A WEBINAR BY IT-CONDUCTOR

ANATOMY OF AN SAP CYBER ATTACK



FREE WEBINAR

WEDNESDAY, JULY 29TH,2026

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

HOSTED BY LINH NGUYEN,
CEO, AND CO-FOUNDER OF IT-CONDUCTOR

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

Why SAP needs its own cyber operations platform

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

SESSION 3 · TODAY

Anatomy of an SAP cyber attack

A realistic attack path from compromised credentials to business disruption and how SACO responds.

DISCLAIMER

For educational purposes only

All vulnerability details, attack techniques, and exploitation methods shown in this session are provided strictly for educational and awareness purposes.

Nothing in this presentation is intended to enable, encourage, or condone unauthorized access, testing, or exploitation of any system without explicit, written permission.

Always act in accordance with your organization's security policies and applicable law.

BEFORE THE WALKTHROUGH

A cyberattack is a sequence, not an event

It moves from a compromised account to business disruption — one connected chain, not a single alert.

Traditional tools may catch isolated indicators along the way. They struggle to connect the full path inside an SAP environment.

Today, we walk that path stage by stage and show where visibility breaks down, and how it's restored.

THE ATTACK CHAIN

Seven stages, one continuous path



From a single compromised credential to a business-critical incident — each stage looks routine in isolation.

THE ATTACK CHAIN · PHASE 1 OF 3

Access & escalation

1 Compromised Admin Account

WHAT HAPPENS

An attacker gains access to a privileged SAP account, often through credential theft or phishing.

DETECTION GAP

Looks like a normal login. No SAP-specific context flags the privilege at risk.

2 Privilege Escalation

WHAT HAPPENS

Access expands beyond the original account's scope through added roles or authorizations.

DETECTION GAP

Authorization changes rarely trigger alerts outside SAP-native logs.

THE ATTACK CHAIN · PHASE 2 OF 3

Lateral movement

3 RFC Abuse

WHAT HAPPENS

Remote Function Call connections are used to move between systems with trusted access.

DETECTION GAP

RFC traffic looks like normal system-to-system communication to a generic SOC.

4 Malicious Transports

WHAT HAPPENS

Unauthorized code or configuration changes move through the transport system into production.

DETECTION GAP

Transports are an SAP-specific mechanism, invisible to standard change tools.

THE ATTACK CHAIN · PHASE 3 OF 3

Exploitation & impact

5 Kernel Exploitation

WHAT HAPPENS

The attacker targets the SAP kernel or OS layer to gain deeper system control.

DETECTION GAP

Kernel-level activity requires SAP Basis expertise most SOC teams don't have.

6 Data Exfiltration

WHAT HAPPENS

Business-critical data — financial, customer, or operational — is extracted from the system.

DETECTION GAP

Data movement inside SAP often bypasses network-layer DLP tools.

7 Business Disruption

WHAT HAPPENS

Operations are interrupted, data is corrupted, or business processes are taken offline.

DETECTION GAP

By the time impact is visible, the attack has already succeeded.

THE REVEAL

Where traditional SOC, SIEM, and SOAR lose visibility

- Privileged access & role changes
- RFC communication between systems
- Transport-based code and config changes
- Kernel and OS-layer activity
- Data movement inside SAP

Each blind spot looks routine on its own. Together, they're an attack.

HOW SECUREOPS RESPONDS

Detect. Correlate. Orchestrate.

1

Detect

Continuously monitor SAP-specific activity — RFC, transports, authorizations, kernel — that generic tools miss.

2

Correlate

Connect isolated events into a single attack narrative across the full SAP stack.

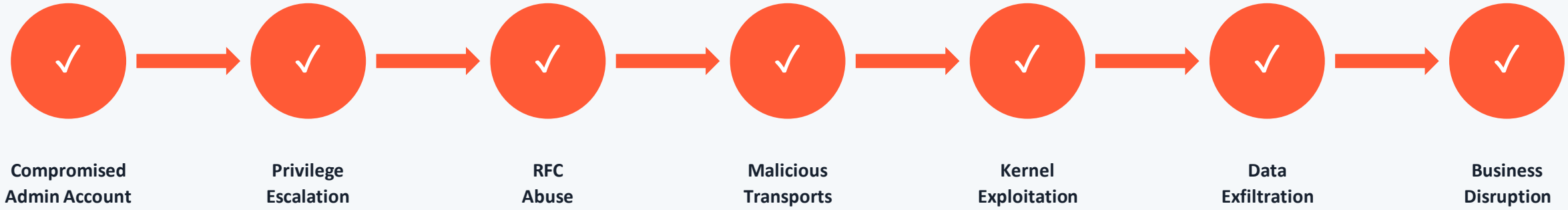
3

Orchestrate

Trigger a governed remediation response, with approval gates and audit evidence.

FULL CIRCLE

Visibility restored across the full chain



Every stage — visible, correlated, and actionable. SecureOps turns seven blind spots into one governed response.

WHY TIMING MATTERS

“By the time business impact is visible, the attack has already succeeded.”

SAP Autonomous Cyber Operations closes the gap earlier — at the stages where detection still has time to matter.

COMING UP

This is session 3 of the series

SAP AUTONOMOUS CYBER OPERATIONS

More sessions are on the way

We're continuing to build out SAP Autonomous Cyber Operations as a series — stay registered for details on what's next.

Watch your inbox for the next session announcement.

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?