SECURONIX™

SOLUTION BRIEF

SAP Security Monitoring Using Securonix Analytics-Driven SIEM

SAP is synonymous with enterprise business. It drives multiple business applications and is the custodian for massive amounts of critical, sensitive data. SAP systems are growing in complexity as organizations expand beyond the base capabilities. This growth causes security risk to rise. Organizations are slow to apply patches and updates, as they fear business disruption. This hesitation allows threats to emerge across modules, so threat correlation is also an important part of ensuring SAP security. Therefore, a holistic approach to SAP security through comprehensive threat detection and analytics, effectively correlating alerts to identify real threats, is essential.

Security Challenges

There are several security challenges that can put your business-critical applications and sensitive data at risk:

- Unauthorized or excessive access privileges
- Misuse of privileged accounts (i.e., firefighter accounts)
- Misconfigurations or unauthorized configuration changes
- Misuse of sensitive transaction codes (t-codes)
- Account compromise and unauthorized logins

The SAP logging mechanism is cumbersome and can make monitoring security events challenging.

Securonix has built in API connectors to natively collect transaction logs necessary for monitoring SAP. The connector is programmed to pull the following information from SAP:

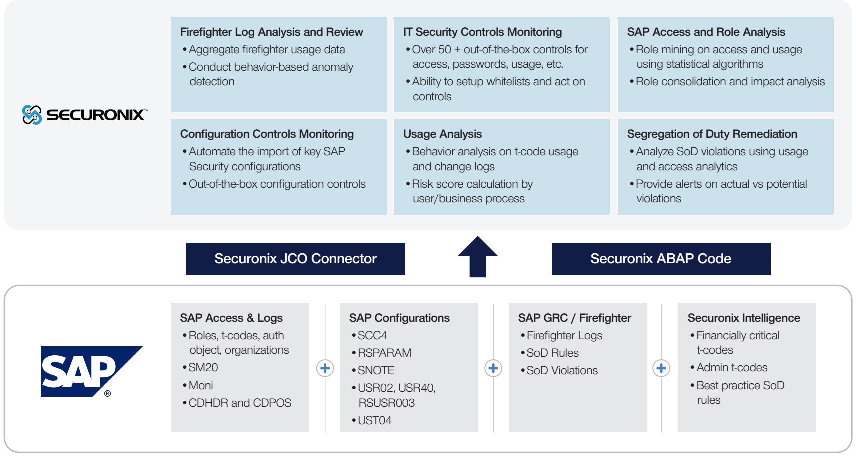
- Account information
- Access privileges (roles, t-codes, authorizations, etc.)
- Usage security events

Securonix uses a non-dialog account in SAP to connect and fetch the required data.

Upon collecting the relevant security events, Securonix enriches the data with identity context and processes it to identify tangible threats, including data compromise, unauthorized access attempts, suspicious traffic, and several others.

Solution Benefits

- Streamlined, direct connecter-based integration enables fast event gathering.
- Complete SAP log coverage, including SM19/SM20, MONI, GRC/Firefighter, CDHDR, and CDPOS.
- Data Insights: Securonix for SAP enables you to visualize activities and changes in your SAP infrastructure with out-of-the-box dashboards and reports that can be easily customized.
- Enrich data with additional context to use for threat modeling.
- Link information from multiple SAP transaction types for comprehensive threat identification.



SECURONIX

Firefighter Log Analysis and Review
- Aggregate firefighter usage data
- Conduct behavior-based anomaly detection

IT Security Controls Monitoring
- Over 50 + out-of-the-box controls for access, passwords, usage, etc.
- Ability to setup whitelists and act on controls

SAP Access and Role Analysis
- Role mining on access and usage using statistical algorithms
- Role consolidation and impact analysis

Configuration Controls Monitoring
- Automate the import of key SAP Security configurations
- Out-of-the-box configuration controls

Usage Analysis
- Behavior analysis on t-code usage and change logs
- Risk score calculation by user/business process

Segregation of Duty Remediation
- Analyze SoD violations using usage and access analytics
- Provide alerts on actual vs potential violations

Securonix JCO Connector

Securonix ABAP Code

SAP

SAP Access & Logs
- Roles, t-codes, auth object, organizations
- SM20
- Moni
- CDHDR and CDPOS

