A webinar by IT-Conductor

Rise of SAP Autonomous Operation webinar series



Wednesday, August 26th, 2026

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

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

AI Agents for SAP Security Operations

PART OF A SERIES

Building toward one idea, one session at a time

Today: using agent AI to convert SAP security evidence into decisions and actions.

S1	S2	S3	S4	S5	S6	S7 · TODAY
Why existing SAP security approaches leave a remediation gap	Why SAP needs its own cyber operations platform	Anatomy of an SAP cyber attack	The Four Pillars of SAP Autonomous Cyber Operations	Autonomous Patching Without Downtime	Detect. Decide. Remediate.	AI Agents for SAP Security Operations

The series is moving from “what is the gap?” to “how do we close the loop?”

WHAT IS HAPPENING IN THE REAL WORLD OF CYBERSECURITY

Offense and Defense are BOTH Becoming Agentic

"Attackers increasingly can identify vulnerabilities, develop exploits and move through complex environments with increasing speed and scale, while frontier models are also becoming increasingly capable at vulnerability discovery, secure-code review, incident response and patch validation." - OpenAI

Traditional SAP security

Detect → Ticket → Assign → Analyze → Schedule → Patch → Validate

Often takes days, weeks or months.

Agentic SAP security

Observe → Analyze → Correlate → Decide → Orchestrate → Validate → Learn

Can increasingly operate continuously.

GOVERNANCE: AI proposes and coordinates. Policy governs. Humans retain authority over high-impact actions. Automation executes deterministically. Everything produces evidence.

THE REAL CHALLENGE

SAP security has plenty of data. The hard part is connecting it.

The bottleneck is not collection — it is interpretation across sources that were never designed to explain each other.

Core idea

A CVE can be critical — but only if the affected component is installed. A parameter can be weak — but risk changes if the system is internet-facing, alerts are active, or audit evidence shows suspicious use.

1 Collect — 2 Correlate — 3 Judge — 4 Explain — 5 Act

This is where agent analysis adds value: not another dashboard, but a repeatable way to connect facts and explain what matters.

BETTER THAN SCRIPTS

An agent is a specialist with a defined job, tools, and context

Keep the AI simple: a bounded worker that evaluates current evidence before producing an operational result.

Traditional automation

- Executes fixed steps
- Same response regardless of context
- Stops when data does not match the expected path
- Usually reports symptoms, not implications

Agentic analysis

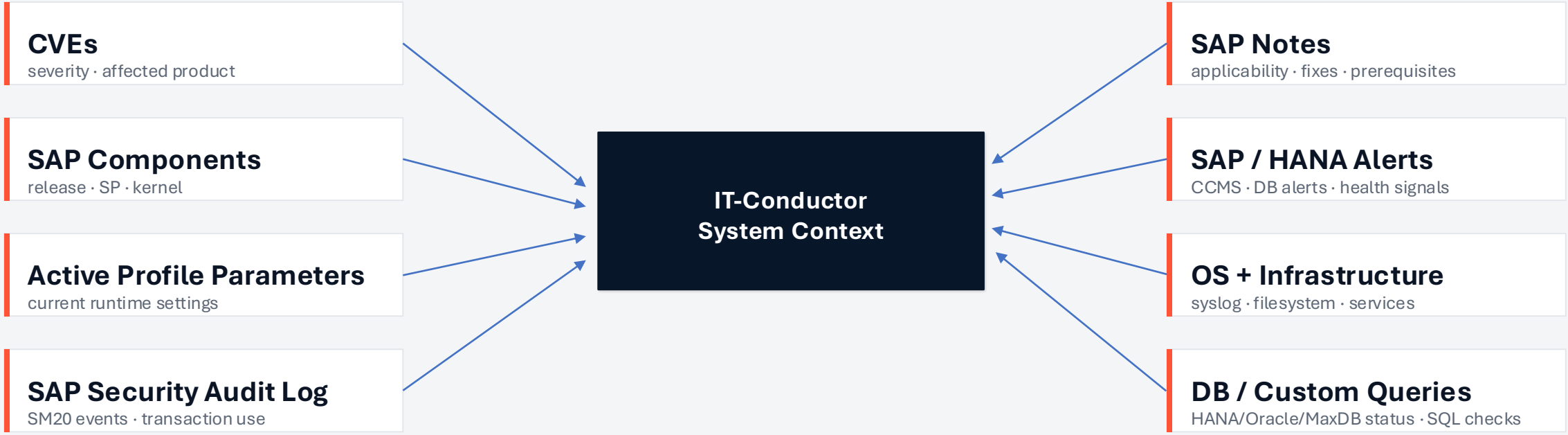
- **Reads evidence from multiple sources**
- **Interprets what is missing or contradictory**
- **Applies SAP security perspective**
- **Produces findings, remediation guidance, and tickets**

The "common sense" comes from combining the agent definition with real system context it can retrieve.

THE EVIDENCE

IT-Conductor already has the security picture — in pieces

The agent connects those pieces into one system-aware context.



Plus incidents, change history, service relationships, runtime status, database state, jobs, network signals, and other data collected by IT-Conductor adapters.

THE ANALYSIS

One body of evidence. Multiple security perspectives.

Different agents can inspect the same system context with different responsibilities.

