SAP Security Group Deutschland

Innovation gemeinsam erleben

3./4. Juni 2025

SAP Security Monitoring für hybride SAP-Landschaften

Marc Spitzer, Xiting GmbH

Inhaltsverzeichnis

Herausforderungen für das SAP Security Monitoring

Aktuelle SAP Security Monitoring Herausforderungen

Datenschutzgesetze (DSG, GDPR) und neue IT-Regularien (NIS2, DORA)

- Datenschutzgesetze erfordern zunehmend die **separate Protokollierung** bei der Handhabung von personenbezogenen Daten
- Für **CH** ist seit Sept. 23 eine neue Verordnung des DSG in Kraft , **Kap 1, Art. 4 – Protokollierung**
  - Bei Verarbeitung von **„besonders schützenswerten Personendaten“** (User Master, Business Partner)
  - Dies ist auf **alle Applikationen** inkl. Datenbanken anzuwenden, welche personenbezogenen Daten automatisiert verarbeiten.
  - Aufbewahrung der relevanten Logs **in externem System für mindestens ein Jahr**

Integration SAP Landschaften & Cloud Transformation

- Keine **native Möglichkeit** zur Anbindung von SAP-Systemen an applikations-neutrales SIEM- oder Storage-Systeme (wie z.B. Splunk, Elastic)
- Anbindung zahlreicher unterschiedlicher Satellitensysteme und Anwendungen in **hybriden SAP-Landschaften** (On-Premise und SaaS)
- SAP Cloud und SaaS – Anwendungen mit produktiven Daten haben einen gleichen oder **höheren Schutzstandard** einzuhalten (Externe Zugriffe, Hohe Konnektivität

Herausforderungen und Erfahrungen mit der Integration von Cloud Logs

1. Abhängigkeit von Schnittstellen / APIs für die Integration von Cloud Logs

- Die Integration von Cloud Audit Logs erfordert jeweils die Implementierung neuer Schnittstelle (z.B. API-basierte Zugriffe) per Cloud Anwendung.
- API-basierte Zugriffe müssen vorhanden, freigegeben (SAP Clean Core Strategie & Zero-Footprint) und performant sein.
- Cloud-APIs haben geringe Flexibilität hinsichtlich Einstellungsmöglichkeiten im Standard (vgl. 4 BTP fixe Audit Log Kategorien vs. 200+ konfigurierbare ABAP SAL Events).
- BTP Audit Log Management Service etabliert sich langsam als Standard API für BTP-Anwendungen und weiterer Cloud-Anwendungen (wie IAS)
  - BTP-Anwendungsentwickler müssen diese Logs jedoch bewusst implementieren für Ihre Anwendung.

Es benötigt ein zentrales SAP Cloud Hub zur Konsumierung, Interpretation und erweiterter Konfiguration unterschiedlicher Cloud Log-APIs

Herausforderungen und Erfahrungen mit der Integration von Cloud Logs

2. Unterschiedliche Log-Quellen und Log-Formate:

- Cloud-Applikationen liefern ihre Security Logs oft in unterschiedlichen Formaten und mit unterschiedlichen Felddefinitionen. Diese Unterschiede erschweren eine konsistente und einheitliche Analyse.
- Cloud-Logs sind häufig sehr technisch und nicht durch Security-Anwender lesbar.

→ **Zentrale Threat Detection, welche die Cloud Logs interpretieren, Bedrohungsmuster analysieren und aufbereiten kann**

3. Datenverfügbarkeit und -speicherung:

- In Cloud-Umgebungen ist es schwierig, langfristig auf Sicherheitsdaten zuzugreifen oder diese zu speichern, da Speicherorte und Aufbewahrungsrichtlinien oft vom Cloud-Anbieter vorgegeben werden. (Beispiel BTP Audit Log Management Service Free vs. Paid)

