

02 · ELIMINATE — INTELLIGENT EVENT MONITORING

Detection Without Context Is Just Noise

Critical infrastructure environments generate enormous volumes of events across OT and IT devices alike. Without the knowledge to interpret them, every alert looks the same. Intelligent Event Monitoring (IEM) transforms raw device output into actionable intelligence — with built-in remediation guidance specific to the device, the vendor, and the event.

THE CHALLENGE

Event Monitoring Is Broken

Most environments cannot tell a critical event from background noise.

- Generic SIEM and log management tools apply generic correlation rules to device output — producing alerts with no operational context.
- Security teams receive notifications but lack the vendor-specific knowledge to assess severity or determine next steps.
- Operations teams are excluded from the detection loop — they only hear about events after the damage is done.
- No path from alert to remediation exists within a single platform — response requires jumping between disconnected tools.

**An alert without context is not intelligence.
It is a task with no instructions attached.**

THE SOLUTION

Event Intelligence Built for the Devices in Your Environment

ConsoleWorks Intelligent Event Monitoring (IEM) is not a passive log collector. IEM modules are vendor-specific knowledge libraries — built to understand the output of the exact devices deployed in your environment. Where generic tools see raw text, IEM sees a firmware login attempt on a Schweitzer relay, an unexpected configuration write on a Rockwell PLC, or a communication path change on a GE turbine controller. The same depth of intelligence applies across IT devices in your environment — servers, workstations, and network infrastructure included. The difference is not detection. It is understanding.

Each IEM module maps device output to a defined event taxonomy, applies severity context appropriate to the device type and operational role, and surfaces the result with remediation guidance — already embedded. Operators do not need to research what an event means or consult external documentation. The intelligence comes with the alert.

Vendor-Specific Event Modules

IEM modules are built for specific device vendors and models — not generic pattern matchers. Each module understands the native output format, expected behaviors, and anomaly signatures for that device type.

Embedded Remediation Guidance

Every IEM event surfaces with context and recommended response steps — built into the alert itself. Operators know what happened, what it means, and what to do next without leaving the platform.

Continuous Log Aggregation

ConsoleWorks aggregates log data across all managed devices into a unified event stream. Every event is timestamped, attributed to a specific device and identity, and retained for audit and investigation.

Operational Dashboard Visibility

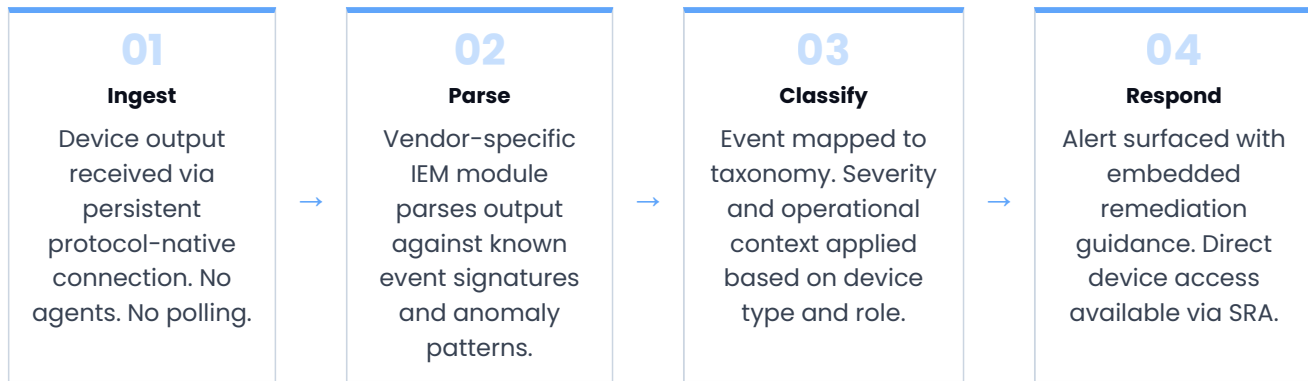
Event status is surfaced in real-time operational dashboards — giving security, compliance, and operations teams a shared view of active events, severity distribution, and response status across the environment.

HOW IEM WORKS

From Device Output to Closed Loop

IEM operates continuously against the device connections ConsoleWorks already maintains. Because ConsoleWorks holds persistent, protocol-native connections to managed devices — with no agents required — it receives device output as it is generated, without polling delays or passive traffic inference. Every event is processed immediately against the applicable IEM module for that device.

The processing pipeline moves in four stages: raw device output is ingested and parsed by the vendor-specific IEM module; the event is classified against the defined taxonomy; severity and operational context are applied; and the resulting alert is surfaced with embedded remediation guidance. For devices under Secure Remote Access management, operators can initiate a direct connection to the affected device from within the event view — moving from detection to response without leaving the platform.

