SECURITY INSIDER

READERS' CHOICE SECURITY INSIDER AWARD 2026

Bedrohungen Netzwerke Plattformen Applikationen Identity- und Access-Manageme

Bedrohungen › Malware › Mini Shai-Hulud: Manipulierte npm-Pakete im SAP-CAP

Update: mini Shai-Hulud breitet sich weiter aus

Supply Chain Angriff auf SAP CAP durch bösartige npm-Pakete

05.05.2026 Aktualisiert am 15.05.2026 · Von Melanie Staudacher · 4 min Lesedauer

30 heise online heise+ entdecken

heise+ Newsticker Security IT & Tech Developer KI Entertainment W

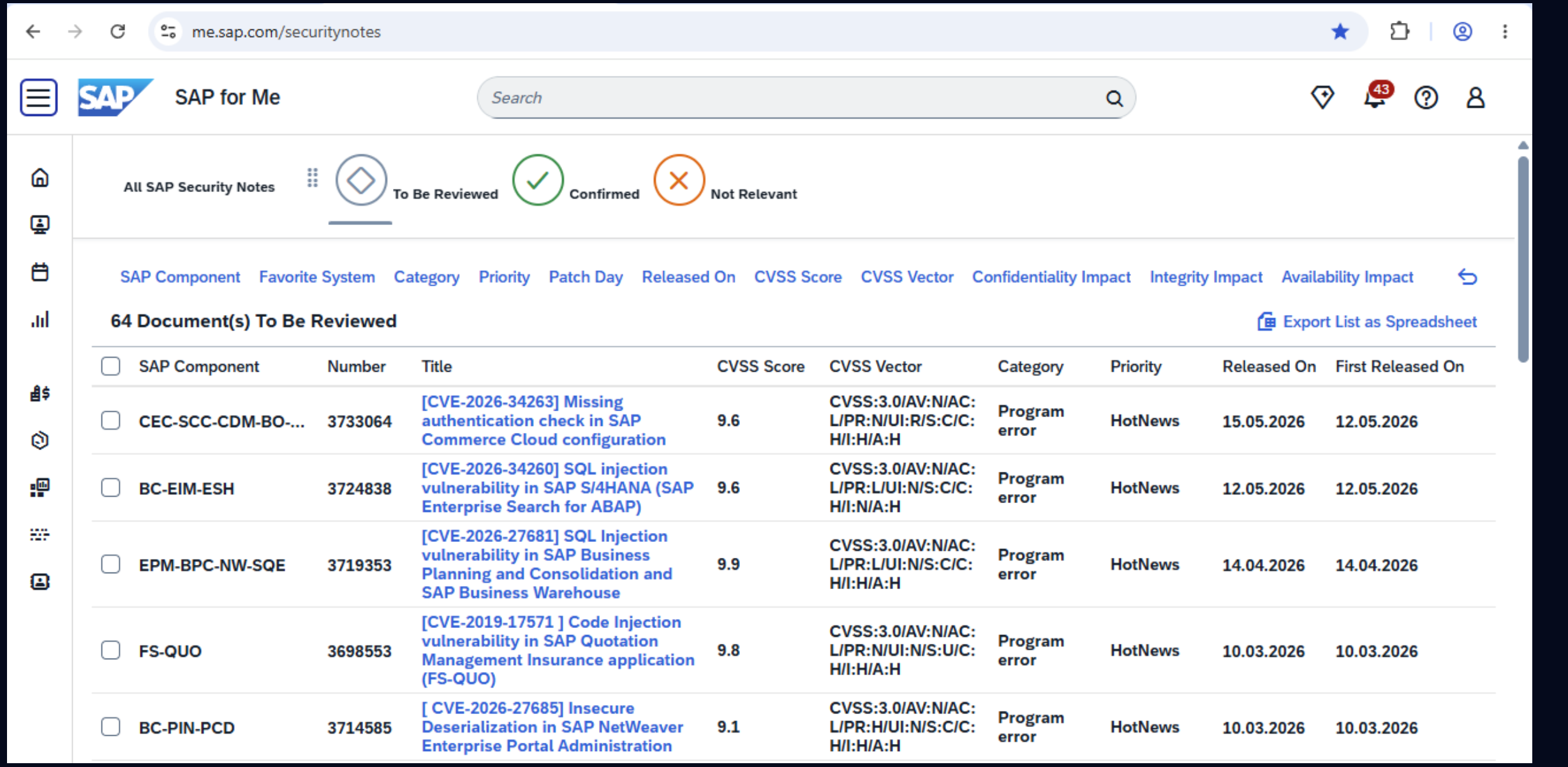
heise online › Security › Bösartige npm-Pakete: SAP-Software kompromittiert

Bösartige npm-Pakete: SAP-Software kompromittiert

Mehrere npm-Pakete von SAP waren einer Supply-Chain-Attacke ausgesetzt. Dahinter steckt die Hackergruppe TeamPCP, sagen Sicherheitsforscher.

