smarterSec Security Platform

Safeguarding Your SAP Environment

Understanding and mitigating key vulnerabilities in SAP

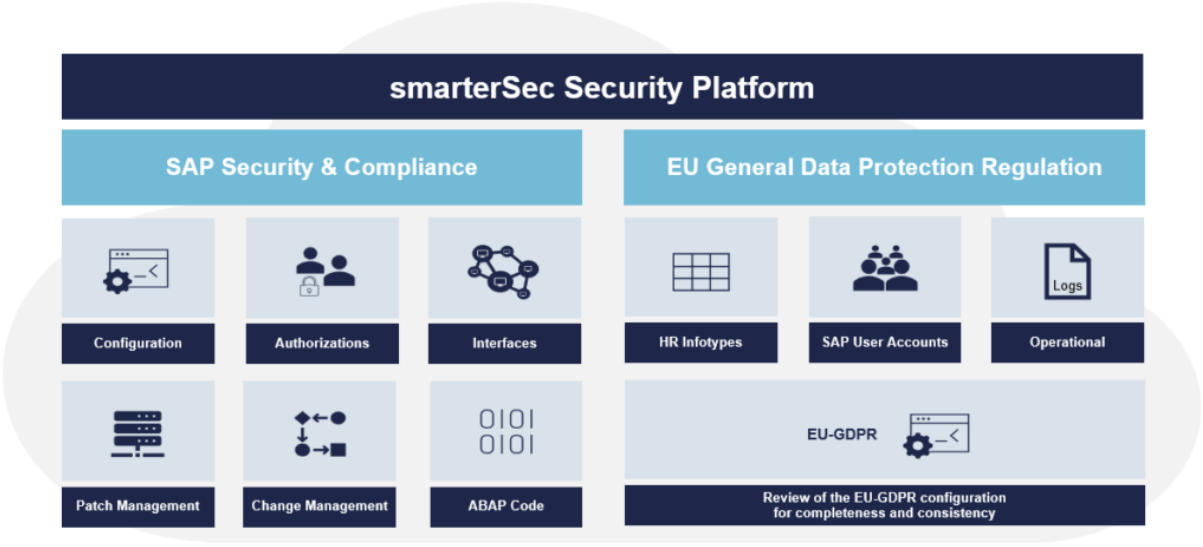
smarterSec™

KEY CHALLENGES IN TODAYS SAP SECURITY & COMPLIANCE

SAP system landscapes are the backbone of companies worldwide and contribute to the efficient design of processes. The high level of complexity, integrations and the different technologies present major challenges when it comes to securing their SAP systems and complying with internal and external regulations. Attackers often exploit the "human factor" as the weakest link in the security chain to obtain sensitive data such as passwords. It is therefore not surprising that 70% of all attacks occur from "inside" the company, i.e., from within the company's own network. This makes it even more important to proactively prepare for new attacks. Because where awareness and training fail, technical protection mechanisms make the difference.

SOLUTION OVERVIEW

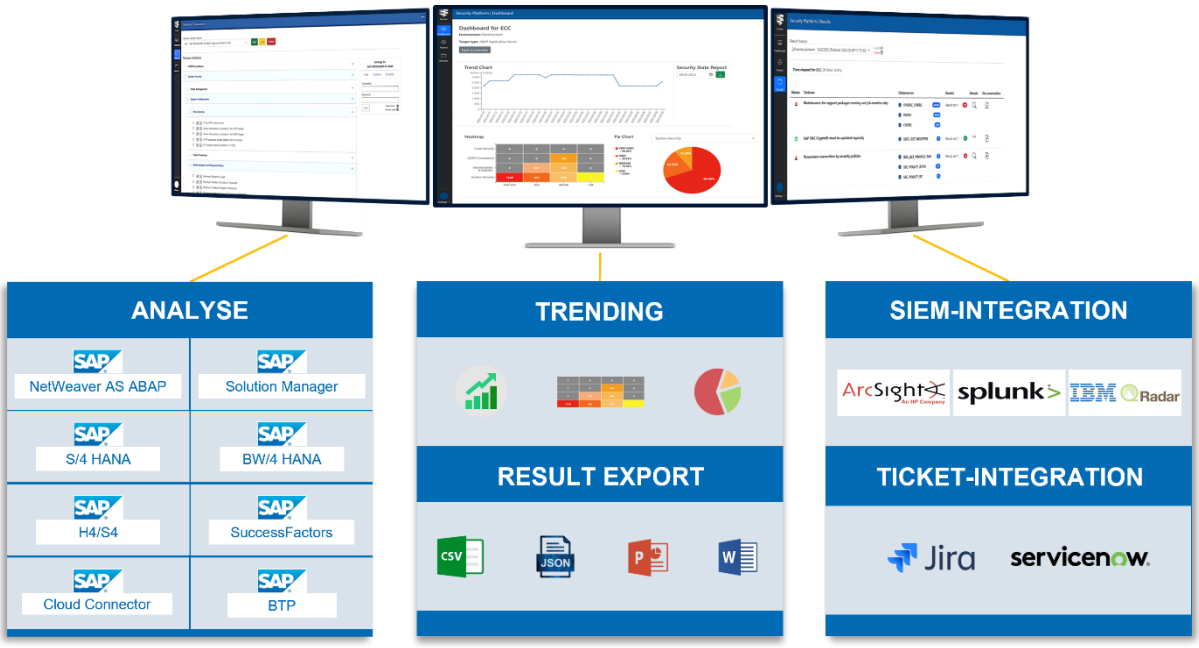
To adequately protect your SAP systems, continuous monitoring through comprehensive vulnerability analysis is required. The **smarterSec Security Platform** continuously and fully automatically monitors all security and compliance-relevant settings and events in your SAP system landscape.



