Security Compass
ADVISORY

aws Azure Google Cloud

Adversarial Simulation

With an experienced team, flexible engagement design, and proven attack simulation methods, Security Compass helps you reach your security and compliance goals by providing a clear picture of real-world risk.

Defend Against Technical and Human Threats

Red teaming helps your business determine its readiness to defend at all levels of the attack chain, testing a full range of Tactics, Techniques, and Procedures (TTPs), including both technical exploits and social engineering.

Adapt to Business Goals and Maturity

We adapt our adversarial simulation approach to your business needs. In addition to pure red teaming, we can also perform a purple team engagement, giving your internal blue team real-time visibility of attacks and how well your existing defenses and controls work.

Fuel Strategic Decision Making

Aligned with MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework, we cover the entire attack chain and provide detailed analysis of your organization's detection and protection maturity mapped to individual TTPs.

Our 7-Step Red Teaming Engagement Process

1. Planning

Work with business stakeholders to determine the scope and objectives of the adversarial simulation.

2. OSINT

Use sources including Google searches, social media, IP blocks, ASN records, DNS records, and metadata to gain a solid foundation of public information that's accessible to attackers.

3. Active Reconnaissance

Gather information from the network through methods including host discovery, scanning, subdomain enumeration, email address validation, and on-site physical reconnaissance.

4. Initial Compromise

Access the network through phishing, social engineering, or physical intrusion.

5. Persistence and Lateral Movement

Achieve sustained access to the network via persistence mechanisms and expand access to additional systems on the network.

6. Achieve Objectives

Attempt to achieve the objectives defined in the planning phase in order to show potential impact of a real-world attack.

7. Reporting

Produce professionally crafted and revised reports with a timeline of all activity, test case results, observations, and recommendations to inform strategic decision making by security and compliance teams.

Industry Leaders in Attack Simulation

Security Compass has more than **20 team members** with OSCP, OSWE, or GPEN certifications, many of whom have trained with industry leaders in red teaming at conferences including Black Hat and NorthSec.

Put our cutting-edge offensive security experience to work for you and learn how prepared your company is to defend against real-world attackers.

Contact Us

aws Azure Google Cloud