MICROSOFT SENTINEL BLOG 4 MIN READ

The Worm in the Supply Chain: How Defender for Endpoint and Sentinel for SAP BTP Caught Shai-Hulud



SAP Component	Number	Title	CVSS Score	CVSS Vector	Category	Priority	Released On	First Released On
CEC-SCC-CDM-BO-...	3733064	[CVE-2026-34263] Missing authentication check in SAP Commerce Cloud configuration	9.6	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H	Program error	HotNews	15.05.2026	12.05.2026
BC-EIM-ESH	3724838	[CVE-2026-34260] SQL injection vulnerability in SAP S/4HANA (SAP Enterprise Search for ABAP)	9.6	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:H	Program error	HotNews	12.05.2026	12.05.2026
EPM-BPC-NW-SQE	3719353	[CVE-2026-27681] SQL Injection vulnerability in SAP Business Planning and Consolidation and SAP Business Warehouse	9.9	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H	Program error	HotNews	14.04.2026	14.04.2026
FS-QUO	3698553	[CVE-2019-17571] Code Injection vulnerability in SAP Quotation Management Insurance application (FS-QUO)	9.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Program error	HotNews	10.03.2026	10.03.2026
BC-PIN-PCD	3714585	[CVE-2026-27685] Insecure Deserialization in SAP NetWeaver Enterprise Portal Administration	9.1	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H	Program error	HotNews	10.03.2026	10.03.2026

SIT Dortmund 2026

SAP im Visier. Wir haben die Hebel.

Angreifer sind schneller als unsere Patch-Zyklen – SAP ist längst Ziel, nicht Beifang.

SAP HOT NEWS 2026 (JAN–MAI)

11 CVEs ↑ +83 % YoY

mit CVSS ≥ 9,0 – Spitzenwert 9,9 in S/4HANA Finance. Nach drei Jahren Rückgang dreht der Trend.

SAP SECURITY NOTES · EXPORT 28.05.2026

ANGRIFFSFENSTER SCHRUMPFT

<24 Std.

bis KI-gestützte Exploits live sind. „Mini Shai-Hulud" stahl SAP-npm-Credentials, bevor irgendein Patch-Zyklus griff.

THE HACKER NEWS · ONAPSIS

REALER GESCHÄFTSSCHADEN

2,1 Mrd. $

Quartalsverlust eines globalen Fertigers – ein SAP-Ransomware-Vorfall, sechs Wochen Produktionsstillstand.

ONAPSIS EXECUTIVE THREAT OVERVIEW 2026

BSI-LAGEBERICHT 2025

DE

119 / Tag

neue Schwachstellen pro Tag in DE (+24 % YoY). 950 Ransomware-Fälle – 80 % treffen den Mittelstand.

BSI · DIE LAGE DER IT-SICHERHEIT

GLOBALE BEDROHUNGSLAGE

52 %

aller Angriffe weltweit sind Erpressung & Ransomware. Deutschland: Nr. 2 in Europa, Identitätsangriffe +32 %.

MICROSOFT DIGITAL DEFENSE REPORT 2025

BITKOM WIRTSCHAFTSSCHUTZ 2025

202 Mrd. €

jährl Schaden Cyberattacken (70 % von 289 Mrd. €). 65 % fürchten um Existenz – nur jedes 2te Unternehmen fühlt sich vorbereitet.

BITKOM WIRTSCHAFTSSCHUTZ 2025

DER MFA-SCHILD

99 %

der Identitätsangriffe stoppt phishing-resistente MFA. Die günstigste Kontrolle, die jede SAP-Landschaft heute aktivieren kann.

