5 Steps for Kick-starting Holistic SAP Security in 1 Day

SecurityBridge

Step 1: Access a comprehensive SAP Security Knowledge Base

- Utilize an up-to-date SAP Security Knowledge Base for event guidance and mitigation recommendations
- Stay informed on SAP Security-related insights to respond to incidents effectively

Step 2: Activate a security shield with pre-configured rules

- Implement rule-based or AI-based SAP Security monitoring to detect cyberattacks
- Consider tools like SecurityBridge Threat Detection, which offers hundreds of configured and active out-of-the-box listeners to detect known threats

Step 3: Empower SAP Users in SAP Security

- Notify account owners of unusual logins from new devices or IP addresses
- Use identity protection tools, such as SecurityBridge Identity Protection, to alert SAP users of unusual access and automate mitigation steps like account blocking

Step 4: Set up a Security Dashboard for instant access to all necessary information

- Create a dashboard that includes monitoring status, vulnerability rating, patching status, and a summary of critical code vulnerabilities
- Use the dashboard as a starting point for detailed analysis, forensics, and mitigating actions

Step 5: Build a security roadmap to harden SAP systems

- Prioritize fixes for critical, easy-to-address vulnerabilities to strengthen security
- Use compliance tools (e.g. SecurityBridge compliance checks) to evaluate risks, streamline remediation, and track hardening progress with trend reports