



# SAP Security: Schutz geschäfts- kritischer Systeme

Christian Schuller – Security Consultant

**claranet**

Make  
modern  
happen®



A top-down view of a desk setup. On the left, a white laptop is partially visible with a pair of black-rimmed glasses resting on its keyboard. To the right of the laptop is a white computer mouse. In the top right corner, there is a white cup filled with dark coffee. In the bottom left corner, there is a white spiral-bound notebook with a blue pencil resting on it. A red circular sticker with the text 'Make modern happen' is placed on the laptop's surface.

# Agenda

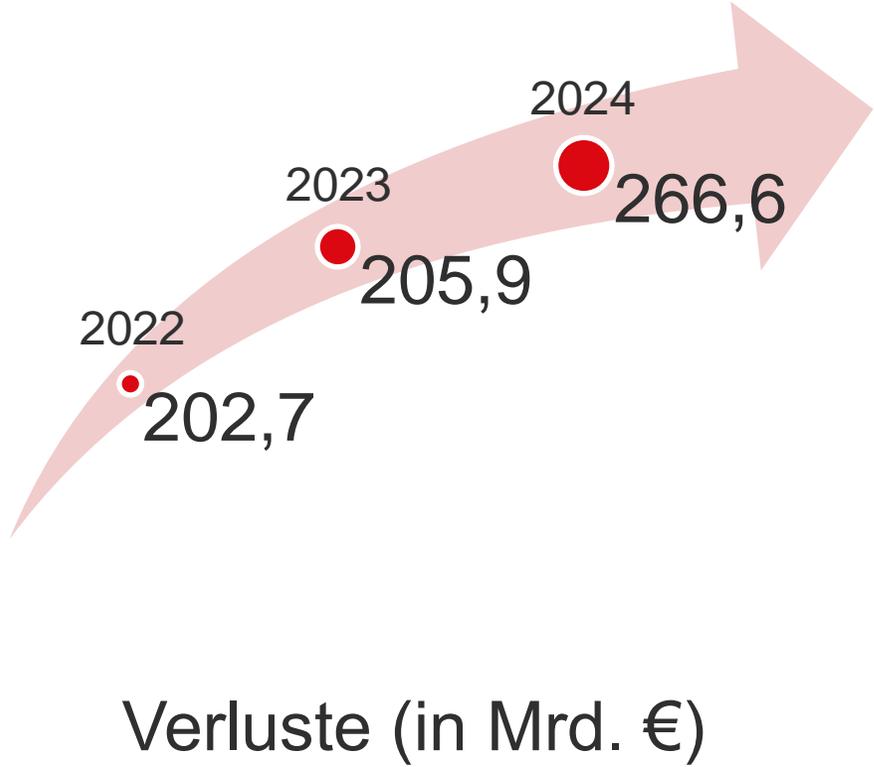
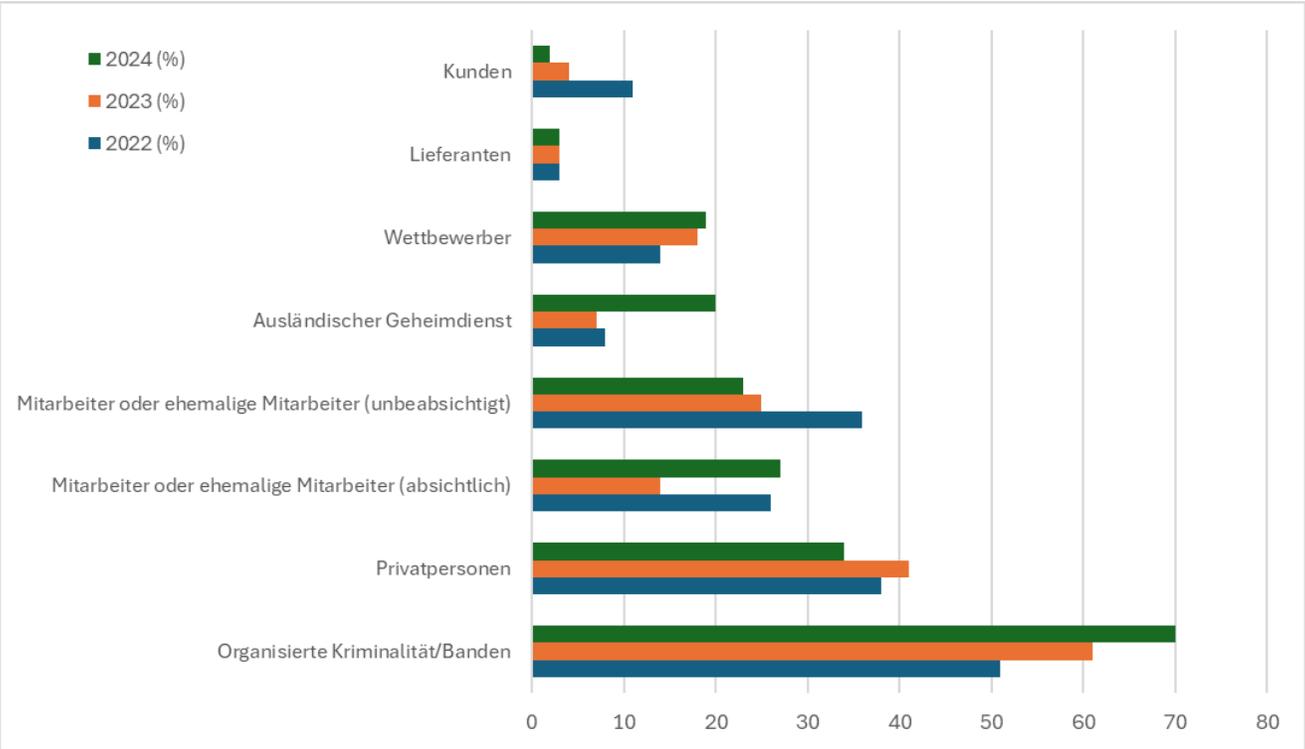
---