MDDR 2025 · ENISA THREAT LANDSCAPE 2025

BSI · KRITIS-REIFE

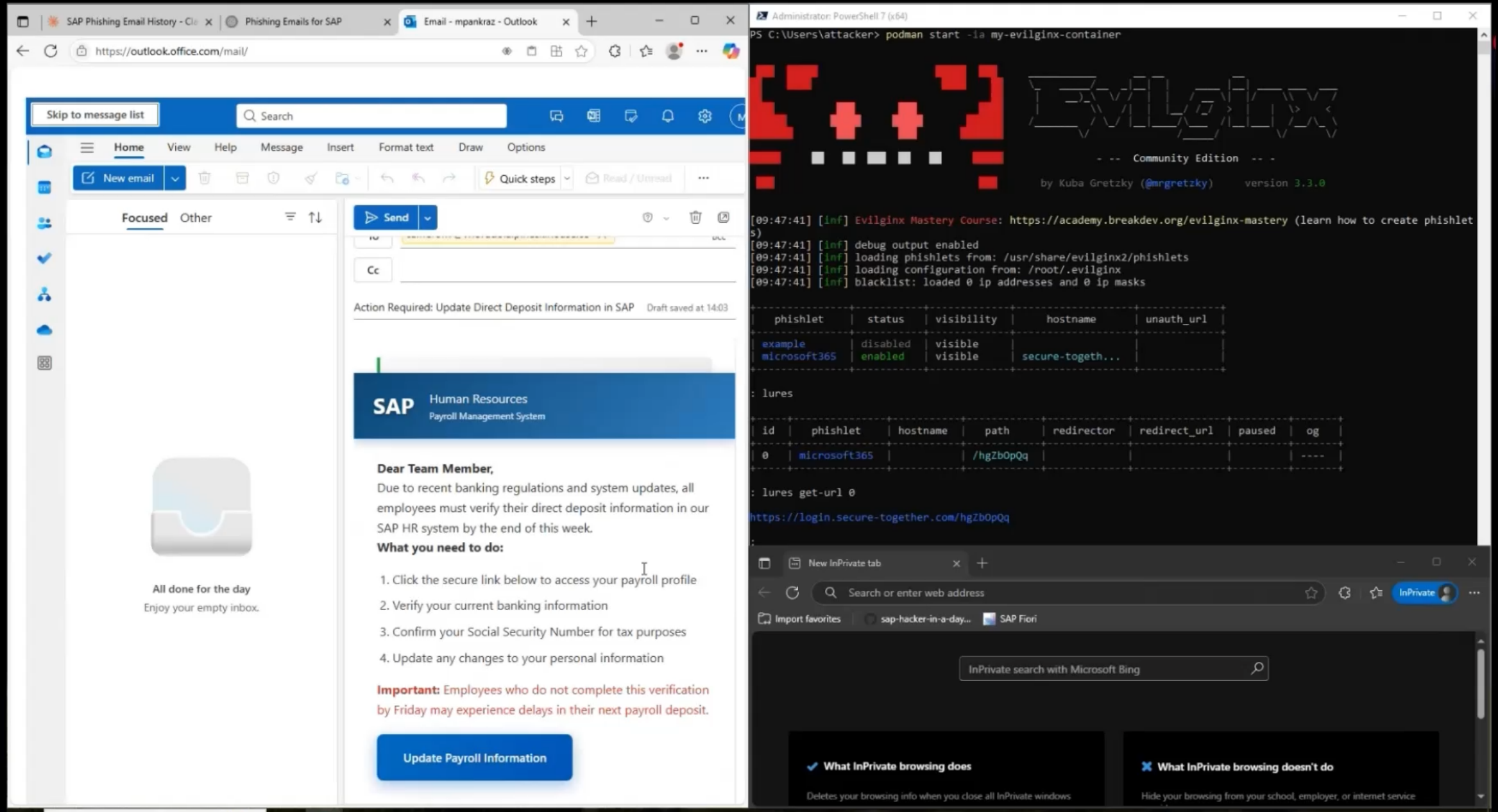
80 %

der KRITIS-Betreiber haben ein ISMS. Aber die Lücken liegen dort, wo es zählt: Business Continuity und Angriffserkennung.

