Delivering Real-Time IAM for SAP Systems

Today, with the cyber threat landscape continually pushing its boundaries to bypass the strongest security measures, the occurrence of an IT incident has become less of an 'if' and more of a 'when.' And due to their near-ubiquitous implementation in businesses of all sizes across numerous industries, SAP systems have become a key target that cybercriminals exploit to gain access to confidential data. The reason behind this is simple, SAP users typically on a network have access to data from multiple disparate silos to do their jobs effectively. This is a problem because users with wide-ranging access are attractive points of attack.

At the same time, as the number of employees using personal devices to perform daily tasks has been skyrocketing since the pandemic, enterprise IT infrastructures across markets have become significantly more vulnerable to cyber threats. Therefore, organizations that use SAP systems need an access and identity governance deployment that ensures holistic security for all SAP environments with a firm.

The German akquinet AG addresses this need with SAST SUITE, the software portfolio of SAST SOLUTIONS, which is designed to aid businesses in detecting access and identity violations in real-time. All this proactively, and not when the damage has already been done. The SAST SUITE was developed to help companies in optimizing their processes with respect to detecting anomalies and unwanted behaviour while accessing SAP systems. Currently, SAST SUITE is available for both SAP S/4HANA and SAP ERP and provides support for a successful migration as well.

According to Ralf Kempf, CTO of SAST SOLUTIONS, SAP security concerns are derived from flawed system configurations that leave too many gaps for attackers, the misuse of user roles and authorizations and, the undesired behaviour of users in the system. "Our SAST SUITE allows clients to set up role management, eliminate conflicts from the segregation of duties and, better control the access rights of all users," says Kempf. Additionally, the software can also automatically adjust user authorisations without causing hindrances in day-to-day business.

> “Our SAST SUITE allows clients to set up automatic role management, eliminate conflicts from the segregation of duties and, better control the access rights of all users”

Further discussing the need for robust IAM for SAP systems, Kempf elaborates, "Identity and user access management alone is not enough from a security perspective. IAM solutions should always be part of a holistic security strategy and also offer features that enable automated detection of user misconduct (e.g., "changing of security settings") and allow structural countermeasures to be taken." Taking this into account, the SAST SUITE provides separate solutions with clearly defined functionalities that are designed for specific aspects within the SAP and IAM arenas. These offerings are built as an integrated package that allows users to seamlessly combine different capabilities based on their unique requirements. Moreover, the SAST portfolio is backed by process models from NIST (National Institute of Standards and Technology), ISO2700x, or BSI (Federal Office for Information Security in Germany), which is at the heart of SAST SUITE's unmatched prowess in detecting identity and access discrepancies in real-time.

With such strong core competencies, a number of success stories have been initiated by these string core competencies since the foundation of SAST SUITE in 2002. In one instance, the company assisted Japanese pharmaceutical giant, Takeda, in enhancing their critical authorizations and identity governance processes. Initially, client users had to work with different accounts on their existing SAP Ariba implementation as the cloud deployment distributes order processes across a variety of systems. As a result, Takeda IT personnel struggled to effectively monitor segregation of duties (SoD) risks across the disparate systems. For this purpose, a cross-SoD matrix with audit content for ERP and S/4HANA systems in combination with Ariba was developed and integrated into SAST SUITE. This facilitated the client to identify cross-SoD risks in a heterogeneous system landscape. "Our SAST SUITE can be integrated with any applications in an IT landscape through interfaces and analyze them for SoD violations, as well as critical authorizations. Furthermore, vulnerabilities are identified automatically and SAST SUITE offers recommendations and solutions for remedying them," states Kempf. At the end of the collaboration, Takeda had enhanced their security reporting, identified risks and conflicts between roles, SoD and otherwise, and minimized them.

Presently, the SAST SUITE is regularly enhanced with innovative features that come directly from real-world project scenarios. A transformative new offered with SAST SUITE since mid-2021 is a security dashboard that enables users to navigate through various levels down to the details of the alert message, thereby significantly enhancing their ability to identify vulnerabilities. "The security dashboard determines the current security status based on predefined risk indicators, shows causes for security gaps, analyzes and illustrates the historical development, and provides high-quality risk information at a glance at any time," explains Kempf.

Looking ahead, SAST SUITE aims to continue helping its client achieve a level of transparency that enables holistic real-time threat detection and, as a result, a qualified and rapid response, even to unforeseen threats. ES