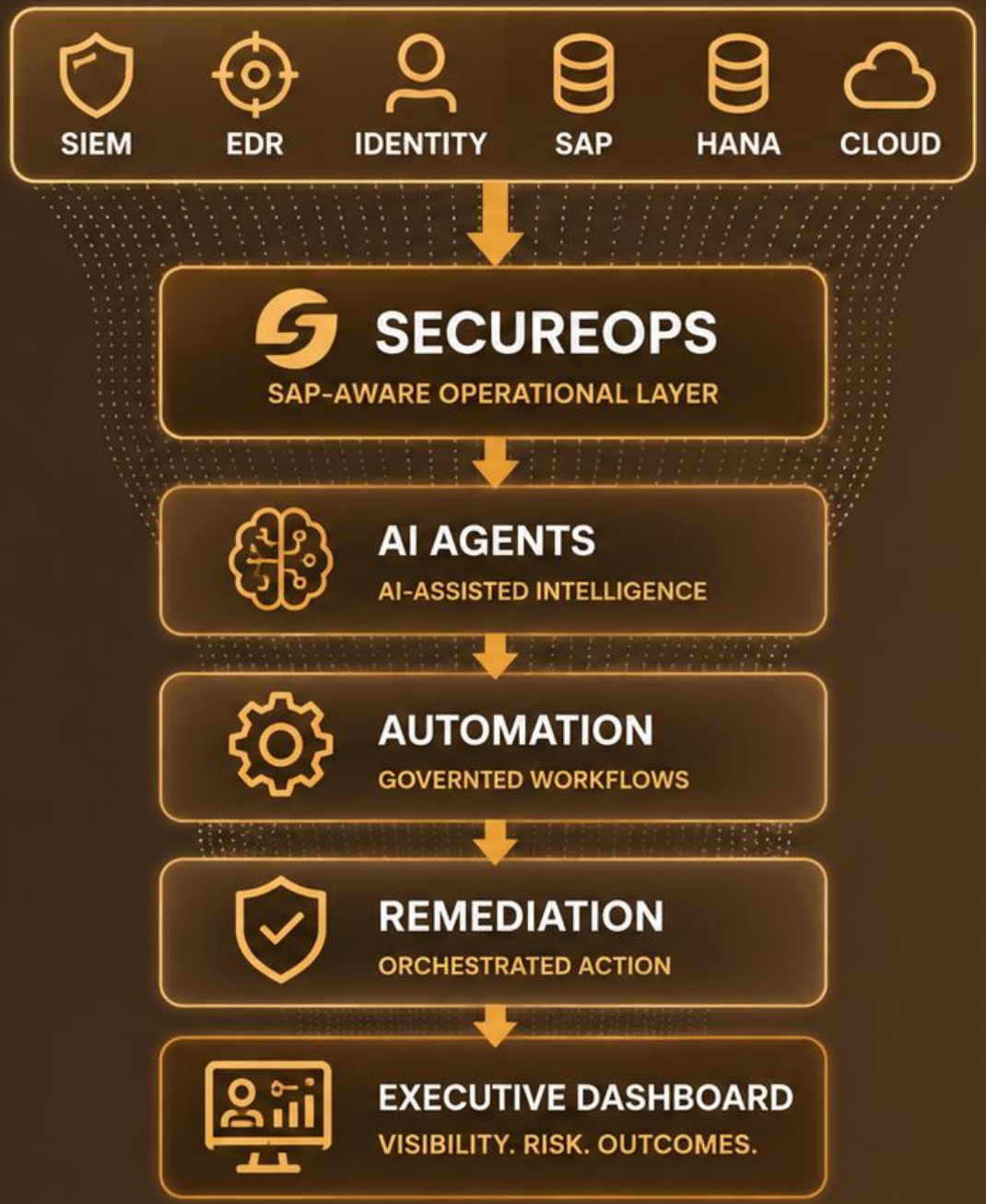


A WEBINAR BY IT-CONDUCTOR

BUILDING AN AUTONOMOUS SAP SECURITY OPERATIONS CENTER

Wednesday, september 16th, 2026

8:30 AM PDT | 11:30 AM EDT | 5:30 CEST

Hosted by Linh Nguyen,
CEO, and Co-Founder of IT-Conductor

COLD OPEN

The alert that has nowhere to go

Your SIEM fires. Your EDR flags an anomaly. Both point at something SAP-related — and then what?