- **Aktuelle Bedrohungslage**
  - SAP-Security in Zahlen
  - Warum SAP-Security wichtig ist
  - Was sind die größten Bedrohungen
  - Wie Sicherheitsvorfälle erkannt werden
- **Strategien zur Abwehr**
  - Die Rolle von SIEM für SAP-Sicherheit
  - SAP SIEM Integration
- **Beispiel BCS: SAP SIEM Integration**
- **Fazit & Ausblick**

**claranet**

Make  
modern  
happen®

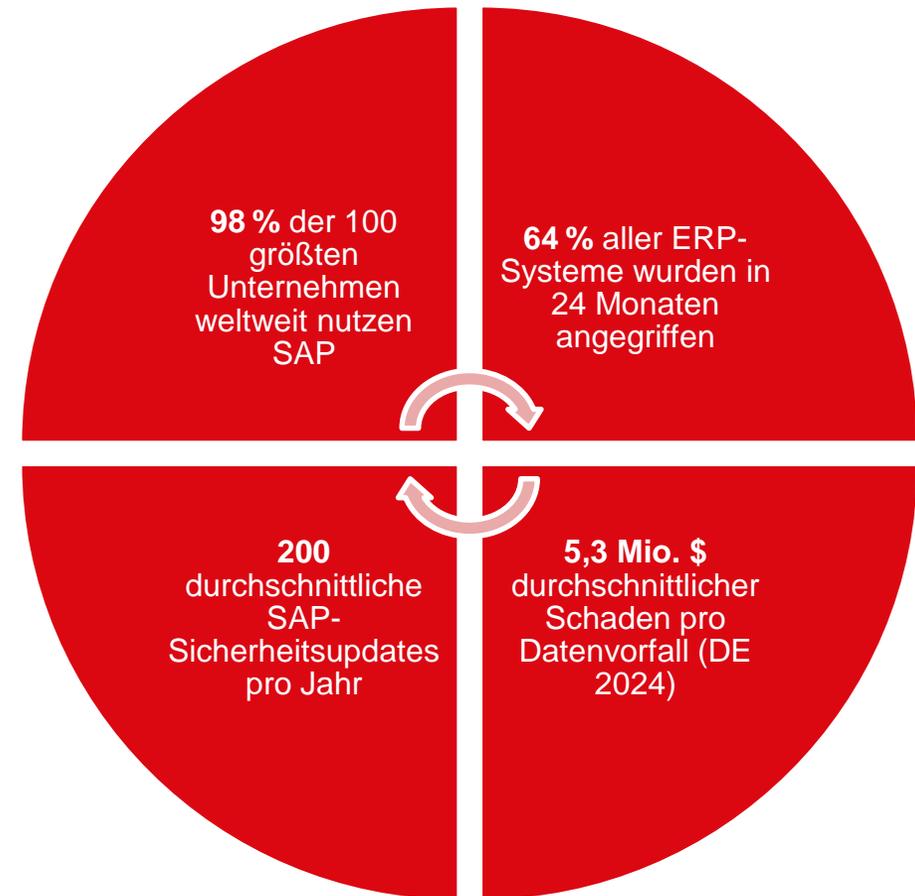
# Aktuelle Bedrohungslage



# Aktuelle Bedrohungslage

- **Warum SAP-Security wichtig ist**
  - SAP-Systeme sind Ziel von Cyberangriffen