→ **zentrale Log-Extraktion und Persistierung auf externem SIEM-System**

Beispiel BTP Audit Log Management Service

User user/sap.default/mspitzer@xiting.de

Category audit.configuration

Data


```
"space_id": "4e103f72-8b8c-40c7-8791-fd2afd51c4c4",
"app_or_service_id": "f69a0abe-0cee-4d6f-a97d-3a44e9395c07",
"als_service_id": "47dc5776-73b2-4358-b62b-2693d59ad522",
"user": "user/sap.default/mspitzer@xiting.de",
"category": "audit.configuration",
"format_version": "",
"message": {
  "uuid": "d07bb11c-3f55-49a6-b6a3-b3db08059dfb",
  "user": "user/sap.default/mspitzer@xiting.de",
  "time": "2025-03-12T12:51:47.276805Z",
  "id": "ff55108e-200d-4c44-8cfa-53bf9ea1341a",
  "success": true,
  "object": {
    "type": "scim user",
    "id": {
      "crudType": "CREATE",
      "creationTimestamp": "2025-03-12T12:51:47.276805Z",
      "origin": "sap.default",
      "onBehalfOf": "user/sap.default/mspitzer@xiting.de"
    }
  },
  "attributes": [
    {
      "name": "complete",
      "new": "{\"id\":\"unknown\",\"meta\":{\"version\":0},\"userName\":\"mspitzer@xiting.com\",\"name\":{\"formatted\":\"null null\"},\"emails\":[{\"value\":\"mspitzer@xiting
          .com\",\"primary\":true}],\"groups\":[],\"phoneNumbers\":[],\"active\":true,\"verified\":true,\"origin\":\"aq3dwdfuf-platform\"}"
    }
```

Beispiel BTP Audit Log Management Service

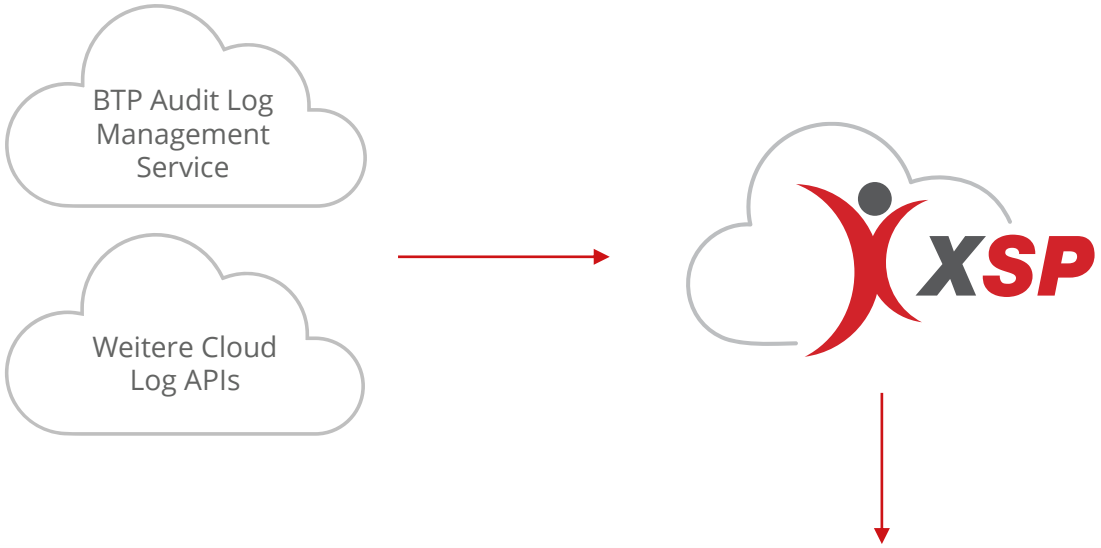
User user/sap.default/mspitzer@xiting.de

Category audit.configuration

Data


```
"org_id": "8f45531c-7503-436e-b5db-42025c278271",
"space_id": "4e103f72-8b8c-40c7-8791-fd2a7d51c4c4",
"app_or_service_id": "f69a0abe-0cee-4d6f-a97d-3a44e9395c07",
"als_service_id": "47dc5776-73b2-4358-b62b-2693d59ad522",
"user": "user/sap.default/mspitzer@xiting.de",
"category": "audit.configuration",
"format_version": "",
"message": {
  "uuid": "b119df34-34bb-4322-b909-9bb8512a1020",
  "user": "user/sap.default/mspitzer@xiting.de",
  "time": "2025-03-12T12:52:18.075375Z",
  "id": "af5cab58-c538-4324-8456-55c013584ef0",
  "success": true,
  "object": {
    "type": "xs_rolecollection2user",
    "id": {
      "tableName": "xs_rolecollection2user",
      "crudType": "CREATE",
      "creationTimestamp": "2025-03-12T12:52:18.075375Z",
      "origin": "sap.default",
      "onBehalfOf": "87467ca1-c8cb-4bec-bb45-4bf0e64d431b",
      "user_id": "02ff51fe-85ce-411e-8765-829cd5d98cf5",
      "rolecollection_identity_zone_id": "076b81b7-2b1c-4cbe-813e-6a483b3025fe",
      "rolecollection_name": "Subaccount Administrator"
    }
```