SOC

The alert is correctly detected. It is correctly triaged. Then it hits a wall: nobody on the ticket knows what it means inside SAP.

Is this SAP-relevant?

- Which SID, client, role?
- Is the component even installed?
- Is it internet-facing?

Who owns the response?

- SOC doesn't know SAP
- Basis doesn't watch the SIEM
- The ticket sits, unassigned

What's the safe next step?

- Patch, compensate, or escalate?
- Who approves it?
- How is it proven closed?

Tools already detect the problem. The gap is what happens between detection and action.

WHY NOW

Most organizations already have the detection layer

The investment already happened. The operational layer above it did not.

SIEM

Correlates events and alerts across the enterprise

EDR

Detects anomalous behavior on endpoints and servers

Identity

Governs authentication and access across systems

Cloud Security

Monitors posture across cloud infrastructure

1 Detection tools → 2 SAP context → 3 Coordinated action → 4 Executive visibility

The tools already exist. What's missing is the layer that turns their signals into SAP-specific, governed action.

WHAT YOU'LL WALK AWAY WITH

By the end, attendees should see the architecture, not just the concept

1

See

the architecture of an autonomous SAP Security Operations Center

2

Understand

how existing signals become SAP-specific decisions

3

Learn

how AI agents and automation close the loop to remediation

4

Leave with

a practical view of what to connect first

WHERE THIS FITS

Webinar #10 brings the series together into one architecture

Every prior episode becomes a component of the SOC we build today.

#6	#7	#8	#9	#10
Autonomous decisions	AI agents for SAP security	Without 24×7 experts	Compliance to resilience	Building the SOC

Decisions, agents, scarce expertise, and continuous resilience all converge here: one architecture that connects existing seaurity investments to SAP-aware action.

THREE ROLES, ONE ARCHITECTURE

CISO, SAP platform owner, and automation architect all need the same layer

Each role sees a different half of the problem today.

CISO / SOC Leader

"My SOC sees everything except SAP."

Needs: SAP-aware enrichment, coordinated response, executive-level visibility

SAP Basis / Platform Owner

"I can act, but I never see the alert until it's already a fire."

Needs: early context, safe playbooks, change-aware execution

Automation / AI Architect

"I can build agents, but they need a structure to plug into."

Needs: a reusable finding model, assignment logic, guardrails

Which security signal source is hardest to connect to SAP context today?

AUDIENCE POLL

Which security signal source is hardest to connect to SAP context?

Live poll #1

- A **SIEM**
- B **EDR**
- C **Identity platform**
- D **Cloud security**
- E **ServiceNow / GRC**

CORE THESIS

The shift: from detection-rich to operationally connected

SecureOps is the layer that sits above existing tools, not another tool beside them.

Detection-rich

- SIEM, EDR, identity all detect
- Alerts pile up across tools
- SAP context lives in someone's head
- Response depends on who's online

