IT-Conductor SecureOps

AUTONOMOUS SAP SECURITY OPERATIONS

About IT-Conductor SecureOps

IT-Conductor SecureOps is IT-Conductor's SAP Autonomous Cyber Operations platform. It combines SAP-native monitoring, AI-assisted decision intelligence, and governed automation to help SAP, security, and compliance teams move from detection to remediation — without replacing the SIEM, GRC, or Cloud ALM tools already in place.

Product Overview

IT-Conductor SecureOps continuously monitors SAP Security Notes, CVEs, configuration drift, and privileged access risk, then correlates findings into a single, governed remediation workflow — with approval gates and audit-ready evidence at every step.

Key Features

- **SAP-Native Detection:** Continuously monitors SAP Security Notes, CVEs, configuration drift, and access risk across on-premise, RISE, and BTP landscapes.
- **AI-Assisted Prioritization:** Correlates findings and ranks what matters most, so teams act on real risk first.
- **Governed Automation:** Executes approved remediation playbooks with human approval gates before changes go live.
- **Audit-Ready Evidence:** Captures evidence continuously, so compliance becomes a byproduct of operations, not a scramble.
- **Works With What You Have:** Complements SIEM, GRC, and Cloud ALM rather than replacing them.

How it works?

IT-Conductor SecureOps operates as a continuous cycle across your SAP landscape — from on-premise ABAP systems to BTP and RISE. The following steps outline how a finding moves from detection to a governed, evidenced fix:

1.Detect:

- SecureOps continuously monitors SAP Security Notes, CVEs, configuration drift, and privileged access across the landscape.

2.Correlate:

- Findings are connected into a single risk picture, cutting through noise from disconnected tools.

3.Prioritize:

- AI-assisted analysis ranks findings by real risk and business impact, surfacing what to act on first.

4.Decide:

- Recommended remediation actions are proposed, mapped to the approval workflows already in place.

5.Remediate:

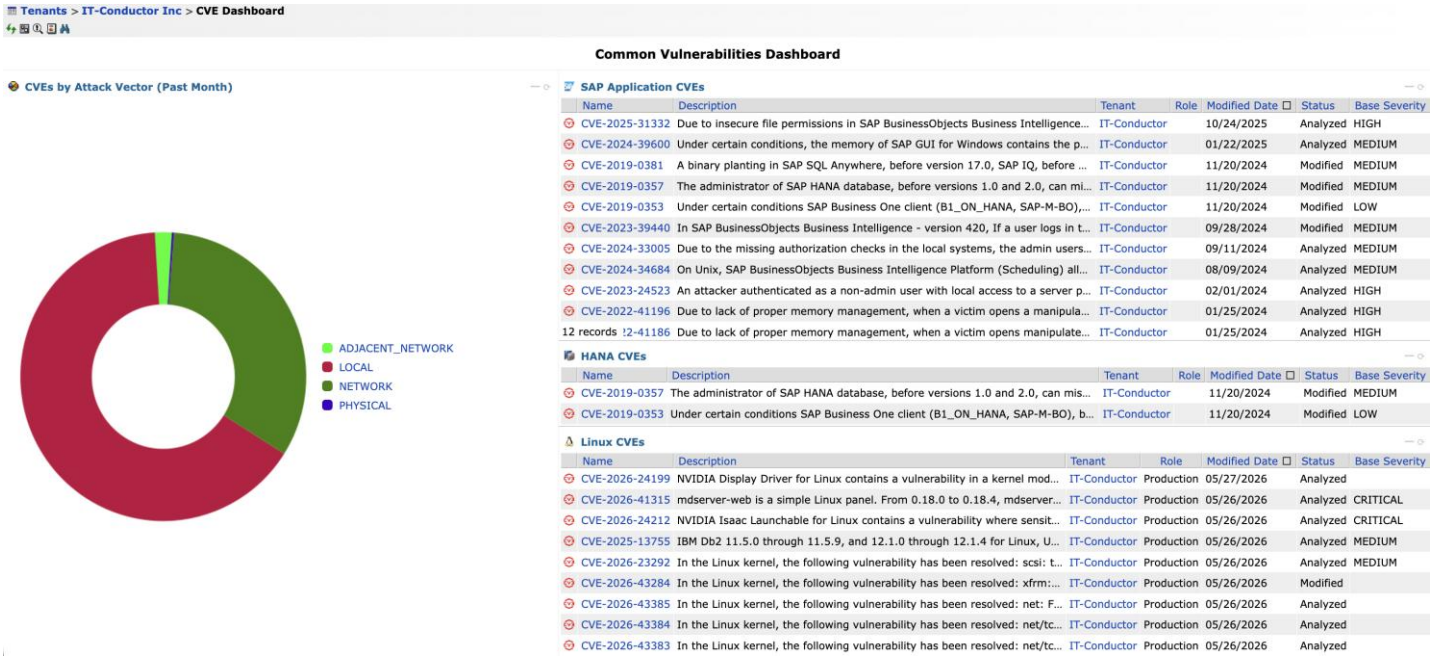
- Approved fixes are executed through governed automation — patches, parameter changes, or access updates — with human sign-off at each gate.