  - Komplexe Angriffe führen zu Datenverlust & Ausfällen
  - Sicherheitsstrategie gewinnt an Bedeutung
- **Risiken & Angriffsvektoren**
  - Bisher: Fokus auf IT-/Finanzkontrollen
  - SAP enthält geschäftskritische Daten
  - Angriffe über bekannte Schwachstellen
- **Was Unternehmen tun sollten**
  - Ganzheitliche SAP-Sicherheitsstrategie einführen
  - Systeme aktiv überwachen
  - Bedrohungen proaktiv erkennen und abwehren

## SAP-Security in Zahlen



# Aktuelle Bedrohungslage

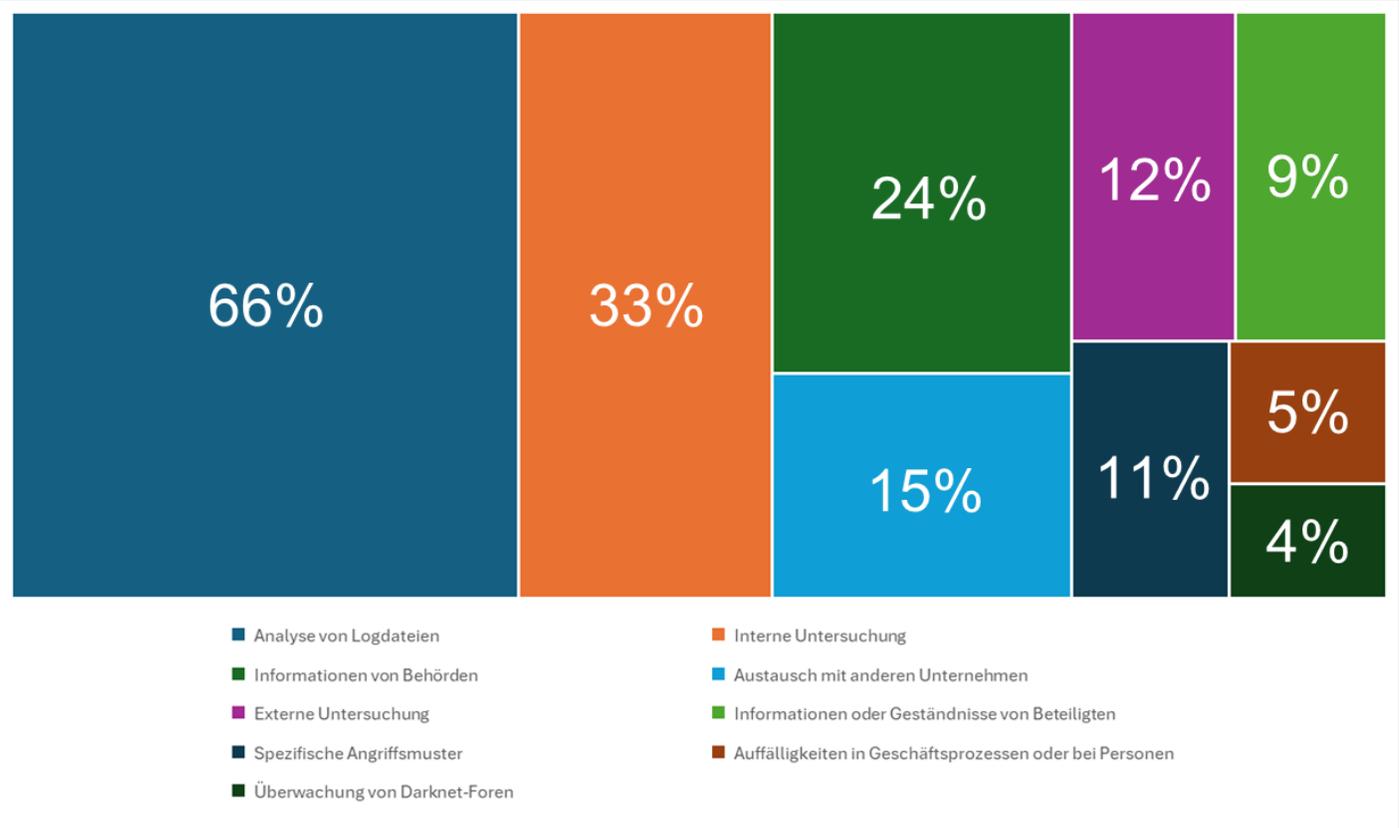
---

Was sind die größten Bedrohungen?

