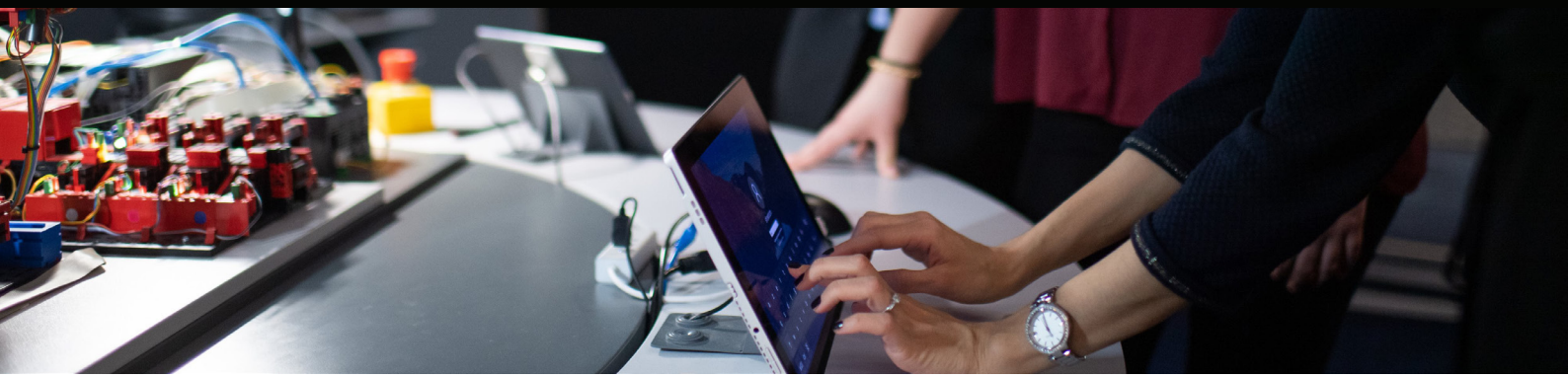
Orange Cyberdefense



SensePost assessments

Red Teaming

Key benefits

Ongoing, real-world attack
Our ethical hackers attack an organisation's users, web estate, public-facing applications and perimeter just like a determined and motivated attacker would while providing opportunities for defenders to test incident response and detection capabilities.

Post-exploitation actions on objectives
With a foothold inside the organisation, focus shifts to targeting specific IT infrastructure that would help in achieving a set of pre-determined goals. In contrast to the breadth approach in an internal network assessment, a Red Team assessment has a clear goal in mind, leveraging anything to help achieve that. With carefully thought through goals, this actions on objectives phase aims to help demonstrate risk by compromising important business-critical systems.

Service description

Significantly more sophisticated than an internal assessment, Red Team assessments simulate real-world, covert, multi-phase attacks as they would be performed by real and persistent criminals.

These assessments are based around "goals" agreed up front which have a significant impact on the focus of the assessment. Careful thought and planning need to go into the goals, considering possible security failures in 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 for any likely attack scenario 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 the way, rather than focusing on initial vectors only. More importantly, this allows for network defenders to practice incident response capabilities, and tweak detections where applicable.

Modern adversaries can take several forms. Our ethical hackers study and practice the behaviour of attack groups, but also research new and novel attack techniques to effectively impersonate the type and sophistication of attacks an organisation may face. A scoping process helps to identify the expected attackers a target organisation may be face, and tailors the assessment to effectively advance the overall security maturity as an outcome. Broadly speaking, the types of attackers would fall into the following categories:

- **Opportunists** look for easy to exploit vulnerabilities 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 business systems well enough to bypass their rules. Examples here are "ghost employees" or supplier payment fraud. Couple these with malicious actors that are skilled at technically manipulating systems in ways no one intended and the chances of a successful attack becomes highly probable.
- **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, 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

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

- **Reconnaissance**
  Discovering and collecting public information to be used in further attacks, or appearing as a legitimate business entity in the form of a malicious domain used in spear phishing attacks is one example of many possible ways to approach an attack. Activities typically 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).

- **Perimeter breach**
  Depending on the goals, a perimeter breach serves as the initial entry vector onto a network. This is most often achieved by exploiting a vulnerability in an Internet facing system, malware delivered through phishing exercises, or via a set of weak credentials that is used to access Remote Access Services. Depending on time constraints, this phase is often simulated in an "assume breach" scenario whereby a specific payload is executed to accelerate moving towards the final Actions on Objectives phase.

- **Lateral movement**
  With a foothold on the internal network, this stage of the attack is where further reconnaissance of the internal network and user behaviour is conducted with the aim of identifying systems key to achieving the pre-determined goals. A beachhead would typically be established for redundant and persistent communications into the network. In some cases, and if needed, achieving the goals will include a compromise of a Microsoft Active Directory domain. However, critical business systems can often be accessed via other means, negating the need to target a potentially highly monitored target such as Active Directory.

- **Actions on objectives**
  With the appropriate access and understanding of the relevant infrastructure, the actions on objectives phase is the technical execution of a pre-determined goal to both demonstrate the ability to exploit, but also demonstrate the associated risks of a complete attack chain leading up to an attack. Examples include learning entity-specific SWIFT processes in order to make transactions or creating false suppliers and payments in a manner that passes business specific rules.