

No. 61

SAP INCIDENT RESPONSE

Ransomware and Incident Response for SAP

Preparing for, responding to and recovering from attacks on SAP systems, explained for beginners

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 61

Ransomware and Incident Response for SAP

Preparing for, responding to and recovering from attacks on SAP systems, explained for beginners

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

Ransomware and Incident Response for SAP
Preparing for, responding to and recovering from attacks on SAP systems, explained for beginners

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. SAP, SAP S/4HANA, SAP Fiori, SAP Gateway, SAP BTP, SAP Build Work Zone and other SAP products mentioned are trademarks or registered trademarks of SAP SE in Germany and other countries. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by SAP SE or any other vendor named in this book.

The information in this book is provided for education. Product features change between releases; always confirm details in the official documentation for your release before changing a production system. Screens marked “Illustration” are simplified drawings, not captures of real SAP software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this book 1

PART I · FOUNDATIONS

1 Why SAP is a ransomware target 5
2 Lessons from recent attacks 7
3 The attack chain 9
4 Incident response basics 11

PART II · PREPARE

5 Know your exposure 14
6 Patching critical notes fast 15
7 Hardening and admin access 17
8 Backup strategy 18
9 Protecting backups 20
10 Detection readiness 22
11 Incident response plans and playbooks 23
12 Exercises 25

PART III · RESPOND

13 The first hour 27
14 Containment 29
15 Evidence and forensics 31
16 Investigating in SAP 33
17 Communication and reporting 34
18 The ransom question 35

PART IV · RECOVER

19 Recovery strategy 37
20 Rebuild and restore 38
21 Verifying integrity 39
22 Returning to business 40

FREE SAMPLE · ojayo.com

23 Lessons learned 41
24 RISE and cloud landscapes 42
25 Worked example: Northline Logistics 43
Checklists 45
Glossary 46
Further reading 47

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

What this book covers, who it is for, and how to use it.

When SAP stops, the business stops: orders cannot be taken, goods cannot ship, and invoices cannot be paid. That makes SAP an attractive target for **ransomware** groups, who encrypt systems and steal data to pressure victims into paying.

In 2025, attackers exploited a critical vulnerability in SAP NetWeaver Visual Composer, tracked as **CVE-2025-31324**, and public reports linked follow-on activity to ransomware groups. The Mandiant **M-Trends 2026** report, as summarized by Onapsis, highlights SAP as a top target. This book explains, for beginners, how to **prepare for, respond to and recover from** attacks on SAP systems.

Which versions this book covers

- SAP S/4HANA, SAP ERP and SAP NetWeaver ABAP and Java systems on SAP HANA and other databases.
- On-premise, hosted and **RISE with SAP** landscapes, with notes on shared responsibility.
- Incident examples and vulnerabilities reported publicly through 2026.

This book gives general guidance. It is not legal advice. Involve legal counsel, insurers and specialist responders in real incidents.

Who this book is for

- **SAP Basis and security teams** who must recover systems.

FREE SAMPLE · ojayo.com

- **SOC and incident response teams** new to SAP.
- **IT leaders** who plan resilience and approve budgets.
- **Business continuity managers**.

How the book is organized

- **Part I — Foundations** (Chapters 1–4): why SAP is targeted, recent attacks, the attack chain and incident response basics.
- **Part II — Prepare** (Chapters 5–12): exposure, patching, hardening, backups, backup protection, detection, response plans and exercises.
- **Part III — Respond** (Chapters 13–18): the first hour, containment, evidence, investigation, communication and the ransom question.
- **Part IV — Recover** (Chapters 19–25): recovery strategy, rebuild and restore, integrity checks, returning to business, lessons learned, the cloud and a worked example.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP
Practical advice you can use straight away.

IN SAP
Product-specific details and names.

WATCH OUT
Common misunderstandings.

KEY IDEA
The one thing to remember from a section.

FREE SAMPLE · ojayo.com

A note on screens and examples

Screens are **simplified illustrations**, not copies of real tools. Company names, hosts and times in the examples are invented.