Herausforderungen und Erfahrungen mit der Integration von Cloud Logs



Xiting Security Platform als SAP Cloud Hub

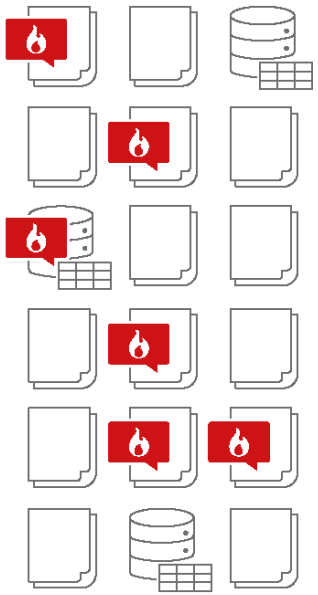
- Zentrale Extraktion der Cloud Logs via APIs
- Interpretation, Normalisierung und Konfiguration der Logs (Feld Mappings, Filterung, Identity Consolidation)
- Bedrohungsanalyse per Threat Detection
- Persistierung oder Forwarding an ext. SIEM Systeme

Events (117,506) Monitoring*

Date	Time	Severity Description	Event Name	Message	Message Category
03/12/2025	13:42:21	High 7	Role Assignment in BTP	SAP BTP Subaccount XSP Development - Assignment of authorizations to own user: Subaccount administrator to mspitzer@xiting.com	Threat
03/12/2025	13:42:21	Medium 5	Creation of User in SAP BTP Cockpit	SAP BTP Subaccount XSP Development - Creation of user mspitzer@xiting.com	Threat

SAP Security Monitoring Lösungskonzepte in hybriden SAP-Landschaften

Einsatzszenarien (High-Level)

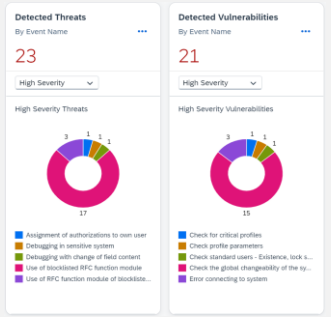


SAP Logs & Tabellen
der Zielsysteme

Xiting Security Monitoring
als Stand-Alone Solution
Und / oder Middleware zu ext. SIEM

