Orange Cyberdefense

SensePost assessments

Security Consulting

Key benefits

Going, being, talking:
To use an example, we prefer to not stop at advising that strong passwords should be used, and then giving some examples. Instead we test the implementation to understand the cause of what could result in a weak password.

You are getting the facts:
Interaction with a real-world hacker, who understands what it means to circumvent security controls enables you to leverage that knowledge and perspective to implement effective architecture and defences.

Systems thinking:
For example, configuration reviews go beyond the review – it looks at the implementation of that configuration to validate whether the configuration, within the ecosystem, is effective.

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

Service description

Security consulting addresses the niche need organisations have when it comes to cybersecurity. Ethical hacking is not simply an aggregate of different types of assessments: it is the actions organisations take to pro-actively identify vulnerabilities in their security posture which would give rise to business risk.

In taking action, the first step is often not to simply perform an external or internal assessment, but rather to have a meaningful and deliberate conversation with the aim of understanding requirements. This is an even more important conversation at incubation of a new service, infrastructure, application or similar. Some conversations where external security consulting may benefit your decision-making process would be:

• Developing a roadmap towards implementing an information Security Management System and understanding the landscape of standards, accreditations, certifications, best practices and frameworks.

• Understanding the threat landscape pertaining your specific organization with a threat modelling exercise. The intent with threat modelling is not to stop at a tabletop exercise, but to determine which threats are relevant from a security perspective within a business context and include business processes when considering attack paths.

• Performing an architecture review to identify obvious security gaps in your infrastructure.

In conjunction with threat modelling and architecture reviews, bespoke consultation exercises can also be performed with highly focussed objectives. For example:

• Performing a Configuration and Implementation review of your specific infrastructure. This could include any components from cloud service providers to the configuration of a database.

• Reviewing the security of your Kubernetes cluster or serverless environment.

• Confirm if your zero-trust framework has been implemented to be effective at its intent

• Application code reviews.

• Perform password analysis to ensure that a password policy is effective and not ineffectively restrictive.

• Reviews of the security, physical and technical, of equipment such as corporate laptops and other custom build devices.

• Perform a review of how resources can work remotely, and securely. This includes looking at the VPN and remote access technologies beyond the configuration, but as it has been implemented as part of an end to end solution.

Security consulting with the SensePost team is an exercise of fact-finding and truth-telling which underpin an organisation's decision-making ability.

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

- Threat modelling
- VPN and remote working capability review
- Device security review
- Application code reviews
- Security Architecture reviews
- Source Code Reviews
- Configuration implementation reviews