps: Configuration Change`	Configuration modifications
`ComplianceOps: PCI-DSS Event`	Event relevant to PCI-DSS compliance
`ComplianceOps: HIPAA Event`	Event relevant to HIPAA compliance
`ComplianceOps: SOX Event`	Event relevant to SOX compliance
`ComplianceOps: GDPR Event`	Event relevant to GDPR compliance