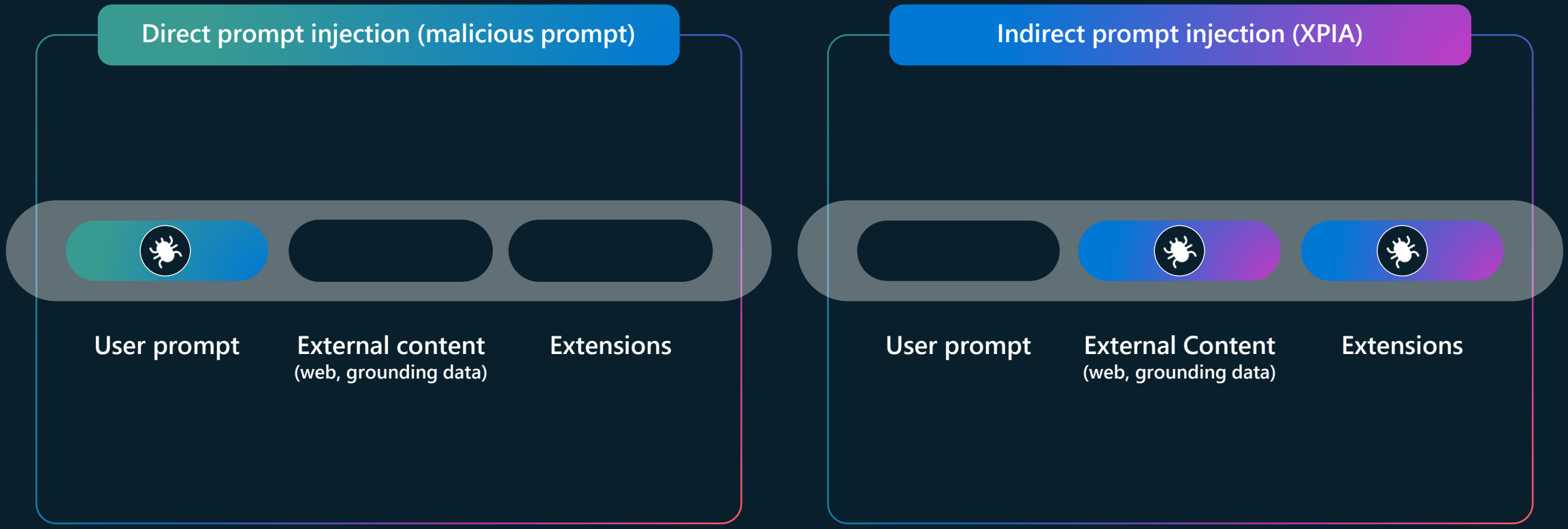
BSI-LAGEBERICHT 2025

Angreifer brauchen Zeit. Verteidiger brauchen Sicht.

