LOGZILLA DOCUMENTATION

Otops

LogZilla App Store application: Otops

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

Overview

OTOps provides unified Operational Technology and ICS monitoring across all log sources. Events from SCADA systems, PLCs, DCS controllers, and HMIs are aggregated into a single dashboard with consistent severity levels.

App Function

- Aggregate OT/ICS events from installed vendor apps
- Provide unified dashboard for cross-vendor OT visibility
- Assign severity levels based on Event Type
- Alert on safety events and security threats

Vendor Documentation

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

Device Configuration

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

Incoming Log Format

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

- `Event Type`: Safety, Alarm, Process Control, Maintenance, Threat

Parsed Metadata Fields

Tag Name	Example	Description
`OTOps Event`	`1`	Rollup tag for OT/ICS events
`OTOps Severity Level`	`Critical`	Aggregated severity based on Event Type

Severity Level Assignment

Severity	Condition
Critical	Safety interlocks, Security threats
High	Process alarms, Control changes
Medium	Maintenance, Configuration

Log Examples

Safety Interlock

```
safety-plc: Safety interlock triggered on reactor-01, emergency shutdown
```

Process Alarm

```
scada: High temperature alarm on heat-exchanger-03, value=185C threshold=180C
```

Unauthorized Access

```
ot-security: Unauthorized Modbus write to PLC-001 from 192.168.100.50
```

Dashboard

The OTOps dashboard provides:

- Key metrics: Total events, safety, alarms, process control
- Unique devices and controllers
- EPS gauge and time chart for rate monitoring
- Event Type distribution over time
- Top devices, vendors, and programs
- Severity distribution

- Live event stream with OT context

Triggers

Trigger	Description
`OTOps: Safety Event`	Safety interlock or shutdown
`OTOps: Security Threat`	Unauthorized access or attack
`OTOps: Alarm`	Process alarm triggered
`OTOps: Process Control`	Setpoint or control change
`OTOps: Maintenance`	Maintenance mode activity