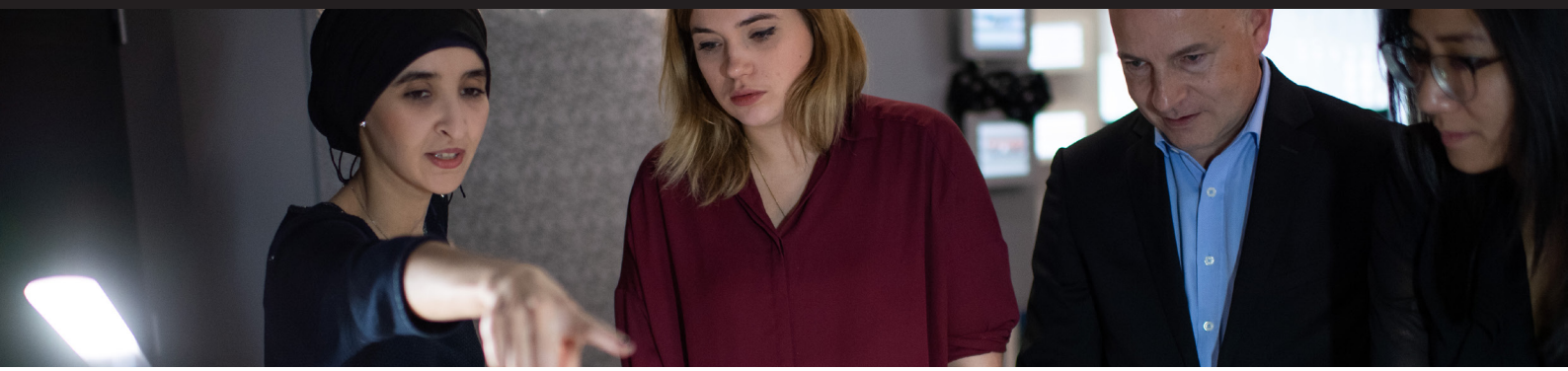
Orange
Cyberdefense



SensePost assessments

Spot Check Penetration Test

Key benefits

Reduce risk of attack
Mimicking real hacker behaviours provides a higher level of assurance.

Comprehensive assessment
Exhaustive, multi-layered vulnerability assessment using a combination of tools and techniques.

Discover all your vulnerabilities
Exploring all potential vulnerabilities and attack methods increases the likelihood of finding potential security issues.

Prioritise your risks
False positives are eliminated by expert analysts, with reporting focused on the issues that matter the most to your organisation.

Tailored approach
Our ethical hackers simulate cyber-criminals, identifying security issues beyond the capability of automated tools.

Service description

Recent high profile hacks have shown that hackers exploit common vulnerabilities using well understood and documented techniques. Every organisation is a target, even those without high value information assets. Compromised systems are a valuable commodity. They are often used to amplify DDoS attacks, act as a jump point for hacking other businesses and to send spam or host illegal content. Cybercriminals will scour the internet for vulnerable systems and organisations with weak IT security. It is important to identify your weaknesses before cybercriminals do.

As part of our comprehensive portfolio of Security Assessment Services, a Spot Check Penetration Test attempts to identify and compromise vulnerable systems. Working under strict ethical guidelines our ethical hackers simulate an attack from the perspective of a hacker. We use all the skills and resources at their disposal to compromise the system or application under review.

We start by conducting a vulnerability scan against the target using a combination of commercial and proprietary tools. The results of the scans are reviewed and vetted by an expert analyst and any false positives are removed. Where possible, vulnerabilities are exploited to prove their validity. We'll then provide a detailed report outlining all the vulnerabilities discovered, prioritised by risk, as well as the recommended remediation steps. Our detailed findings provides the information you need to prevent a real hacker compromising your business.

Key service features:

- **Test performed by ethical hackers**
  Orange Cyberdefense's security analysts apply 17 years of ethical hacking experience to deliver a detailed security assessment of your external environment or web application
- **Comprehensive scanning tools**
  We apply a combination of seven best-of-breed scanning tools, Orange Cyberdefense custom-developed tools and expert human verification
- **Vulnerability verification**
  Assessment results are verified against known vulnerability databases and attack methods to ensure all possible security issues are explored
- **Detailed analyst reporting**
  Our ethical hackers review all false positives to present:
  - Executive summary of findings with recommendations, risk summary and network health assessment
  - Detailed information on vulnerabilities prioritised by ease of exploit and potential impact
- **Tailored to your organisation**
  Our assessment techniques adapt according to the findings from our initial vulnerability scans

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

- The Spot Check Penetration Test can be performed on any external IP address or unauthenticated web application.
- The test is conducted remotely for a period of four days on either ten IP addresses or one application as designated by the client.
- Fully compliant with relevant industry standards, including OSSTMM, NIST and OWASP ASVS testing guides.