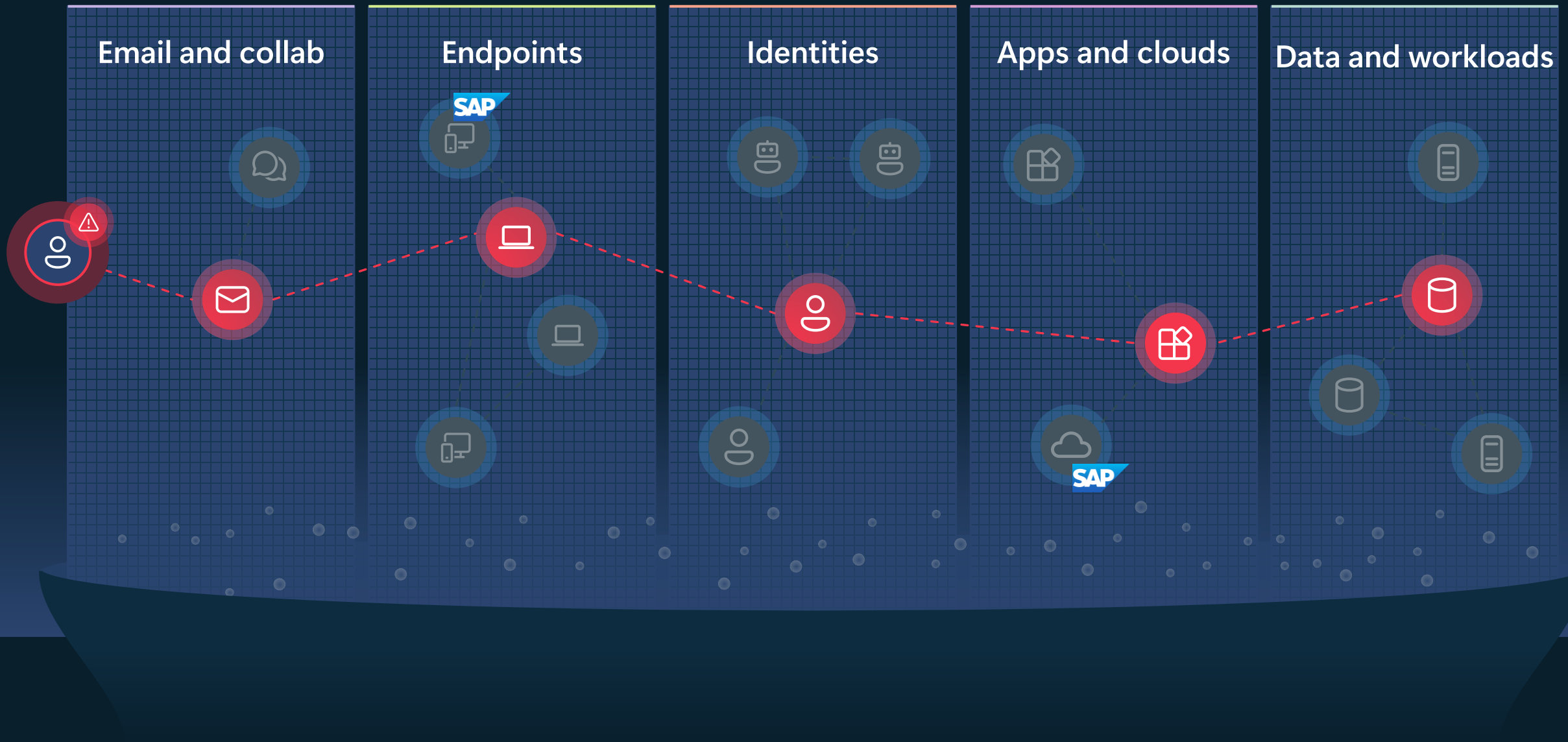
- SEHEN
- ENTSCHEIDEN
- HANDELN


SAP Phishing Email History - Cl
Phishing Emails for SAP
Email - mpankraz - Outlook
https://outlook.office.com/mail/
Skip to message list
Search
Home
View
Help
Message
Insert
Format text
Draw
Options
New email
Quick steps
Focused
Other
All done for the day
Enjoy your empty inbox.
Send
Cc
Action Required: Update Direct Deposit Information in SAP
Draft saved at 14:03
SAP
Human Resources
Payroll Management System
Dear Team Member,
Due to recent banking regulations and system updates, all employees must verify their direct deposit information in our SAP HR system by the end of this week.
What you need to do:
1. Click the secure link below to access your payroll profile
2. Verify your current banking information
3. Confirm your Social Security Number for tax purposes
4. Update any changes to your personal information
Important: Employees who do not complete this verification by Friday may experience delays in their next payroll deposit.
Update Payroll Information
Administrator: PowerShell 7 (x64)
PS C:\Users\attacker> podman start -ia my-evilginx-container
Evilginx
- -- Community Edition -- -
by Kuba Gretzky (@mrgretzky)
version 3.3.0
[09:47:41] [inf] Evilginx Mastery Course: https://academy.breakdev.org/evilginx-mastery (learn how to create phishlets)
[09:47:41] [inf] debug output enabled
[09:47:41] [inf] loading phishlets from: /usr/share/evilginx2/phishlets
[09:47:41] [inf] loading configuration from: /root/.evilginx
[09:47:41] [inf] blacklist: loaded 0 ip addresses and 0 ip masks
phishlet | status | visibility | hostname | unauth_url
example | disabled | visible |
microsoft365 | enabled | visible | secure-togeth...
: lures
id | phishlet | hostname | path | redirector | redirect_url | paused | og
0 | microsoft365 | | /hgZbOpQq | | | | ----
: lures get-url 0
https://login.secure-together.com/hgZbOpQq
New InPrivate tab
Search or enter web address
InPrivate
Import favorites
sap-hacker-in-a-day...
SAP Fiori
InPrivate search with Microsoft Bing
What InPrivate browsing does
Deletes your browsing info when you close all InPrivate windows
What InPrivate browsing doesn't do
Hide your browsing from your school, employer, or internet service
Type here to search
Regn i annalkan
DEU
12:09 PM
6/4/2025

