A webinar by IT-Conductor

WEBINAR #11

The Economics of Autonomous SAP Cyber Operations

Reducing risk. Optimizing resources.
Creating business value.



Wednesday, September 23, 2026



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



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



COLD OPEN

The invoice nobody sees until it's too late

Ransomware and outages disrupt the business. Patch delays extend the exposure window. Manual security work quietly consumes your scarcest SAP hours.

WHAT IT COSTS WHEN IT GOES WRONG

- Unplanned downtime on a production SID
- Ransomware containment and recovery
- Emergency, after-hours remediation

WHAT IT COSTS EVERY DAY IT DOESN'T

- Specialists doing repetitive manual triage
- Patch backlogs that quietly extend exposure
- Audit season scrambles for evidence

Episode hook: the finding gets fixed either way. The question is whether it costs you a weekend, a headcount, or a board conversation.

WHY NOW

SAP cyber risk finally has a seat at the budget table

Security spend is under more scrutiny than ever and SAP is where the scrutiny lands hardest.

INSURANCE

Cyber insurers increasingly require provable, continuous controls — not a point-in-time checklist.

HEADCOUNT

SAP-specific security skills remain scarce and slow to hire, even when budget is approved.

COMPLIANCE

Frameworks now expect continuous evidence, not an annual snapshot handed to an auditor.

BUDGET

Security spend is flat or shrinking while the SAP attack surface keeps growing.

1 **Cost of inaction**

2 **Cost of manual ops**

3 **Cost of detection tools**

4 **Value of autonomy**

The tools already exist. What's missing is a way to show what they're worth — in dollars, not just alerts closed.

WHAT YOU'LL WALK AWAY WITH

Four things this session covers

1

See

the true cost stack behind SAP cyber operations

2

Understand

how automation changes the unit economics

3

Learn

a simple framework for building your own ROI case

4

Leave with

a 30-day plan to start the conversation internally

WHERE THIS FITS

Webinar #11 puts a number on everything the series has built

Every prior episode becomes a line item in the economics we build today.

#7	#8	#9	#10	#11
AI agents for SAP security	Without 24×7 experts	Compliance to resilience	Building the SOC	The economics

Decisions, agents, scarce expertise, and continuous resilience all have a cost — and a cost of not having them. Today we put that in dollars.

THREE ROLES, ONE NUMBER

CISO, CFO, and SAP platform owner all ask the same question differently

Each role feels the cost from a different angle.

CISO / SOC Leader

“What does a breach or missed patch actually cost us?”

Needs: risk quantification, defensible metrics for the board

CFO / Finance

“Why does security keep asking for more headcount and tools?”

Needs: a clear cost-avoidance and productivity case

SAP Basis / Platform Owner

“I'm the one doing the manual work no one sees.”

Needs: proof that automation gives time back, not just more dashboards

AUDIENCE POLL

What's the biggest hidden cost in your SAP security program today?

Live poll #1

- A — Manual remediation labor
- B — Compliance & audit prep
- C — Delayed patch / extended exposure
- D — Outsourced or contracted security experts
- E — Tool sprawl & duplicate licensing
- F — Cyber Insurance

CORE THESIS

The shift: from a security cost center to a measurable P&L line

SecureOps doesn't just close findings — it changes what each finding costs to close.

COST-CENTER MODEL

- Spend is a sunk cost
- Value is hard to defend at renewal
- Manual work scales with headcount, not with risk
- ROI is anecdotal

MEASURABLE MODEL

- Spend maps to hours reclaimed and risk reduced
- Renewal makes the case with its own data
- Automation scales with risk, not headcount
- ROI is a number you can show the board

The goal isn't a smaller security budget. It's a security budget that visibly buys down risk.

THE COST STACK

Five cost categories most organizations never add up

SAP cyber risk isn't one line item, it's a stack.

1

Downtime & incident cost

Ransomware containment, recovery, and lost transactions on a production SID.

2

Delayed remediation cost

Every day of extended exposure carries risk that compounds, not resets.

3

Manual labor cost

Scarce SAP specialists spending hours on repetitive triage instead of higher-value work.

4

Detection-tool cost

Licenses for tools that find issues but stop short of closing them.

5

Compliance & audit cost

Internal evidence-gathering time, plus external auditor fees, repeated every cycle.

THE HIDDEN COST OF MANUAL COMPLIANCE

Compliance is often the least visible line item and one of the largest

Continuous frameworks turned point-in-time audits into a recurring tax.

WHAT IT USED TO BE

- Annual or quarterly audit
- Spreadsheet evidence, gathered once
- One auditor conversation

WHAT IT'S BECOMING

- Monthly or continuous attestation
- Evidence gathered manually, every cycle
- Internal team plus external auditor, repeated

Every cycle spent gathering evidence by hand is a cycle not spent reducing risk.

WHAT CHANGES THE ECONOMICS

Detect. Decide. Remediate. Prove. — priced at every stage

The same operating loop from Webinar #10, now with a cost lens on each stage.