Vulnerability

Does the installed software create exposure to a CVE or Security Note?

same evidence

Configuration

Do active parameters and settings weaken the system posture?

same evidence

Behavior

Do audit records or alerts show unusual or suspicious activity?

same evidence

HANA / DB

Does the database layer add risk, misconfiguration, or patch exposure?

same evidence

Response

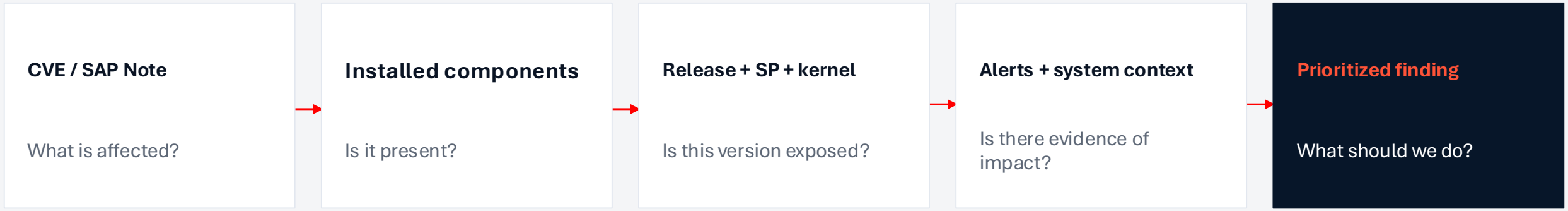
Do separate signals belong to the same security issue — and what should happen next?

same evidence

EXAMPLE 1 · VULNERABILITY INTELLIGENCE

From “there is a CVE” to “this system has actionable exposure”

The agent connects public vulnerability intelligence with the actual SAP software state and operational evidence around it.



Example inference: if a prerequisite component is outdated, SAP note applicability may under-report relevant notes. A “zero missing notes” result becomes less trustworthy — and the remediation plan should start with that prerequisite.

EXAMPLE 2 · CONFIGURATION + BEHAVIOR

A weak setting matters more when surrounding evidence agrees

Agents can combine configuration posture with observed activity and alerts.

Active profile parameter

e.g., insecure or weaker-than-baseline setting

Security Audit Log

privileged actions, failed logons, critical transactions

SAP / HANA alert

active alert on related system or DB component

Linux / DB evidence

OS or database condition supports the same issue

Security issue

The configuration weakness is not isolated; the audit, alert, OS, and DB evidence increase confidence that the issue deserves action.

Agent output can explain why the severity changed: not just “parameter weak,” but “parameter weak + suspicious behavior + active alert + supporting infrastructure evidence.”

CROSS-LAYER ANALYSIS

SAP security does not stop at the ABAP or HANA boundary

Security issues often span SAP, database, operating system, and infrastructure evidence.

SAP APPLICATION	Notes · components · profiles · jobs · audit log
SAP / HANA DATABASE	DB alerts · system health · patch and configuration state
OPERATING SYSTEM	Linux syslog · filesystem · package · host events
OPERATIONAL RECORD	Incidents · changes · maintenance windows · previous findings

One analysis

A security issue can look like an SAP problem but actually depend on DB or OS evidence — or the other way around.

This matters most for incidents where the first visible symptom is SAP, but the root cause may be database, OS, network, or change-related.

THE OUTPUT

The result should look like a senior consultant's write-up — not an AI transcript

A finding is useful only when evidence, reasoning, and next steps are clear enough for operations to act.

01 **ISSUE**
What is wrong and why it matters

02 **EVIDENCE**
Which systems, values, logs, alerts, and notes support it

03 **IMPACT**
What can happen if the condition remains

04 **RECOMMENDATION**
Specific SAP / HANA / OS / DB action

05 **VALIDATION**
How to prove the fix worked

06 **OPERATIONS**
Incident, comment, notification, audit trail

The agent closes the analysis loop into the same operational system where customers already manage incidents, changes, and evidence.

THE SPECIALISTS

Meet the SAP security agents

Not separate products — specialized responsibilities operating over the same IT-Conductor data and governance.

Vulnerability Agent

CVE + Security Note applicability and exposure

Configuration Agent

Secure baseline drift and active parameter posture

Audit / Identity Agent

Privileged activity, unusual access, and audit evidence

HANA Security Agent

Database-layer security posture and alerts

Incident Response Agent

Correlates separate signals into one response case

Compliance Agent

Turns findings and actions into defensible evidence

Different questions. Shared evidence. One operational record.

GOVERNANCE, NOT GUESSWORK

Every agent works inside the same governance model

1	**No new SAP data path**	Agents analyze IT-Conductor data already collected and normalized.
2	**Named tools only**	The agent calls defined platform functions — not arbitrary shell commands or ad-hoc URLs.
3	**Normal operational objects**	Findings, incidents, comments, and notifications remain reportable and auditable.
4	**Human gate where it matters**	Read-only analysis first. Approval gates remain for remediation actions.

Trust comes from boundaries and traceability — not from asking customers to "trust the AI."

WHAT THE LIVE WALKTHROUGH SHOULD PROVE

One system. One analysis. One operational outcome.



THE TAKEAWAY

Turn SAP security data you already have into decisions you can act on

The agent layer is valuable when it connects evidence, explains the risk, and closes the result into secure operations.

01 Bring SAP, HANA, DB, OS, and vulnerability evidence into one context.

02 Analyze the same evidence from vulnerability, configuration, behavior, and incident perspectives.

03 Produce prioritized issues, remediation guides, validation steps, tickets/comments, and audit trail.

Start with a read-only SAP Security Operations assessment

Questions?