LOGZILLA DOCUMENTATION

Authops

LogZilla App Store application: Authops

LogZilla App Store · Generated April 29, 2026 · logzilla.ai/docs/logzilla-appstore/authops

Overview

AuthOps provides unified authentication monitoring across all log sources. Authentication events from Cisco, Palo Alto, Linux, Windows, and other vendors are aggregated into a single dashboard with consistent severity levels.

App Function

- Aggregate authentication events from installed vendor apps
- Provide unified dashboard for cross-vendor authentication visibility
- Assign severity levels based on Event Type and Auth Success
- Alert on authentication anomalies and security events

Vendor Documentation

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

Device Configuration

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

Incoming Log Format

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

- `Event Type`: Session, Privilege Escalation, Account Management
- `Auth Success`: true/false for login success/failure

Parsed Metadata Fields

Tag Name	Example	Description
`AuthOps Event`	`1`	Rollup tag for authentication events

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

Severity Level Assignment

Severity	Condition
Critical	Privilege Escalation, Account Management
High	Failed Authentication (Auth Success: false)
Medium	Session without auth status
Low	Successful Authentication (Auth Success: true)

Log Examples

SSH Login Success

```
sshd[1234]: Accepted publickey for admin from 192.168.1.100 port 22
```

SSH Login Failure

```
sshd[5678]: Failed password for invalid user root from 10.0.0.1 port 22
```

Privilege Escalation

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

Dashboard

The AuthOps dashboard provides:

- Key metrics: Total events, failed auth, privilege escalation, account mgmt
- Unique users and hosts counts
- EPS gauge and time chart for rate monitoring
- Event Type distribution over time
- Top users, hosts, and source IPs
- Severity distribution and MITRE techniques
- Live event stream with auth context

Triggers

Trigger	Description
`AuthOps: Privilege Escalation`	Sudo/su/dzdo privilege escalation
`AuthOps: Account Management`	User/group account changes
`AuthOps: Failed Authentication`	Authentication failure detected
`AuthOps: Session Event`	Session start/end events