6.Validate & Evidence:

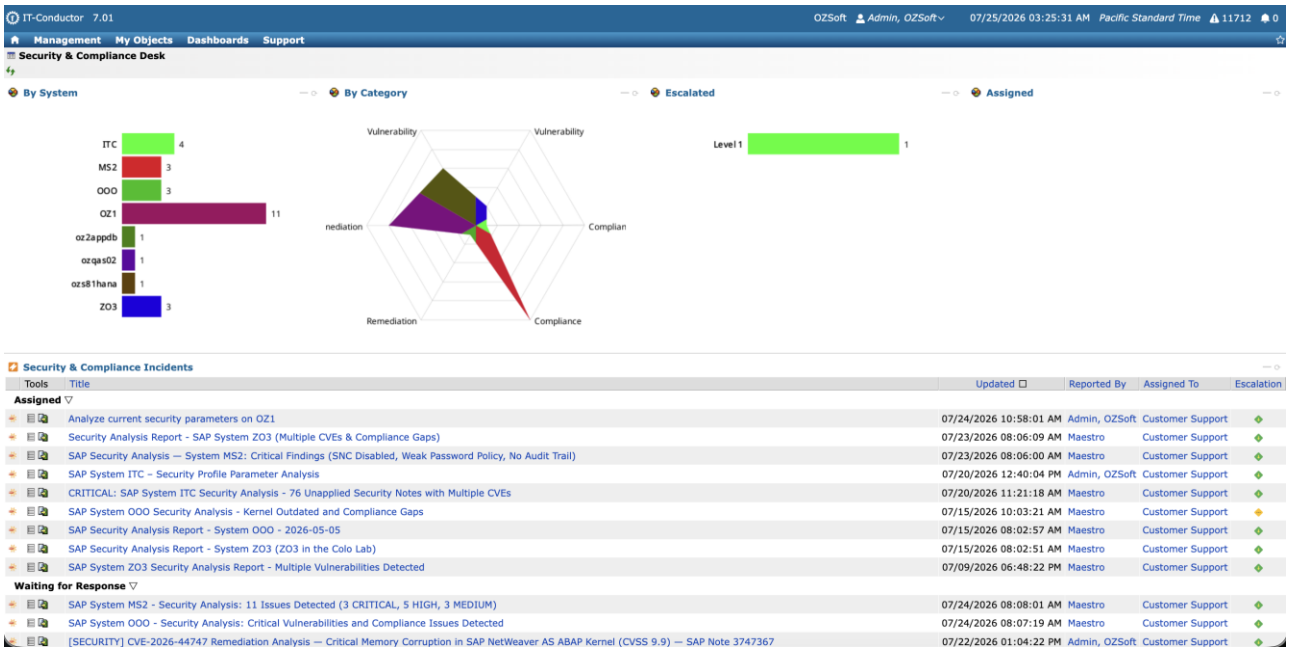
- Every action is validated after remediation, with evidence captured automatically for audit and compliance reporting.