Threats, Vulnerabilities
& relevante SAP Logs

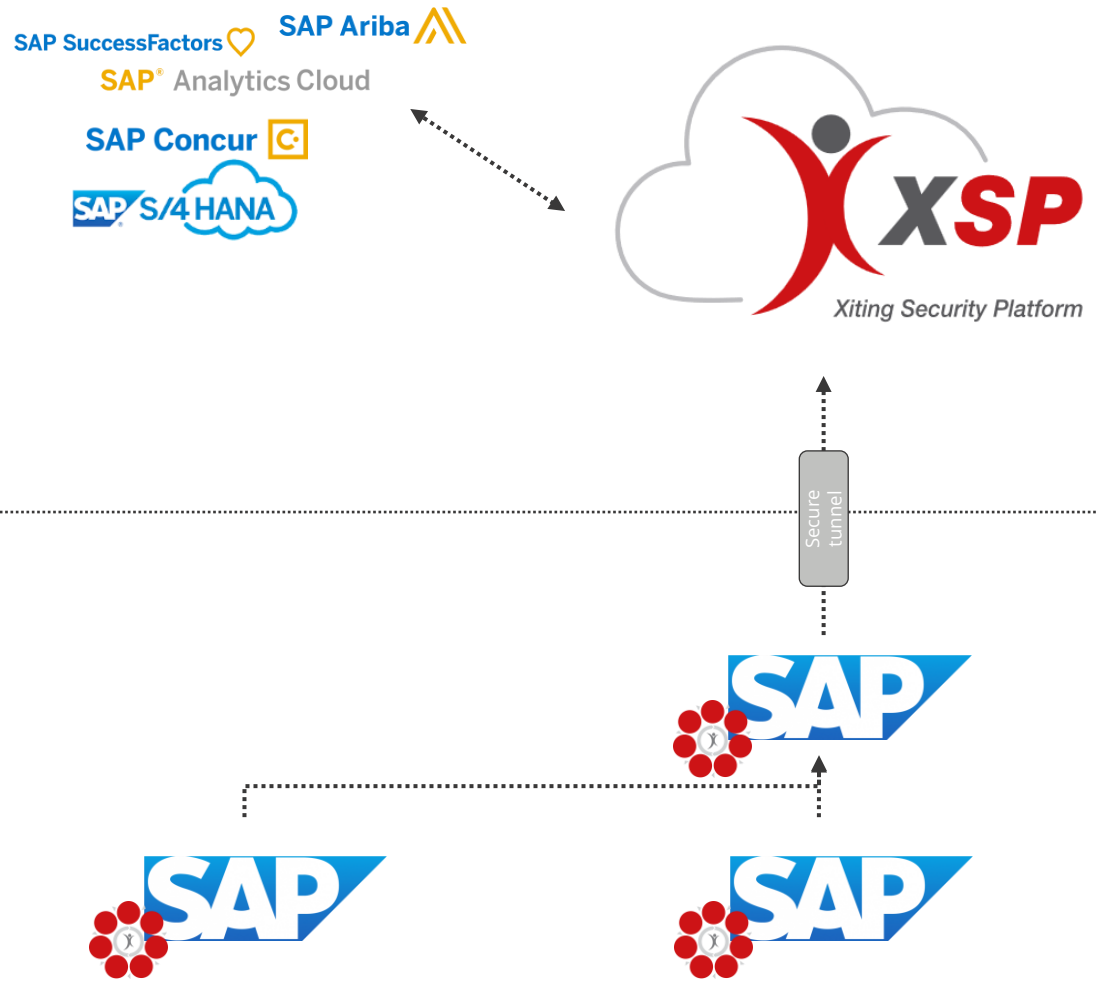
Vulnerabilty & Compliance
Monitoring von Schwachstellen mit ca. 150 vorgefertigten Checks



Extraktion von SAP Logs
Erfüllung von Datenschutzgesetzen & Forensik & zentrales Log-Management

