Splunk® Security for SAP® Solutions

Help safeguard your SAP environment with Splunk

Splunk® Security for SAP® solutions offers:

Risk-based alerting

Rapid setup

Consolidated views

Security monitoring

Forensic investigations

SAP environments contain business-critical applications and sensitive data that, if compromised, could be devastating to a business. Conventional tools to monitor and secure SAP deployments have traditionally stood apart from the core security operations stack used by security teams. Furthermore, the diversity of log formats used by SAP systems, applications and products makes it challenging to scrutinize SAP threat data with security analytics solutions. Consequently, security teams find it difficult to leverage security operations tools and processes to safeguard high-value SAP assets and data. To help ensure adequate protection, organizations must bring their SAP estates into the fold of threat monitoring, detection, investigation and response workflows.

Splunk Security for SAP solutions

Splunk Security for SAP solutions is an SAP Endorsed Application that allows security teams to harness the power of Splunk to help safeguard their SAP environments. Data and alerts from SAP live side by side and can be searched and correlated with all other security telemetry analyzed by Splunk, so security teams can centrally detect, investigate and prioritize alerts.

SAP specific analytics and visuals

Splunk Security for SAP solutions uniquely leverages SAP Enterprise Threat Detection to collect and analyze security alerts and telemetry coming from SAP. Once Splunk Security for SAP solutions is connected to a Splunk instance, pre-built dashboards populate automatically with SAP data, so security teams can quickly start monitoring their SAP environments and triage SAP alerts utilizing Splunk's powerful investigative tools and built-in correlation searches. Dashboards, KPIs and searches are completely customizable and easy to tune to a team's specific requirements.

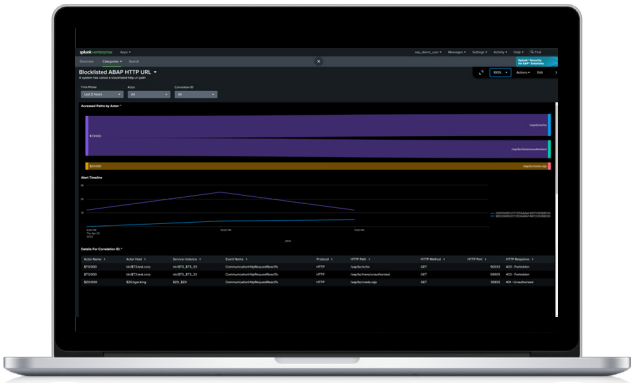
Unified security telemetry

Security teams will benefit from using SAP alerts and data as part of their Splunk threat detection and investigation capabilities. Suspicious activities within SAP, such as lateral movement between development and production systems or unusual privilege escalation, can be further investigated within Splunk to determine if they are part of a larger attack. SAP alerts can be added to Splunk Enterprise Security's Risk Based Alerting (RBA), helping security teams prioritize alerts by business risk and improve detection accuracy within the SAP environment. With Splunk Security for SAP solutions, analysts can combine SAP business-level context with the security and infrastructure telemetry in Splunk to improve the quality of detections and reduce security risks around an organization's most critical business applications and data.

Key Capabilities

Pre-built dashboards, KPIs and correlation searches

Splunk Security for SAP solutions comes with SAP-specific, out-of-the-box dashboards, metrics and analytics designed to help security teams gain value quickly.



Threat hunting and investigation

Insights from suspicious SAP application and user activities can be used by threat hunting teams as they define the story and blast radius of an attack. Using Splunk Security for SAP solutions, investigators can follow suspicious activities that move laterally into an SAP instance or exfiltrate data from an SAP instance.

Prioritize your work by risk

For organizations that use Splunk Enterprise Security, SAP alerts and telemetry feed directly to Splunk Enterprise Security's RBA framework. RBA helps teams to prioritize alerts by organizational risk, while streamlining investigations by grouping all the corroborating events into a single notable.

Use Splunk Security for SAP solutions to solve critical but difficult to implement security use cases

Solving such use cases typically requires manual correlation by security and SAP teams or custom-built infrastructure. Let Splunk Security for SAP solutions bring it all together for you so your teams can focus on security.

- Assess a user with suspicious elevated user privileges in SAP for additional indicators of compromise
- Automatically investigate and escalate low volume reconnaissance on critical SAP web endpoints
- Quickly investigate and triage distributed brute force login attacks utilizing multiple terminal IDs.

SAP® Endorsed App
Premium Certified

Learn more about how Splunk Security can protect your business with data, analytics, automation and end-to-end integrations. Not yet using Splunk? Download Splunk for free. Whether cloud, on-premises, or both, Splunk has a deployment model that will fit your needs.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

23-196003-Splunk Security for SAP Solutions Guide -SG-102