- Zu hohe Benutzer- und Rollenrechte
- Verzögerte oder fehlende Sicherheitspatches
- Unsichere Systemkonfigurationen und Einstellungen
- Unsicherer kundenspezifischer Code
- Fehlende Protokollierung und SIEM-Anbindung

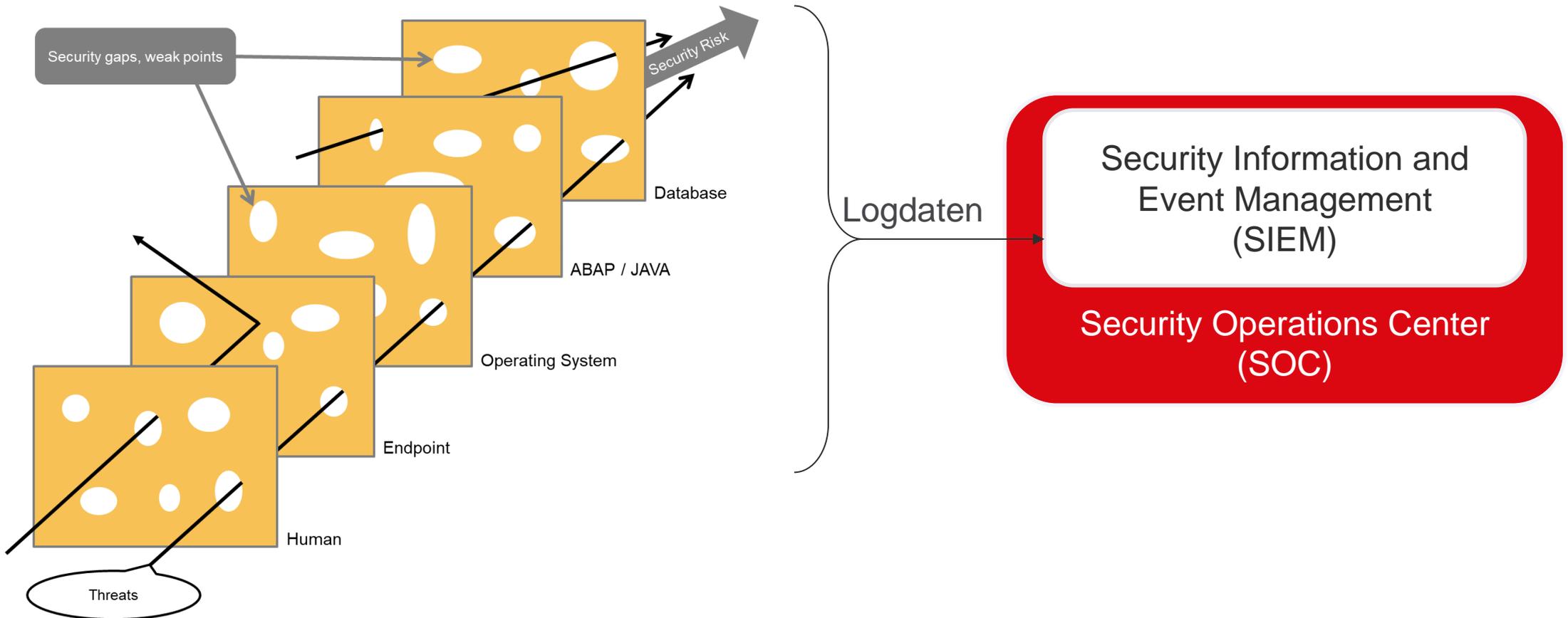
# Aktuelle Bedrohungslage

- Wie Sicherheitsvorfälle erkannt werden



Quelle: Bitkom – Corporate Security 2024,  
<https://www.bitkom.org/sites/main/files/2024-11/bitkom-study-corporate-security-2024.pdf>

# Strategien zur Abwehr



# Strategien zur Abwehr

---



## Die Rolle von SIEM für SAP-Sicherheit

(SIEM: Security Information and Event Management)

