A webinar by IT-Conductor

Rise of SAP Autonomous Operation webinar series

# SAP SECURITY WITHOUT 24x7 SAP EXPERTS

WEDNESDAY, SEPTEMBER 2ND, 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 2:17 AM problem

*A critical SAP security signal arrives when the SAP expert is offline.*

**2:17 AM**

*A critical SAP note applies to production. SOC sees noise. Basis is asleep. Change board meets tomorrow.*

## Do we patch now?

- Do we wait?
- Could introduce outage
- Could expand exposure

## Do we compensate?

- Who owns the call?
- Must prove control
- Must be auditable

***Episode hook: security response cannot depend on finding the right person at the right hour.***

WHY NOW

# A skills gap becomes a resilience gap when SAP is business-critical

**95%**

of cybersecurity professionals report at least one skill need in their organization.

**59%**

cite critical or significant cybersecurity skill needs.

**CVSS 10.0**

appeared in SAP Security Patch Day — August 2026.

***SAP security needs expert-guided automation, not expert-dependent operations.***

EPISODE THESIS

WHAT YOU'LL WALK AWAY WITH

# By the end, attendees should know what to do differently next week

1

**Recognize**

where 24×7 SAP security coverage fails in real operations.

2

**Model**

SAP cyber response as a governed decision loop, not a hero escalation.

3

**Design**

guardrails that make autonomy safe for SAP change control.

4

**Start**

with a 30-day plan for expert-guided automation.

WHERE THIS FITS

# Webinar #8 connects AI agent capability to continuous resilience governance

| #5 | #6 | #7 | #8 | #9 |
|---|---|---|---|---|
| Patching without downtime | Autonomous decisions | AI agents for SAP security | Without 24×7 experts | Compliance to resilience |

*After showing what AI agents can do, this episode answers the executive question: "How do we rely on automation safely when the SAP expert is not online?"*

THREE ROLES, ONE PROBLEM

# Three roles. One after-hours SAP cyber response problem.

## SAP Basis / Platform Owner

*“I know the landscape, but I cannot be everywhere.”*

Needs: patch intelligence, safe playbooks, change windows, rollback discipline.

## SOC / Security Operations

*“I see alerts, but I lack SAP context.”*

Needs: SAP-aware correlation, severity context, escalation rules, evidence.

## CISO / Risk & Compliance

*“I need assurance that response is governed.”*

Needs: resilience metrics, traceability, approvals, continuous control evidence.

***Who owns after-hours SAP cyber response today?***

AUDIENCE POLL

# Who owns after-hours SAP cyber response today?

*Live poll #1 — use this to make the coverage gap visible.*

- A **SAP Basis**
- B **SOC**
- C **GRC / Compliance**
- D **MSSP**
- E **Not defined**

THE CORE TENSION

# Every organization wants 24×7 coverage. Few can staff it with 24×7 SAP depth.

## Business requirement

- Always-on detection
- Rapid triage
- Evidence-backed remediation
- Audit-ready controls

## Operating constraint

- Scarce SAP experts
- After-hours gaps
- Manual approvals
- Tool fragmentation

***Move from expert-dependent execution to expert-governed autonomy.***

THE BOTTLENECK MAP

# The human bottleneck map across the SAP cyber response chain

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| **Signal** | **Context** | **Decision** | **Action** | **Proof** |
| SAP notes, CVEs, audit logs, failed logons, config drift | Which SIDs, clients, kernels, add-ons, roles, interfaces are affected? | Exploitability, business criticality, compensating controls, downtime risk | Apply note, adjust parameter, disable user/RFC, transport fix, collect evidence | Approvals, validation, evidence, audit trail, resilience score impact |

***Which of these five steps fails first after hours?***

THE MISSING LAYER

# Generic security signals become actionable only when mapped to SAP landscape reality

| Generic signal | SAP context | Governed action |
| --- | --- | --- |
| CVE severity | SID / client / role | Patch now |
| Network exposure | Kernel / add-on level | Compensate |
| Failed logons | Business criticality | Escalate |
| EDR alert | Transport path | Defer with exception |
| Cloud finding | Change window | Prove closure |

