EKSELENS · ERIO PROGRAMME

ERIO × Your SOC — stream decision intelligence into the panel analysts already live in

ERIO's risk rescores, new signal hits and executive decisions stream into Splunk, Microsoft Sentinel, IBM QRadar and LogRhythm / Elastic out of the box — in CEF, LEEF or native Splunk JSON. One connector; four CISO-visible logos; zero new consoles for your team to learn.

Event stream reaching your SIEM

- **risk_score_change** — material delta crossings on supplier / entity / control risks, with before, after and magnitude.
- **signal_ingested** — new sanctions, cyber, ESG or financial-distress hits attached to a subject.
- **decision_recorded** — Owner / Executive sign-offs and overrides, with actor + outcome fields.
- **automation_paused** — tenant kill-switch + automation guardrail state changes (for compliance evidence).

One use-case per SOC

SPLUNK

"Supplier failure-risk heatmap by business unit"

```
sourcetype=erio:risk event="risk_score_change"
| stats max(score_after) avg(delta) by risk_title
| where max(score_after) >= 0.7
```

MICROSOFT SENTINEL

"Alert when a sanctioned UBO appears"

```
ERIORiskSignal_CL
| where event_s == "signal_ingested"
| where source_s == "sayari" or source_s == "sanctions"
| where magnitude_s == "major"
```

IBM QRADAR

"Executive-override timeline for audit"

```
SELECT UTF8(payload) AS event, devTime
FROM events
WHERE LOGSOURCETYPENAME(devicetype)='ERIO'
  AND name='decision_recorded'
LIMIT LAST 90 DAYS
```

LOGRHYTHM / ELASTIC

"DORA — material ICT-service risk uplifts"

```
event.dataset:"erio.risk"
AND event.action:"risk_score_change"
AND erio.delta:>=2.0
AND erio.direction:"up"
```

Transports & wire format

- **Splunk HEC** — JSON event body, `Authorization: Splunk <token>`.
- **Microsoft Sentinel** — Azure Log Analytics HTTP Data Collector API (no AAD app needed).
- **Generic HTTPS CEF / LEEF** — fits QRadar HTTPS Receiver, LogRhythm Open Collector, Securonix & Elastic.
- CEF per the ArcSight dictionary, LEEF 2.0 spec-compliant with explicit tab-delimiter declaration.

Governance & safety

- Tenant kill-switch pauses every outbound stream in one click.
- Per-exporter mock mode so analysts can demo dashboards before a licence key lands.
- Delivery stats (sent, failed, last status) recorded for every event — audit-ready by default.
- Self-test endpoint fires a synthetic event without leaking into production alerting.