Cyberdefense

AD Domain Penetration Test

Identify your security deficiencies before a criminal does.

Orange Cyberdefense offers an opportunity to conduct an in-depth security analysis of your AD Domain and identify security deficiencies before anyone with a criminal intent gets ahead.

Security incidents and data leaks are often caused by employees and are a risk for your organization. However, these risks are often underestimated or unknown. In addition, technology and security measures are perceived as complex and restrictive, and may be circumvented.

Employees often act subconsciously and are therefore vulnerable to malicious activities. These parties use social engineering methods such as phishing and pre-texting to gain access to information, systems, data and buildings via employees in order to achieve their goals. In addition to this, laws and regulations necessitate the need to be in control and ensure that employees are cyber-aware.

The pentester conducting the security analysis will bring their own laptop and simulate an attacker, and use common attack techniques trying to breach your internal infrastructure.

These are our steps

- Vulnerability Assessment of a C-Class IP network (254 hosts)
- Penetration test AD Domain
- Report review - A personal review of the report by a security consultant is included through a virtual meeting room or at your location.

All security assignments include a start-up meeting where we jointly go through the requirements when conducting the security analysis.