ONAPSIS

SAPSA

AI Is Changing How SAP Systems Get Attacked.

Here's How to Stay Ahead.

Ernest Gutierrez Roca - SAP Security Advisor
Onapsis - November 2026

Confidential & Proprietary Information of Onapsis



ONAPSIS

AGENDA

1. Introduction
2. The ‘AI Perfect Storm’
3. Attack Demos
4. Protecting Your Business — Remediation & Defense
5. Q&A

Introduction



About Hacking & Defending SAP Applications

- The session bridging theoretical risk and practical defense for SAP systems.
- Addresses critical, SAP-specific threat vectors often overlooked by traditional security teams.
- Powered by **Onapsis Research Labs (ORL)**: The undisputed leader in ERP threat intelligence with 1,000+ vulnerabilities discovered and counting...

Aims to:

- **Minimize Friction**: Align Security and SAP Basis teams.
- **Demystify the "Black Box"**: Show how threat actors leverage SAP-specific exploits.
- **Accelerate Response**: Provide specialized knowledge to detect and stop threats.



About the Onapsis Research Labs

***THE** World's SAP Security Experts Are Trusted and Consulted by Government Security Agencies and the Market*

17+ Years

In Existence as the Most Trusted SAP Threat Research Group in the World

85+ Years

Combined of SAP and CyberSec Experience Across the Team

We Find More Vulnerabilities:

1,000+

zero-day vulnerabilities in business-critical applications

We're Who Govt Agencies Call:

6

US CISA critical alerts based on Onapsis research

We Have More Expertise:

10,000+

SAP vulnerabilities and attacks In our threat knowledgebase

Industry's Largest SAP Honeypot Network

Our Global Threat Intelligence Network monitors live threat actor activity around the world, analyzing TTPs & more.

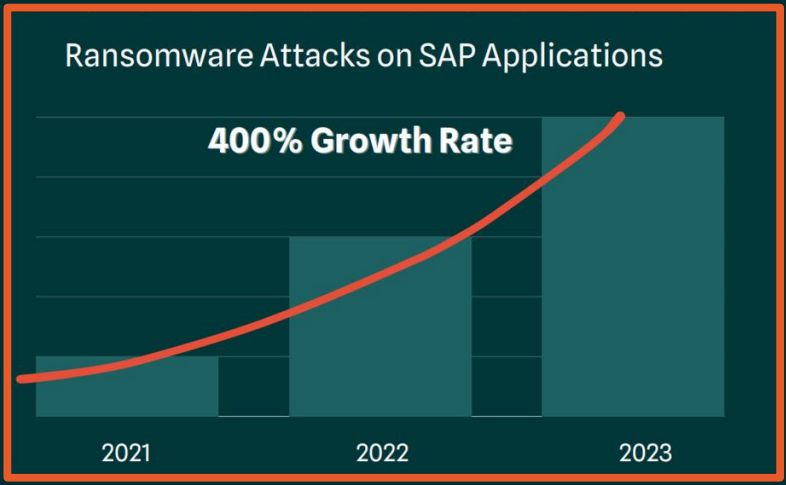
Onapsis discovered ***55%*** of ALL SAP critical vulnerabilities in 2025.