Threat Detection
Monitoring von Bedrohungen mit ca. 60 vordefinierten Patterns

Xiting Security Platform (XSP) als Cloud Hub in hybriden SAP-Landschaften



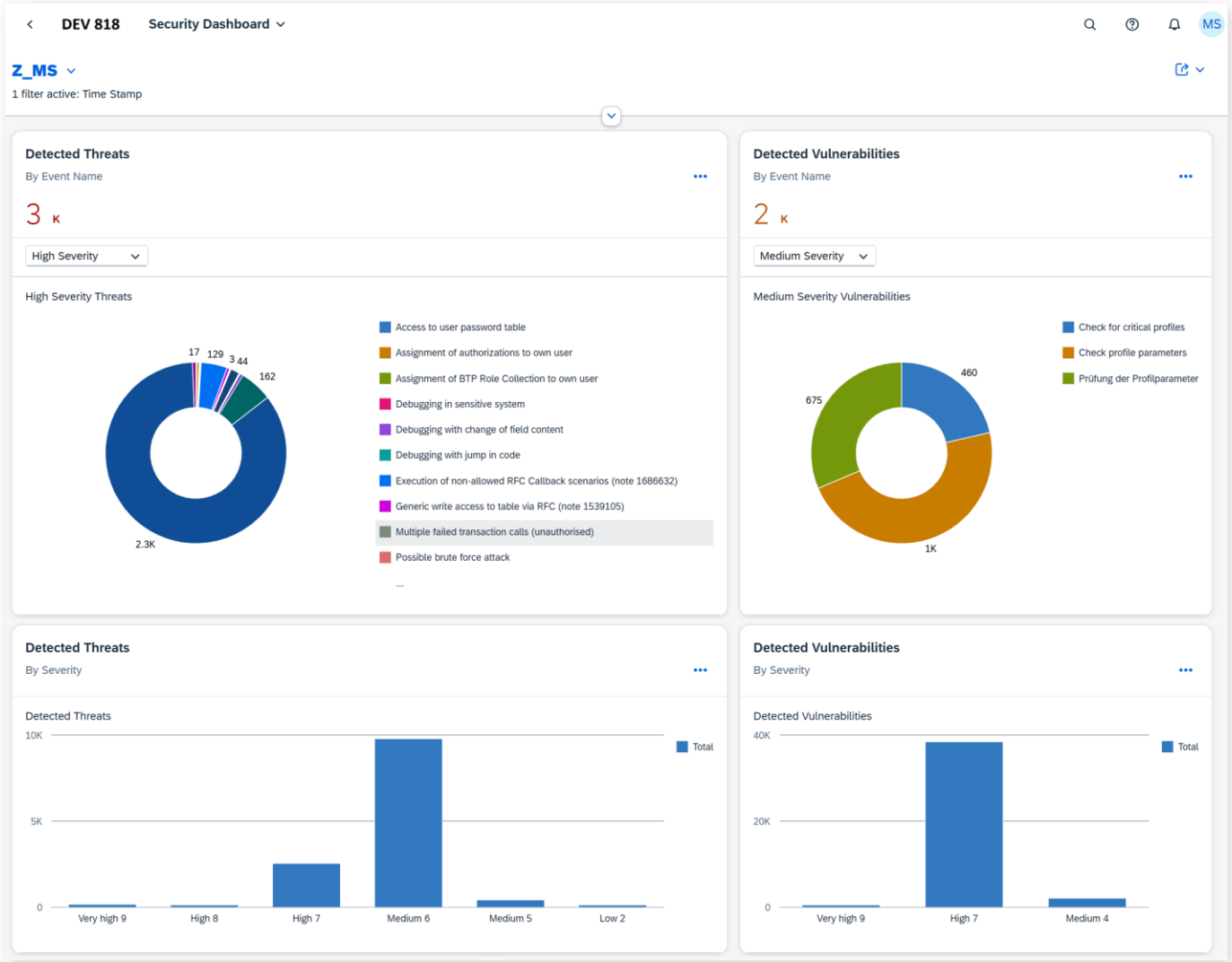
XSP Security Monitoring

- Zentrales Cloud Hub & Integration Cloud Log APIs
- Security Monitoring Apps & Dashboards
- Konsolidierung von Identitäten in der hybriden Landschaft
- Systemübergreifende Risikoanalyse

