SAP Security:
Schutz geschäfts-kritischer Systeme

Christian Schuller – Security Consultant

claranet | Make modern happen®

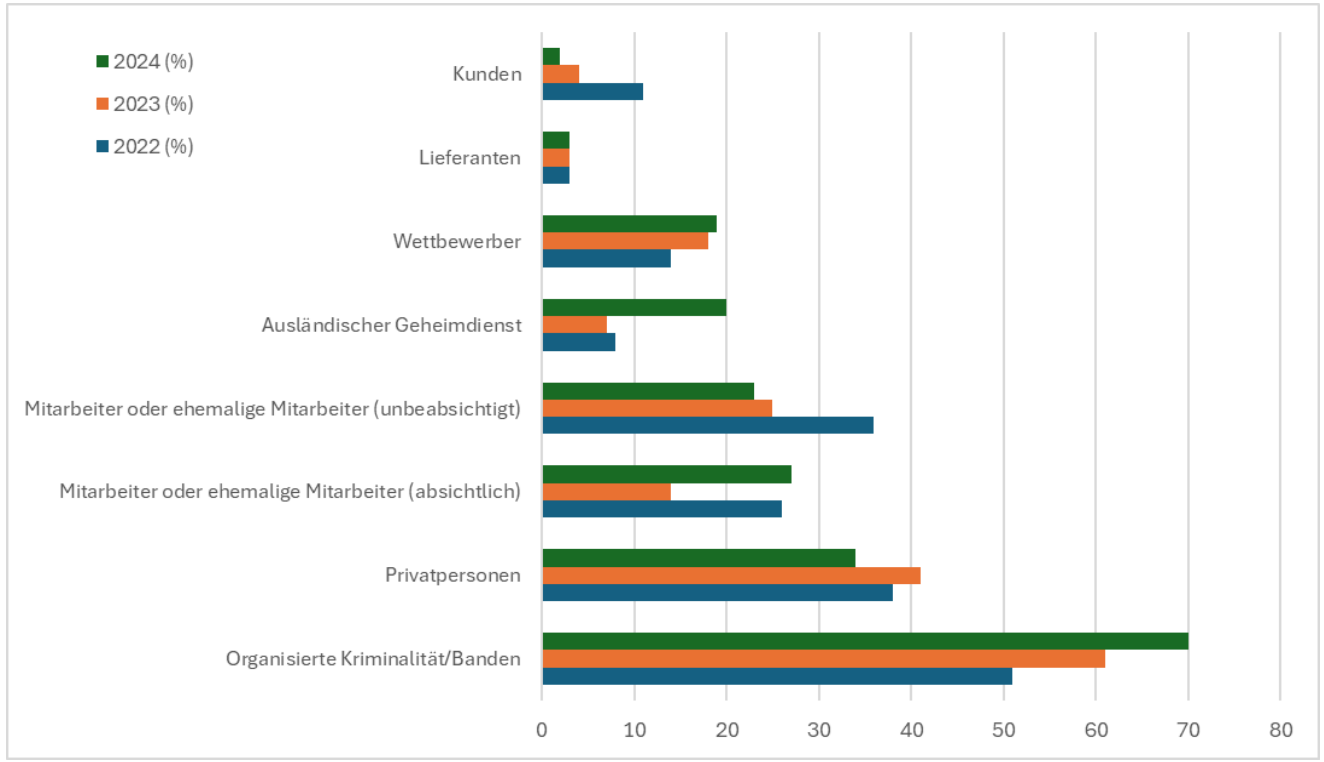
PUBLIC
Verantwortlich: Claranet GmbH
Version 1.0 – 03.07.2025