- Spezifische Bedrohungserkennung für SAP-Systeme
- Ereignis-Korrelation über Systeme hinweg
- Überwachung in „Near Realtime“ mit schneller Alarmierung
- Erkennung von Anomalien und unregelmäßigem Verhalten
- Risikoevaluation und Berichterstattung

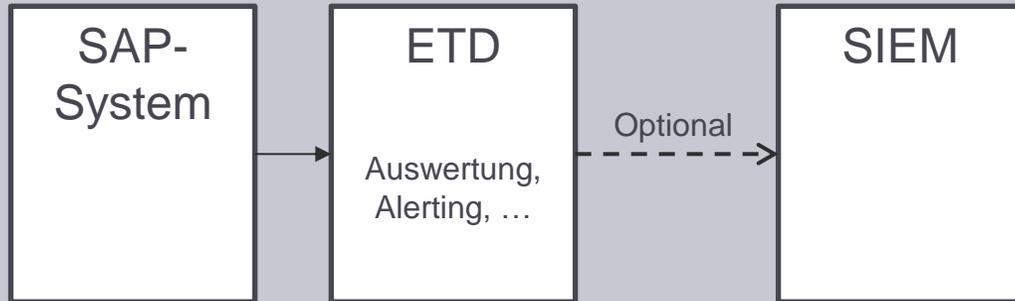
Claranet SecuritySuite for SAP technology

**claranet**

Make  
modern  
happen®

# Strategien zur Abwehr: SAP SIEM Integration

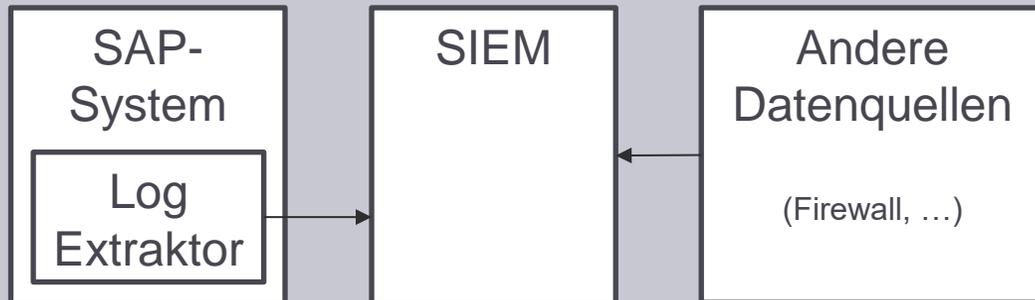
## Enterprise Threat Detection (ETD)



