SAP Security Assessment Checklist

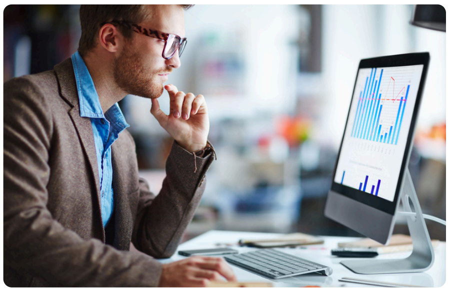
Key Components

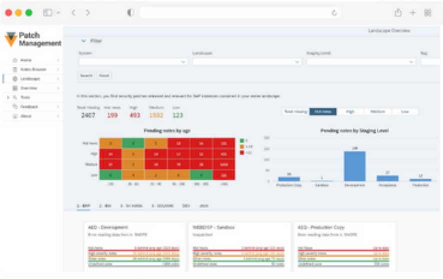
Roles and Authorizations Review

- Regularly review user access permissions
- Ensure roles are updated, especially after job function changes
- Use tools like SAP GRC to streamline the review of complex role information

Transaction Monitoring

- Continuously monitor SAP transactions for unusual activities that could indicate potential breaches.
- Monitor transactions and remote access to detect unauthorized activities and ensure policy compliance



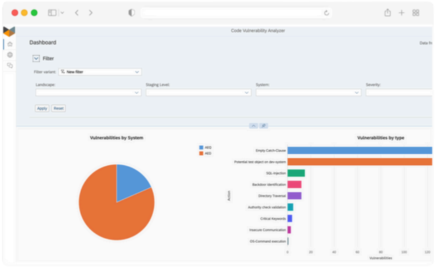


Vulnerability and Patch Management

- Continuously manage patches to address known vulnerabilities and defend against evolving threats.
- Apply security patches promptly to maintain SAP systems' protection, integrity, and reliability.

Custom Code Security

- Regularly review custom ABAP code for potential security flaws exploitable for cyber attacks.
- Use the SecurityBridge Code Vulnerability Analyzer (CVA) to identify and fix security flaws in ABAP code before deployment, to ensure secure custom code.



Transport Security

- Secure data transport routes in SAP systems using firewalls and SAP routers.
- Monitor and control data exchanges to protect sensitive configurations.

SAP Security Assessment Checklist

SecurityBridge

Compliance Testing

- Ensure SAP systems **adhere to industry-specific regulations** and cybersecurity frameworks (e.g., NIST CSF).
- Perform **regular security assessments** to validate compliance with data protection standards.

Tools for SAP Security Testing

- Use **vulnerability scanners**, penetration testing tools, security logging, and code analysis utilities to identify weaknesses in SAP systems.
- Leverage **automated solutions** in SAP to improve efficiency, accuracy, and coverage across the system landscape.
- Continuously **identify and mitigate potential threats** to maintain a robust security posture.

Data Protection

- **Data Encryption**: Implement strong encryption, including SAP Cryptographic Library and custom keys, to protect sensitive data in SAP systems during storage and transmission.
- **Network Segregation**: Isolate critical SAP systems from less secure zones to prevent unauthorized access and enhance data security.
- Enforce **two-factor authentication** for secure remote access.

Regular Security Maintenance

- Schedule **regular SAP security assessments** to maintain a strong security posture of SAP systems.
- Engage **SAP security management experts** to manage the complexity of SAP infrastructure and ensure compliance with strict security requirements.
- Use a **security automation tool like SecurityBridge** to reduce manual workload and avoid costly gaps in security management.