Operationally connected

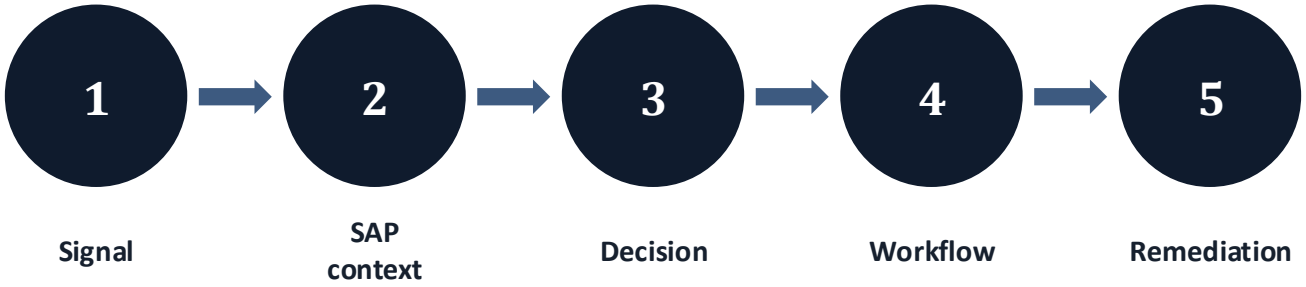
- Signals correlate into one finding
- SAP context applied automatically
- AI agents recommend the next step
- Governed automation closes the loop

The goal is not to replace SIEM, EDR, or identity platforms. The goal is to finish what they start.

THE SIGNAL-TO-ACTION GAP

Where detection stalls before it becomes SAP-specific action

The weak point is usually the handoff between detection and SAP context.



THE MISSING LAYER

Existing signals become actionable only when mapped to SAP reality

SecureOps translates generic security signals into SAP-aware operational decisions.

Existing signal	SAP context	Governed action
SIEM correlation	SID / client / role	Patch now
EDR behavioral alert	Component & kernel level	Compensate
Identity anomaly	Business criticality	Escalate
SAP / HANA / cloud posture	Change window	Defer with expiry
		Prove closure

THE ARCHITECTURE

The autonomous SAP Security Operations Center



SecureOps doesn't replace what you have — it sits above it, orchestrating people, process, and AI into SAP-specific action.

BEYOND AUTOMATION

SecureOps is an Agents Orchestration platform — not just automation

Efficient cyber operations isn't scripts running tasks. It's people, process, and AI, converging under governed orchestration.

People

Basis, security, HANA, cloud, SOC, compliance, and business owners — each with clear ownership.

Process

Routing rules, SLAs, approval policies, and escalation paths that make outcomes repeatable.

AI

Specialist agents that analyze, recommend, and execute inside the boundaries people and process define.

GOVERNED ORCHESTRATION

This convergence — not automation alone — is the core to an efficient cyber operations team.

THE OPERATING MODEL

Detect. Correlate. Decide. Remediate. Prove.

One operating loop, applied to every signal source.

1	2	3	4	5
Detect	**Correlate**	**Decide**	**Remediate**	**Prove**
Ingest signals from SIEM, EDR, identity, SAP	Map to SID, component, business criticality	AI-assisted risk scoring and recommendation	Governed automation, approval-gated	Evidence, validation, executive score

Operating principle: every signal source feeds the same loop — not five different processes.

THE REUSABLE CORE

One finding model, many use cases

Encode a finding once — with applicability, criticality, and scoring — and reuse the structure everywhere.

Security finding

A CVE, SAP Security Note, or SIEM/EDR alert mapped to an SAP system

Configuration finding

A drift from secure baseline or hardening standard

Performance finding

A degraded job, queue, or resource condition

Compliance finding

A control gap identified against a framework requirement

Same structure, same scoring model, same workflow engine — whatever the finding type turns out to be.

BEHIND THE AUTOMATION

The SACO team hierarchy

A concise, scalable taxonomy that maps into ServiceNow, Jira, or SAP Cloud ALM.