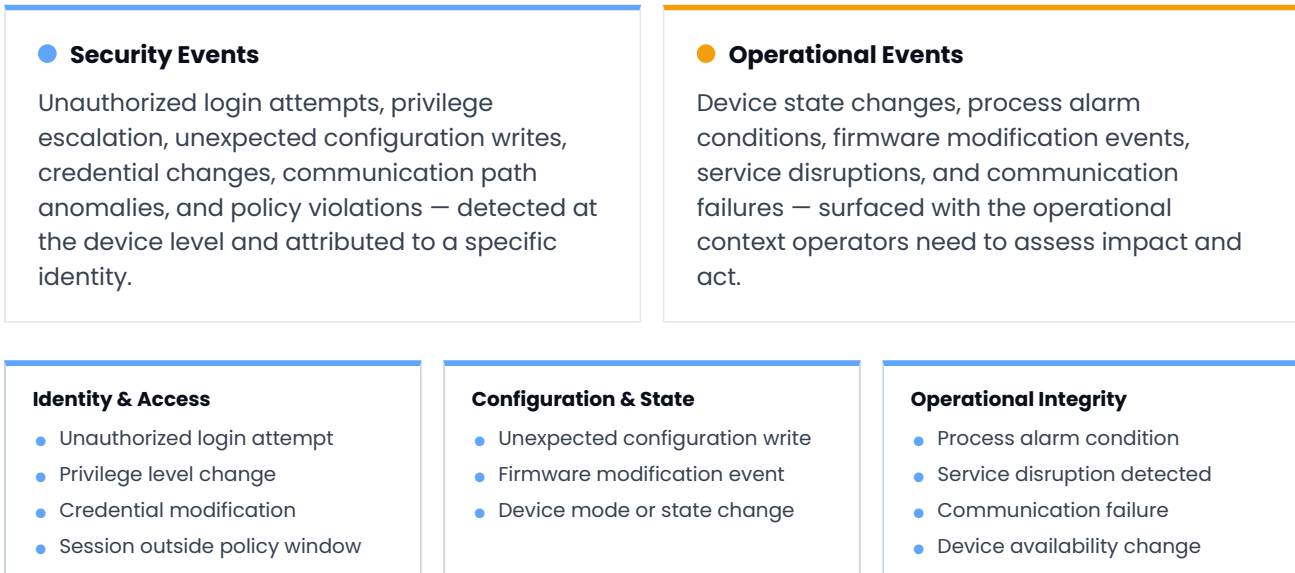


Generic tools detect events. IEM understands them — with vendor-specific context and remediation guidance built in from the start.

WHAT IEM DETECTS

Vendor-Specific Intelligence Across Your Environment

IEM modules are organized by vendor and device class. Each module defines the event signatures, severity thresholds, and remediation guidance appropriate to that specific device type — not a generic baseline applied uniformly across all assets.



IEM AND THE PLATFORM
Detection That Connects to Everything Else

IEM does not operate in isolation. Because ConsoleWorks holds the asset record, the access history, the configuration baseline, and the measurement state for every managed device, every IEM event is enriched with the full context of that device at the time of detection. When privilege escalation is detected on a router, ConsoleWorks already knows who had access, what the baseline configuration was, and whether the device was in a scheduled maintenance window.

This integration produces something no standalone event monitoring tool can provide: an alert that is not just attributed to a device, but to an identity, a session, a configuration change, and a measurement state — all in one record.

EVENT — CORP-RTR-CISCO-07 · PRIVILEGE ESCALATION — ENABLE MODE ACCESS				Remediate
SEVERITY High	DEVICE TYPE Cisco IOS Router	IEM MODULE Cisco IOS / IOS-XE	DETECTED 14:22:07 UTC	
IDENTITY Contractor Session — J. Torres	SESSION ACTIVE Yes — Outside Window	CONFIG BASELINE Drift Detected	SRA ACCESS Available	

For assets under Secure Remote Access management, operators can connect directly to the affected device from within the event view — moving from detection to investigation without leaving the platform. The complete session record, including all commands executed and configuration changes made during the session, is retained and available for audit.

IEM CONNECTS TO THE FULL CONSOLEWORKS PLATFORM
Asset Record

Every event is enriched with the full asset record — device type, vendor, firmware, criticality, and compliance obligations.

Access History

Identity attributed to every event — tied to the active session, the user, and the access policy in effect at detection time.

Config Baseline

Configuration events are automatically compared against the CCM baseline — before and after capture surfaces exactly what changed.

Direct Access

For SRA-managed devices, operators initiate a direct connection from within the event view — no tool switching required.

AUDIT & COMPLIANCE
Every Event. Every Identity. Every Change.

Every event processed by IEM is retained in a tamper-evident log — timestamped, attributed to a specific device and identity, and linked to the session and configuration state at the time of occurrence. This creates an unbroken chain of evidence from event detection through response, available for audit against any compliance framework at any time.

For regulated environments, IEM-generated event records satisfy logging requirements across NERC CIP, NIST SP 800-82, IEC 62443, and other frameworks — without additional tooling, manual log correlation, or post-incident reconstruction. The audit trail is built as events occur, not assembled after the fact.

No standalone event monitoring tool can produce an alert attributed to an identity, a session, a configuration state, and a measurement result — simultaneously. ConsoleWorks IEM does, because all of that context already exists in the platform.