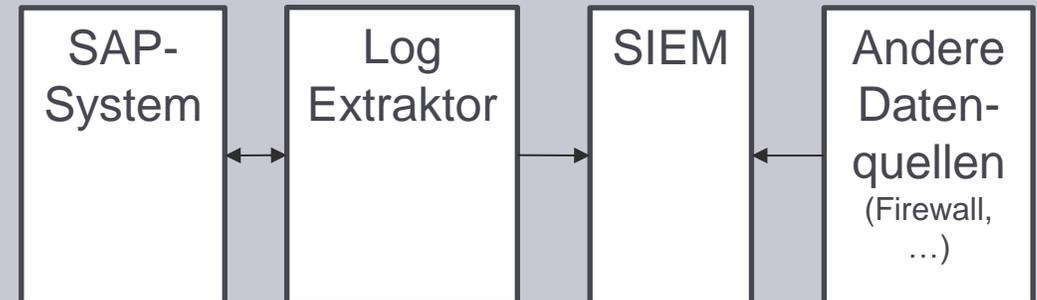
## Embedded SIEM



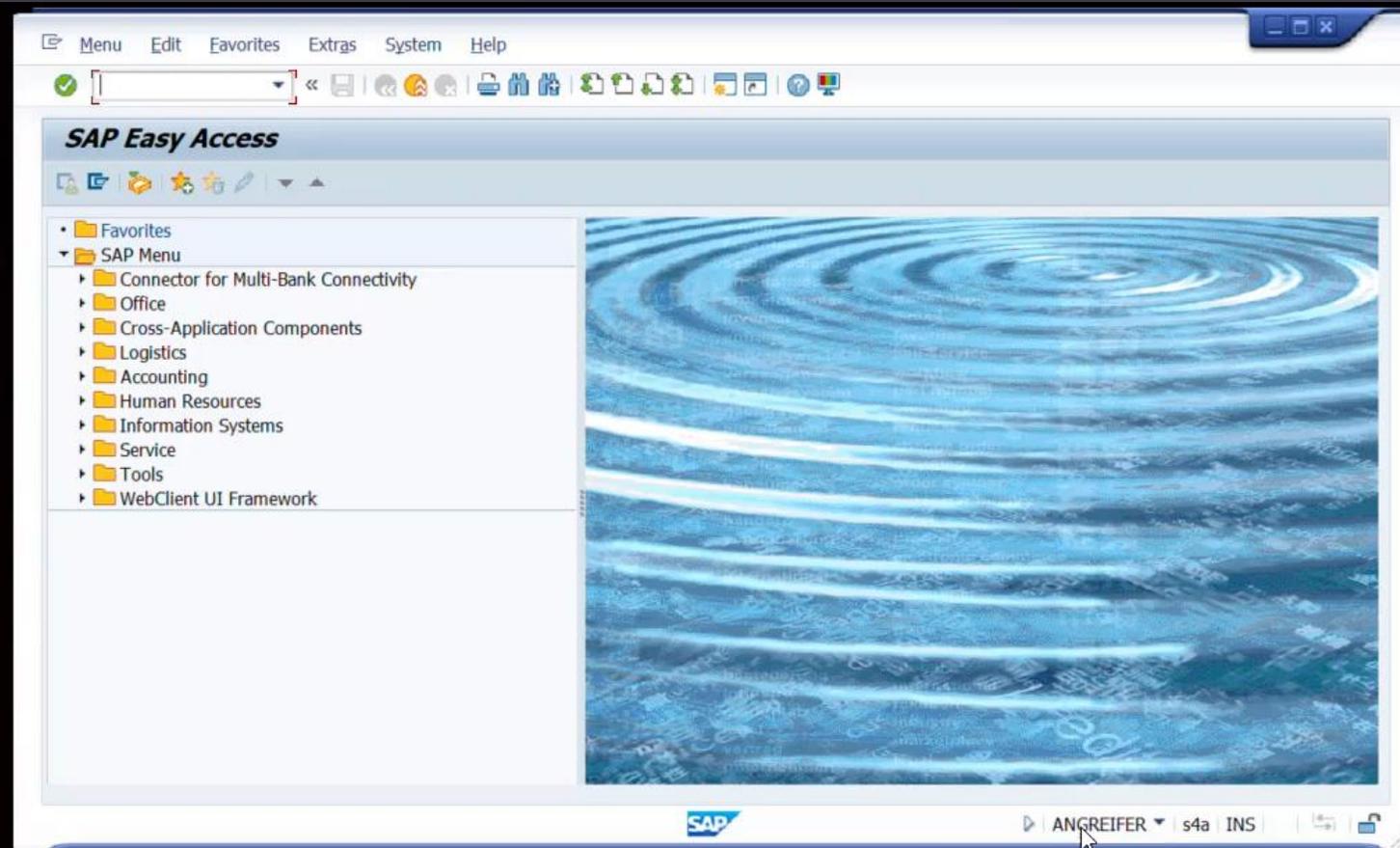
## ABAP Add-on / Transport



## Extern, Keine Codeänderungen



# Beispiel BCS: SAP SIEM Integration – Angreifer Sicht



# Beispiel BCS: SAP SIEM Integration – Events

TIME CREATED ▼	SENSOR	CUSTOM FIELD 1	CUSTOM FIELD 4	EVENT NAME ⚡	USERNAME ⚡	CUSTOM FIELD 9
Wed, Jun 18 2025, 04:51 PM	SAP-Sensor VMware	S4A	SI_SYSLOG	Goto ABAP Debugger: Source:(125)->(322)   ByteCode:AUTH(	ANGREIFER	
Wed, Jun 18 2025, 04:51 PM	SAP-Sensor VMware	S4A	SI_SYSLOG	> In program CL_SUID_TOOLS=====CM00G , line 0125, event AUTH_CHECK_INTERNA	ANGREIFER	
Wed, Jun 18 2025, 04:51 PM	SAP-Sensor VMware	S4A	SI_SYSLOG	Field content changed: SY-SUBRC -> 0	ANGREIFER	
Wed, Jun 18 2025, 04:51 PM	SAP-Sensor VMware	S4A	SI_SYSLOG	> In program CL_SUID_TOOLS=====CM00G , line 0322, event AUTH_CHECK_INTERNA	ANGREIFER	
Wed, Jun 18 2025, 04:51 PM	SAP-Sensor VMware	S4A	SI_SAL	User master record SAP_ADMIN was changed.	ANGREIFER	SAP_ADMIN
Wed, Jun 18 2025, 04:51 PM	SAP-Sensor VMware	S4A	SI_SAL	Password changed for user SAP_ADMIN in client 100	ANGREIFER	SAP_ADMIN
Wed, Jun 18 2025, 04:51 PM	SAP-Sensor VMware	S4A	SI_CHGDOC_UR	User changed - Password changed: 'New Password 1'->'New Password 2'	ANGREIFER	SAP_ADMIN
Wed, Jun 18 2025, 04:49 PM	SAP-Sensor VMware	S4A	SI_SYSLOG	Goto ABAP Debugger: Source:(36)->(322)   ByteCode:AUTH(7	ANGREIFER	
Wed, Jun 18 2025, 04:49 PM	SAP-Sensor VMware	S4A	SI_SYSLOG	> In program CL_SUID_TOOLS=====CM00G , line 0322, event AUTH_CHECK_INTERNA	ANGREIFER	
Wed, Jun 18 2025, 04:49 PM	SAP-Sensor VMware	S4A	SI_SYSLOG	> In program LSUSEU11 , line 0056, event AUTH_CHECK_TCODE	ANGREIFER	
Wed, Jun 18 2025, 04:49 PM	SAP-Sensor VMware	S4A	SI_SYSLOG	Goto ABAP Debugger: Source:(26)->(56)   ByteCode:CALY(26	ANGREIFER	
Wed, Jun 18 2025, 04:49 PM	SAP-Sensor VMware	S4A	SI_SYSLOG	> In program CL_SUID_TOOLS=====CM00G , line 0036, event AUTH_CHECK_INTERNA	ANGREIFER	
