From Compliance to Continuous Cyber Resilience



A webinar by IT-Conductor

WEDNESDAY, SEPTEMBER 9TH, 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 day after Patch Tuesday

A new SAP security release is not a compliance artifact. It is an operational decision trigger.

SEPT 8

SAP publishes security notes. The compliance calendar says "next audit." Attackers read the same release notes.

Do we patch now?

- Could introduce outage
- May require downtime
- Needs owner and approval

Do we compensate?

- Tighten access
- Reduce exposure
- Increase monitoring

Can we prove control?

- Evidence trail
- Exception expiry
- Risk trend updated

Every Patch Tuesday should become a continuous resilience loop, not a monthly scramble.

WHY NOW

Compliance is periodic. SAP cyber risk is continuous.

Frameworks matter — but they do not automatically run SAP-safe remediation.

ISO

Policies, scope, risk treatment, management review

NIST

Govern, identify, protect, detect, respond, recover

CIS

Continuous vulnerability management and prioritized controls

SOC 2

Evidence of control design and operating effectiveness

1 **Periodic evidence** → 2 **Continuous validation** → 3 **Continuous remediation** → 4 **Continuous reporting**

Compliance asks: "Can we demonstrate control?" Resilience asks: "Are controls working right now?"

WHAT YOU'LL WALK AWAY WITH

By the end, attendees should know what to change before the next patch cycle

1

Translate

compliance into SAP control objectives

2

Turn

Patch Tuesday into an autonomous triage loop

3

Operationalize

continuous validation, remediation, reporting

4

Define

safe decision boundaries for autonomous actions

WHERE THIS FITS

Webinar #9 turns autonomous action into continuous assurance

The series now moves from capability to governance and evidence.

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

After showing how SAP systems can be patched, analyzed, and remediated autonomously, episode #9 answers the board-level question: "How do we prove resilience continuously?"

THREE ROLES, ONE OUTCOME

Compliance, security, and SAP operations need the same source of truth

The failure mode is not lack of frameworks — it is fragmented execution.

GRC / Audit

"I need evidence that controls are operating — not just designed."

Needs: control mapping, exceptions, proof, trend reporting

SOC / Security

"I see risk, but I need SAP context and a safe next step."

Needs: correlation, triage, severity, response path

SAP Basis / Platform

"I can remediate, but I need prioritization and change-safe orchestration."

Needs: applicability, pre-checks, windows, rollback

Who owns continuous SAP cyber resilience today?

AUDIENCE POLL

Where does SAP security compliance break down today?

Live poll #1

- **A** Framework mapped, but not operationalized
- **B** Controls tested annually or quarterly
- **C** SAP context missing from SOC evidence
- **D** Patch exceptions live in spreadsheets
- **E** No continuous executive resilience score

CORE THESIS

The shift: from audit preparation to resilience operation

The compliance program should be continuously fed by real SAP cyber operations.

Compliance mode

- Periodic assessment
- Manual evidence collection
- Point-in-time remediation status
- Exception tracking after the fact

Resilience mode

- Continuous validation
- Automated evidence capture
- Risk-ranked remediation queue
- Exceptions with owner and expiry

The goal is not more audit activity. The goal is an operating model that keeps evidence current because controls are continuously exercised.

THE TRIGGER

SAP Security Patch Day should start a closed-loop workflow

September 8 is the trigger; September 9 should be the decision checkpoint.

1	2	3	4	5
Release	**Correlate**	**Decide**	**Remediate**	**Prove**
SAP notes, CVEs, priority	SID, component, version, exposure	Patch, compensate, defer, close	Automated safe playbook	Evidence, score, report

Patch Tuesday is not the end of compliance. It is the beginning of continuous validation and remediation.

THE BOTTLENECK MAP

Where periodic compliance fails continuous SAP risk

The weak point is usually the handoff between evidence, decision, and remediation.



Question for attendees: which link is weakest in your SAP landscape — requirement mapping, detection, decision, remediation, or proof?

THE MISSING LAYER

Generic compliance controls become actionable only when mapped to SAP reality

SACO translates control intent into SAP-aware operational decisions.

Control intent

- NIST / CIS / ISO / SOC 2
- Patch management
- Access controls
- Logging and monitoring

SAP context

- SID / client / role
- Kernel / component level
- Business criticality
- Change window

Governed action

- Patch now
- Compensate
- Escalate
- Defer with expiry
- Prove closure

THE OPERATING MODEL

Detect. Decide. Remediate. Prove. Continuously.

A continuous cyber resilience loop for SAP.

1	2	3	4	5
Detect	**Validate**	**Decide**	**Remediate**	**Prove**
Collect SAP-aware signals	Map to controls and systems	Rank risk and choose path	Orchestrate approved action	Update evidence and score

Operating principle: compliance evidence is generated as a byproduct of governed SAP cyber operations.

CONTINUOUS VALIDATION

Know whether SAP controls are working right now

Validation turns control requirements into live posture checks.

Validate platform

Kernel, HANA, OS, agent, cloud, network, backup state

Validate configuration

Security parameters, audit log, RFC, services, interfaces

Validate application

SAP Notes, custom code, transports, exposed components

Validate IAM

Users, roles, privileges, SoD, anomalous activity

Continuous validation answers: "Which controls are effective, degraded, or unknown?"

CONTINUOUS REMEDIATION

Remediation should not wait for the audit finding

SACO converts validated gaps into governed action paths.

1	2	3	4	5
Patch now	**Compensate now**	**Escalate**	**Defer with expiry**	**Close**
Applicable, critical, exposed, change-safe	Patch blocked, exposure must be reduced	Policy boundary exceeded or expert review required	Business exception, owner, due date, proof	Not applicable or already remediated

Autonomy is not just "apply the patch." It is making the safest governed decision at the speed of risk.