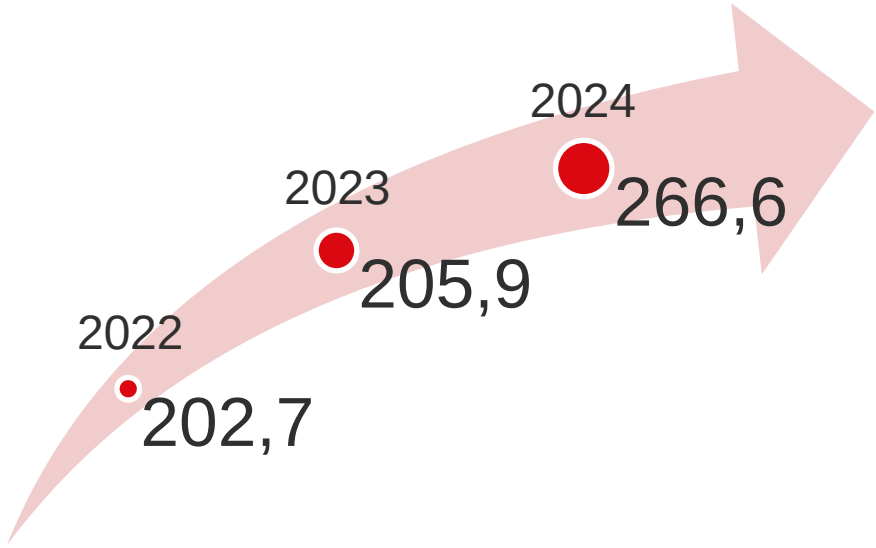
Agenda

- **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





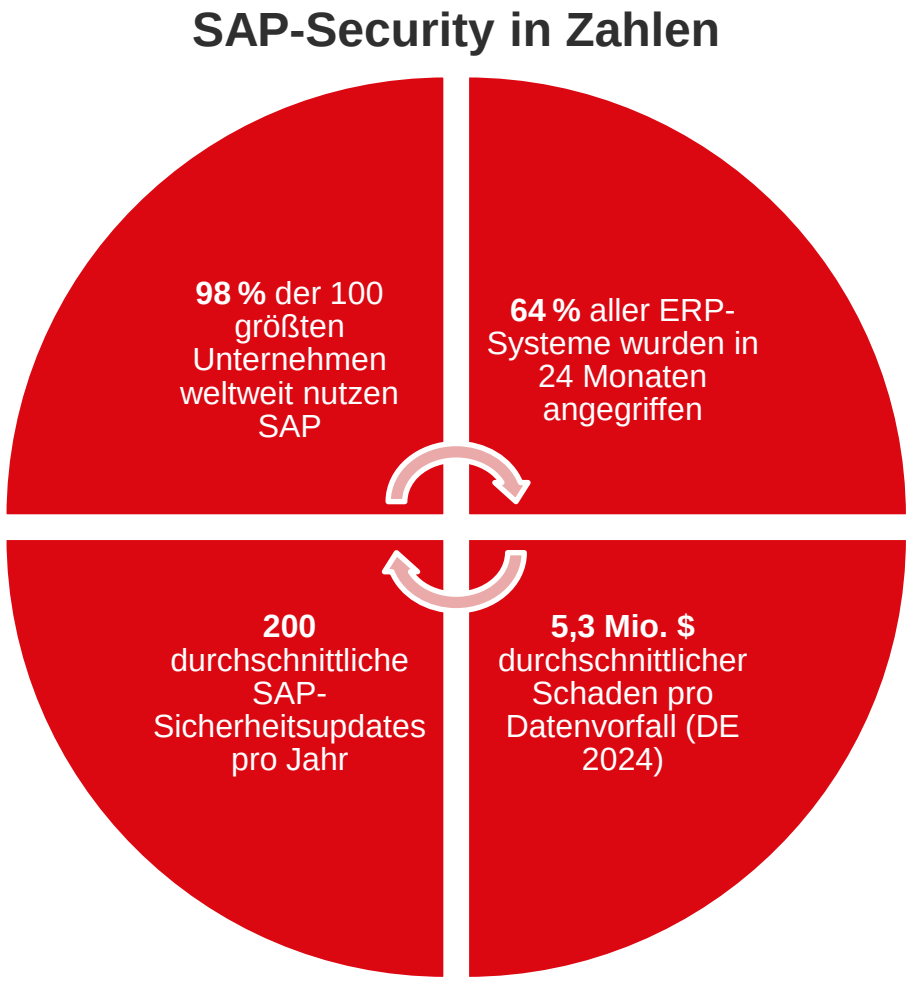
Verluste (in Mrd. €)

