AUTONOMOUS CYBER RESILIENCE
FOR SAP OPERATIONS

A Webinar by IT-Conductor

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

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

WEDNESDAY
JUNE 24TH 2026

WEBINAR AGENDA

Opening Poll Audience pulse — confidence in SAP threat detection & current tooling

The Problem Why SAP remediation backlogs spiral — detection, ownership, and tooling gaps

Polls 2 & 3 Greatest security concerns and current remediation maturity

Live Demo Dashboard → AI-powered analysis → Maestro remediation → service desk verification

Platform + Service What IT-Conductor delivers as a combined platform and managed security service

Poll 4 + Q&A Future state priorities and open discussion

How confident are you in your organization's ability to detect SAP security threats before they impact business operations?

A. Very Confident
Automated detection & alerting in place

B. Somewhat Confident
Some tooling, mostly manual review

C. Not Confident
Relying on audits and incident response

D. No Visibility
We don't actively monitor SAP

THE GROWING SAP SECURITY REMEDIATION PROBLEM

Ignored Reports

EarlyWatch Alert reports exceed 100 pages. Most findings receive little action.

Slow Manual Process

Review → validate → coordinate → change request → test → approve → deploy. Weeks pass.

Ownership Gaps

Who owns patching? Who approves? SOC, Basis, and App teams coordinate manually.

Reactive, Not Proactive

Remediation gets pushed until an audit finding, ransomware, or incident forces action.

Dormant Accounts Linger

HR deactivates at AD level, but SAP accounts persist for weeks — an open door.

RFC & Integration Risk

Failed RFC logon attempts every 5 minutes go unnoticed. Attack surface grows silently.

Which area creates your greatest SAP cybersecurity concern today?

A. Platform & Infrastructure Vulnerabilities

B. Access Management & Identity

C. Application Code & Configuration

D. Third-Party & Integration Connectivity

How does your team currently handle SAP security remediation findings?

A. Mostly manual — email & ticket coordination

B. Partially automated — scripts, still manual review

C. Scheduled — monthly or quarterly audit cycles

D. Reactive — we act when an audit or incident forces it

IT-CONDUCTOR - ONE PLATFORM, END TO END

1 DETECT	2 ANALYZE	3 DECIDE	4 REMEDIATE	5 VERIFY
Continuous security telemetry and automated scans identify Security Audit Log anomalies, OS and SAP CVEs, missing security notes, configuration drift, and emerging risks across SAP, SAP HANA, operating systems, and connected infrastructure.	AI-powered report scores findings by priority — risk level, IP analysis, session patterns, user behavior — 1-week-3-week-5-week action plan	Security team reviews the dashboard, selects high-priority items: lock this user, patch this host, update this parameter	Maestro creates the ticket, invokes the tool: user lockout, OS/kernel patch via service catalog, SAP note transport via ChAI™	Post-action health check re-runs the scan. Findings resolved. Audit trail complete. Compliance confirmed.

Autonomous APM/ML/AI-driven analysis in steps 1-2 | IT-Conductor Maestro™ orchestrates steps 3–5 | ChAI™ handles Change Management automation

LIVE DEMO — STEP 1 & 2: DETECT & ANALYZE

GLOBAL SECURITY DASHBOARD

- Cross-system consolidated security score
- Critical findings by category: Platform / Access / Code
- Open CVEs & missing SAP Security Notes (Hot News, High priority)
- Remediation ticket status & SLA tracking
- User anomaly alerts: dormant, over-privileged, suspicious logins

SYSTEM-LEVEL SECURITY VIEW (OZ1)

- Security Audit Log (SM20): logon failures, brute-force, IP anomalies
- Privileged users active in production (SAP_ALL, DDIC, batch)
- RFC failure patterns — integration accounts hitting every 5 min
- Parameter compliance vs. security baseline (login, SNC, gateway)
- Missing security notes applicable to this system's components

AI-Powered Analysis (Contextual)

Scheduled daily analysis produces scored, prioritized findings with risk levels (High / Medium / Low), suspicious IP flagging, session behavior patterns, and a **1-week / 3-week / 5-week action plan** — so teams always know what to fix first.