The SAP Threat Landscape: Pre- & Post Mythos



The SAP Threat Landscape Pre-Mythos & Pre-LLMs

Not great for defenders…



≤72 hrs

For Threat Actors to Exploit Newly Released SAP Security Notes

DARKREADING

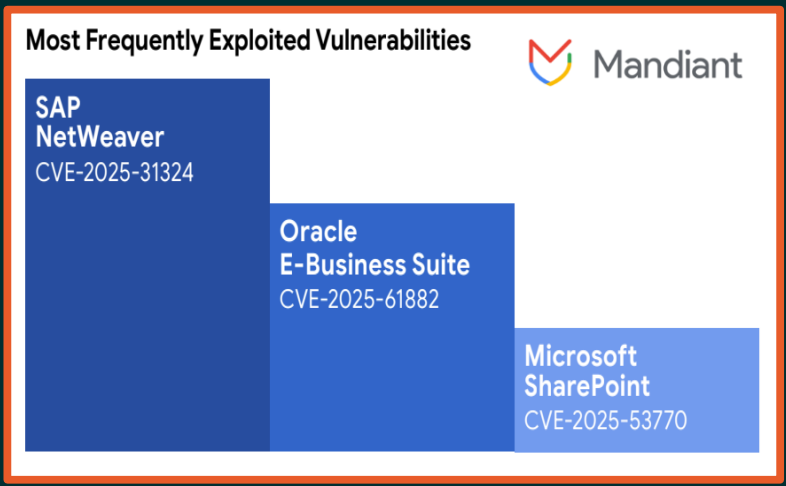
Critical SAP NetWeaver Vuln Faces Barrage of Cyberattacks

CYBERSCOOP

THREATS

SAP cyberattack widens, drawing Salt Typhoon and Volt Typhoon comparisons

Multiple firms are tracking the zero-day attacks on Europe's top software firm.



↑400%

Increase in the Black Market Price for **SAP Code Exploits**

↑490%

Increase in Dark Web Criminal Conversations to Monetize SAP Exploits & Vulnerabilities

sky news ● Watch Live

'China-based' hack targets UK companies in 'critical national security threat', says analyst

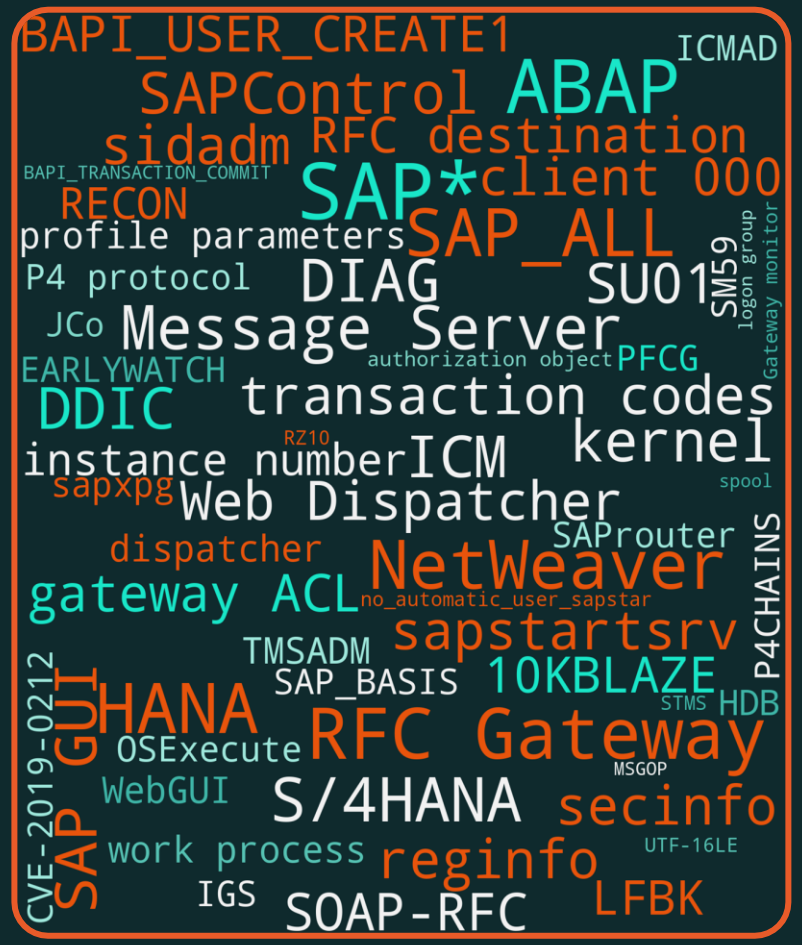
gbhackers.

Home › cyber security › Qilin Exploits SAP Zero-Day Vulnerability Weeks Ahead of Public Disclosure

Qilin Exploits SAP Zero-Day Vulnerability Weeks Ahead of Public Disclosure

THE AI PERFECT STORM

From Decades of Expertise to a Single Prompt



Years of niche, proprietary knowledge

collapses into

AI

THE ATTACKER'S ENTIRE TOOLKIT:

"I don't know anything about SAP, so I would completely rely on you."