claranet | Make modern happen®

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

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

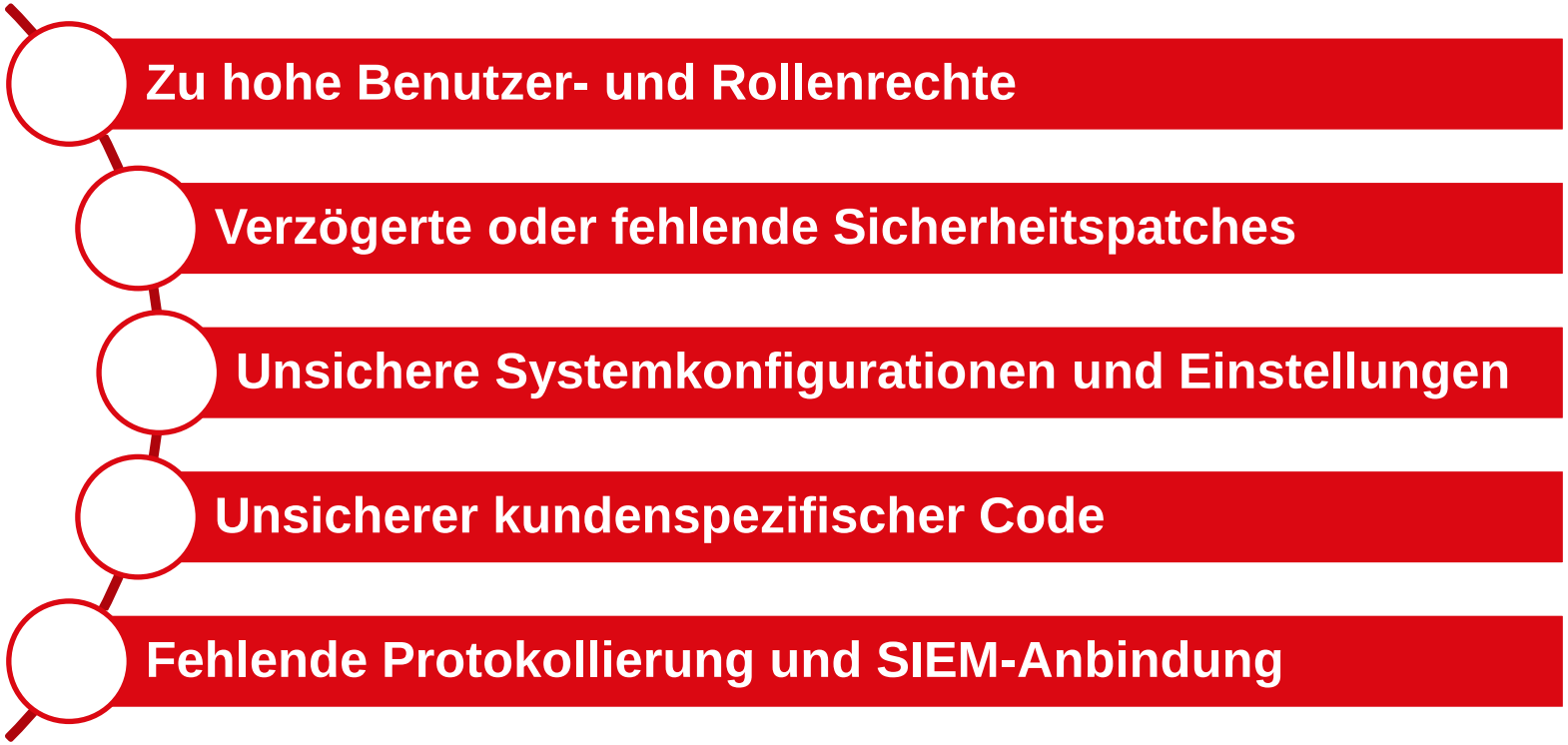


claranet | Make modern happen®

Quelle: KPMG – SAP Security (2025), https://hub.kpmg.de/de/whitepaper-sap-security

Aktuelle Bedrohungslage

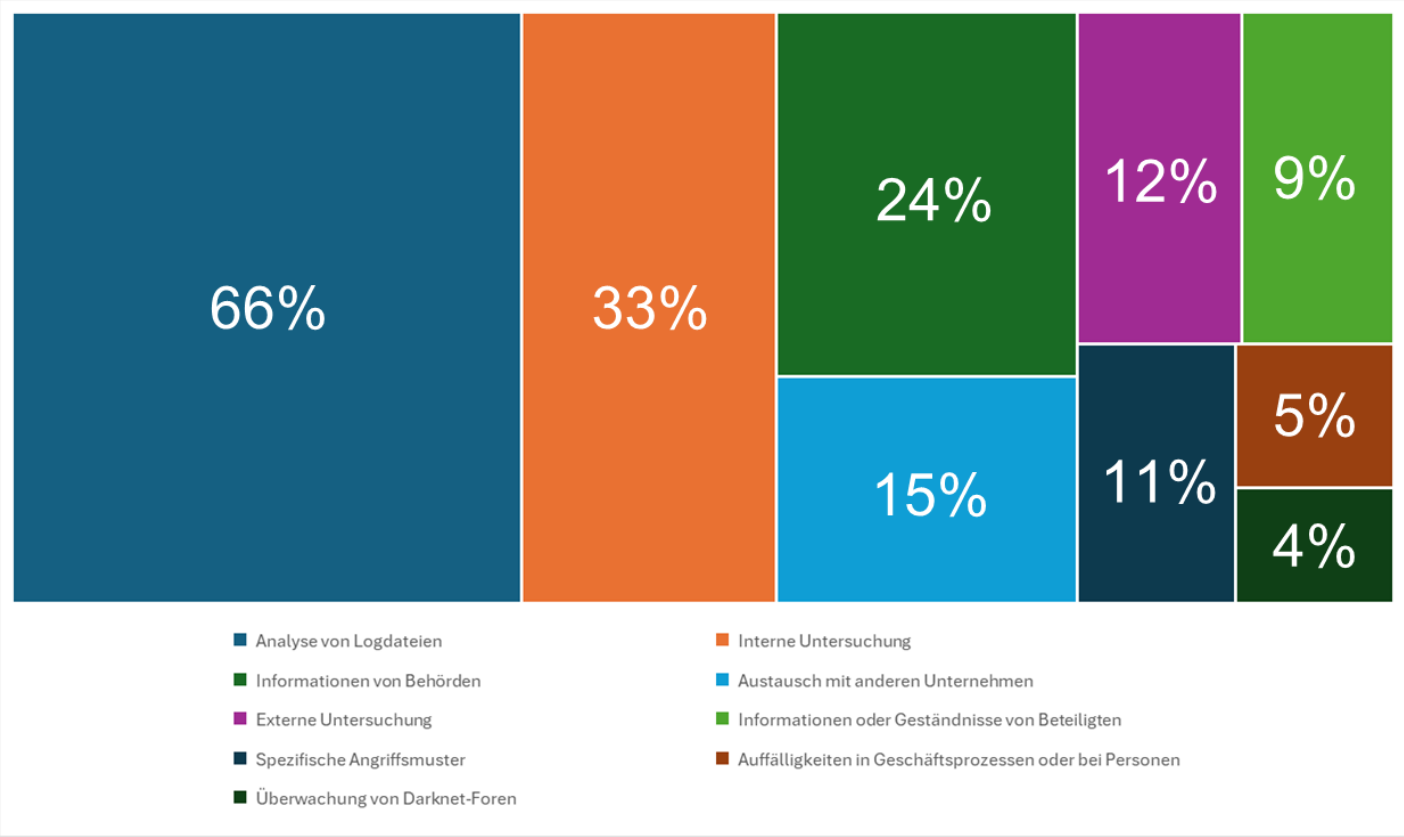
Was sind die größten Bedrohungen?