The integrated checks cover the security of ABAP and HANA-based SAP systems, ensuring platform-independent, comprehensive protection. Individual security policies can be stored for each SAP system to meet different protection requirements within the SAP system landscape.

SECURE YOUR SAP LANDSCAPE

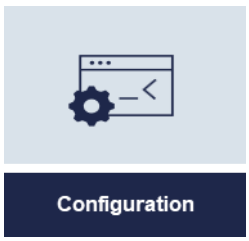
The **smarterSec Security Platform** is a zero-footprint solution for analyzing business-critical IT infrastructure. Designed with SAP landscapes in mind, it does not require the installation of additional software or add-ons within the SAP environment to operate. Instead, it uses remote scanning techniques to receive information about the system and identify potential vulnerabilities, misconfigurations, and other security issues as well as GDPR violations.



This approach enables comprehensive security monitoring without affecting the performance or stability of a source system and provides near real-time threat detection and analysis capabilities.

The following is an overview of the most critical areas in SAP systems that need to be properly secured and continuously monitored.

Configuration: Strengthening the Weakest Link



Inadequate system configurations present several threats in SAP environments, creating opportunities for internal and external attackers to exploit those vulnerabilities. Misconfigurations may lead to unauthorized access, data leaks, or even system downtime. SAP systems should always be configured according to the industry best practices.

Common Solutions and Limitations

SAP Basis teams often rely on manual configuration checks, which are time-consuming and prone to human error. Additionally, misconfigurations may go unnoticed for an extraordinarily long time until a security incident occurs.

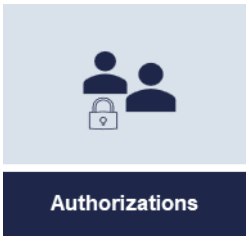
Automated analysis and monitoring with smarterSec

The smarterSec Security Platform is characterized by its ability to quickly identify configuration vulnerabilities and provide detailed guidance for mitigation. The highly automated approach not only highlights existing misconfigurations, but also continuously monitors any changes that could introduce new vulnerabilities. This proactive approach ensures that your SAP systems always run securely and stable.

Conclusion

Configuration vulnerabilities are the Achilles' heel of SAP environments. The smarterSec Security Platform's automated approach of analyzing and continuously monitoring the configuration of SAP systems provides the best defense against potential exploits.

Roles & Authorizations: Navigating the Maze of Permissions



Roles and authorizations are critical components in the SAP system landscape, determining who has access to what within the SAP systems. Inadequate authorization policies and management can lead to unauthorized access, data breaches, or even sabotage. With 70% of cyber-attacks occurring from inside, the role and authorization management are essential elements in securing SAP systems.

Common Solutions and Limitations

Traditional methods involve manual audits and periodic reviews, which are resource-intensive and often result in oversights. Manually identifying and resolving authorization issues in a timely manner is impossible in today's complex SAP systems.

Automated analysis and monitoring with smarterSec

The smarterSec Security Platform automates the identification of role and authorization vulnerabilities through regular scan cycles. By continuously monitoring and analyzing user permissions, our solution quickly identifies any deviations from defined roles. This ensures that access privileges are aligned with business requirements and mitigates the risk of unauthorized activities.

Conclusion

Roles and authorizations are the gatekeepers of SAP security. The automated approach with the smarterSec Security Platform ensures a robust defense against potential breaches due to bad authorization management and provides organizations with full transparency.

Interfaces: Unveiling Potential Exploits

Interfaces

Interfaces act as bridges between internal and external systems of the SAP environments, creating opportunities for potential exploitation if not properly secured. Vulnerabilities in these interfaces can expose critical data and compromise the system integrity. For instance, an inadequately secured interface might enable unauthorized access or data manipulation.

Common Solutions and Limitations

Interface teams rely on manual investigations or integration teams to identify and remediate interface vulnerabilities. However, these approaches are time consuming, subject to error and can lead to delayed response times.

