Orange Cyberdefense

SensePost assessments

Cloud Security

Key benefits

Best practices
From both testing and using many of the major Cloud Service Providers, our testing methodologies incorporate real-world experience in Cloud Service Provider infrastructure and application hosting in the cloud.

Knowing our client
A unique presales engagement allows for a thorough understanding of scope. This enables the assessment to be aligned with client requirements focussing on what's important without compromising the security value-add while providing assurance in your organisation's solutions deployed in the cloud.

You get to consume the benefits of the cloud, knowing security has been done right.

Service description

As digital transformation drives organisations to adopt and include cloud infrastructure into their core business, the attack surface changes as well, leaving different attack vectors available for exploitation by attackers. As the saying goes, "the cloud is just someone else's computer" falls somewhat short of describing the environment and its associated risks.

A cloud security assessment in many ways has parallels to a traditional infrastructure assessment. While the manifestation of risk's may be different, threats such as credential disclosure facilitating lateral movement and privilege escalation is as realistic on cloud infrastructure as it is on self-hosted infrastructure, with some nuance.

Cloud infrastructure security is typically a function of:

• Understanding how it is accessed, publicly or privately

• How it is configured – best practices are available from all the major Cloud Services Providers (CSP's)

• Understanding how services, functionality, features and technologies interact

• Solution Specific criteria – Each organisation implements its own combinations of solutions where those solutions are custom-written applications or a set of services where they are simply a tenant. The SensePost team leverages its experience in understanding the solution as it is implemented, and assess it for its intended business purpose, taking the nuance of the underlying cloud infrastructure into account.

As a team we've accrued in excess of 20 years' experience in understanding infrastructure vulnerabilities and demonstrating the extent of these vulnerabilities when chained to obtain privileged access to critical assets, and in so doing, compromising it.

Special considerations for cloud security assessments include:

• (X)aaS – What is my CSP providing me? Platform-, Infrastructure- or Software as-a-service?

• Is the CSP hosting your infrastructure on shared resources, or is it private to you and your organisation?

• What access model has been implemented on their infrastructure?

• What technologies are in place? Are these technologies actual hardware, or virtual?

• Serverless environments.

• Microservices and orchestration; consider technologies like docker and Kubernetes and alike

• Most of the CSP's work with a shared risk model; where does this correlate to your risk boundary in terms of liability

One of the key characteristics of cloud security is that it can scale to meet its clients' needs. In response to this, so does our service; from assessing the functional behaviour of an API to the deep-seeded technical operation of a Kubernetes cluster in a financial services organisation.

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

In our methodology we cover various best practices as well as these specific components as time allows:

- Define test scenarios, and then assess those scenarios with regards to the applicable technology stack
- Credential management
- Test for encryption where applicable
- Correct remote access setup
- Minimal Internet exposed service configuration
- Review the configuration of various services used
- Review IAM for AWS or other identity management configuration for other CSP's
- Service and Network Segmentation
- Zoning
- Zero-trust Architectures
- Network security model
- Compliance
- CSP Subscriptions and account relationships