claranet | Make modern happen®

Aktuelle Bedrohungslage

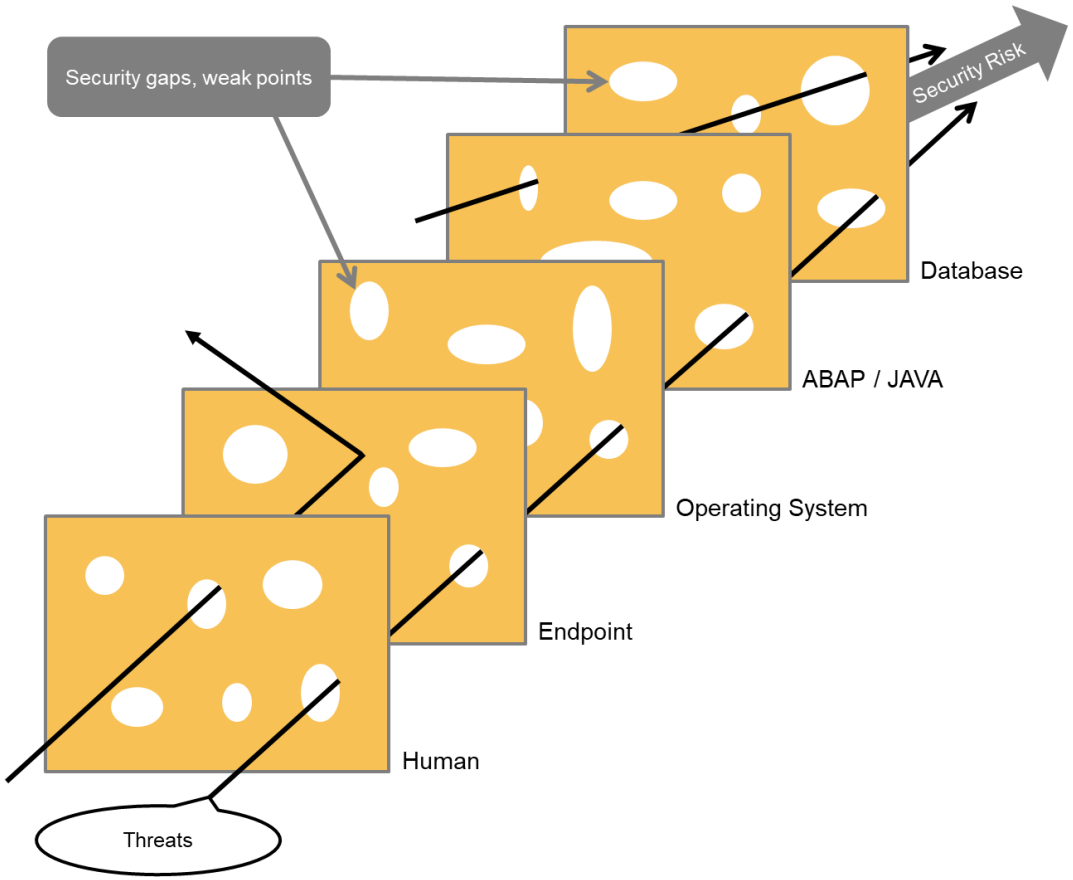
- Wie Sicherheitsvorfälle erkannt werden



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

claranet | Make modern happen®

Strategien zur Abwehr



Logdaten

Security Information and Event Management (SIEM)

Security Operations Center (SOC)

