

No. 73

SAP THREAT INTELLIGENCE

Threat Intelligence for SAP

Using threat intelligence to prioritize patches, detect attacks and protect SAP, explained for beginners

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 73

Threat Intelligence for SAP

Using threat intelligence to prioritize patches, detect attacks and protect SAP, explained for beginners

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

Threat Intelligence for SAP

Using threat intelligence to prioritize patches, detect attacks and protect SAP, 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 threat intelligence for SAP 5
2 Threat intelligence basics 7
3 The SAP threat landscape 9
4 Threat actors 11

PART II · SOURCES

5 SAP Security Notes and Patch Day 14
6 CISA KEV and exploit likelihood 16
7 Vendor research 17
8 Incident and industry reports 18
9 Sharing communities 19
10 Your own telemetry 20
11 Judging sources 21

PART III · USING INTELLIGENCE

12 Prioritizing SAP patches 23
13 Exposure assessment 25
14 Intelligence for SAP cloud and RISE 27
15 MITRE ATT&CK for SAP 29
16 Indicators and behaviors 31
17 Detection engineering 32
18 Threat hunting 34
19 Supporting incident response 36

PART IV · BUILDING A PROGRAM

20 Building the program 38
21 Tools and integration 40
22 Reporting to leaders 41

FREE SAMPLE · ojayo.com

23 Metrics 42
24 Common pitfalls 43
25 Worked example: Riverbend Chemicals 44
Checklists 46
Glossary 47
Further reading 48

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.

SAP releases dozens of Security Notes every month. No team can apply all of them immediately. **Threat intelligence** answers the question that matters most: which weaknesses are attackers actually using right now, and are we exposed?

The need has become urgent. Onapsis, summarizing the **Mandiant M-Trends 2026** report, states that a critical SAP NetWeaver flaw was the most frequently exploited vulnerability of the previous year, and that Mandiant and Google Threat Intelligence observed at least four separate threat clusters exploiting it as a zero-day in early 2025.

This book explains, for beginners, how to use threat intelligence for SAP: the intelligence lifecycle, the SAP threat landscape, sources such as SAP Patch Day and the CISA Known Exploited Vulnerabilities catalog, prioritizing notes, exposure checks, MITRE ATT&CK, indicators and behaviors, detection, hunting, incident response, and building a program.

Which versions this book covers

- SAP systems on-premise, in RISE and in SAP cloud services.
- Public threat reporting from 2024 to 2026, including M-Trends 2026 and the 2026 Verizon Data Breach Investigations Report as discussed by SAP security vendors.

Threat information ages quickly. Use this book for methods, and current sources for facts.

FREE SAMPLE · ojayo.com

Who this book is for

- **SOC and threat intelligence analysts** new to SAP.
- **SAP security and Basis teams** who decide what to patch first.
- **Security managers** building SAP into their intelligence program.

How the book is organized

- **Part I — Foundations** (Chapters 1–4): why intelligence matters for SAP, intelligence basics, the SAP threat landscape and threat actors.
- **Part II — Sources** (Chapters 5–11): Patch Day, CISA KEV, vendor research, incident reports, sharing communities, your own telemetry and judging sources.
- **Part III — Using intelligence** (Chapters 12–19): prioritizing patches, exposure, cloud services, MITRE ATT&CK, indicators and behaviors, detection, hunting and incident response.
- **Part IV — Building a program** (Chapters 20–25): program design, tools, reporting, metrics, pitfalls 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.

FREE SAMPLE · ojayo.com

KEY IDEA

The one thing to remember from a section.

A note on screens and examples

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

FREE SAMPLE · ojayo.com

PART I

Foundations

These chapters explain why threat intelligence matters for SAP, the basics of intelligence work, the current SAP threat landscape and the actors behind it.

FREE SAMPLE · ojayo.com

CHAPTER 1

Why threat intelligence for SAP

Intelligence tells you which risks are real today.

Too many notes, too little time

SAP Patch Day brings many notes each month. Teams must decide which to apply now and which can wait. Severity scores alone do not show which flaws attackers are exploiting.

Attackers move fast

Onapsis reports that threat actors begin exploiting newly released SAP vulnerabilities within 72 hours of a patch release, and that Microsoft documented the Storm-1175 group exploiting SAP NetWeaver flaws less than 24 hours after disclosure.

SAP is no longer niche

Onapsis notes that ERP security was long treated as a niche operational issue, but the M-Trends 2026 findings show threat actors have made SAP a primary target.

What intelligence gives you

- **Priorities**: what to patch first.
- **Detection ideas**: what to look for.
- **Context**: who attacks SAP and why.

FREE SAMPLE · ojayo.com

- **Arguments**: evidence for management decisions.

KEY IDEA

Threat intelligence turns "everything is critical" into "these three things need action today".

FREE SAMPLE · ojayo.com

CHAPTER 2

Threat intelligence basics

Intelligence is information that supports a decision.

Data, information, intelligence

- **Data**: raw facts, such as an IP address.
- **Information**: data with context, such as "this IP scanned SAP portals".
- **Intelligence**: analyzed information that supports a decision, such as "this campaign targets our unpatched portal; patch it today".

The lifecycle

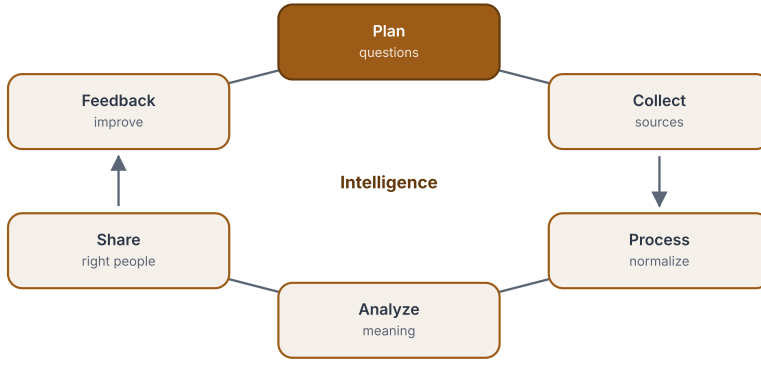


Figure 2.1 The threat intelligence lifecycle.

1. **Plan**: decide which questions matter, such as "which SAP flaws are exploited?".
2. **Collect** from sources.
3. **Process** into a usable format.

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
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 (you are reading this)

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

Threat Intelligence for SAP

Enjoyed it? The full book has 53 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.