1

Detect

Continuous, not a quarterly scan, it avoids the cost of a missed window

2

Decide

AI-assisted scoring replaces hours of manual triage

3

Remediate

Governed automation replaces after-hours firefighting

4

Prove

Evidence generated automatically, not assembled by hand each cycle

Operating principle: every stage you automate removes a recurring labor cost, not just a one-time fix.

BUILDING THE BUSINESS CASE

A simple framework for modeling your own ROI

Four numbers, compared side by side.

A

Cost of inaction

Probability-weighted cost of a critical incident or a missed patch window.

B

Cost of manual operations

Loaded cost of the specialist hours spent on triage and remediation today.

C

Cost of detection-only tools

Licenses for tools that surface findings but don't carry them to closure.

D

Cost of autonomous operations

Platform cost, offset by hours reclaimed and risk reduced.

The business case isn't "security vs. no security." It's which of these four you're already paying for and how much of it is invisible.

WORKED EXAMPLE

Illustrative model: closing a 12-point resiliency gap

Figures are illustrative, based on IT-Conductor's SRI effort-estimation model — not a specific customer.

A system scoring 68 (Moderate) targets 80 (Strong). The resiliency model estimates the engineering hours, downtime, and systems involved — the same inputs that go into a cost comparison.

1

Baseline the gap

2

Price the manual path

3

Price the automated path

4

Compare the two

5

Show the payback

WORKED EXAMPLE · STEP 1 OF 5

Baseline the gap

Start with what the resiliency model already estimates.

68 Current SRI (Moderate)	**80** Target SRI (Strong)	**142 hrs** Estimated engineering effort
6 hrs Estimated downtime	**43** Critical vulnerabilities removed	**14** Affected systems

This is the same estimate the platform produces automatically — no separate exercise required.

WORKED EXAMPLE · STEP 2 OF 5

Price the manual path

142 hours doesn't happen in one sitting — it happens in a scramble across teams.

Base effort	142 hours × blended specialist rate
Coordination overhead	Context-switching across Basis, security, and change management
Extended-timeline risk	Every week of delay is another week of exposure

The hours are the same. The cost is higher because manual work is interrupted, escalated, and re-explained.

WORKED EXAMPLE · STEP 3 OF 5

Price the governed-automation path

Same 142 hours of work — executed as one coordinated, approval-gated cycle.

- Pre-checks, approval, and execution run back-to-back, not queued behind other tickets
- Fewer people needed to babysit the change window
- Downtime compressed toward the estimated 6 hours, not extended by rework

Automation doesn't remove the work. It removes the friction around the work.

WORKED EXAMPLE · STEP 4 OF 5

Compare the two paths

Same starting point, same target — different cost of getting there.

MANUAL PATH

- Longer timeline, queued behind other work
- More people touched per finding
- Evidence assembled after the fact

AUTOMATED PATH

- Compressed timeline, one coordinated cycle
- Fewer people, approval-gated execution
- Evidence captured automatically, as it happens

The gap between the two paths is the number you bring to the budget conversation.

WORKED EXAMPLE · STEP 5 OF 5

Show the payback

Multiply this one gap by every system in the landscape, every cycle, every year.

One resiliency gap, priced once.
Now multiply it by every system, every patch cycle, every audit period — that's the number that changes the conversation.

MEASURING THE SHIFT

Metrics that show economics, not just activity

Track cost and time, not just findings closed.

156+ hrs

Hours reclaimed annually through automation

MTTR

Reduced from hours to minutes on known findings

Cost / finding

Blended cost to take one finding to closure

Audit prep time

Hours spent assembling evidence per cycle

Cost / cycle

Blended cost per remediation cycle, manual vs. governed

Coverage %

Share of signal sources producing SAP-specific action

Executive translation: the story isn't “we closed more tickets.” It's “we spend less to close each one — and can prove it.”

GETTING STARTED

The 30-day plan to build your own business case

A practical path to putting a number on your SAP security economics.

Week 1

Baseline today's costs

Manual hours, tool spend, audit prep time

Week 2

Estimate the cost of inaction

One recent incident or missed patch window, priced

Week 3

Pilot governed automation

One use case, hours reclaimed measured

Week 4

Present the model

Side-by-side comparison, ready for budget season

THE EXECUTIVE ARGUMENT

What changes when the economics are visible

The before/after executives need to hear.

BEFORE

- Security spend is a request, defended case by case
- Cost of inaction is invisible until it happens
- Manual hours scale with headcount
- ROI is anecdotal

AFTER

- Security spend maps to hours reclaimed and risk reduced
- Cost of inaction is modeled ahead of time
- Automation scales with risk, not headcount
- ROI is a number you can show the board

You don't need a bigger budget. You need a budget that shows its own math.

Your SAP security program already has a cost. Now you can see it.

Model your own numbers with a Cost of Inaction assessment — baseline your manual effort, tool spend, and exposure, and see what governed automation is worth in your environment.

Request a Cost of Inaction Assessment

Q&A

Detect. Decide. Remediate. Autonomously.