Automated analysis and monitoring with smarterSec

The smarterSec Security Platform automatically identifies known vulnerabilities within SAP interfaces. Continuous monitoring ensures immediate identification of changes that could introduce new vulnerabilities or reopen previously resolved ones. This proactive approach enhances the overall security posture, allowing organizations to stay one step ahead of potential threats through their interfaces.

Conclusion

Interfaces are critical touchpoints in the SAP system landscape that require continuous monitoring. Automated analysis and monitoring with the smarterSec Security Platform provides an excellent solution to ensure that your SAP environment remains resilient against evolving cyber threats.

Patch-Management: Staying Ahead of Exploitable Gaps

Patch Management

Regular patch management in SAP system landscapes is crucial to mitigate vulnerabilities caused by outdated software versions. Failure to stay current with patches can expose SAP systems to known exploits and compromise their integrity. The timely implementation of SAP Security Patches is an integral part of securing your SAP systems.

Common Solutions and Limitations

Many organizations struggle to implement patches on a regular basis and face challenges in tracking, testing, and applying patches as soon as they are released. This often results in delayed responses to critical vulnerabilities that are publicly available and therefore easy to exploit.

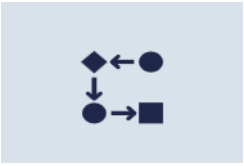
Automated analysis and monitoring with smarterSec

The smarterSec Security Platform automates the analysis of missing patches in SAP systems, streamlining the entire process. It identifies missing patches, assesses their criticality, and gives mitigation advice where necessary. This ensures that your SAP environment is always up-to-date and protected against known vulnerabilities.

Conclusion

Patch management is a race against time. With the automated analysis, the smarterSec Security Platform provides a proactive solution, helping organizations stay up to date in the ever-evolving landscape of cyber threats.

Change-Management: Navigating the System Modifications



Change is inevitable in SAP environments, but it introduces one of the biggest risks if not managed properly. Unauthorized or unmonitored changes can lead to vulnerabilities, impacting system stability and security. The correct configuration of the SAP Transport Management System (TMS) is an essential part in securing the change management process in SAP systems.

Common Solutions and Limitations

Traditional analysis of the SAP Transport Management System (TMS) relies on manual reviews, leaving room for oversight and misconfiguration. Identifying vulnerabilities manually can be challenging, especially in large and complex SAP landscapes.

Automated analysis and monitoring with smarterSec

The smarterSec Security Platform automates the analysis of the SAP Transport Management System (TMS) and monitors the changes continuously. By automatically identifying misconfigurations, it enhances visibility and accelerates response times, reducing the window of vulnerability.

Conclusion

Change in SAP systems is constant, and managing it securely is paramount. Using an automated approach with the smarterSec Security Platform ensures that your SAP system evolves with agility, without compromising on security.

Custom ABAP Code: Enhancing Security of Custom Developments

With ~2 million lines of custom code per SAP system, developing custom ABAP code introduces a unique set of vulnerabilities. The duty to develop secure and compliant custom ABAP code is mostly with the developers. Therefore, a defined ABAP development guideline for secure code development is a prerequisite most companies keep lacking with accuracy and actuality as well as controlling them.

Common Solutions and Limitations

Manual code reviews are time consuming and may miss subtle vulnerabilities. Traditional methods often struggle to keep pace with the rapid development and deployment of custom ABAP code. Coding is packaged in transports and transported from the development systems to quality systems and then to production systems, often without sufficient code reviews.

Automated analysis and monitoring with smarterSec

The smarterSec Security Platform automates the detection of vulnerabilities in custom ABAP code using the SAP Code Inspector (SCI), SAP Add-on for Code Vulnerability Analyzer (CVA) or other third-party tools if available. By identifying security vulnerabilities and providing actionable insights, it empowers organizations to secure their custom ABAP developments without hindering agility.

Conclusion

Custom ABAP code development is a double-edged sword – on the one side it is necessary to build your custom processes inside SAP, on the other hand it represents a massive attack surface if a secure ABAP development process is not followed. smarterSec ensures that your innovations are not compromised through security risks by leveraging the proactive and automated smarterSec Security Platform, reducing the need for organizations to rely on manual tasks.

GENERAL CONCLUSION

In conclusion, securing SAP systems against evolving threats requires a proactive and comprehensive approach. The smarterSec Security Platform stands out as a fully automated security solution that provides automated vulnerability assessment, continuous monitoring, and targeted checks across critical areas like configuration, authorization, interfaces, patch management, change management, and custom ABAP code. By addressing these critical areas in SAP systems, the platform ensures that organizations can fortify their SAP environments against potential exploits, maintain compliance, and stay resilient in the ever-changing cybersecurity landscape.

Realize the future of SAP security and compliance with the smarterSec Security Platform and contact us today.