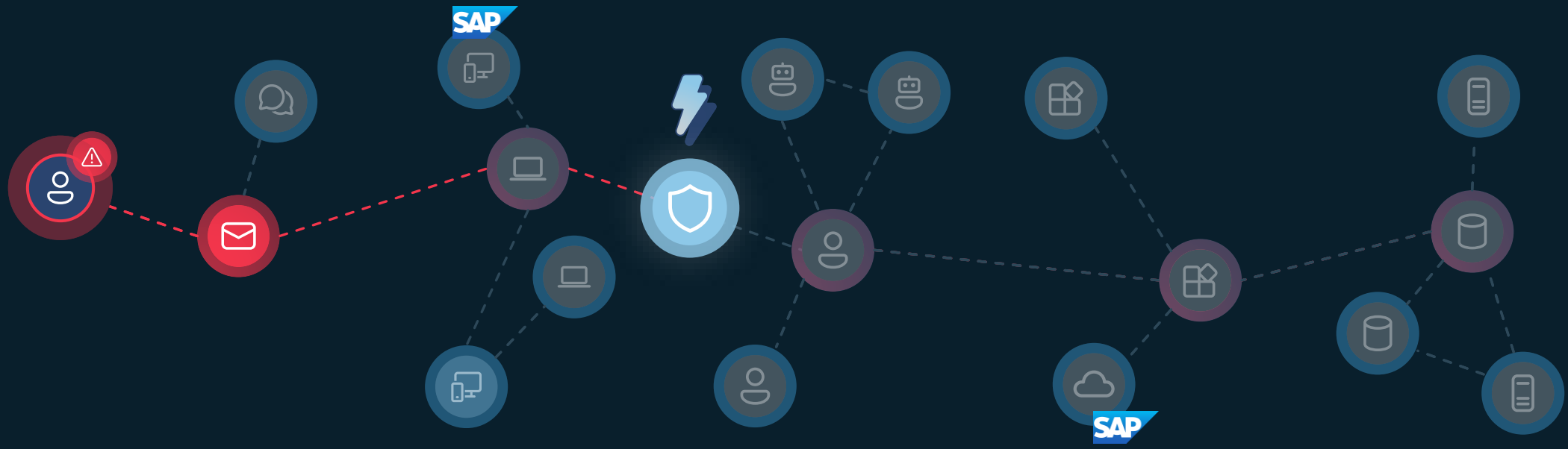
Threats can be embedded in the new GenAI attack surfaces



Attackers think in graphs



Graph-powered security enables enterprise-wide visibility



Unified threat detection and faster response


"ONCE MEN TURNED THEIR THINKING OVER TO MACHINES IN THE HOPE THAT THIS WOULD SET THEM FREE."
THE PROMISE: FREEDOM FROM TOIL. SPACE FOR THOUGHT. TIME FOR LIFE.
COMPLIANCE 97.2%
POPULATION INDEX
POWER THROUGH CONTROL
THOUGHT
MACHINE
AUTOMATION
FREEDOM?
OBEY
CONSUME
DO NOT THINK
BUT THAT ONLY PERMITTED OTHER MEN WITH MACHINES TO ENSLAVE.
– DUNE

Public SAPwned red team exercise materials

Github repos

Blog post

Zava Microsoft Defender Search Suraj Malk

Incidents > User account compromise identified from a known attack pattern (attack disruption)

ID 57083: User account compromise identified from a known attack pattern (attack disruption)

Copilot Manage incident Tasks ...

High | Active | Defender Experts | False alert | Last update time: Apr 16, 2026 7:29 AM | Critical asset | Credential Phish | Attack Disruption | DONOTTOUCH | DONOTTO

Attention: Attack disruption in

Attack story | Alerts (72) | ...mended actions (20) | Summary | Similar

Filters: Severity: Any

Alerts

accessed
sap-ash

Apr 10, 2026 4:31 AM
SAP - Transaction SM4
CAMERONV in a prod
sap.as... Came...