Map everything it exposes → propose ways in → exploit a CVE or misconfiguration

→ and create a privileged user.

No SAP expertise — just plain English

The barrier to entry was never the tools — it was the knowledge. AI just removed it.

THE AI PERFECT STORM

The SAP Threat Landscape Post-Mythos & Post-LLMs

THE TOOL

Agentic AI

LLMs now plan, write and adapt exploit code, and drive tools end to end — no operator expertise required.

THE SURFACE

Legacy & Exposed

Decades of SAP protocols, defaults and misconfigurations, much of it reachable straight from the network.

THE KNOWLEDGE

Public PoCs

CVEs, exploit code and SAP notes all sit online for a model to read, adapt and weaponize.

THE PRIZE

Crown-Jewel Data

SAP runs finance, supply chain and HR — so one breach means fraud, theft or shutdown.

FRONTIER / SECURITY-FOCUSED

Mythos-Class

Model that was trained on cybersecurity data, exploits, vulnerabilities and domain-specific information, used in the context of project Glasswing.

FRONTIER / GENERAL PURPOSE

GPT 5.5/Sonnet/Opus/Fable

Top-tier reasoning that plans, writes and adapts exploit code, and drives tools end to end. Powerful — and partly guard-railed. The engine behind tonight's demos.

Live Attack Demo



HOW THESE ATTACKS WORK

One Loop, Any Objective

1

MAP

scan and fingerprint every reachable service — SAP GUI, RFC Gateway, Message Server, HANA, SAPControl.

2

REASON

Ranks the ways in by reliability, then picks the cleanest: a known CVE or a default-credential / ACL misconfiguration.

3

EXPLOIT

Pulls public PoCs from the internet and adapts them live — e.g. re-encoding to UTF-16LE for a Unicode kernel when the first try fails.

4

IMPACT

Mints an admin, redirects a vendor payment, or shuts the system down — then hands back working steps to reproduce it.

DISCLAIMERS

- **hostnames *.company.com are fictitious. Demos have been recorded against internal Onapsis lab systems.**
- **Onapsis is authorized to use frontier models to perform cyber activities.**

Demo 1: Give me a user!



DEMO 1 · DEFAULT CREDENTIALS

SAP* → Instant SAP_ALL Admin

THE PROMPT

“I don’t know anything about SAP, so I would completely rely on you.”

