A WEBINAR BY IT-CONDUCTOR

DETECT. DECIDE. REMEDIATE.



Wednesday, August 19th, 2026

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

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

PART OF A SERIES

Building toward one idea, one session at a time

S1

Why existing SAP security approaches leave a remediation gap

S2

Why SAP needs its own cyber operations platform

S3

Anatomy of an SAP cyber attack

S4

The Four Pillars of SAP Autonomous Cyber Operations

S5

Autonomous Patching Without Downtime

S6 · TODAY

Detect. Decide. Remediate.

BEYOND THE ALERT

Detection is only the beginning.

The real challenge is understanding what happened, assessing the risk, deciding how to respond, and executing remediation with confidence.

AI-assisted decision-making helps SAP teams move from alerts to action — while maintaining governance, human oversight, and rollback capability.

WHAT EVERY FINDING RAISES

Every finding raises the same five questions

1. Does it affect our landscape?
2. How serious is the risk?
3. Should remediation be automated?
4. Is human approval required?
5. How do we safely roll back if necessary?

THE FRAMEWORK

Detect. Decide. Remediate.

1

Detect

AI-assisted correlation connects fragmented signals into a single, landscape-aware finding.

2

Decide

Root cause analysis and risk scoring determine severity, automation eligibility, and approval needs.

3

Remediate

Governed automation executes with human approval and rollback built in.

DETECT

Does it affect our landscape?

AI-ASSISTED CORRELATION

SAP Security Notes, CVEs, configuration drift, and audit logs are connected into a single finding — tied to what's actually installed, exposed, and business-critical.

A finding isn't real until it's confirmed against what's actually running.

DECIDE

How serious is the risk — and what happens next?

ROOT CAUSE ANALYSIS

What's actually causing this — and is it isolated or systemic across the landscape?

RISK SCORING

Severity, exploitability, exposure, and business criticality combine into one risk score — not a flat severity label.

Together, they answer: should remediation be automated? Is human approval required?

REMEDIATE

Executing with confidence, not just automation

Governed Automation

Approved playbooks execute the remediation — consistently, every time.

Human Approval

A gate before higher-risk changes, matched to the risk score.

Rollback

A deterministic, tested reversal if validation doesn’t pass.

Speed without governance isn’t automation — it’s risk. SecureOps gives you both.

GOVERNANCE, NOT JUST AUTOMATION

Security will never be a fully hands-off solution

Even the best remediation analysis and recommendation still benefits from a conversation — especially for anything outside the standard case.

- Best-effort automation handles the majority of routine findings
- Human consultation stays available for complex, non-standard cases
- Every action is traceable, approved, and reversible

Autonomous doesn't mean unattended.

HOW IT COMES TOGETHER

From finding to action, in one governed flow



The system detects that a finding has an available automation. AI recommends the action and a risk score. Policy or a human approves it. It executes, validates, and logs the evidence.

THE TAKEAWAY

“From alert to action, without losing control.”

Detect. Decide. Remediate. isn’t about removing people from the process — it’s about giving them the correlation, risk scoring, and governed automation to act faster, with confidence.

COMING UP

This is session 6 of the series

WEBINAR 7

AI Agents for SAP Security Operations

Discover how specialized AI agents can automate key SAP security and operational tasks.

Watch your inbox for the registration link.

TAKE THE NEXT STEP

Begin your SAP Autonomous Cyber Operations journey

Start with an assessment to identify:

- Operational gaps
- Remediation bottlenecks
- Automation opportunities

Request a SAP Security Operations Assessment

Questions?