Apr 10, 2026 4:54 AM
Suspicious addition of
sap-ash

Apr 10, 2026 4:55 AM
Suspicious connection
service
sap-ash

Apr 10, 2026 5:00 AM
Azure Resource Manag
suspicious proxy IP ad
Cameron V ash

Apr 10, 2026 5:00 AM
Potential user account
identified through att
Cameron V

Apr 10, 2026 5:01 AM New
Compromised user account in a recognized attack pattern
Cameron V

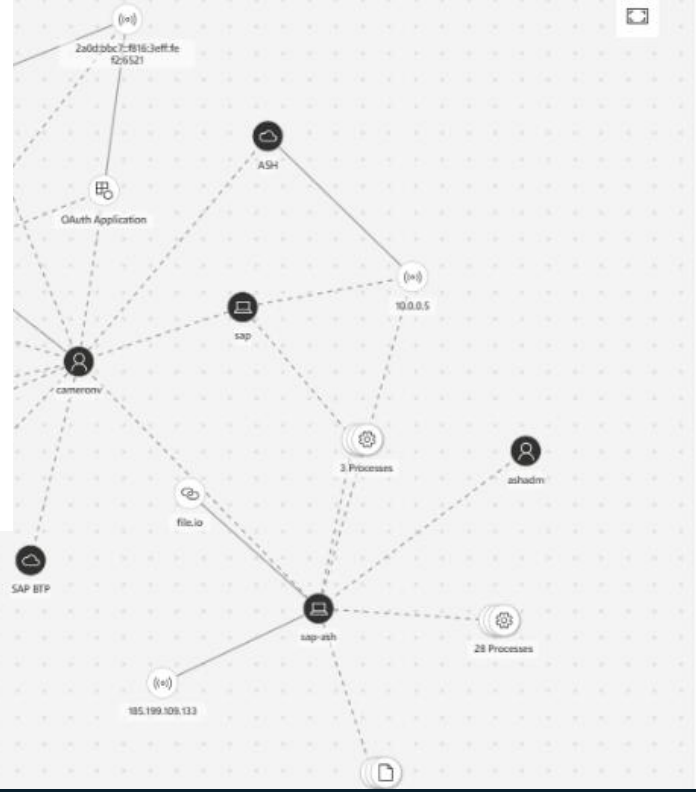
Apr 10, 2026 5:14 AM New
SAP BTP - Malware detected in Business Apps Studio dev space

Microsoft Sentinel for SAP flagged a sensitive transaction use. SM49 allows OS level command execution.

This is the business-risk moment: the attacker is not just on the host, they are inside SAP activity that matters.

*Select the **SAP BTP - Malware detected in Business Apps Studio dev space** alert.*

< >



This incident is ranked as top priority and requires immediate attention.
Notable priority factors:

Disruption actions taken

Attack disruption

Automated response took place.

Disruption incident summary and impact

No information

View actions in activity tab

3 Notable alert types

SAP - Transaction SM49 started by user CAMERONV in a production system, SAP - User CAMERONV has downloaded 13400 bytes of potentially sensitive data , SAP BTP - Malware detected in Business Apps Studio dev space

1 High risk threats

Credential Phish

Martin Pankraz
SAP Champion
SAP SE

Stv. Sprecher AK Cloud Security
DSAG

Product Manager SAP Security
Microsoft

Martin.Pankraz@microsoft.com

Learn more

SAP Cyber Defense live click demo | Microsoft Learn

About Microsoft Sentinel content and solutions | Microsoft Learn

Microsoft Sentinel for SAP RISE solution | Microsoft Learn

Microsoft Sentinel Solution for SAP BTP | Microsoft Learn

Use Sentinel for SAP LogServ Add-on for full coverage | Official SAP Blog

Microsoft Security Community playlist | YouTube

SAP with Microsoft Cloud Channel | YouTube

Aviators Germany | Microsoft Intgeration Community

SAP BTP Activity - dsagwstechxchange

dsagwstechxchange

Are there any outages impacting this resource | Generate a query for this resource | Check service health for this resource

Edit | Open | Help | Auto refresh: Off

Overview | Identity Management | Custom App Audit Coverage

BTP Audit Coverage

This view identifies custom BTP applications that have user logins but no business audit trail. These applications may be missing audit log service bindings or `@AuditLog` annotations, creating security blind spots where user actions are invisible to monitoring.

Time Range: Last hour

Audit coverage score

0 / 1 apps audited (0.0%)

0 %

Custom app audit coverage

Search

Application	XSUAA App Name	Subaccount	Tenant	Audit Status	Logins	First Login	Last Login	Users
dsag	dsag-mealapp-security-cap	sapsit	57070a8b-c114-4ce2-bc75-c96442195f67	Unaudited	1	6/7/2026, 4:29:03.658 PM	6/7/2026, 4:29:03.658 PM	["mapankra@microsoft.com"]