Wed, Jun 18 2025, 04:49 PM	SAP-Sensor VMware	S4A	SI_SYSLOG	Field content changed: SY-SUBRC -> 0	ANGREIFER	
Wed, Jun 18 2025, 04:49 PM	SAP-Sensor VMware	S4A	SI_CHGDOC_UR	User changed - Profile added: "->'SAP_ALL'	ANGREIFER	ANGREIFER

# Beispiel BCS: SAP SIEM Integration – Alerts

TIME CREATED	SENSORS	ALARM SUMMARY	USERNAME	CUSTOM FIELD 9	PRIORITY	ALARM STATUS
Wed, Jun 18 2025, 04:51 PM	SAP-Sensor VMware	 Privilege Escalation Password Reset for Admin User by Another User 19 minutes ago	ANGREIFER	SAP_ADMIN	High	open
Wed, Jun 18 2025, 04:49 PM	SAP-Sensor VMware	 Privilege Escalation Unauthorized User Change via Debugging 21 minutes ago	ANGREIFER	ANGREIFER	High	open
Wed, Jun 18 2025, 04:49 PM	SAP-Sensor VMware	 Privilege Escalation Authorization Bypass via Debugging 21 minutes ago	ANGREIFER		High	open
Wed, Jun 18 2025, 04:49 PM	SAP-Sensor VMware	 Privilege Escalation Assigning High-Risk Profiles 21 minutes ago	ANGREIFER	ANGREIFER	High	open

# Beispiel BCS: SAP SIEM Integration – Alarm Details

☆  **Privilege Escalation** ← previous | next > ✕

Unauthorized User Change via Debugging  
28 minutes ago

[Select Action](#) [Create Rule](#) [Run Playbook](#) 

### Alarm Details

PRIORITY	High
ALARM STATUS	Open 
SAP SYSTEM ID (CUSTOM FIELD 1)	S4A
BCS EXTRACTOR (CUSTOM FIELD 4)	SL_CHGDOC_UR
REPORTING DEVICE RULE ID	U0
FULL MESSAGE	User changed - Password changed: 'New Password 1'->'New Password 2'
USERNAME	ANGREIFER
SAP TRANSACTION CODE (CUSTOM FIELD 7)	KRNL
AFFECTED OBJECT (CUSTOM FIELD 9)	ANGREIFER
STRING3 (CUSTOM FIELD 12)	New Password 2

SEVERITY	10
RULE DESCRIPTION	This implies that an authorization check was bypassed using the SAP Debugger by modifying system variables (e.g., changing 'sy-subrc' values) to gain unauthorized access to restricted transactions, in order to change a user master record (e.g. assign high-privileged profile/role/group, change password, etc..)
SENSORS	SAP-Sensor VMware
LABELS	
INVESTIGATIONS	
NOTES	