CONTINUOUS REPORTING

Evidence should be current before the auditor asks

Continuous reporting turns cyber operations into assurance.

Evidence package

Finding, owner, approval, pre/post checks, logs, validation, closure

Risk narrative

What changed, why it mattered, what action was taken, what remains

Executive score

Resilience trend across platform, configuration, application, IAM

Reporting moves from "collect screenshots later" to "prove control as part of the workflow."

THE TRUST LAYER

Autonomous does not mean unapproved

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

- Control mapping
- Approval policy
- Change windows
- Exception expiry
- Rollback plan
- Evidence capture

DECISION BOUNDARY

Inside boundary: execute. Outside boundary: escalate.

USE CASE 1

Patch Tuesday control validation

Move from “SAP released notes” to “we know what applies and what we did.”

1	2	3	4	5
Ingest	**Map**	**Rank**	**Act**	**Report**
SAP Security Notes and CVE data	Components, versions, SIDs, clients	CVSS, exposure, criticality, compensating controls	Patch, compensate, defer, close	Evidence, score, open risk

Patch management becomes a continuous control, not a monthly spreadsheet reconciliation.

USE CASE 2

Continuous audit readiness

Controls become evidence-producing workflows.

Control objective	Operating workflow	Evidence object	Report
Example: critical SAP security fixes are evaluated and remediated within defined SLA	Detect release, validate applicability, approve path, execute, verify	Finding, decision rationale, owner, approval, logs, validation, exception status	Control health, risk trend, audit pack

The best audit packet is the one produced automatically by good operations.

USE CASE 3

Executive cyber resilience score

Give leadership a current view of SAP resilience, not an old audit snapshot.

Platform

Patch baseline, HA readiness, backup, OS/HANA exposure

Configuration

Hardening status, audit logging, secure parameters

Application

SAP Notes, custom code, transports, exposed services

IAM

Privileged access, SoD, user anomalies, RFC trust

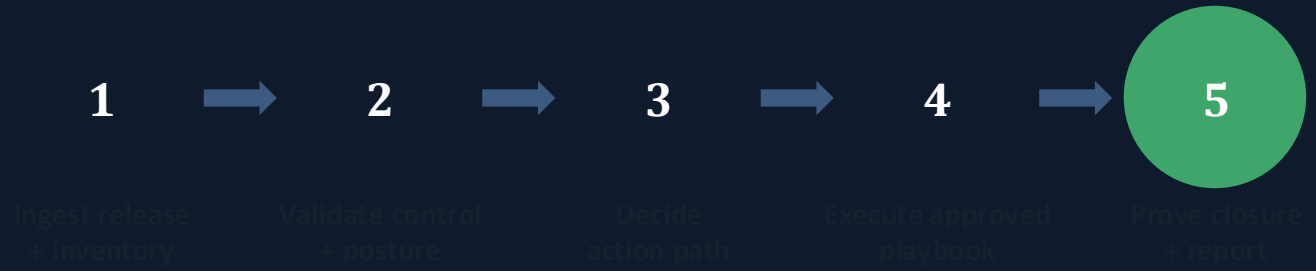
Executives do not need every SAP note. They need exposure trend, remediation velocity, exception aging, and proof completeness.

DEMO SCENARIO

September Patch Tuesday resilience simulation

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

A new SAP Security Note is released on September 8. SecureOps detects applicability to a production SAP component and initiates governed triage.



See how compliance evidence is generated while SAP cyber risk is reduced.

DEMO · STEP 1 OF 5

Ingest and normalize

Turn patch releases and internal telemetry into one SAP-aware finding.

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

The first resilience outcome is not a ticket. It is a finding with SAP context, owner, SLA, and evidence trail.

DEMO · STEP 2 OF 5

Validate applicability and control state

The system determines what applies before humans debate what matters.

Component match

Installed product, add-on, kernel, library, 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 / compensating control present / expert review required.

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. Autonomous only inside pre-defined boundaries.

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, SLA status	Rules refined, playbook updated, exception trend captured

The auditor asks: "Can you prove the right action happened under the right control?"

MEASURING THE SHIFT

Metrics that show continuous resilience, not only compliance activity

Measure reduced exposure and stronger proof.

MTTD

Mean time to detect SAP-relevant risk

MTTA

Mean time to assess applicability

MTTDc

Mean time to decision

MTTR/C

Mean time to remediate or compensate

Proof %

Evidence completeness for closed findings

Exception age

Open risk aging and expiry discipline

Executive translation: reduce unresolved exposure windows while increasing auditability.

GETTING STARTED

The 30-day action plan

A practical path from compliance posture to continuous resilience.

Week 1

Map control objectives

to SAP risk scenarios

Week 2

Build applicability workflow

for Patch Tuesday

Week 3

Pilot governed remediation

and compensating controls

Week 4

Create continuous evidence

and SACO score report

THE EXECUTIVE ARGUMENT

What changes when SecureOps is in place

The operational before/after executives need to hear.

Before

- Compliance evidence is
- reconstructed after the fact.
- Patch risk is triaged manually.
- Exceptions age in spreadsheets.
- Executives see point-in-time status.

After

- SAP controls are continuously
- validated. Patch Tuesday triggers
- governed decisions. Remediation and
- exceptions are tracked. Evidence and scores stay current.

Autonomous SAP cyber operations turns compliance from a periodic project into a continuous resilience capability.

Compliance proves intent. Continuous cyber resilience proves readiness.

Use SAP Patch Tuesday as the recurring trigger to Detect, Decide, Remediate, and Prove — continuously.

Request a demo

Q&A

Detect. Decide. Remediate. Autonomously.