Protect your SAP systems with the Microsoft Sentinel solution for SAP applications

SAP systems and applications handle massive volumes of business-critical data. The SAP ecosystem is complex and difficult for security operations (SecOps) teams to effectively monitor and protect against growing threats. The complex nature of SAP systems means threats can emerge across multiple modules, requiring ongoing monitoring, advanced threat detection, and cross-correlation.

The Microsoft Sentinel solution for SAP applications allows you to monitor, detect, and respond to suspicious activities and guard your critical data against sophisticated cyberattacks for SAP systems hosted on Azure, other clouds, or on-premises infrastructure.

- Monitor all SAP systems layers: Gain visibility at business logic, application, database, and OS layers and leverage Sentinel's built-in investigation tools.
- Detect and automatically respond to threats: Detect suspicious activity including privilege escalation, unauthorized changes, sensitive transactions, and more with out-of-the-box detection capabilities
- Correlate SAP activity with other signals: Accurately detect SAP threats by cross-correlating across all your data sources and SAP infrastructure.
- Customize based on your needs: Build your own detections to monitor sensitive transactions and other business risks.

Deployment and content details

SAP data connector: Delivered as a Docker container image that can be deployed anywhere in the network and integrated to SAP NetWeaver-capable systems, the data connector collects dozens of log files for monitoring business and application risks and includes an ability to synchronize users' authorization data and parameters.

SAP infrastructure data connector: Use Microsoft Sentinel data connectors for your underlying infrastructure (virtual machines, storage, network, Azure Active Directory) while monitoring HANA database audit logs using Microsoft Sentinel Syslog integration.

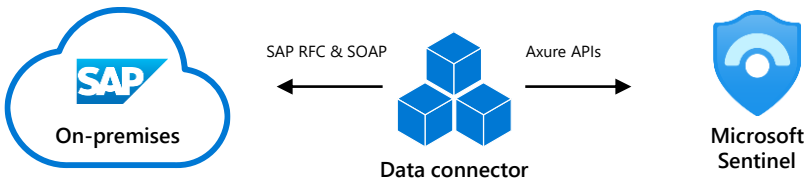
Automated response (SOAR) within SAP systems: Act upon security incidents by using playbooks to perform automated actions within SAP systems such as locking a user.

Built-in security content: Over 200 built-in detections help detect SAP threats like configuration changes, execution of sensitive function modules, suspicious users and admin activity and more.

SAP application logs: Gain deep insights into SAP transactional activities with the SAP security audit log, job log, spool log, change documents, and more.

Simplified deployment: Protect your SAP systems today with simplified deployment and integration via the Azure Marketplace.

Integrated UEBA insights: Gain insights to SAP security data when browsing UEBA entities.



The Microsoft Sentinel solution for SAP applications detects threats like:

Abuse of SAP privileges: A SAP user with developer privileges could exploit those rights to view sensitive documents, such as HR or financial data, or to gain elevated access. With Microsoft Sentinel solution for SAP, your SecOps team can define a granular set of sensitive modules—narrowing detection parameters for production environments or performing specific operations in a development or sandbox system. Preconfigured functions enable you to monitor a baseline from day one, all while retaining the freedom to modify any configuration via Microsoft Sentinel Watchlists.

SAP break-glass users: In SAP environments where usage needs to be carefully monitored because of default "superman" users (DDIC) with elevated privileges, your team can monitor system access and automatically call a playbook that requests SAP basis permissions. Grant only the permissions needed to perform a specific operation using your designated Microsoft Teams channel.

Attempts to bypass SAP security mechanisms: Detect indicators that a user is trying to bypass SAP security mechanisms, such as disabling audit logging (HANA and SAP), executing sensitive function modules, unlocking blocked transactions, or debugging production systems.

Data exfiltration and insider risks: SAP systems contain extremely sensitive data, making them a prime target for data exfiltration. Detect signs of malicious data exfiltration activity such as unusual file downloads, spool takeovers, access to insecure FTP servers, and connections from unauthorized hosts.

Malicious initial access: The Microsoft Sentinel solution for SAP applications detects signs that an attacker has made initial access to your SAP system, including brute force attacks, multiple logins from the same IP address, and privileged logins from unexpected networks.

As a Microsoft partner, we can help you guard your critical data with the Microsoft Sentinel solution for SAP applications and our deployment services.

Contact us to learn how we can help you protect your SAP apps today!

https://cybermsi.com/
(844) 409-1980
info@cybermsi.com