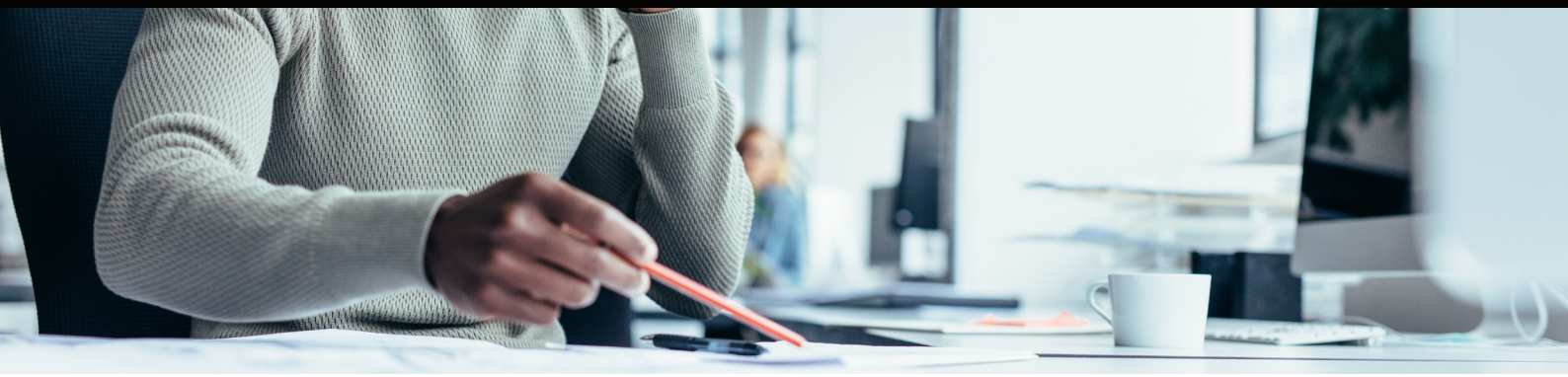
Orange Cyberdefense



SensePost assessments

External Infrastructure

Key benefits

Qualified real-world testing
Using a strict methodology, a review of Internet facing infrastructure from an attackers perspective, using both authenticated and unauthenticated perspectives, provides thoughtful insights into an organisations external thread landscape.

Reduced risk
Comprehensive reviews increase the chance of finding any security issues before a malicious actor does.

Systematic approach
We follow industry recommended practises to allow for consistently reproducible results as well as custom experience-led activities to demonstrate real world risk.

Service description

Almost all organizations have some form of internet presence. External assessments take the approach of assessing externally facing infrastructure, including webservers, fileservers, domains and any related Internet facing hosts. This assessment is geared towards demonstrating how Internet facing infrastructure could be compromised, while mapping the external attack surface.

The SensePost team uses both proprietary and open source toolsets to produce accurate footprint data. Footprinting is either performed on a specific list of external IP ranges or an exercise termed “an extended footprint” whereby IP ranges are also discovered amongst other. The extended footprint can also be leveraged to determine rogue marketing sites, or unattended development environments which pose great business risk.

The service includes a thorough assessment of Internet facing infrastructure for an organisation based on a detailed methodology aligned with best practises (including cloud best practices, CREST, and MITRE). The assessment includes detailed penetration testing, exploitation of vulnerabilities, privilege escalation and pivoting into the target network. More advanced assessments like red teaming include elements of the external assessment in the initial phases while focussing on key objectives.

External assessments can customised to focus on key elements such as the reconnaissance phase to focus on phishing as a means to obtain valid credentials to either take over a mailbox, or more nefariously gain access to the internal network. The focus would not be the successful phish, but rather the security implications of a successful phishing attack.

Why Orange Cyberdefense?

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe. As a leading go-to security provider, we strive to protect freedom and build a safer digital society.

We are threat research, intelligence-driven, offering unparalleled access to current and emerging threats. With a 25+ year track record in information security, 250+ researchers & analysts and 16 SOCs distributed across the world and sales and services support in 160 countries, we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

We are proud of our high-end security research unit, thanks to which we publish regularly white papers, articles and tools on cybersecurity which are widely recognised and used throughout the industry and featured at industry conferences including, Infosec, Manchester DTX, RSA, BlackHat and DefCon.

SensePost is an ethical hacking team of Orange Cyberdefense, offering offensive security consulting services and trainings. With a 20-year track record, SensePost is seen as trusted advisors who deliver insight, information and systems to enable our customers to make informed decisions about information security that support their business performance.

With team members that include some of the world's most preeminent cybersecurity experts, SensePost has helped governments and blue-chip companies both review and protect their information security and stay ahead of evolving threats. They are also a prolific publisher of leading research articles and tools on cybersecurity which are widely recognised and used throughout the industry and feature regularly at industry conferences including Black Hat and DefCon.

Key service components

- Perform a full network survey to determine attack surface area
- Full network enumeration using scanning techniques
- Perform a vulnerability analysis assessment against all identified targets
- Exploitation of discovered issues to demonstrate risk