claranet | Make modern happen®

Strategien zur Abwehr

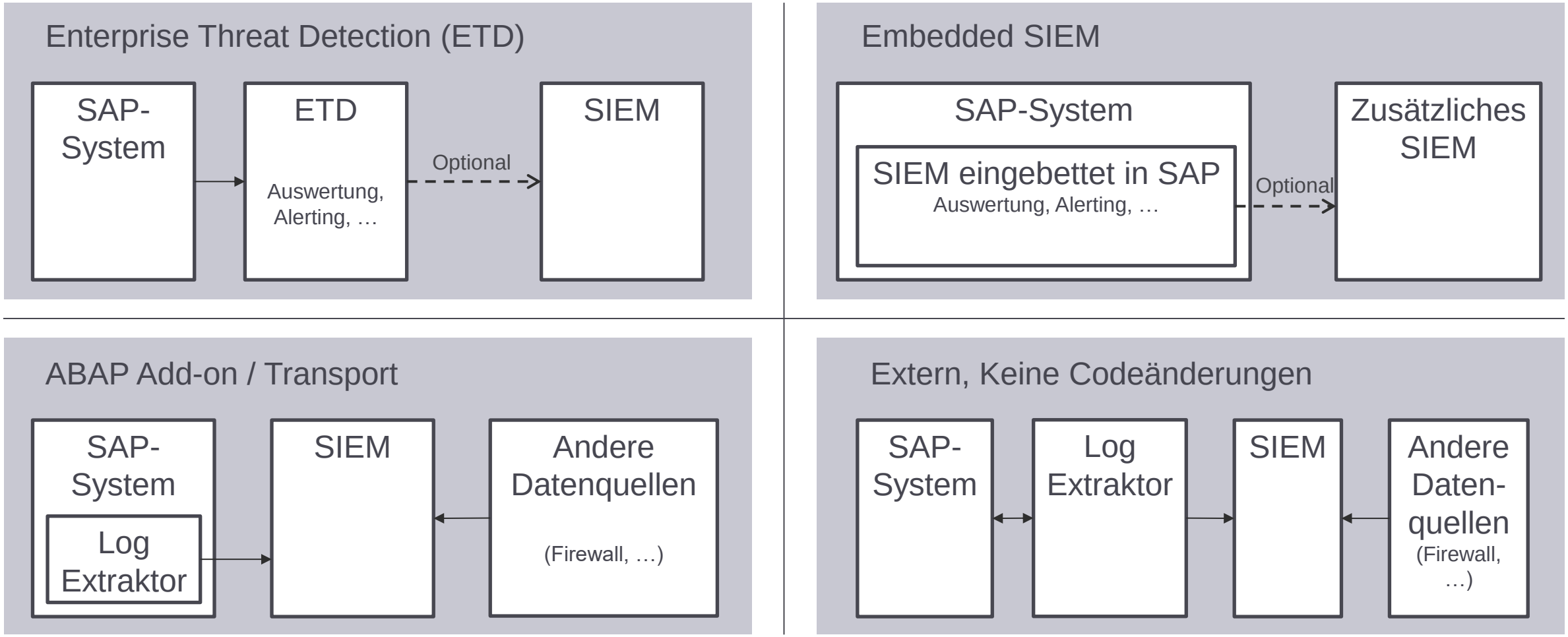
Die Rolle von SIEM für SAP-Sicherheit
(SIEM: Security Information and Event Management)

- 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®

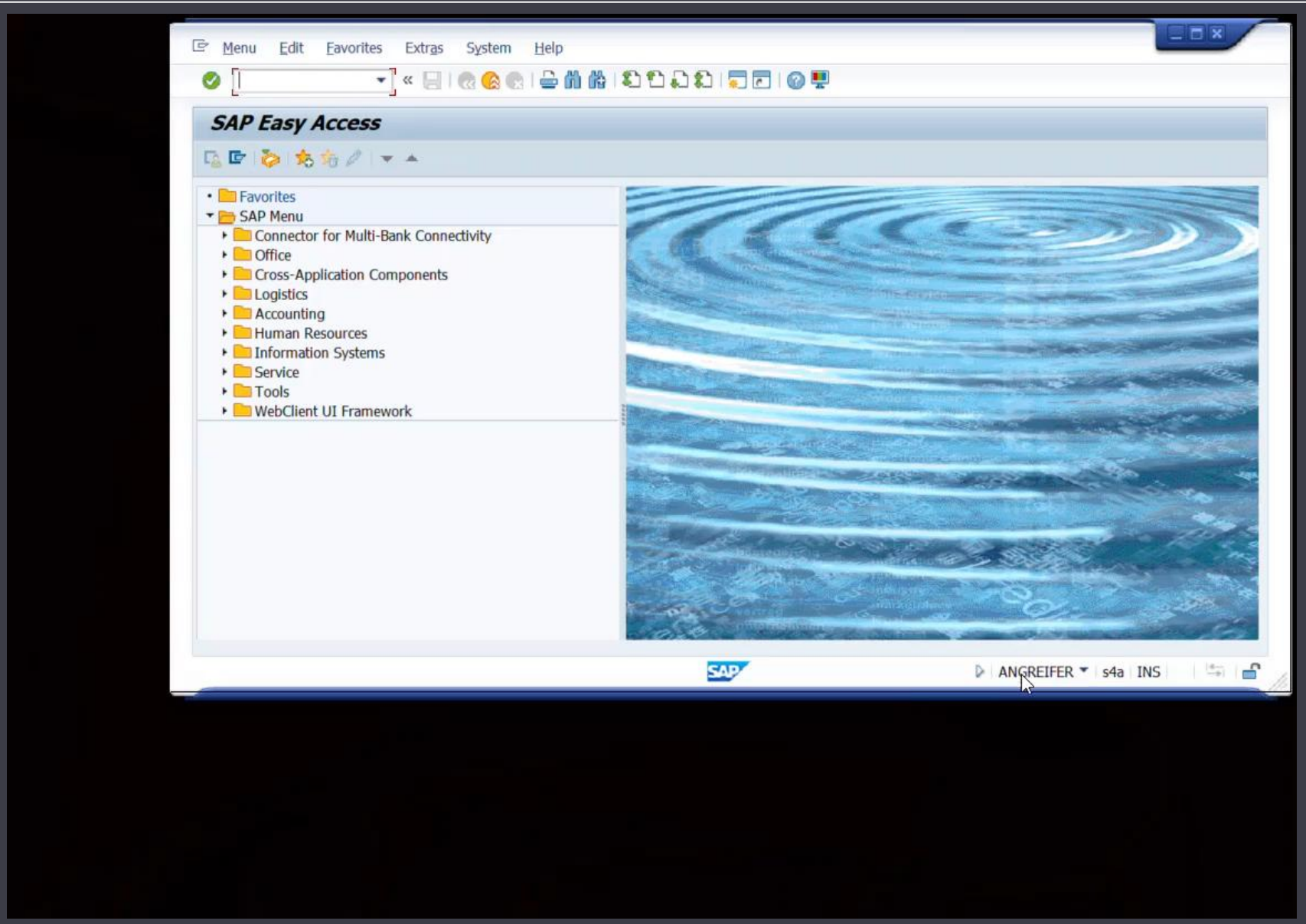
Strategien zur Abwehr: SAP SIEM Integration