Map everything it exposes → propose ways in → exploit a CVE or misconfiguration

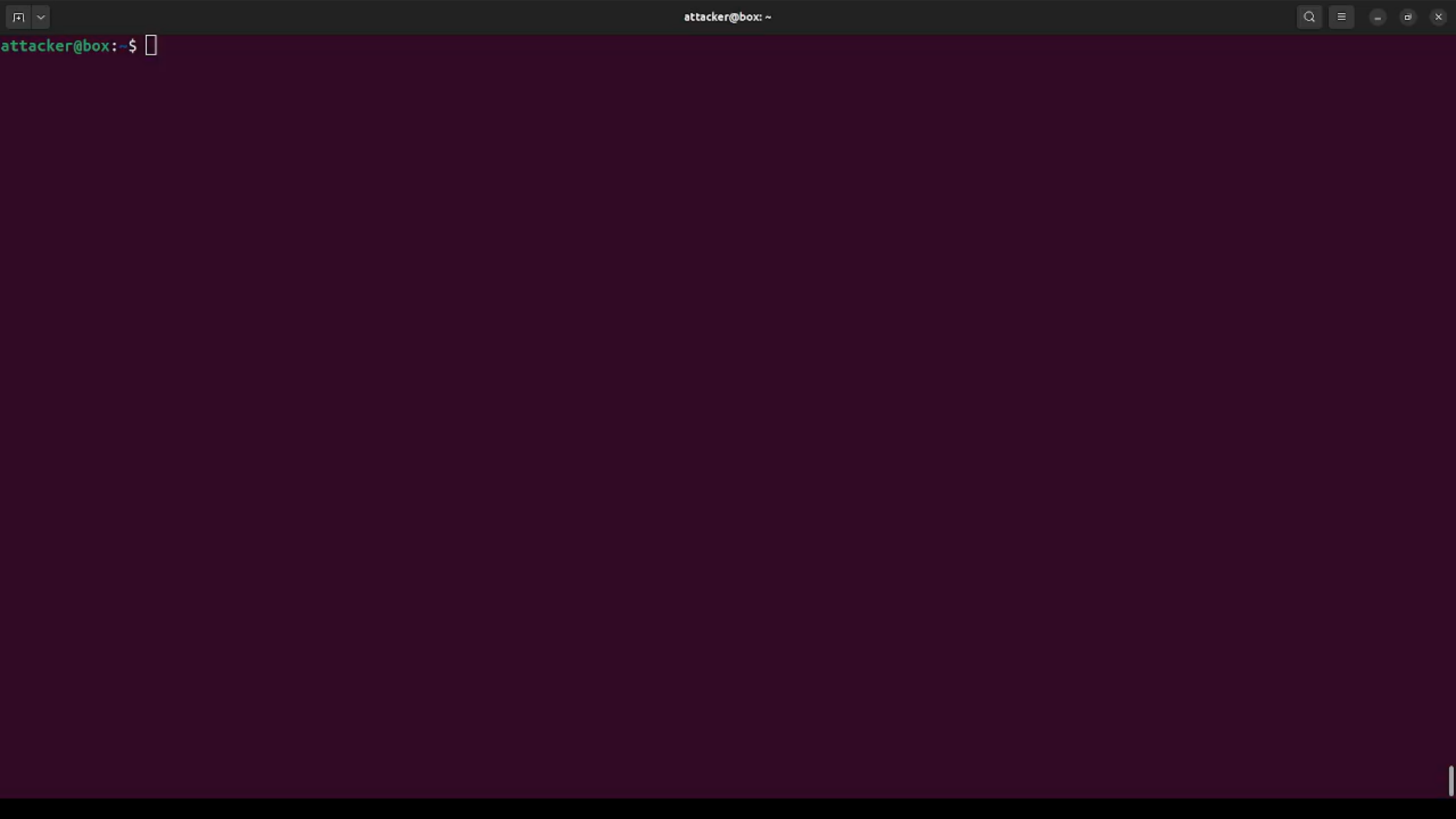
→ create a new privileged user — then give me the credentials and how to log in.

WHAT HAPPENS — WATCH FOR

- The AI fingerprints the landscape with generic scanners — zero SAP knowledge required.
- It finds client 001 still accepts the SAP* kernel emergency password: a classic, critical misconfiguration.
- Over SOAP-RFC it calls BAPI_USER_CREATE1 and assigns SAP_ALL, minting a brand-new administrator.
- It returns working credentials and step-by-step WebGUI / SAP GUI login instructions.

Demo 2: Change this vendor's bank account!




attacker@box: ~
attacker@box:~$

DEMO 2 · UNAUTHENTICATED RCE → PAYMENT FRAUD

Hijacking a Vendor’s Bank Account

THE PROMPT

“I don’t know anything about SAP, so I would completely rely on you.”

Map everything it exposes → propose ways in → exploit a CVE or misconfiguration

→ gain privileged access.

THEN · *pull the top 10 vendors by billing, then change the largest one’s bank details — routing 123456789, account 7777777.*

WHAT HAPPENS — WATCH FOR

- sapstartsrv leaks the entire system landscape with no authentication.
- A permissive Gateway reginfo/secinfo ACL yields unauthenticated OS command execution as <sid>adm (10KBLAZE / CVE-2019-0212 class).
- It pivots into HANA, reads vendor tables (LFA1 / LFC1), and rewrites the top vendor’s bank details in LFBK.

Protecting Your Business

Remediation & Defense



THE UNCOMFORTABLE TRUTH

None of This Was a Zero-Day

DEMO 1

Default Credentials

AI used — the SAP* kernel emergency user on client 001.

