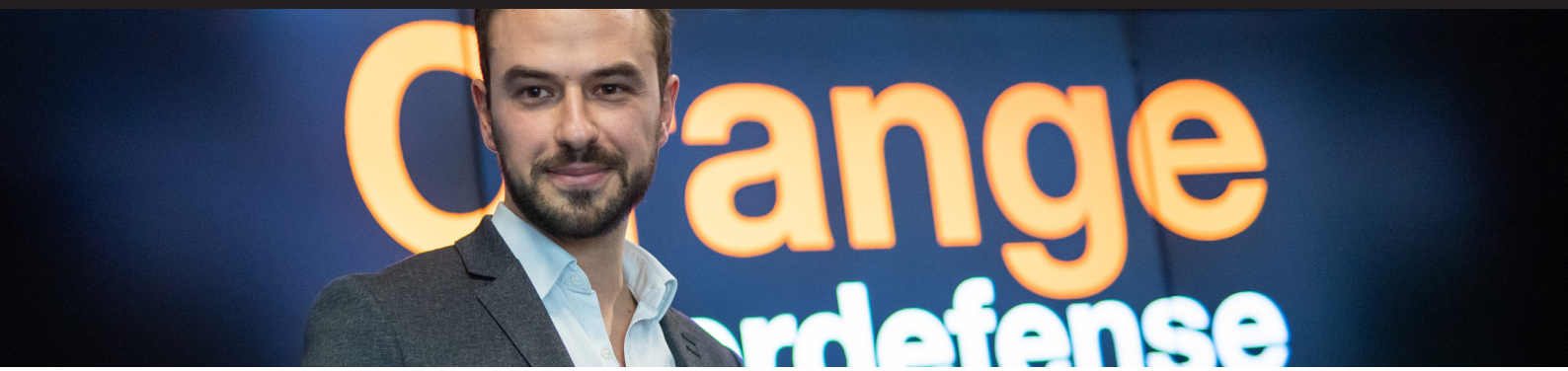
Orange Cyberdefense



Service overview

World-Leading Cybersecurity Consultancy On Budget And On Demand

Service Description

The consultancy retainer service is designed for organisations whose cybersecurity strategy incorporates regular infrastructure, personnel and/or application assessments wishing to work within a planned budget.

Key service components

Advanced footprinting

"Footprinting" is a method of discovering information on the Internet either owned by, related to, or strongly associated to an organisation. Typically, this is performed as a part of reconnaissance conducted before an attack where a malicious actor will collect and analyse publicly available information about the intended target in an effort to map out the attack surface of an organisation or its employees.

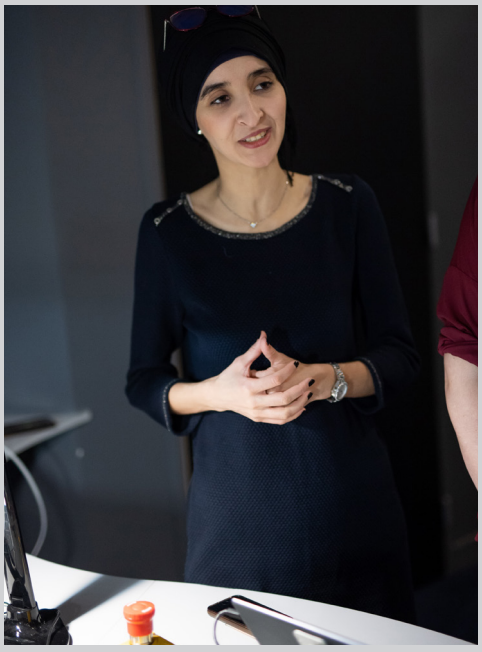
External/internal infrastructure security assessments

A security assessment seeks to locate vulnerable computer systems and networks and then evaluate their security by safely attacking those systems from the perspective of a hacker. Orange Cyberdefense offers two categories of assessment. External testing takes the perspective of an external attacker by looking at how an organisation presents itself on the Internet and attempts to gain access to the internal network.

Internal testing takes the perspective of an attacker that has already gained access to the internal network and looks at potential vulnerabilities on an internal network. The goal of the internal test is to take control of critical systems, gain access to sensitive data and then set up a persistent presence for future access.

Spot-check penetration test

A penetration test seeks to locate vulnerable computer systems and networks and then evaluate the security by safely trying to exploit vulnerabilities through attacking those systems from the perspective of a malicious actor. Penetration Testing, while extremely valuable in determining whether public-facing infrastructure may be offering exploitable vulnerabilities, can be time consuming and expensive, especially when performed on a regular basis.



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.

Executive risk assessment

Most organisations perform internal and external infrastructure security assessments or 'penetration tests' as they are also known. Many organisations also perform regular vulnerability scans on their public-facing and internal infrastructure. The number of organisations performing regular Phishing assessments is growing as awareness of the risk posed by email attachments and email-embedded hyperlinks is becoming more of a reality.

There is however one area, frequently attacked by malicious actors due to its high value, that many organisations do not consider. The organisation's executive branch.

Mobile/source-code/web application assessments

Whether via source-code review performed by specialist Security Analysts, dynamic analysis of an application while it is executing or static analysis of the application in a non-runtime environment, Orange Cyberdefense are able to introduce assurance at any point in the software development life cycle (SDLC) testing both the application and the technical security controls that are relied on to protect against vulnerabilities.