Mandiant

DATASHEET

Cloud Penetration Testing

Benefits

- Identify specific cloud-hosted attack surface risks in your specific environment
- Validate security vulnerabilities in your cloud environment before an attacker exploits them
- Understand the latest cloud security threats facing your organization based on frontline incident response experience
- Harden your cloud environment with actionable, strategic recommendations based on real-world incidents
- Assess your cloud security detection and prevention capabilities through real-world simulation exercises

Identify security threats and validate technology controls relevant to your cloud-hosted environments

Overview

The growing migration to cloud-hosted environments requires organizations to have a mature cloud security posture. Many security-conscious organizations are looking to assess their cloud risks, evaluate cloud threats and validate their cloud technology controls.

Mandiant experts have seen a significant increase in cloud-related incident response engagements, both private and public. The demand for cloud security services is rising in lockstep with the expanded attack surface.

The Mandiant Cloud Penetration Testing service assesses the effectiveness of your existing cloud security defense capabilities and controls. With expertise across the most popular cloud platforms including AWS, Azure and Google, our service is tailored to meet the needs of your organization's cloud-hosted resources.

Our experts perform simulated attacks in your environment that mirror attack behaviors seen on the frontlines of recent Mandiant incident response investigations.

Mandiant provides strategic, technical and actionable recommendations to harden your cloud environment, mature your cloud capabilities, and reduce your overall attack surface.

Our approach

As part of our proven methodology, Mandiant experts:

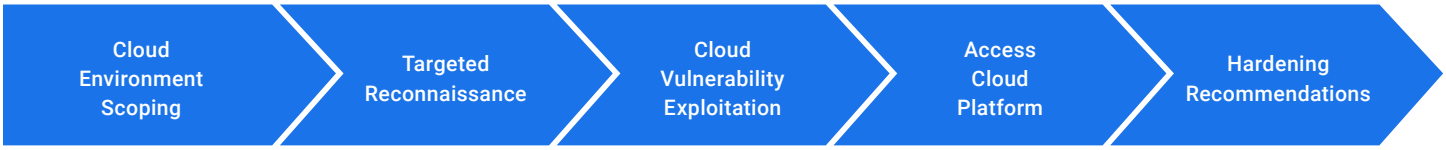
1. Work with you to understand the scope of the specific cloud-hosted environment to be evaluated.
2. Conduct targeted reconnaissance to assess the attack surface of externally exposed systems and services.
3. Attempt to exploit identified vulnerabilities using a combination of publicly available exploits and commercial penetration testing tools. Our experts then conduct realistic attack simulations using internally developed exploits and tools to mirror the latest attacker behaviors as seen on the frontlines.

4. Work to gain access to your cloud platform from the Internet with a mission to steal data from sensitive environments in your network or take control of critical devices to issue malicious commands.
5. Provide hardening recommendations to improve the overall defense and maturity of your cloud environment. Our objective is to help you mitigate attack surface vulnerability and exposure. This activity also leaves your team with attack-related artifacts to review, as well as the option to create similar, valuable indicators and alerts to aid in early detection of future incidents.

Why Mandiant

Mandiant has been at the forefront of cyber security and cyber threat intelligence since 2004. Our incident responders are on the frontlines of the most complex breaches worldwide. We have a deep understanding of both existing and emerging threat actors, as well as their rapidly changing tactics, techniques and procedures.

Summary of engagement phases



Engagement outcomes

- **Executive briefing.** Overview of the service scope and critical findings for executive- and senior level management
- **Technical briefing.** Engagement details that enable you to recreate the findings for future and recurring assessment
- **Risk analysis report.** Fact-based risk analysis to confirm the critical findings are relevant to your specific cloud environment
- **Actionable recommendations.** Strategic and technical recommendations for both immediate and long-term improvements to your cloud security program