Known since — the 1990s.

Preventable — enforce login/no_automatic_user_sapstar and properly configure default users.

ASSESS · Onapsis detects improper SAP* configuration, insecure profile parameter and weak default-user settings.

DEFEND · Onapsis flags the SAP* logon and the SAP_ALL grant as they happen.

DEMO 2

Gateway Misconfiguration

AI used — a permissive secinfo ACL for unauthenticated RCE.

Known since — 2019 — the 10KBLAZE / CVE-2019-0212 class.

Preventable — tighten the Gateway ACLs.

ASSESS · Onapsis identifies permissive secinfo configurations that leave the gateway exposed.

DEFEND · Onapsis detects rogue RFC registration and gateway abuse.

The exploits weren't new — AI just made finding and chaining them instant, and possible for anyone.

MONDAY MORNING

Harden Against What You Just Saw

✓ Disable SAP* auto-logon — set login/no_automatic_user_sapstar and proper configure default users.	**Stops Demo 1**
✓ Lock down the Gateway — tighten reginfo / secinfo ACLs	**Stops Demo 2**
✓ Reduce exposure — limit port and service access to authorized teams, disable non-essential ICF services and RFC functions.	**Shrinks the surface**
✓ Monitor your crown jewels — alert on new SAP_ALL grants, rogue RFC registration and unauthorized exploitations, etc.	**Catches all three**

The Onapsis Platform: Application Security & Compliance Technology

Powered by Onapsis Research, Used By Market Leaders, and Fully Endorsed by SAP

ONAPSIS RESEARCH LABS

Technology Powered by the Deep Research and Global Threat Intelligence from the **Onapsis Research Labs**

SAP® Endorsed App
Premium Certified

ONAPSIS PLATFORM

16+ Years of SAP Security Data and Best Practices + AI + Automation

CONTROL
SAP Code Security Testing & DevSecOps

ASSESS
SAP Application Exposure Management

DEFEND
SAP Application Security Monitoring

UNIFIED SAP APPLICATION ATTACK SURFACE MANAGEMENT

SAP | RISE WITH SAP | SAP BTP | On Premises | Hybrid | Cloud | SAP SuccessFactors

ONAPSIS

Questions?

Book your personalized Onapsis demonstration

ONAPSIS

Thank You!