---

Source  DE-0975   
DE-0975 

Destination  s4a.dev.siem.logpoint.mgt.de.clara.net 

### Associated Events

☆ [User changed - Password changed: 'New Password 1'->'New Password 2'](#)   
Jun 18, 2025, 4:05:12 PM

☆ [> in program CL\\_SUID\\_TOOLS=====CM00G , line 0322, event AUTH\\_CHECK\\_INTERNA](#)   
Jun 18, 2025, 4:49:13 PM

# Beispiel BCS: SAP SIEM Integration – Reports

The screenshot displays the ClaranetOnline security manager interface. The browser address bar shows the URL `stage-online.claranet.de/security-manager#`. The page header includes the Claranet logo, navigation links like "Explore Claranet services" and "Create Ticket", and a user profile for "Test User". The main content area is titled "Managed Detection and Response" and features a navigation bar with status filters: "Offen", "Geschlossen", "Neu", "In Bearbeitung", "Wartet auf Kunde" (with a red '1' indicator), and "Resolved". A search bar and "Aktualisieren" button are also present. The ticket list below shows a single entry with the following details:

Ticketnr.	Beschreibung	Status	Priorität	Erstelldatum	Anzeigen
SEC0009150	Privilege Escalation and Admin Account Compromise	WARTET AUF KUNDE	CRITICAL	20-06-2025 15:04	→

At the bottom of the page, there is a footer with contact information: "claranet | Sales: 069/408018-450 | Support: 069/408018-300 | Impressum | Cookie-Einstellungen | Datenschutzerklärung | v.5.1.0".

# Beispiel BCS: SAP SIEM Integration – Reports

SEC0009150 Privilege Escalation and Admin Account Compromise  
Erstelldatum: 20-06-2025 15:04 WARTET AUF KUNDE

Weitere Ticketdetails

**B I U** Ticket aktualisieren →

Type your update here...

Claranet SOC Hinzugefügt: 20-06-2025 15:04

Security Incident: Privilege Escalation and Admin Account Compromise

-----

GENERAL:  
Detection Date (DD/MM/YYYY): 03/07/2025  
Detection Time: 2:17:22 PM  
Location(s)/Sensor: SAP-Sensor

-----

INCIDENT TIMELINE & RECOMMENDATIONS:

The SOC has been alerted to unauthorized privilege escalation activity involving the user "ANGREIFER" on the SAP system "S4A". The attacker leveraged the debugging functionality to bypass authorization checks, allowing them to assign the "SAP\_ALL" profile to their account at 2:17:22 PM. This profile grants unrestricted access across the SAP system. Following this, the attacker used their elevated privileges to reset the password for the high-privileged "SAP\_ADMIN" account in client 100 at 2:19:42 PM, subsequently gaining control over this critical administrative account. These actions indicate deliberate privilege escalation, possibly by an insider.

We recommend the following measures:

- 1) Revoke "SAP\_ALL" from user "ANGREIFER", disable the account, and revoke any open user sessions
- 2) Reset credentials for "SAP\_ADMIN", disable the account, and revoke any open user sessions
- 3) Investigate for any suspicious activities performed by users "ANGREIFER" and "SAP\_ADMIN".

At this time, no further unauthorized activity has been observed, and we recommend implementing the above measures immediately to mitigate potential risks.

The SOC continues to investigate this incident and will provide ongoing updates as the investigation progresses.

-----

ENTITY INFORMATION:

SAP System ID: S4A  
SAP Client: 100  
Username: ANGREIFER  
Assigned profile: SAP\_ALL  
Affected user: SAP\_ADMIN

-----

Ticket erstellt

# Fazit & Ausblick



- **SIEM-Integration für SAP:**
    - Zusammenspiel von klassischer SAP-Security und zentralem Monitoring
    - Einheitliches Monitoring für SAP- und Nicht-SAP-Systeme
    - Ganzheitliche Erkennung von Bedrohungen durch Ereignis-Korrelation
    - Nahezu Echtzeitüberwachung für schnelle Alarmierung und Berichterstattung
  - **Proaktive Sicherheitsansätze:**
    - Regelmäßige Bewertungen der Sicherheitslage zur frühzeitigen Risikoeinschätzung
    - Klare Delegation von Verantwortlichkeiten für SIEM und Security Management
- ⇒ Abstimmung von Sicherheitsmaßnahmen für eine ganzheitliche und effektive Abwehr