LIVE DEMO — STEPS 3 & 4: DECIDE & REMEDIATE VIA MAESTRO

User Lockout

1. Audit log flags suspicious user (failed logins, VPN IP, DDIC active in prod)
2. Review finding in dashboard — confirm risk level is High
3. Tell Maestro: 'Lock this user in OZ1'
4. Maestro invokes tool → SAP user deactivated, RFC destination disabled
5. Ticket created with approval chain and full audit trail

OS / SAP Kernel Patching

1. CVE analyzer detects affected hosts with outdated kernel version
2. Service request generated: SUSE OS patch / SAP kernel update
3. Maestro invokes OS admin service catalog for target system
4. Patch applied, kernel updated, system verified post-patch
5. Completion logged in service desk — audit-ready

SAP Security Notes (ChAI™)

1. Note download pulls Hot News & High priority CVE-linked notes
2. Gap analysis: missing notes compared against system components
3. Change request auto-opened in Dev/Sandbox for applicable notes
4. ChAI™ transports through QA → Production after approval
5. Note status updated in dashboard — landscape fully tracked

LIVE DEMO — STEP 5: VERIFY & CLOSE THE LOOP

After remediation, IT-Conductor re-runs the scan automatically — confirming the finding is resolved.

✓ User Lockout Confirmed

Account shows as locked in SM20. No further failed logon events. Audit trail complete — approver, timestamp, system recorded.

✓ Patch Applied & Verified

OS/kernel version updated. CVE no longer appears in affected systems list. Daily CVE analyzer confirms clean status.

✓ Security Note Transported

Note status updated from 'Missing' to 'Applied' in landscape view. ChAI™ transport confirmed in QA and Production.

✓ Compliance Report Updated

Daily health check re-scores the system. Risk posture improves. Report ready for audit — findings, actions, evidence all in one place.

PLATFORM + SERVICE DELIVERY — THE FULL PICTURE

THE PLATFORM — IT-Conductor Maestro™

- Automated daily scans across SAP landscape
- AI-powered analysis: risk scoring, action plans
- Maestro orchestrates remediation workflows
- ChAI™ manages SAP transport automation
- Global + system-level security dashboards
- Service desk: every action tracked & auditable

THE SERVICE — Expert-Guided Security Operations

- Prioritized findings delivered as a weekly report
- 1-week / 3-week / 5-week remediation roadmap
- Remote expert services for complex note implementations
- Security posture scoring before & after remediation
- Audit evidence packages — ready for compliance review
- Continuous improvement: detect → fix → verify → repeat

WHY IT-CONDUCTOR MAESTRO™

Agentic Orchestration

Maestro coordinates remediation across SAP Basis, SOC, and application teams without adding operational complexity.

SAP-Native Intelligence

Built specifically for SAP S/4HANA, ECC, HANA DB, Solution Manager and RISE environments.

Governance & Auditability

Every remediation creates a change request with approval workflow, audit trail, and evidence ready for auditors.

Continuous Compliance

Scheduled daily scans, automated reports, and real-time dashboards replace periodic manual audit exercises.

End-to-End Platform

One platform: vulnerability detection, patching, user management, config hardening, and service desk — all connected.

Broad Threat Coverage

Platform · Access & Identity · Code & Config · Third-Party & RFC — all four domains covered in a single view.

What would most accelerate your SAP security operations in the next 12 months?

A. Automated detection & real-time alerting across all systems

B. AI-driven analysis with a prioritized remediation roadmap

C. Automated patch & security note deployment pipeline

D. Unified dashboard + service desk with full audit trail

TAKE ACTION — YOUR SAP SECURITY POSTURE STARTS HERE

Stop treating SAP security remediation as a periodic cleanup exercise.



1

Request a Custom Demo

See Maestro against your landscape — we bring the security findings.

2

Run a Security Assessment

IT-Conductor expert services scan your SAP environment and deliver a prioritized action plan.

3

Start with Maestro Starter

Get visibility and automated alerting deployed in days — not months.

www.itconductor.com