SACO Platform Operations

Health of the SACO platform, connectors, agents, and automation services

SAP Basis Operations

SAP systems, kernels, transports, and technical configuration

SAP Security Operations

Security Notes, hardening, vulnerabilities, and secure configuration

SAP HANA Operations

HANA lifecycle, security, and database administration

Infrastructure Operations

Operating systems, virtualization, storage, and backup

Cloud Operations

Public cloud services, networking, IAM, and cloud-native security

SOC / Incident Response

Active threats, investigations, and containment

Governance & Compliance

Audit, policy enforcement, and risk management

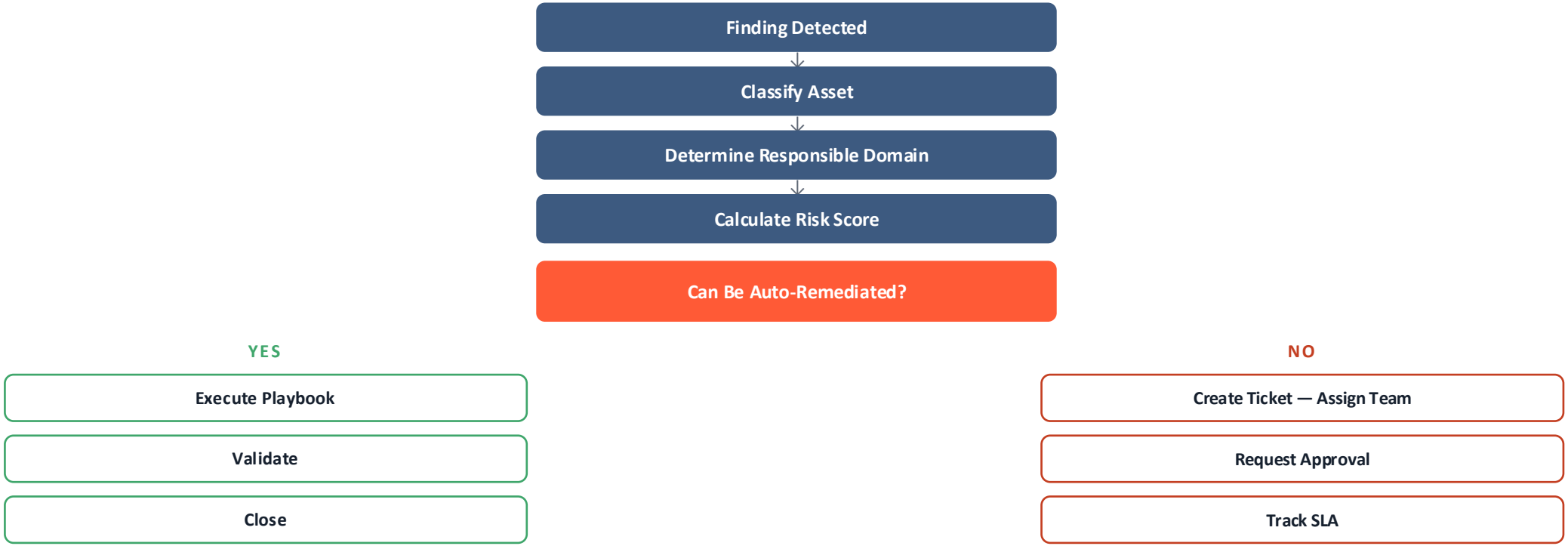
Business Application Owners

Functional validation, business approvals, and risk acceptance

THE ROUTING LOGIC

Autonomous routing for SACO

Every finding is evaluated against the same routing rules.



Clear ownership boundaries for autonomous routing and approval workflows — every time.