FREE SAMPLE · ojayo.com

PART I

Foundations

These chapters explain why attackers target SAP, what recent attacks looked like, how an attack unfolds and the basics of incident response.

FREE SAMPLE · ojayo.com

CHAPTER 1

Why SAP is a ransomware target

SAP holds the data and processes attackers can hold hostage.

Ransomware groups look for the systems whose loss hurts most. SAP often runs finance, supply chain, production and HR, so an outage creates immediate pressure.

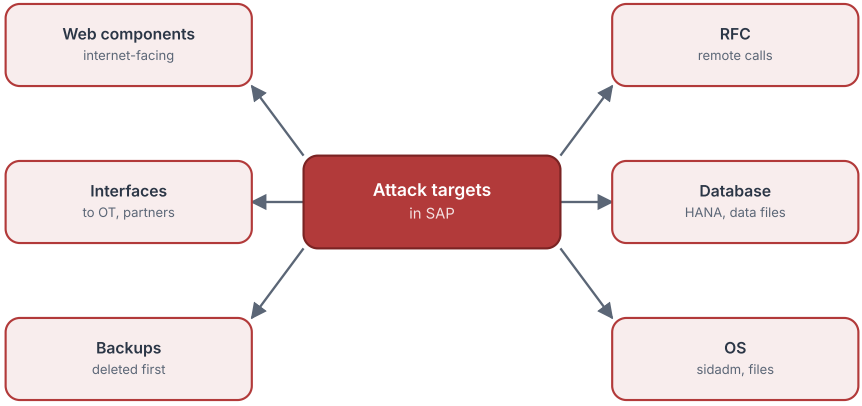


Figure 1.1 What attackers aim for in an SAP landscape.

What makes SAP attractive

- **Business impact**: a stopped ERP system stops revenue.
- **Valuable data**: customer, supplier, employee and financial data can be stolen and used for extortion.
- **Connections**: SAP links to banks, partners, warehouses and sometimes production systems, which helps attackers move further.

FREE SAMPLE · ojayo.com

- **Blind spots**: Onapsis notes that endpoint and network tools rarely understand SAP application logs, so attackers can act unseen.
- **Slow patching**: SAP changes need testing and downtime, so critical fixes may wait weeks.

Double extortion

Modern ransomware groups usually **steal data first** and then encrypt. Even if you restore from backups, they threaten to publish the stolen data.

> **KEY IDEA**
> Good backups solve encryption. They do not solve data theft. You need both prevention and recovery.

FREE SAMPLE · ojayo.com

CHAPTER 2

Lessons from recent attacks

Recent attacks show how fast SAP exploitation moves.

CVE-2025-31324

In April 2025, SAP fixed a maximum-severity flaw in the **Visual Composer metadata uploader** of SAP NetWeaver Java. It allowed **unauthenticated file upload**, which attackers used to place **webshells** and run commands.

Public reporting described:

- Onapsis tracing exploitation back to **January 2025**, before the fix.
- Onapsis and Mandiant confirming compromises across energy, manufacturing, pharmaceuticals, retail, government and other sectors.
- A **second wave** in which other attackers reused webshells left by the first.
- ReliaQuest assessing, with moderate confidence, involvement of the **BianLian** group and observing a backdoor linked to **RansomEXX**.
- Microsoft threat intelligence, as reported in the press, linking the Storm-1175 group's Medusa ransomware activity to exploitation of the flaw.
- CISA adding the CVE to its **Known Exploited Vulnerabilities** catalog on April 29, 2025.

A related flaw, **CVE-2025-42999**, was fixed soon after and chained in attacks.

CVE-2025-42957

Later in 2025, an ABAP code injection flaw reachable through RFC in S/4HANA, rated CVSS 9.9, was reported by SecurityBridge as exploited in the wild.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP (y…
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

Ransomware and Incident Response for SAP

Enjoyed it? The full book has 52 pages and 25 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.