claranet | Make modern happen®

SIEM: Security Information and Event Management

Beispiel BCS: SAP SIEM Integration – Angreifer Sicht



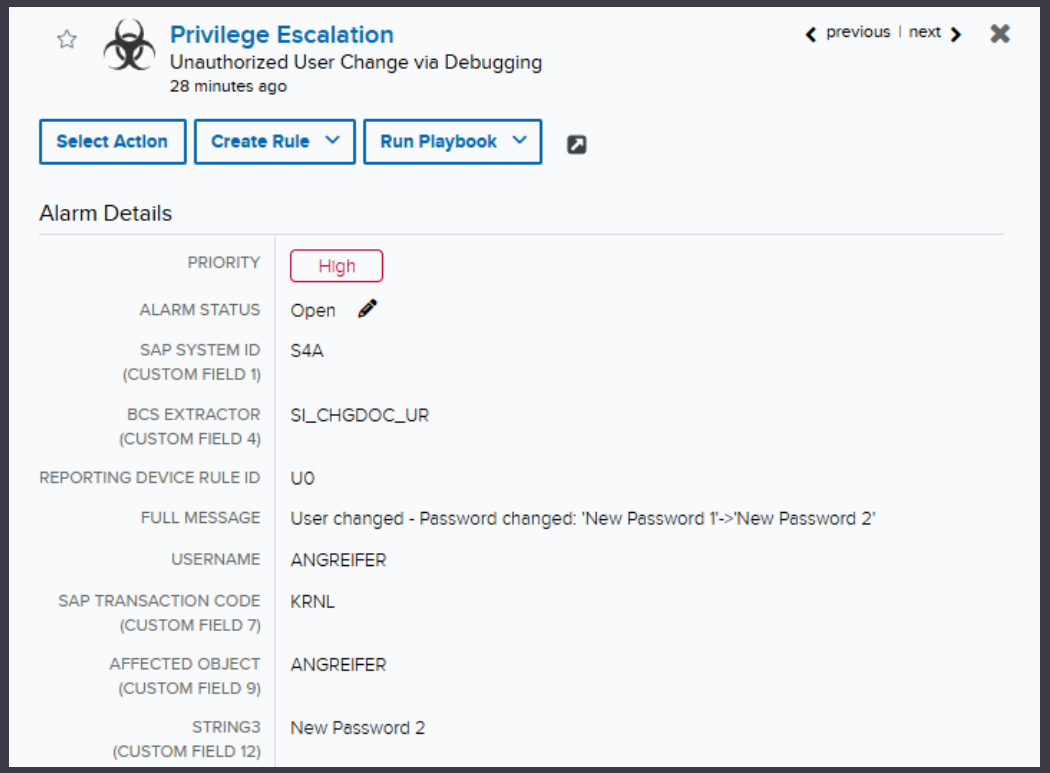
Beispiel BCS: SAP SIEM Integration – Events