PUTTING THE ROUTING TO WORK

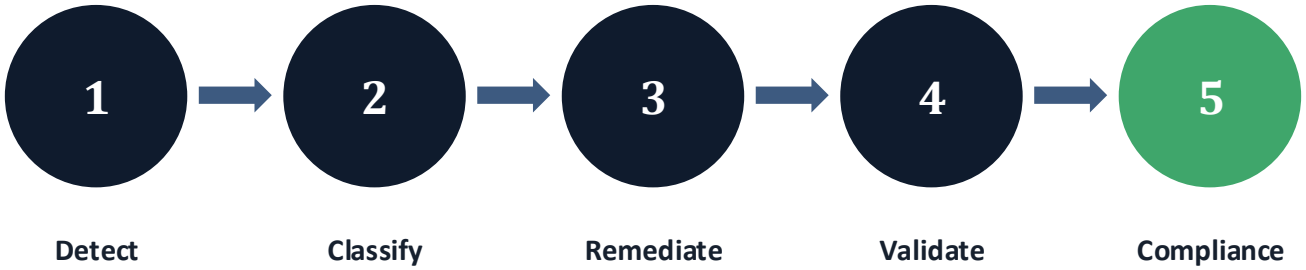
Example assignment matrix

FINDING	ASSIGNED TEAM	AUTOMATION CANDIDATE
Missing SAP Security Note	SAP Basis Operations	Yes
Missing kernel patch	SAP Basis Operations	Yes
Outdated HANA revision	SAP HANA Operations	Yes
Weak login/min_password_lng	SAP Security Operations	Yes
Expiring SSL PSE	PKI & Certificate Management	Yes
SAP_ALL assigned to dialog user	IAM / SAP Security	Conditional (approval required)
Open SAProuter access	Network Security	Yes
Linux OpenSSL CVE	Infrastructure Operations	Yes
AWS Security Group exposure	Cloud Operations	Yes
Critical exploit detected	SOC / Incident Response	Partially (containment automated)

THE FULL LIFECYCLE

From detection to compliance — scored by SRI

Every finding is tracked end to end, and every stage updates the SACO Resiliency Index.



SRI updates at every stage — not just at audit time. A single finding's risk contribution rises, falls, and closes out visibly in the score.

Same weighting as the pillar model: Platform 30% · Configuration 25% · Application 20% · Identity & Access 25%.

THE TRUST LAYER

Autonomous does not mean unapproved

It means pre-approved where policy is clear and escalated where risk is high.

- Escalation rules
- Approval policy
- Change windows
- Exception expiry
- Rollback plan
- Evidence capture

DECISION BOUNDARY

Inside boundary: execute. Outside boundary: escalate.

USE CASE 1

SIEM alert enrichment

Move from “the SIEM fired” to “we know exactly what this means for SAP.”

1	2	3	4	5
Ingest	**Map**	**Assess**	**Recommend**	**Route**
SIEM alert and correlated events	To SAP system, SID, and business process	Criticality, exposure, exploitability	Governed next step, risk-ranked	To the right agent or owner

The SIEM stays the SIEM. SecureOps is what turns its alert into an SAP-specific decision.

USE CASE 2

EDR-to-SAP correlation

Give SOC teams the SAP context an endpoint alert can't provide on its own.

EDR signal	SAP context	Governed action
Anomalous process, suspicious binary, or unusual behavior on an SAP application server.	Which SID, role, and business process the affected host supports — and its criticality.	Isolate, investigate, escalate, or apply a compensating control — with an SAP-aware playbook.

Key promise: the SOC gets an SAP-aware answer, not just another host on a list.

USE CASE 3

Executive SOC dashboard

Give leadership one current view of SAP security operations — not five disconnected tools.

Detection coverage

Which signal sources are connected and contributing findings

Response velocity

Time from detection to decision to remediation

Remediation status

Open, in progress, escalated, and exception-tracked findings

Resilience trend

SACO score trend across platform, configuration, application, IAM

Executives don't need every alert. They need coverage, velocity, status, and trend — in one place.

DEMO SCENARIO

Planned remediation: OS, SAP, and database patching

The foundation of proactive management — patching with minimal business impact.

This month's findings include an OS kernel CVE, an SAP kernel update, and a HANA revision — each owned by a different team, each with its own downtime profile. SecureOps coordinates all three as one planned remediation cycle.



Demo success criterion: attendees see OS, SAP, and DB patches move from finding to validated closure — with business impact minimized throughout.