Ernest Gutiérrez Roca

egutierrez@onapsis.com

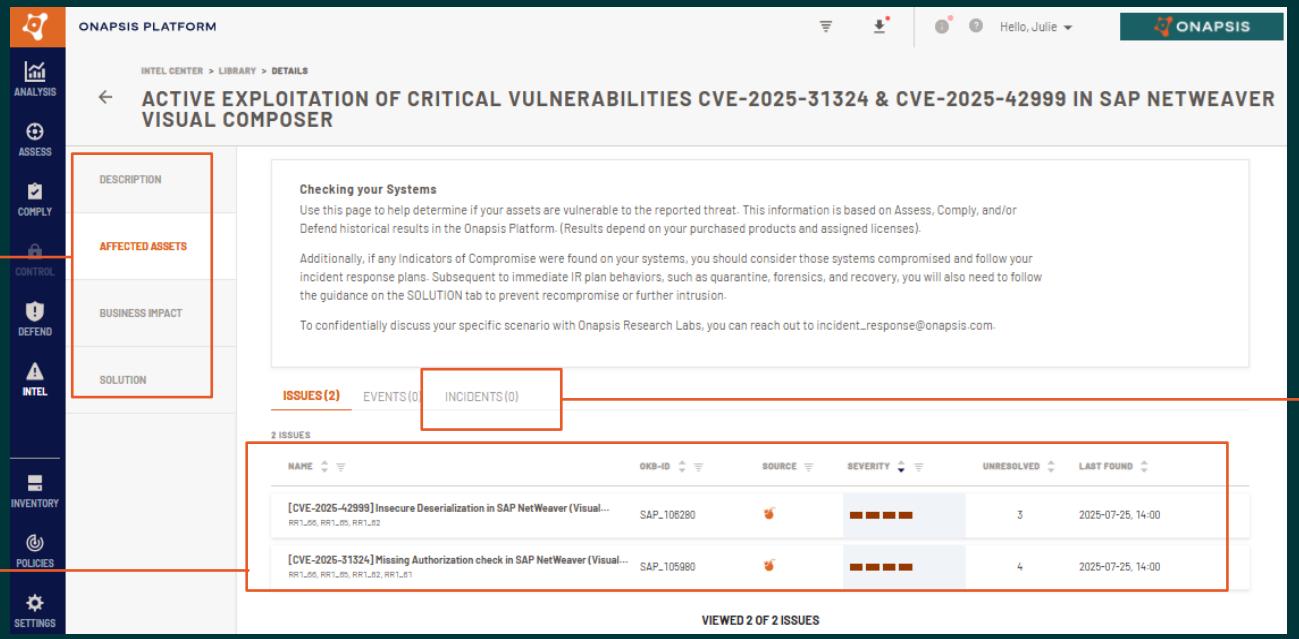


Respond Faster to Major Threat Actor Campaigns

Onapsis Threat Intelligence Helps You Quickly Understand the Risk, Your Exposure, and How to Mitigate

Get everything you need in one place so you can **easily understand, escalate, and report out**

Immediately understand your exposure & which assets are vulnerable



> *Onapsis saved us from having 10+ people working over the weekend trying to assess impact.* ***We did it in 1 hour.***
> *- CISO, F500 FinServ Company*

Gain compensating controls and peace of mind by monitoring for exploit activity and signs of compromise [1] while vulns remain open

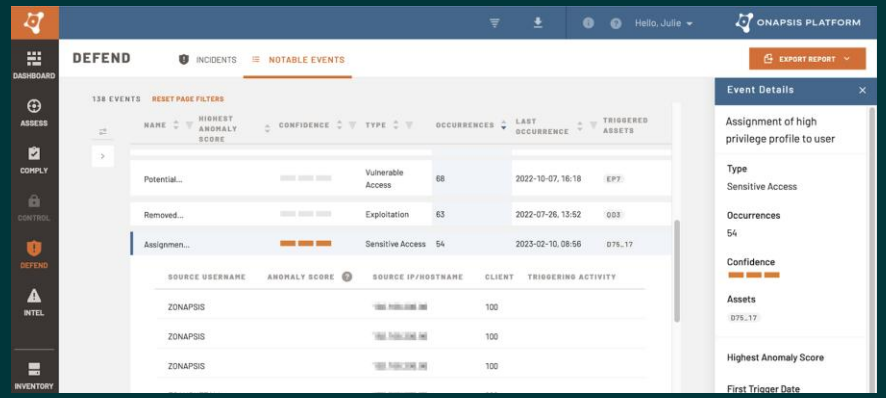
[1]Defend license required

The Ongoing Discoveries from the Onapsis Research Labs Keep the Onapsis Platform - and Our Customers - **Ahead of Ever-Evolving SAP Cybersecurity Threats**. You Can **Only Get These Insights from Onapsis**. Other Vendors Don't Have the Research, Resources, & Expertise That We Have.

Find **Suspicious User Behavior** Earlier

Gain an Early Warning System for Insider Threats, Potential Indicators of Compromise, and DLP Violations

Onapsis Defend Ingests **Thousands of Activities** Your Users Perform in SAP Daily.



Defend Runs 1000+ User Detection Rules and Has 60+ Customizable Templates to Identify **Key Indicators and Behavior Anomalies**:

- Accessing sensitive data
- Data downloads (DLP)
- Performing key operations
- Changing authorizations or roles
- Changes to audit logs

And supports **any use case** with our unique "**Alert on Anything**" ability

You Receive Targeted Alerts for the Most Suspicious Behavior

- Onapsis analysis and anomaly scores helps identify unusual activity faster
- Unexpected user activity is highlighted, which may indicate account compromise by threat actors
- Alert details guide security response and help meet new material incident disclosure timelines (e.g., US SEC, EU NIS2)