***Without SAP context, the SOC sees risk but cannot safely decide. With context, the decision becomes policy-driven.***

THE OPERATING MODEL

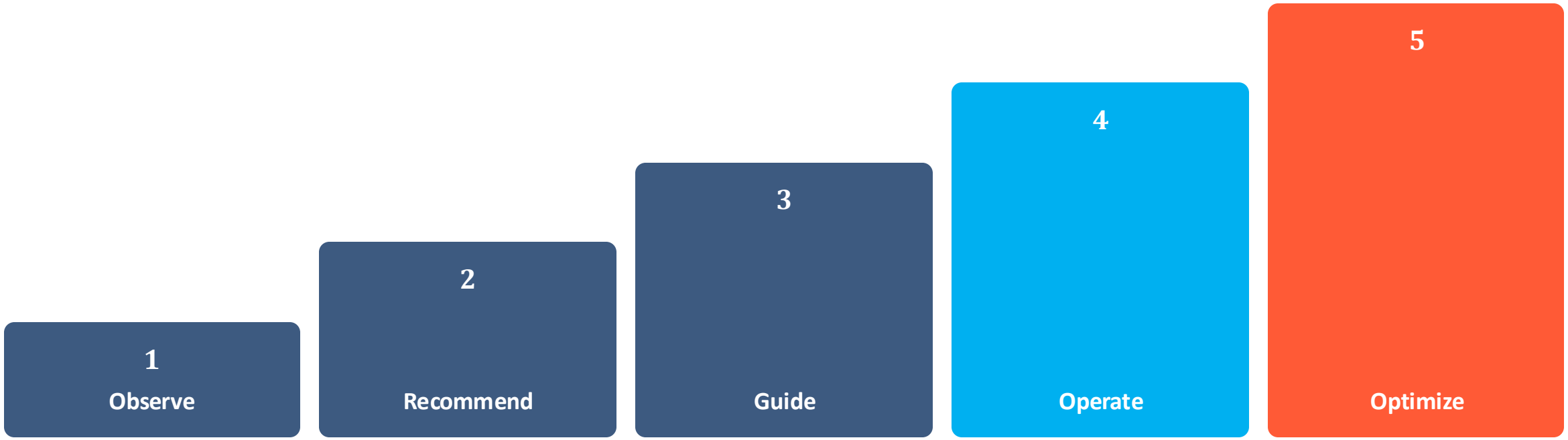
# Not replacing SAP experts — operationalizing their judgment under governance




***Operating principle: the expert defines the decision boundary; SecureOps executes inside that boundary and escalates outside it.***

ADOPTION PATH

# Safe adoption path from visibility to controlled autonomy




| 1 Observe | 2 Recommend | 3 Guide | 4 Operate | 5 Optimize |
|---|---|---|---|---|
| Read-only posture checks and evidence collection | Risk-ranked recommendations and owner routing | Human-approved playbooks with pre/post checks | Policy-approved execution inside defined boundaries | Continuous scoring, learning, and exception management |

THE TRUST LAYER

# Autonomous does not mean unapproved. It means pre-approved where policy is clear.

| | | |
|---|---|---|
| Policy & approvals | Change windows | Exception handling |
| Segregation of duties | Evidence capture | Rollback plans |

DECISION BOUNDARY

*Inside boundary: execute. Outside boundary: escalate.*

MAKING TACIT KNOWLEDGE EXPLICIT

# What “expert judgment” actually means

*Turn tacit SAP Basis/security knowledge into explicit decision rules.*

### Landscape facts

Which systems are production-critical? Which clients contain sensitive data?

### Technical applicability

Does this note match installed components, kernel, add-ons, or exposed services?

### Operational risk

Can it be patched during business hours? Is a restart required? What breaks first?

### Governance constraints

Who approves? What evidence is required? What exception is allowed?

***SecureOps value: encode these rules once, then reuse them consistently across alerts, notes, systems, and teams.***

USE CASE 1

# SAP security note prioritization

*Move from monthly lists to system-specific decisions.*

1

## Release

SAP publishes new and updated Security Notes

2

## Map

Match notes to installed SAP components and versions

3

## Rank

Score by CVSS, exposure, criticality, and compensating controls

4

## Route

Assign owner and decision SLA

5

## Act

Patch, compensate, defer with exception, or close as not applicable

USE CASE 2

# After-hours triage

*Give SOC and MSSP teams SAP-safe decision support.*

Alert arrives → SecureOps correlates → Decision outcome

| SOC signal | SAP-aware context | Governed next step |
| --- | --- | --- |
| High severity finding, failed logon burst, suspicious RFC, or vulnerable component. | Affected SID, client, role, interface, transport path, patch baseline, business criticality. | Escalate, open ticket, run approved check, apply compensating control, or defer with evidence. |

***Key promise: the SOC receives an SAP-aware answer, not just another alert.***

USE CASE 3

# Compensating controls

*When patching cannot happen immediately, risk still needs a governed response.*

1

### Patch now

Critical, applicable, exposed, approved window exists, rollback known.

2

### Compensate now

Patch not possible yet; reduce exposure with configuration, network, access, or monitoring control.

3

### Exception with expiry

Business reason to defer; owner, evidence, due date, and escalation path required.

