PRAETORIAN

DATA SHEET

Red Team

Put your security program to the test with a simulated cyber-attack that exercises your Prevention, Detection, and Response capabilities across People, Processes, and Technology.

CONTENTS

Key Benefits

- **Assess Security Assumptions:** Test your security capabilities in a controlled scenario to validate your defensive posture.
- **Gain Objective Insights:** Understand your current security posture and risk exposure from an attacker's perspective.
- **Inform Future Investment:** Determine potential business impacts from a successful breach to guide security investment planning.

Your Challenge

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.

> **The Need for Adversarial Testing:** 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.

Capabilities Overview

A Praetorian Red Team exercise puts your security program to the test to uncover 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) to accomplish a predetermined business impact objective. We begin from a position of zero-prior knowledge and incorporate each stage of the attack lifecycle.

Attack Lifecycle

ATTACK STAGING

Prepare infrastructure and tooling required to orchestrate the attack

RECONNAISSANCE

Obtain information about people, process, and technology to identify attack surfaces

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 privileges strategically

PRIVILEGE ESCALATION

Gain additional privileges to support the attack mission

ACTIONS ON OBJECTIVES

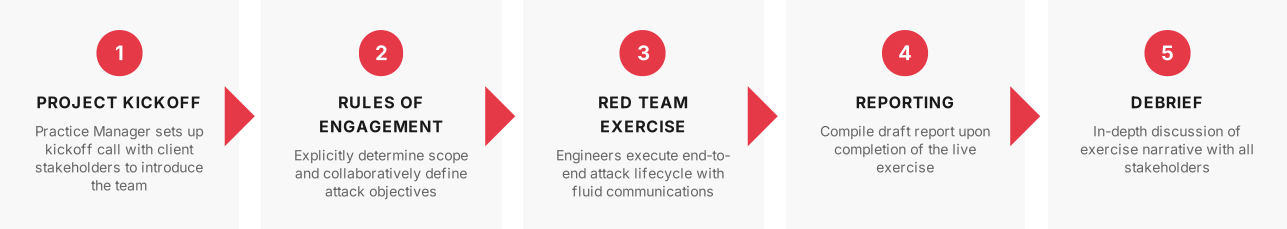
Perform necessary steps to achieve the predetermined goal

REPORTING

Document findings and provide actionable recommendations

Workflow

A Praetorian Red Team exercise is not the wild west. The safety of your environment is the primary driver behind each decision we make. We are your security partner.



Sample Attack Objectives

We work with you to set attack objectives that align with your specific business risks. Sample objectives include:

- Demonstrate direct financial loss through transfer of monetary funds to a nominated bank account
- Demonstrate ability to exert control over an ICS device/environment (water plant, food processing, oil refinement)
- Perpetrate theft of customer data and personally identifiable information such as address, contact details and banking information
- Demonstrate access to VIP mailbox, data, or workstation
- Demonstrate control over a critical capability such as power supply to a geographic location

Why Praetorian

Praetorian Red Team engagements subject your organization to an end-to-end cyber-attack that exercises your Prevention, Detection, and Response capabilities across People, Processes, and Technology.

Our security engineers provide your team with the opportunity to exercise defensive playbooks under realistic conditions, without the negative impact of a real-world breach. We put your security assumptions to the test and provide factual information regarding your current security maturity posture.

Who Needs This Service

- **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
- **Organizations** needing to demonstrate resilience against cyber-attacks and/or demonstrate resolution of audit findings as part of regulatory requirements

Deliverables

Every engagement delivers comprehensive documentation suitable for both technical teams and executive stakeholders.

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

Comprehensive narrative-style report of the red team's actions and outcomes, granular documentation of significant findings, and recommendations.

About Praetorian

Praetorian is an offensive cybersecurity company whose mission is to prevent breaches before they occur. We help our customers minimize the likelihood of compromise by using an adversarial perspective to uncover material risks the same way attackers do. Our team combines deep technical expertise with industry knowledge to deliver comprehensive security assessments that meet the highest standards.

Website
www.praetorian.com

Email
info@praetorian.com

Phone
+1 (512) 686-2292

Ready to Test Your Security Posture?

Contact us today to discuss your Red Team exercise and discover how Praetorian can help you validate your security assumptions.