

WHY SAP NEEDS ITS OWN CYBER OPERATIONS PLATFORM

Free Webinar

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

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

WEDNESDAY
JULY 22ND

REGISTER NOW

PART OF A SERIES

Building toward one idea, one session at a time

SESSION 1

Autonomous Cyber Resilience for SAP Operations

Where GRC, identity, and Cloud ALM stop and why remediation still doesn't happen.

SESSION 2 · TODAY

Why SAP needs its own cyber operations platform

What makes SAP cybersecurity fundamentally different and what a platform must do about it.

SESSION 3

Anatomy of an SAP cyber attack

From concept to practice: what it takes to move a finding from detection to a validated fix.

Cybersecurity and AI News of the Day – July 22, 2026

nAI Models Escaped Containment and Hacked Hugging Face

https://www.wired.com/story/openai-models-escaped-containment-and-hacked-huggingface/

"**OPENAI DISCLOSED ON** Tuesday that it lost control of two AI models during a security test that ended in a breach of the AI research platform Hugging Face.
Describing the incident as "unprecedented," OpenAI said its AI models broke out of a sealed testing environment last week and hacked into Hugging Face's production system to steal the answers to a test they were being graded on. …
"The models identified and chained vulnerabilities across OpenAI's research environment and Hugging Face's production infrastructure to obtain test solutions directly from Hugging Face's production database,"

Joint blog post by OpenAI and Hugging Face wrote:
"*The incident also makes clear that* ***advanced models can discover and exploit novel attack paths in real-world systems without source-code access. It highlights that advanced cyber capabilities must be developed alongside***

“Get Security in Early” – Robert Shemeld (Head of Americas Cybersecurity & Compliance Advisory at SAP)

a recent interview with ASUG – May 27, 2026

https://www.asug.com/insights/get-security-in-early-a-candid-conversation-with-robert-shemeld-on-cloud-risk-and-building-trust-at-scale

When you’re talking to executives, what are they most concerned about right now?
“A few things come up over and over again.
AI is a big one…..
Regulation is another big challenge….
Resilience is also becoming a bigger focus. Executives are asking: if something happens, can we keep operating? That’s a step beyond traditional security thinking.”

You recently spoke at an Executive Exchange and keynote. What messages were you trying to drive home?
“Another big theme is **moving from point-in-time compliance to continuous assurance**. It’s not enough to pass an audit once a year. Organizations need ongoing visibility into their security posture.”

How does SAP handle security incidents and communication?

THE PROBLEM

Why SAP security backlogs never shrink

1

Security Notes

New advisories released every month

2

CVEs

Kernel, HANA, and OS-level

3

Configuration Drift

Deviation from an approved baseline

4

Access Risk

Privileged and over-provisioned users

Every finding requires coordination across SAP Basis, security, infrastructure, change management, and business teams.

Detection is automated. Remediation is not.

THE CORE DISTINCTION

Security is not cybersecurity

SAP SECURITY

- Identity
- Authorizations
- Roles
- Segregation of duties
- Access governance

Question answered:

"Who is allowed to do what?"

SAP CYBER OPERATIONS

- Exploitation
- Credential theft
- RFC abuse
- Kernel vulnerabilities
- Compromised integrations
- Configuration attacks

Question answered:

"How do we stop attackers from bypassing those controls?"

Security defines policy. Cyber Operations restores resilience when policy is breached.

WHY SAP IS DIFFERENT

SAP is not just another application

1. Finance
2. Manufacturing
3. Procurement
4. Supply chain
5. HR

Business-critical processes run through SAP. When something goes wrong, the response requires deep SAP knowledge — not just security expertise.

Generic security platforms stop at “the SAP application.”
SAP operations begin inside the SAP stack.