***Autonomy is not only "apply the patch." It is also "make the safest governed decision when the patch cannot happen yet."***

DEMO SCENARIO

# 2:17 AM SAP incident simulation

*Make the operating model tangible with one end-to-end story.*

*A new critical SAP Security Note is released. SecureOps detects applicability to a production-connected component and initiates governed triage.*




***Demo success criterion: attendees see how expert governance scales safely, not how AI guesses its way through SAP change.***

DEMO · STEP 1 OF 5

# Ingest and normalize

*Turn external security releases and internal telemetry into a single work item.*

### INPUTS

- SAP Security Notes
- CVE metadata
- System inventory
- Kernel/add-on levels
- Audit/config signals

### SECUREOPS PROCESSING

- Normalize source data
- Link to SAP component
- Identify landscape scope
- Create triage object
- Open evidence trail

### OUTPUT

- One SAP-aware finding
- Owner assigned
- Affected systems listed
- Decision SLA set
- Evidence package started

***One SAP-aware finding with owner, affected systems, decision SLA, and evidence package started.***

DEMO · STEP 2 OF 5

# Assess applicability

*The system decides what applies before humans debate what matters.*

**Component match**

Installed product, add-on, kernel, library, or interface

**Exposure**

Internet-facing, partner-facing, internal-only, protected segment

**Criticality**

Production role, business process, data sensitivity, dependency chain

**Control state**

Existing parameter, access restriction, monitoring, patch baseline

***Outcome: applicable / not applicable / needs expert review***

DEMO · STEP 3 OF 5

# Decide with guardrails

*Decision support should produce a governed answer, not a vague recommendation.*

**DECISION INPUTS**

- Risk score
- Affected production SIDs
- Exploitability / exposure
- Business impact
- Downtime estimate

**POLICY ENGINE**

**GOVERNED OUTCOMES**

- Patch now
- Compensate now
- Escalate to expert
- Defer with exception
- Close as not applicable

***Approver required for higher-risk actions.***

DEMO · STEP 4 OF 5

# Execute safely

*Execution is orchestration with controls, not a blind one-click change.*

1

**Pre-checks**

Health, backups, locks, capacity, dependencies

2

**Approval**

Policy-defined approver or emergency path

3

**Runbook**

Patch, parameter, role/user, RFC, or compensating workflow

4

**Post-checks**

Service health, logs, version, security status

5

**Rollback**

Triggered when health or validation fails

DEMO · STEP 5 OF 5

# Prove and learn

*Closure is not complete until evidence and resilience impact are visible.*

| Evidence | Score | Learning |
| --- | --- | --- |
| Ticket, approval, logs, screenshots, commands, validation | Pillar score, risk reduction, residual exposure | Rules refined, playbook updated, exception trend captured |

***The question for auditors and executives is not "did someone do something?" It is "can we prove the right action happened under the right control?"***

MEASURING THE SHIFT

# Metrics that matter

*Measure the shift from expert-dependent to expert-governed operations.*

### 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

### SACO score

Trend across platform, configuration, application, IAM

***Executive translation: reduce unresolved exposure windows while increasing auditability.***

GETTING STARTED

# The 30-day action plan

*A practical path to SAP security without 24×7 SAP experts.*

**Week 1**

### Map coverage gaps

Identify after-hours SAP decisions that depend on named experts.

**Week 2**

### Encode judgment

Document applicability, criticality, approval, and escalation rules.

**Week 3**

### Pilot playbooks

Start with read-only assessment and human-approved remediation.

**Week 4**

### Measure and expand

Track decision time, remediation time, and evidence completeness.

THE EXECUTIVE ARGUMENT

# What changes when SecureOps is in place

*The operational before/after executives need to hear.*

## Before

- Coverage depends on who is awake,
- which spreadsheet is current, and
- whether the right SAP expert can
- interpret the alert.

## After

- Governed playbooks route, decide,
- remediate, compensate, and prove
- closure across SAP systems with clear boundaries

***Autonomous SAP cyber operations turns scarce expertise into reusable operational capacity.***

STRATEGIC TAKEAWAY

COMING UP

# Bridge to webinar #9

*From “security without 24×7 experts” to continuous cyber resilience.*

WEBINAR #9

## From compliance to continuous cyber resilience

Detect → Decide → Remediate → Prove becomes the operating backbone for compliance, assurance, and resilience reporting.

*TODAY: make SAP expert judgment available when risk cannot wait.*

*NEXT: prove resilience continuously instead of preparing evidence after the fact.*

# SAP cyber risk is 24×7.
# SAP expertise rarely is.

*The path forward is not ungoverned AI. It is SAP-aware autonomous operations with expert-defined boundaries, approved playbooks, and continuous proof.*

**Register for the series and see SecureOps in action**

## *Q&A*

*Detect. Decide. Remediate. Autonomously.*