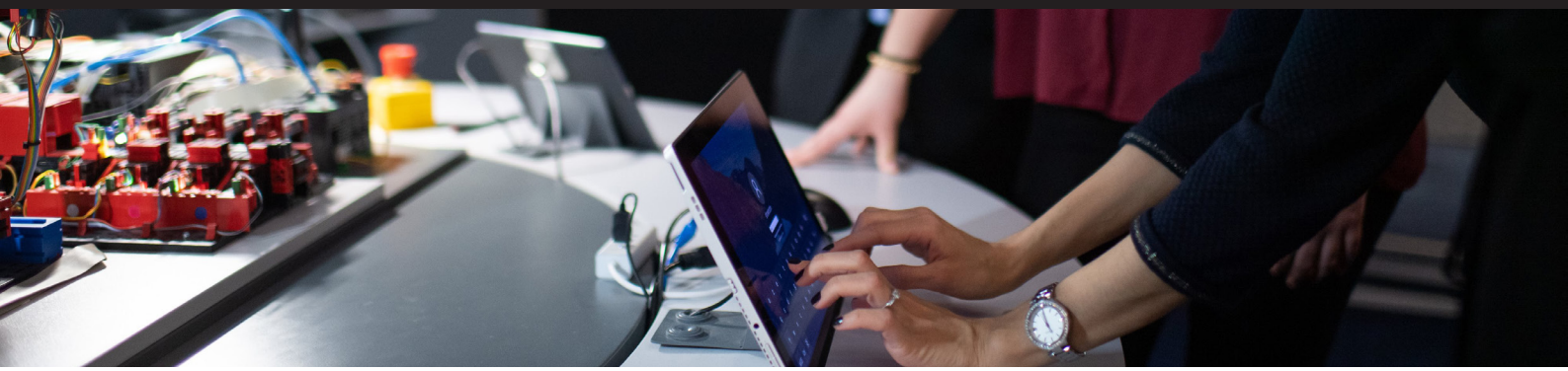
Orange
Cyberdefense



Service overview

Goal-Orientated Penetration Tests

Key benefits

Ongoing, real-world attack
Our Ethical hackers attack an organisation's users, web estate, public-facing applications and perimeter exactly as determined and directed attackers would.

Post-exploitation manoeuvring
Once we have gained access to the internal network, we will establish a persistent presence and explore the network's assets for further compromise.

Exfiltration
We will find the agreed trophies -most critical assets- and seek to compromise the organisation's access to them or remove copied data.

Service description

Significantly more sophisticated than a standard Penetration Test, Goal Orientated Penetration Testing, also known as Red Team Assessments, assessments simulate real-world, covert, multi-phase attacks as they would be performed by real and persistent criminals.

These assessments are based around certain "goals" agreed up front. These goals are designed around possible critical failures of your most important business functions. For example, a goal could be to gain access to a material amount of money, or secret business information, or large amounts of data under regulatory scrutiny. These goals are important for replicating a real-world attack, as real criminals have such motives. The methods used to attain these goals are as unrestricted as feasible, allowing likely attack scenarios to be played out. The results of the assessment are vital to escalate cyber risk to a business level by demonstrating the business risk of such an attack. Additionally, knowing the full attack chain enables intelligent defences to be placed along it, rather than focusing on initial vectors only.

Modern adversaries can take several forms. SensePost studies the behaviour of attack groups to impersonate the style and expertise of attack an organisation may face. Broadly, they fall into the following categories:

- **Opportunists** are looking for easy opportunities and "low hanging fruit." They either do not possess the skill for more advanced attacks, or do not have a need for utilising such skill. Examples here are website defacements, or petty theft.
- **Insiders** are the traditional "white collar criminals" who know the business systems well enough to bypass their rules. Examples here are "ghost employees" or supplier payment fraud.
- **Hackers** are skilled at technically manipulating systems in ways no one intended. Examples here are banking trojan authors, custom ransomware or some organised criminals.
- **Advanced attackers** are typically cross-functional teams of both skilled technical hackers as well as highly knowledgeable business users. These range from organised crime to nation states.

Why Orange Cyberdefense

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group. As Europe's go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Orange Cyberdefense retains a 25+ year track record in information security, 250+ researchers and analysts 16 SOCs, 10 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries.

We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

Key service components

Armed with appropriate modus operandi for the range of adversaries your organisation is likely to face, we will take one or many of the following approaches:

- Reconnaissance involves hunting for public information to be used to choose targets, or appear as a legitimate business entity. These activities include gathering technical information (such as e-mail addresses, or Wi-Fi network names) to business relevant information (such as job roles or business functions).
- The perimeter breach serves as the initial entry vector onto the network. This is most often via malware delivered through phishing exercises, exploiting vulnerabilities in Internet-facing systems, or via physical co-location attacks against Wi-Fi or unprotected network ports.
- Lateral movement is the stage of the attack where further reconnaissance of internal user behavior is conducted and relevant privileged access is obtained. A beachhead will be established, and redundant and persistent channels are covertly established to maintain access. In some cases, this will include compromise of the Microsoft Active Directory domain, but frequently, critical business systems can be accessed via other means.
- Action on technical objectives once objective-appropriate target systems and users within the relevant business unit have been identified, this phase will include the exploitation of the specific target systems and infrastructure.
- Action on business objectives is where the target business systems and processes are exploited to achieve the overall objectives. Examples include learning entity-specific SWIFT codes in order to conduct transactions, or creating false suppliers and payments in a manner that passes business specific rules.