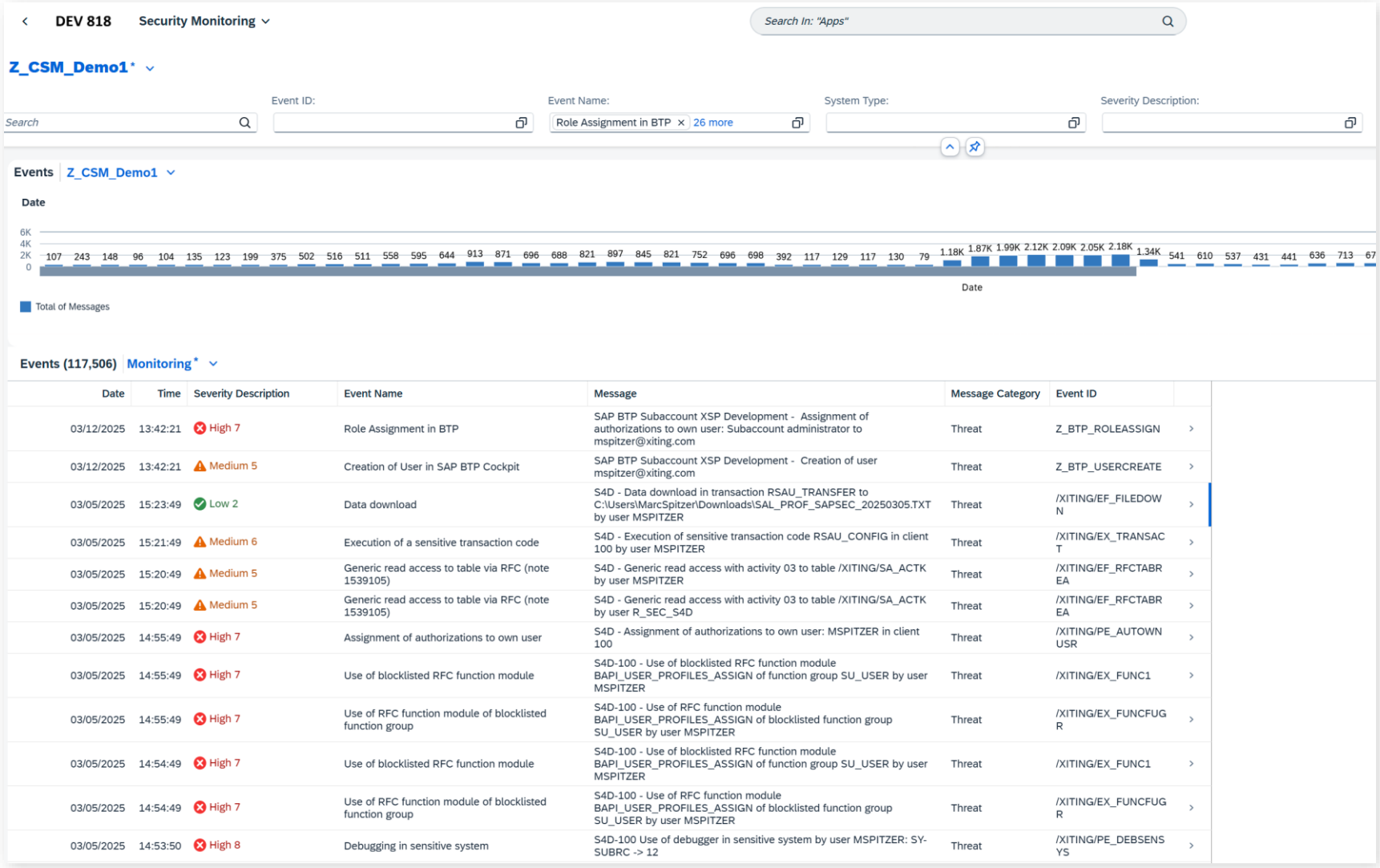
XSP OnPremise Plugin (SIEM Connector & Security Architect)

- Zentrales Hub für alle AnyPremise SAP Systeme (ABAP, HANA, Java)
- Threat Detection
- Schwachstellen & Compliance Monitoring
- Anbindung externer SIEM-Systeme

