JioCloud

DATA SHEET

JioCloud SIEM

See every threat. Respond before it costs you.

JioCloud Security Information and Event Management (SIEM) solution gives security teams the visibility and speed needed to stay ahead of modern threats. It aggregates and correlates log data in real time across your entire IT and cloud environment - from endpoints and servers to network infrastructure and applications - surfacing security alerts before they escalate into incidents.

Built and hosted entirely on Indian infrastructure, JioCloud ensures complete data residency in line with the DPDP Act and India's regulatory requirements, so you never trade compliance for capability.

COLLECT	DETECT	CORRELATE	RESPOND

NEXT-GEN SIEM **SOAR**

CloudXP SIEM — from raw logs to automated response, on a single platform.

Key Features

Event Correlation
Connects the dots across security events and logs from every source, spotting the patterns and sequences that signal an active threat - turning raw noise into clear, actionable intelligence.

Real-Time Threat Detection
Start with pre-configured detection rules out of the box, or build custom detectors tailored to your environment. Every connected technology is monitored continuously, so threats are surfaced the moment they emerge.

Anomaly Detection
Applies machine learning to security event data, automatically surfacing anomalies and behavioural deviations that rule-based detection alone may miss.

SOAR
Security Orchestration, Automation and Response automates remediation workflows in response to detected threats, reducing mean time to respond and freeing analysts from manual containment tasks.

Threat Intelligence Platform
Upload IOC sources in STIX2 format and match them against selected log fields in real time - any match automatically triggers an alert.

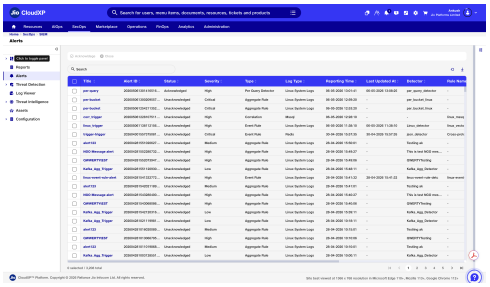
Alerts and Notifications
Auto-alert mechanisms flag potential security threats and send notifications based on alert severity and category.

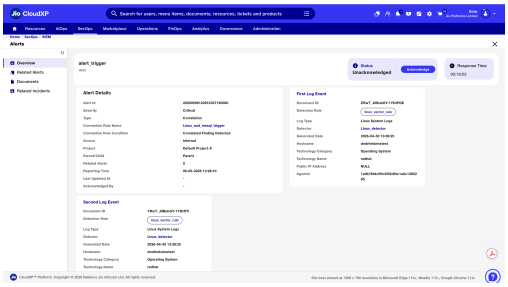
Dashboards & Reports
Interactive dashboards surface key security metrics, events, and insights, alongside standard reports that can be generated on demand or scheduled for compliance audits and executive reporting.

Log Viewer
A built-in log viewer with both raw and parsed views lets users inspect ingested log data directly, without ever leaving the platform.

Custom Parsers
Extend SIEM coverage beyond the out-of-the-box catalog. Define custom log types with Grok-based parsers for any source - proprietary applications on agents, network devices via syslog, or containerised applications on Kubernetes with namespace-level collection scoping.

Data Residency & Regulatory Compliance
Log data is stored exclusively on Indian cloud infrastructure, ensuring complete in-country residency - aligned with the DPDP Act, CERT-In's 180-day retention directive, and sector mandates from RBI, SEBI, and IRDAI.





© 2024 Reliance Jio Platforms Limited. All rights reserved. JPL.CloudSales@ril.com I jio.com/enterprisecloud

JioCloud

Benefits

Real-Time Detection & Automation
Catch malicious activity as it happens and automate routine tasks, freeing analysts to focus on what matters.

Business Continuity
Detect and respond faster to minimize downtime and keep your business running.

Data & IP Protection
Monitor access to critical systems to safeguard sensitive data and intellectual property.

Regulatory Compliance
Get the visibility and audit trails your compliance teams need to meet evolving regulations.

Insider Threat Mitigation
Detect and contain insider threats before they escalate.

Complete Data Residency
Keep security data within India at all times, aligned with the DPDP Act.

Supported Technologies

Operating System: Windows, Linux

App Management & Containers: Kubernetes (Audit logs), Kubernetes (Container logs), Kong Gateway

Network: WAF, Cisco ASA, Cisco FTD, Palo Alto

Security: TrendMicro Deep Security (Anti-Malware

Identity & Access: Okta, Microsoft Entra ID (Azure AD), Ping Identity, ADFS

Databases: MSSQL, MySQL, Postgres, MongoDB, Redis

Cloud: Azure Event Hub

Any Technology · Custom Parsers
Not on the list above? Use Custom Parsers to define your own log format - map raw fields to a structured schema and immediately unlock detection, correlation, alerting, and reporting for that source. Collection via agent log file paths, Windows Event Channels, and syslog forwarding (coming soon).

Capabilities at a glance

A side-by-side comparison of JioCloud SIEM against traditional, fragmented security tooling.
All capabilities listed are included in JioCloud SIEM.

Category	Capability	Traditional / Fragmented Tools	JioCloud SIEM
Detection & Correlation	Event Correlation	Manual cross-referencing across siloed tools	Automated correlation across all log sources, in real time
	Anomaly Detection	Rule-based alerts only	ML-powered detection of deviations rules alone would miss
	Threat Intelligence	Manual IOC lookups	STIX2 feed ingestion with automatic real-time matching
Response & Automation	Incident Response	Manual, ticket-driven workflows	Built-in SOAR with automated remediation playbooks
	Alerting	Basic, email-only notifications	Severity- and category-based multi-channel alerts
Visibility & Reporting	Log Management	Separate log management platform required	Integrated log viewer (raw + parsed) in the same platform
	Dashboards & Reporting	Manual exports, static reports	Interactive dashboards, on-demand or scheduled reports
Integration Coverage	Technology Support	Limited, siloed integrations per tool	25+ technologies natively: network, identity, cloud, EDR, databases
	Custom Sources	Requires vendor development	Self-service Custom Parsers with Grok-based field mapping
Compliance & Residency	Data Residency	Often hosted outside India	100% Indian infrastructure, DPDP Act aligned
	Regulatory Alignment	Manual compliance mapping	Built-in alignment with CERT-In, RBI, SEBI, IRDAI mandates

** Comparison is representative. Feature availability may vary by deployment model and configuration.*

© 2024 Reliance Jio Platforms Limited. All rights reserved. JPL.CloudSales@ril.com I jio.com/enterprisecloud