SecureOps in Action:

Continuous visibility: SAP, HANA, and Linux CVEs in one dashboard

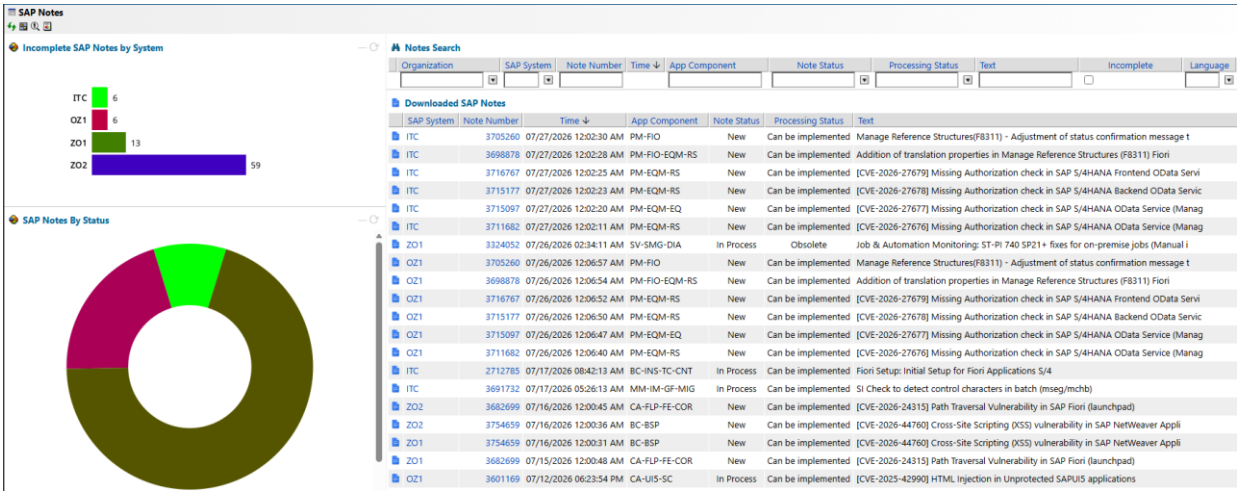


Every open finding, triaged and assigned from the Security & Compliance Desk

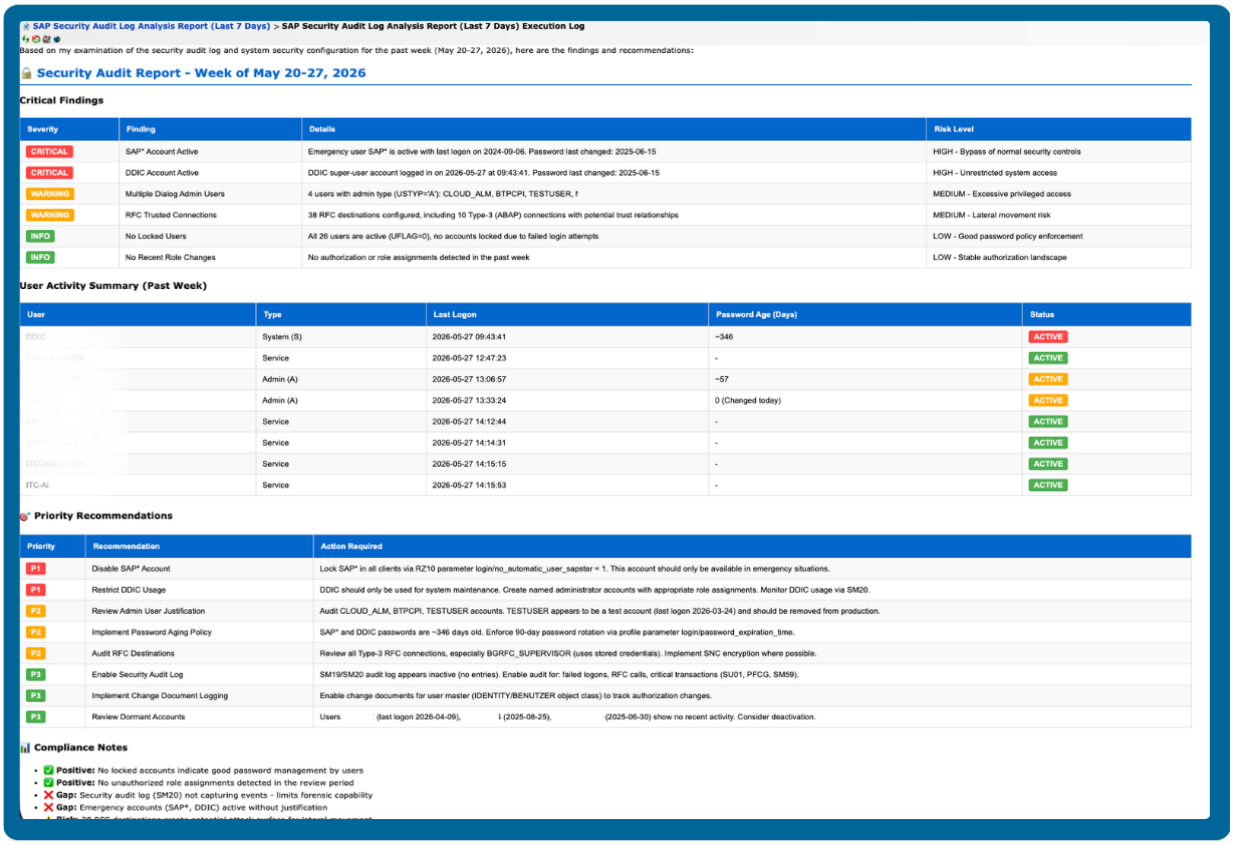


SecureOps in Action:

SAP Notes tracked and prioritized across every system, in one view



SecureOps reviews the security audit log and system configuration, then produces critical findings, risk ratings, and prioritized recommendations without a manual review.



AI-ranked recommendations, mapped to each finding, with the action required spelled out

SecureOps in Action:

A detected vulnerability becomes a governed incident — automatically.
Note: *SecureOps opens a tracked incident with severity, CVSS score, affected component, and full context — ready for approval and remediation.*

Escalation, severity, and CVSS scoring are captured automatically from the underlying finding.

Priority Remediation Roadmap

Priority	Action	Ref	Effort
P0 — Immediate	Set login/no_automatic_user_sapstar=1	C1 / SAP Note 3186820	Low
P0 — Immediate	Implement SAP Notes 3716767, 3715177, 3715097 (OData Auth CVEs)	S4CORE / SAP_GWFND	Medium