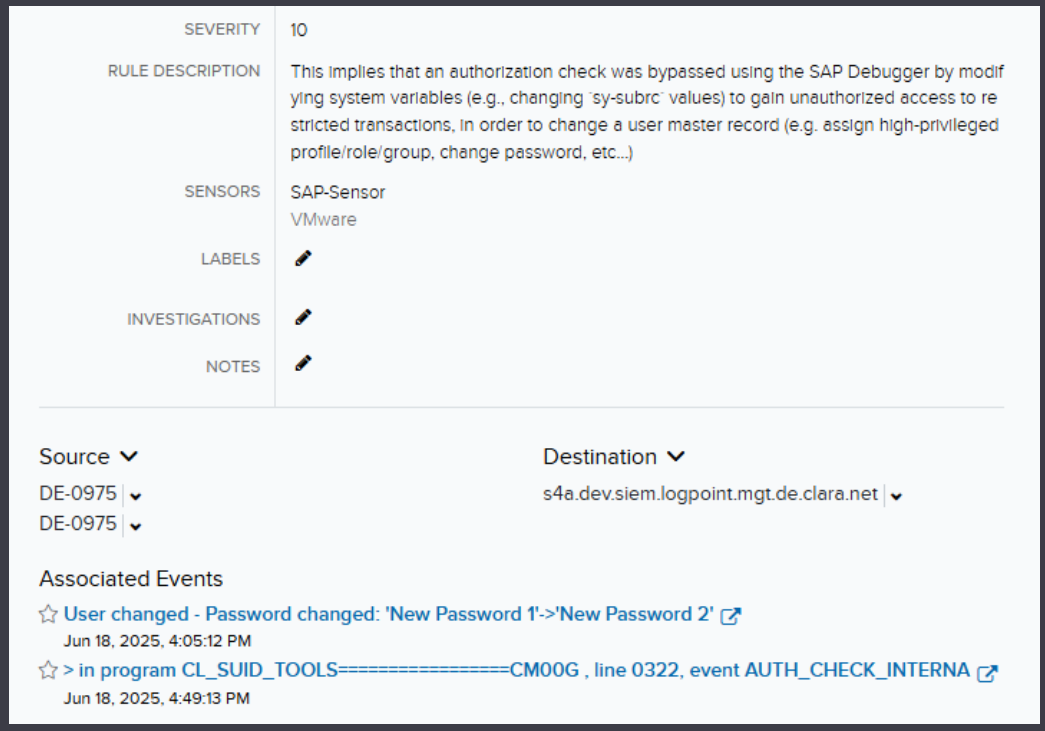
TIME CREATED	SENSOR	CUSTOM FIELD 1	CUSTOM FIELD 4	EVENT NAME	USERNAME	CUSTOM FIELD 9
Wed, Jun 18 2025, 04:51 PM	SAP-Sensor VMware	S4A	SI_SYSLOG	Goto ABAP Debugger: Source:(125)->(322) I ByteCode:AUTH(	ANGREIFER	
Wed, Jun 18 2025, 04:51 PM	SAP-Sensor VMware	S4A	SI_SYSLOG	> In program CL_SUID_TOOLS==========CM00G , 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) I 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) I 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

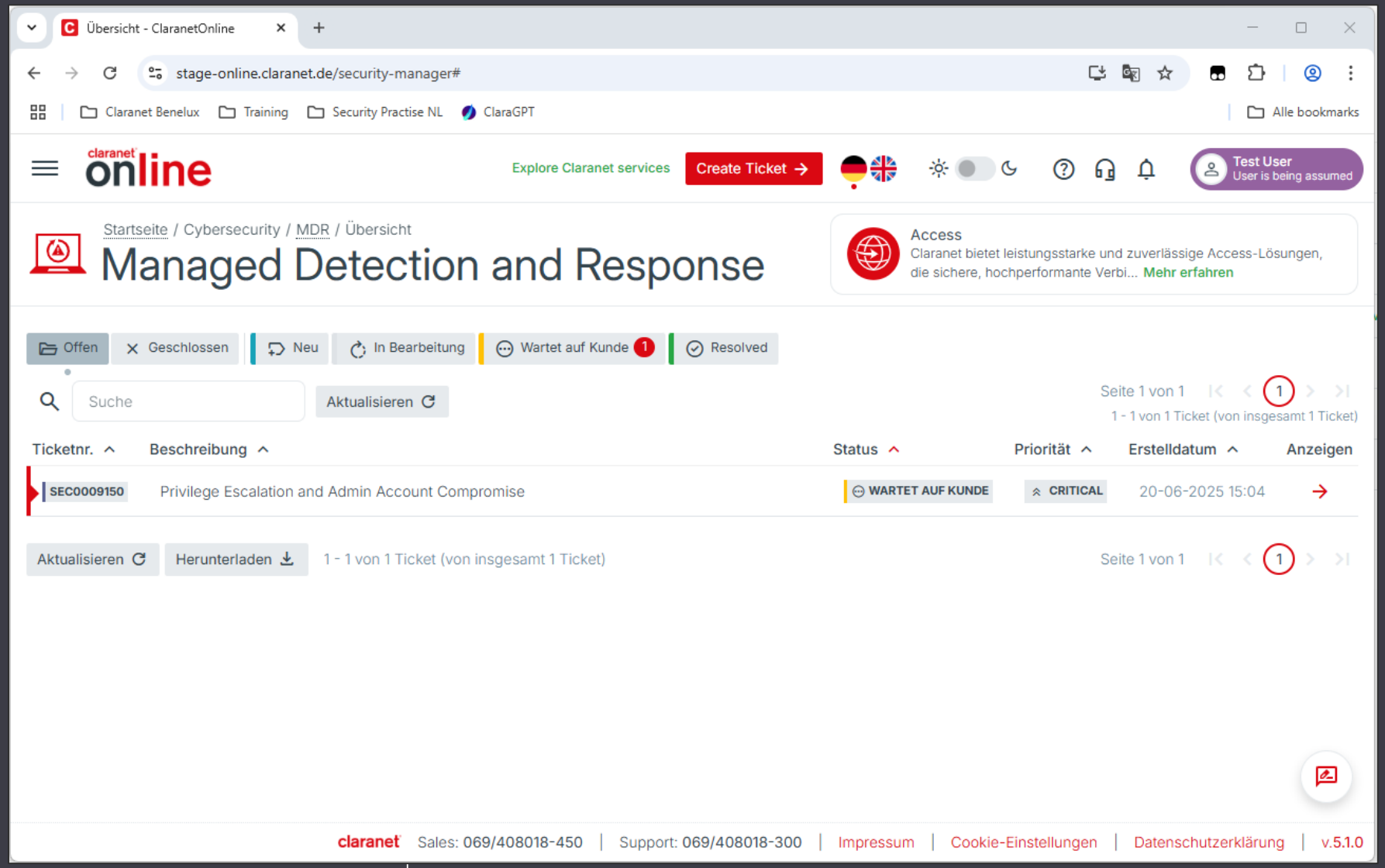
TIME CREATED	SENSORS	ALARM SUMMARY	USERNAME	CUSTOM FIELD 9	PRIORITY	ALARM STATUS
Wed, Jun 18 2025, 04:51 PM	SAP-Sensor VMware	Privilege Escalation Password Reset for Admin User by Another User 19 minutes ago	ANGREIFER	SAP_ADMIN	High	open
Wed, Jun 18 2025, 04:49 PM	SAP-Sensor VMware	Privilege Escalation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