SAP Configurations
- SCC4
- RSPARAM
- SNOTE
- USR02, USR40, RSUSR003
- UST04

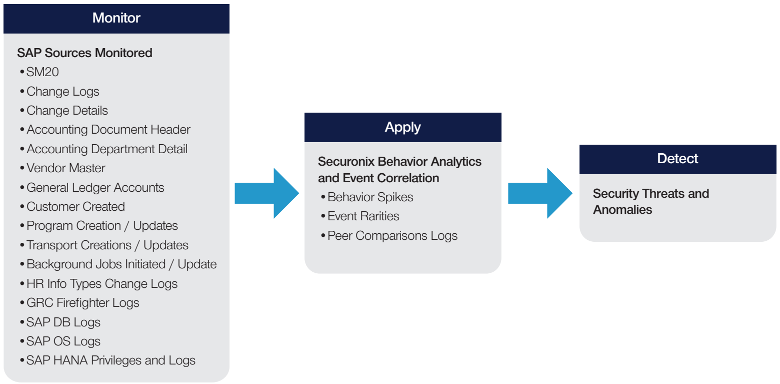
SAP GRC / Firefighter
- Firefighter Logs
- SoD Rules
- SoD Violations

Securonix Intelligence
- Financially critical t-codes
- Admin t-codes
- Best practice SoD rules

Figure 1: Securonix-SAP Analytics

Multi-Level Security Across Account Activity, Access, and Usage

The Securonix platform monitors several SAP transaction types using behavioral and peer analytics to identify anomalous privilege assignments, activities by rogue accounts unassociated with actual users, privileged account misuse (such as SAP_ ALL privilege accounts), as well as account activity changes and transaction spikes. With monitoring support across multiple SAP data sources combined with a large packaged content library, Securonix provides support for a large and growing range of SAP security use cases.



Monitor

SAP Sources Monitored
- SM20
- Change Logs
- Change Details
- Accounting Document Header
- Accounting Department Detail
- Vendor Master
- General Ledger Accounts
- Customer Created
- Program Creation / Updates
- Transport Creations / Updates
- Background Jobs Initiated / Update
- HR Info Types Change Logs
- GRC Firefighter Logs
- SAP DB Logs
- SAP OS Logs
- SAP HANA Privileges and Logs

Apply

Securonix Behavior Analytics and Event Correlation
- Behavior Spikes
- Event Rarities
- Peer Comparisons Logs

Detect

Security Threats and Anomalies

Figure 2: Securonix SAP Multi-Level Security

Sample Use Case Scenario

Identity Based Analytics

Detect orphan accounts, dormant accounts, and unused accounts with system level access.

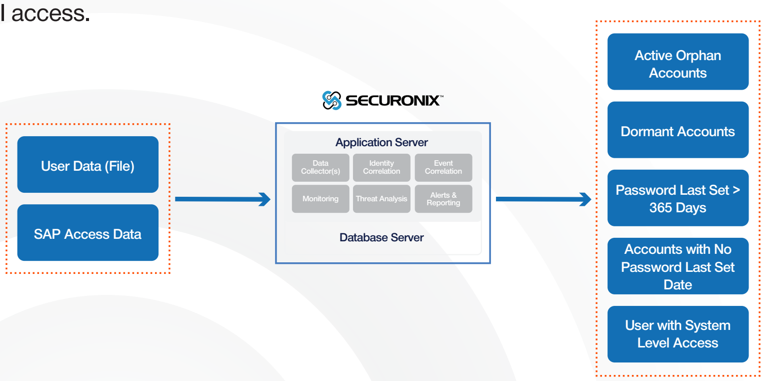


Figure 3: Securonix Identity Analytics for SAP

Key Use Cases

- Suspicious SAP role and account modifications
- Unusual or rare t-code usage
- Authentication attempts from rare geolocations
- Critical/secure t-code execution.
- Suspicious activity for system/high privilege accounts
- Suspicious application interactions.
- Device issues leading to privilege anomalies
- Unauthorized or excessive access privileges
- Segregation of duties (SoD) violations and misuse

About Securonix

The Securonix platform delivers positive security outcomes with zero infrastructure to manage. It provides analytics-driven next-generation SIEM, UEBA, and security data lake capabilities as a pure cloud solution, without needing to compromise. For more information visit www.securonix.com.

SECURONIX™

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000