P0 — Immediate	Activate virus scan profile /SOAP_CORE/WS_RECEIVE	CCMS FU9 Alerts	Low
P1 — Urgent	Set password expiration policies (C2-C5)	RZ10 profile changes	Low
P1 — Urgent	Disable sapgui/user_scripting (set to FALSE)	H1 / SAP Note 1707360	Low
P1 — Urgent	Enable SNC (snc/enable=1) and configure sapcrypto	H2	High
P1 — Urgent	Set icf/set_HTTPonly_flag_on_cookies=1	H3	Low
P2 — Short-term	Implement SAP Notes 3601169, 3676970 (SAPUI5 CVEs)	SAP_UI 816	Medium
P2 — Short-term	Investigate RFC logon failures (SMDAGENT_OZ1, S81SLT01)	SecAuditLog / CCMS	Medium
P2 — Short-term	Enforce password complexity: login/min_password_specials=1	H4	Low
P3 — Planned	Enable SPNEGO/Kerberos SSO (spnego/enable=1)	H5	High
P3 — Planned	Set snc/only_encrypted_rfc=1 and snc/only_encrypted_gui=1	H6, H7	Medium
P3 — Planned	Enable multi-login restriction and ticket host restriction	M1, M2	Low

Detailed Security Analysis powered by IT-Conductor Maestro and dedicated Agentic AI Security Agents

SAP Security Posture Analysis — OZ1 (July 14, 2026 Patch Tuesday)

Generated 2026-07-14 by IT-Conductor Security Analytics Agent | Target System: OZ1 (Object 6619108743471685) | Kernel 793 / SAP Release 758 / HANA DB

