NO MONKEY

ADVISORY

SAP Penetration Testing

Stress Test Your System

To get governance about vulnerabilities and their severity to SAP applications, a penetration test using a grey box approach provides an efficient way to determine and classify vulnerabilities in an SAP application. As a result, activities to remediate vulnerabilities or mitigate the risk they expose can be conducted.

What You Can Expect

The service provides a report of the identified vulnerabilities and their severity according to the German Federal Office of Information Security (BSI's) base protection level (APP.4.2) for the 'must requirements' under section § 3.1 for SAP ERP systems.

The grey box approach helps organizations identify threats and vulnerabilities across the entire cyber kill-chain, which indirectly helps the security team recognize their capabilities in detecting attacks or breaches that affect their SAP environment. The below lists a brief illustration of the different tasks done throughout the service period:

- Identify exploitable vulnerabilities affecting the organization's SAP environment.
- Identify threats that can allow a breach or attack to happen.
- Provide mitigation and remediation recommendations to avoid malicious activities with the network.
- Additional activity: Review the blue teams' capabilities to detect threats and malicious activities within their environment and network.

The final report will document an executive summary of the top vulnerabilities found, a detailed walk-through of the pentest, and recommendations on mitigating and patching vulnerabilities.

Get in Touch

To improve your security defenses, you must first learn to see your risk and vulnerabilities through the lens of the SAP landscape. We can show you how to do that. Are you ready?

Your contact person: Jochen Fischer (jochen.fischer@no-monkey.com, +49 6221 3216891)