DEMO · STEP 1 OF 5

Classify and prioritize

Turn three unrelated patch sources into one prioritized remediation plan.

OS finding

- Linux/Windows CVE
- Vendor patch bulletin
- Affected server inventory

SAP finding

- SAP kernel patch level
- Security Note applicability
- Component & add-on scope

Database finding

- HANA revision status
- Vendor security advisory
- Replication & backup state

Each finding is scored and ranked the same way — severity, exploitability, exposure, business criticality — regardless of layer.

DEMO · STEP 2 OF 5

Determine team and automation candidate

The assignment matrix decides who owns it — and whether it can run unattended.

OS kernel CVE

Infrastructure Operations — automation candidate: Yes

SAP kernel patch

SAP Basis Operations — automation candidate: Yes

HANA revision

SAP HANA Operations — automation candidate: Yes

Business-critical exception

Business Application Owners — approval required before scheduling

Most patch types are automation candidates. What changes is the approval and scheduling path around them.

DEMO · STEP 3 OF 5

Schedule with guardrails

Minimizing business impact starts with when and how the window is chosen.

SCHEDULING INPUTS

- Downtime tolerance
- Business criticality
- HA / DR readiness
- Dependency sequencing
- Change window availability

POLICY ENGINE

GOVERNED OUTCOMES

- Patch now, in window
- Stagger by team / layer
- Rolling, no-downtime path
- Defer with exception
- Escalate to CAB

The goal isn't the fastest patch — it's the patch that clears with the least business disruption.

DEMO · STEP 4 OF 5

Execute the patch playbooks

OS, SAP, and database patches run through the same disciplined sequence.

1

Pre-checks

Health, backups, locks, capacity, dependencies

2

Approval

Policy-defined approver or emergency path

3

Patch

OS kernel, SAP kernel, or HANA revision — rolling where possible

4

Post-checks

Service health, logs, version, security status

5

Rollback

Triggered automatically when validation fails

DEMO · STEP 5 OF 5

Validate and update the SRI score

Closure isn't complete until the resiliency score reflects the reduced risk.

Evidence	Score	Learning
Change record, approval, logs, pre/post validation, screenshots	Platform pillar score rises; SRI reflects reduced exposure immediately	Scheduling rules refined, playbook updated, next cycle informed

Three patch types, three teams, one governed cycle — and one number that shows the result.

MEASURING THE SHIFT

Metrics that show a connected SOC, not just a busy one

Measure coverage and velocity, not just alert volume.

Coverage %

Share of signal sources connected to SAP context

MTTD

Mean time to detect SAP-relevant risk

MTTA

Mean time to assess applicability

MTTDc

Mean time to decision

MTTR

Mean time to remediate or compensate

Proof %

Evidence completeness for closed findings

Executive translation: more of the enterprise's security stack now produces SAP-specific action.

GETTING STARTED

The 30-day action plan

A practical path to connecting your existing security stack to SAP.

Week 1

Inventory signal sources

and SAP landscape scope

Week 2

Map one source to SAP context

start with SIEM or EDR

Week 3

Pilot governed remediation

for one use case

Week 4

Stand up the executive view

coverage, velocity, trend

THE EXECUTIVE ARGUMENT

What changes when the operational layer is in place

The before/after executives need to hear.

Before

- SIEM, EDR, and identity detect
- risk. SAP context lives with
- individuals. Response depends
- on who's available and what
- they remember.

After

- Every signal source feeds one
- SAP-aware loop. AI agents
- correlate, decide, and route.
- Governed automation remediates.
- Executives see one score.

You don't need new detection tools. You need the layer that turns what you already have into SAP-specific, governed action.

Your SOC already sees everything. Now it can act on SAP, too.

Connect the signals you already have to the SAP context, decisions, and governed automation that turn them into action.

Request a demo

Q&A

Detect. Decide. Remediate. Autonomously.