System Overview

SID: OZ1 — SAP Release: 758
Kernel Release: 793 — DBMS: HDB (SAP HANA)
Role: DEMO — App Host: ozs81hana
DB Host: ozs81hana (10.0.1.146) — Time Zone: GMT-07:00

Scan Summary

31	6	50	100	50	2
SAP Notes (New)	CVE-Related	CCMS Security Alerts	Sec Audit Log Events	Components	Critical Issues

Critical Security Issues Detected

CRITICAL-1: Virus scan profile /SIHTTP/HTTP_UPLOAD not active
HTTP file uploads are not being scanned for viruses. **50 CCMS alerts** with severity 255 (highest) and dozens of FU9 Security Audit Log entries confirm this is a persistent, ongoing issue. The system is exposed to malware via unscanned HTTP uploads. Detected on 2026-07-14 from 10:09:22 onwards, reported by SecurityAudit.

CRITICAL-2: Non-encrypted SAPGUI communication (TOLERATED)
Sec Audit Log entry (BUJ, severity Medium) detected on 2026-07-13 14:02:25 from host ozmain01 (10.0.1.25). SAPGUI connections are not using SNC encryption — credentials and business data traverse the network in plaintext. The "(TOLERATED)" flag indicates a known but uncorrected policy violation.

Unpatched SAP Security Notes (CVE-Related)

Note	CVE	Description	Affected Component	Severity
3713902	CVE-2026-44770	Missing Authorization check in SAP S/4 HANA (Create Single Payment)	S4CORE	HIGH
3682699	CVE-2026-24315	Path Traversal Vulnerability in SAP Fiori (launchpad)	SAP_UI	HIGH
3754659	CVE-2026-44760	Cross-Site Scripting (XSS) in SAP NetWeaver App Server	SAP_BASIS / SAP_ABA	HIGH
3407617	CVE-2024-21735	Improper Authorization check in SAP LT Replication Server	SAP_BASIS	MEDIUM
3601169	CVE-2025-42990	HTML Injection in Unprotected SAPUI5 applications	SAP_UI	MEDIUM
3676970	CVE-2025-42873	Denial of Service (DoS) in SAPUI5 (Markdown-it)	SAP_UI	MEDIUM

Added Value for SAP Basis & Security Teams

IT-Conductor SecureOps is particularly valuable for teams stretched thin across Basis, security, and compliance, providing:

- Reduced Manual Effort: Automates the SAP Security Note and CVE triage that currently consumes Basis team hours every week.
- Governed, Not Uncontrolled: Every automated fix runs through approval gates — nothing executes without sign-off.
- Works Across Deployment Models: Supports on-premise, RISE, and BTP landscapes from a single platform.
- Audit-Ready by Default: Continuously generates the evidence compliance teams currently assemble by hand.
- Built for SAP, Not Retrofitted: SAP-native context — RFC, transports, kernel, authorizations — that generic SOC, SIEM, and SOAR tools don't have.

Part of the SAP Autonomous Cyber Operations Platform

SecureOps is part of IT-Conductor's broader automation suite. Together, they provide a comprehensive SAP operations platform, including:

- IT-Conductor Maestro™: The agentic AI layer that powers SecureOps' detection, correlation, and orchestration.
- FLUX (SID Refresh): SAP-native Post Copy Automation for system refreshes and copies.
- Process Automation: Streamlining and automating routine SAP Basis and operations tasks.
- Change Request Management (ChAI): Automates the process of managing SAP change requests, ensuring traceability and compliance.
- SAP User Lock/Unlock: Automates locking and unlocking SAP users, enhancing security and administrative efficiency.

By bundling SecureOps with these automation tools, IT-Conductor delivers a single platform that spans SAP performance, operations, and cyber resilience.

IT-CONDUCTOR HEADQUARTER
20660 Stevens Creek Blvd., Suite 261
Cupertino, CA 95014
USA

Email: info@itconductor.com

Worldwide: +1 (408) 658-9998

For further information visit
http://www.itconductor.com