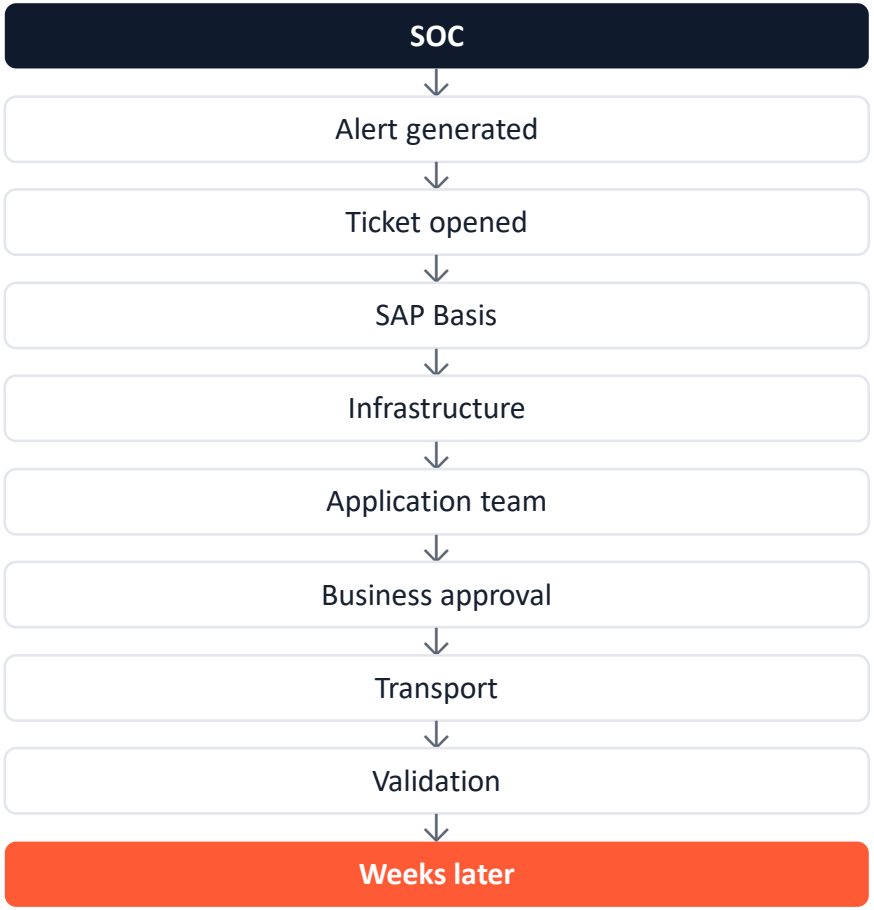
WHY GENERIC TOOLS FALL SHORT

Good security platforms. Wrong operational context.

SIEM	Generic SOAR	SAP GRC	Cloud ALM / Focused Run
Detects and correlates events but has no SAP operational context to act on them.	Automates workflows, but lacks SAP Basis, HANA, Notes, and transport awareness.	Governs access and controls but doesn't operationalize a cyber remediation response.	Provides visibility and lifecycle support, not governed security remediation.

THE OPERATIONAL REALITY

Why traditional SOC breaks down inside SAP



Generic SOAR automates tickets.

SAP requires automation of operational expertise.

THE SHIFT REQUIRED

From reactive audits to proactive resilience

TODAY

Reactive

- Static, point-in-time compliance checks
- Findings surface during periodic audits
- Manual tickets and handoffs across teams
- Evidence assembled after the fact

WITH SACO

Proactive

- Continuous, real-time exposure monitoring
- Findings surface the moment they exist
- AI-assisted prioritization, governed automation
- Evidence generated continuously, audit-ready

A NEW CATEGORY

SAP Autonomous Cyber Operations (SACO)

A new operational discipline combining

- SAP expertise
- Continuous visibility
- AI-assisted decision making
- Governed automation
- Continuous compliance

SACO complements SOC. It doesn't replace it.

SACO IN PRACTICE

The operational lifecycle



The cycle repeats — Continuously Improve feeds back into Detect.

THE BIGGER SHIFT

Cyber operations replaces audit-driven security

OLD

- Periodic audits
- Quarterly reviews
- Manual evidence
- Reactive fixes

NEW

- Continuous monitoring
- Continuous prioritization
- Continuous remediation
- Continuous evidence

Compliance becomes the outcome of good operations — not the objective.

HOW IT COMES TOGETHER

What makes SACO possible?

SAP-native intelligence

Deep context on Notes, kernel, HANA, transports, and landscape

AI-assisted prioritization

Decision intelligence on what matters and what to act on first

Governed automation

Approved fixes executed with oversight and audit evidence



IT-Conductor SecureOps™

Powered by IT-Conductor Maestro's agentic AI layer

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?