Red Team Exercise

Your organization has invested in a cybersecurity program to mitigate material risk to your assets. Yet you are concerned your defensive perspective might be hampering your ability to see gaps in your people, process, and technology. You need a partner to adopt an adversarial approach under controlled circumstances so you can see the impact a breach would have on your business interests.

A Praetorian Red Team exercise puts a client’s security program to the test in order to uncover any remaining vulnerabilities and inform future security investment. All Praetorian Red Team engineers have demonstrated expertise across multiple industries with intimate knowledge of enterprise technologies and modern environments, including Cloud environments, DevOps stacks, and modern SaaS focused deployments.

Offensive approach. The Praetorian Red Team leverages both public and private attacker tactics, techniques, and procedures (TTPs) in an attempt to accomplish a predetermined business impact objective. We begin the exercise from a position of zero-prior knowledge, and incorporate each stage of an attack lifecycle:

**ATTACK STAGING**
- Prepare the infrastructure and tooling required to orchestrate the attack.

**RECONNAISSANCE**
- Obtain information about the client’s people, process, & technology to identify attack surfaces and provide intelligence to attacks.

**INITIAL ACCESS**
- Identify and exploit attack vectors to gain initial access to the target environment.

**PERSISTENCE**
- Establish a persistent foothold within the target environment.

**LATERAL MOVEMENT**
- Compromise additional assets and gain additional privileges in a strategic fashion that supports the attack mission.

**PRIVILEGE ESCALATION**
- Understand the standard operating procedures surrounding the attack objectives and perform necessary steps to achieve the goal.

**ACTIONS ON OBJECTIVES**

---

**KEY BENEFITS**

- **Assess** security assumptions and capabilities in a controlled scenario.
- **Gain** objective insights on current security posture to understand risk exposure.
- **Determine** the potential business impacts that may result from a successful breach, to inform future security investment planning.
Boards of Directors seeking to ascertain the risk of a high profile attack and understand potential impacts to the business, its customers, and partners.

Security teams wanting to run their playbooks or justify new security initiatives, budget cycles, or recent security investment

Organisations needing to demonstrate resilience against cyber-attacks and/or demonstrate resolution of audit findings as part of previous engagements or regulatory requirements.
DEVELOPERS

Executive Summary
Includes project goals, potential business risks highlighted by the red team’s actions, and strategic recommendations for improving resilience against targeted cyber-attacks.

Outbrief
An in-depth discussion that walks through the engagement and its outcomes with all project stakeholders and engagement participants.

Technical Findings Report
Includes comprehensive narrative-style report of the red team’s actions and the outcomes thereof, granular documentation of significant findings, and recommendations from the engagement.