Zentrales Security Dashboard für hybride SAP-Landschaften



Zentrale Security Monitoring App für hybride SAP-Landschaften



Date	Time	Severity Description	Event Name	Message	Message Category	Event ID
03/12/2025	13:42:21	High 7	Role Assignment in BTP	SAP BTP Subaccount XSP Development - Assignment of authorizations to own user: Subaccount administrator to mspitzer@xiting.com	Threat	Z_BTP_ROLEASSIGN
03/12/2025	13:42:21	Medium 5	Creation of User in SAP BTP Cockpit	SAP BTP Subaccount XSP Development - Creation of user mspitzer@xiting.com	Threat	Z_BTP_USERCREATE
03/05/2025	15:23:49	Low 2	Data download	S4D - Data download in transaction RSAU_TRANSFER to C:\Users\MarcSpitzer\Downloads\SAL_PROF_SAPSEC_20250305.TXT by user MSPITZER	Threat	/XITING/EF_FILEDOWN
03/05/2025	15:21:49	Medium 6	Execution of a sensitive transaction code	S4D - Execution of sensitive transaction code RSAU_CONFIG in client 100 by user MSPITZER	Threat	/XITING/EX_TRANSACT
03/05/2025	15:20:49	Medium 5	Generic read access to table via RFC (note 1539105)	S4D - Generic read access with activity 03 to table /XITING/SA_ACTK by user MSPITZER	Threat	/XITING/EF_RFCTABREA
03/05/2025	15:20:49	Medium 5	Generic read access to table via RFC (note 1539105)	S4D - Generic read access with activity 03 to table /XITING/SA_ACTK by user R_SEC_S4D	Threat	/XITING/EF_RFCTABREA
03/05/2025	14:55:49	High 7	Assignment of authorizations to own user	S4D - Assignment of authorizations to own user: MSPITZER in client 100	Threat	/XITING/PE_AUTOWNUSR
03/05/2025	14:55:49	High 7	Use of blocklisted RFC function module	S4D-100 - Use of blocklisted RFC function module BAPI_USER_PROFILES_ASSIGN of function group SU_USER by user MSPITZER	Threat	/XITING/EX_FUNC1
03/05/2025	14:55:49	High 7	Use of RFC function module of blocklisted function group	S4D-100 - Use of RFC function module BAPI_USER_PROFILES_ASSIGN of blocklisted function group SU_USER by user MSPITZER	Threat	/XITING/EX_FUNCFUGR
03/05/2025	14:54:49	High 7	Use of blocklisted RFC function module	S4D-100 - Use of blocklisted RFC function module BAPI_USER_PROFILES_ASSIGN of function group SU_USER by user MSPITZER	Threat	/XITING/EX_FUNC1
03/05/2025	14:54:49	High 7	Use of RFC function module of blocklisted function group	S4D-100 - Use of RFC function module BAPI_USER_PROFILES_ASSIGN of blocklisted function group SU_USER by user MSPITZER	Threat	/XITING/EX_FUNCFUGR
03/05/2025	14:53:50	High 8	Debugging in sensitive system	S4D-100 Use of debugger in sensitive system by user MSPITZER: SY-SUBRC -> 12	Threat	/XITING/PE_DEBSENSYS

Aufbau eines SAP Security Monitoring und SOC

Implementation Phase

Erstellung des Lösungskonzepts / Target Operating Modell inkl. Dokumentation:

- Compliance-Vorgaben & Bedrohungs-Patterns
- Prozessmodellierung & Responsibilities für Detect & Response Prozesse
- Architektur und Infrastruktur
- Alerting & Incident Handling

Techn. Implementierung Systeme & Software

- Implementierung der Software inkl. Konnektoren / Adpater Log type Konfiguration & Standardisierung
- Log Outage Optionen und Einstellungen

Definition Patterns & Vulnerabilities (Security Use-Cases)

- Out-of-box Pattern Individualisierung
- Entwicklung Customer Patterns
- Dokumentation / SOP (Standard Operating Procedure)

Test Operation

Security Use-Case Testing & Optimization

- Testen der Event- und Alert-Generierung der Threat Patterns & Vulnerabilties
- Eliminierung False-Positives und Optimierung der Patterns
- Kategorisierung der Patterns nach Severity und Reifegrad, um Prozesse zu vereinfachen und automatisieren

Go-Live & Übergabe in den Betrieb / SOC

- Training
- Integration in etwaige bestehende Prozesse
- SOC Readyness sicherstellen & Übergabe

Security Operation Center

- Überwachung, Erkennung, Analyse und Untersuchung von SAP-Cyberbedrohungen
- Sicherstellen, dass Cybersicherheits-Tools in gutem Zustand sind und effizient sowie kostengünstig eingesetzt werden
- Entwicklung und Anpassung von Erkennungsmechanismen an neue Bedrohungen und Verbesserung der Reaktion auf Vorfälle
- Integration zusätzlicher Systeme
- Ausbau der hybriden Landschaft und Integration von SaaS-Anwendungen
- Implementierung zusätzlicher Compliance- und Schwachstellenprüfungen sowie Bedrohungsmuster
- Sicherstellen einer nahtlosen Integration der SAP-Bedrohungs- und Erkennungssysteme in bestehende SoC-Prozesse und Playbooks
- Table-Tops und Pentests der Operation

Xiting Project

Kick-Off Workshop

Cut-Over Testing

Complete Testing

Go-Live

Xiting Managed Service

Fragen und Diskussionen

Marc Spitzer

SAP Security Developer

Xiting GmbH
Obere Ringstraße 17 | DE-79859
Schluchsee

E-Mail: mspitzer@xiting.com
Tel. +49 7656 9888155
Mobile: +49 172 130 22 56

Dankeschön

Für Ihre Aufmerksamkeit

Wenn Sie weitere Informationen benötigen, können Sie mich gerne kontaktieren.