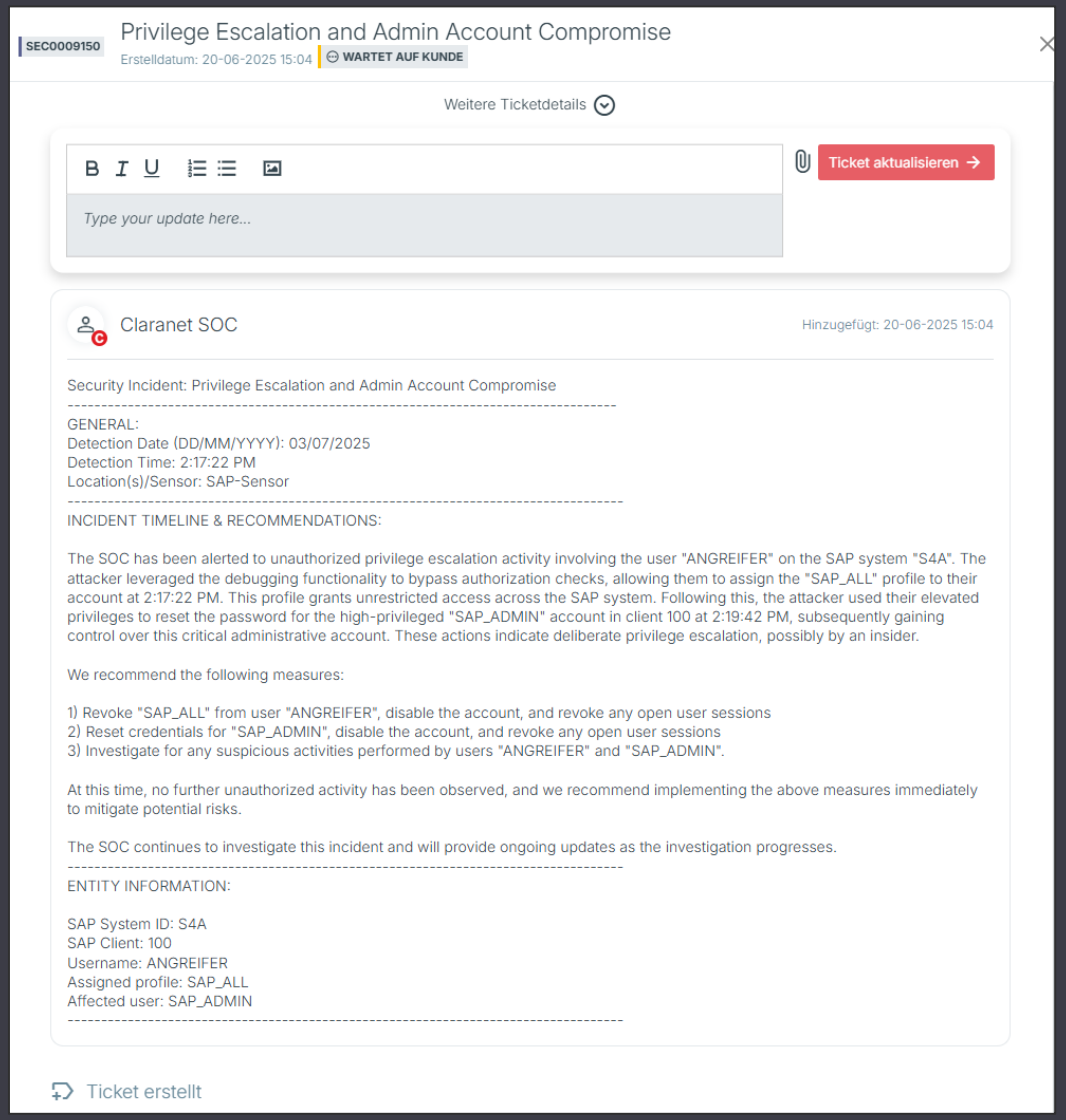




Beispiel BCS: SAP SIEM Integration – Reports



Beispiel BCS: SAP SIEM Integration – Reports



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 Delegierung von Verantwortlichkeiten für SIEM und Security Management

⇒ Abstimmung von Sicherheitsmaßnahmen für eine ganzheitliche und effektive Abwehr

claranet | Make modern happen®

PUBLIC
Verantwortlich: Claranet GmbH
Version 1.0 – 03.07.2025