praetorian

DATA SHEET

Red Team Exercise

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

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. 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.

OUR SOLUTION: CAPABILITIES OVERVIEW

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

PRIVILEGE ESCALATION

Compromise additional assets and gain additional privileges in a strategic fashion that supports the attack mission

ACTIONS ON OBJECTIVES

Understand the standard operating procedures surrounding the attack objectives and perform necessary steps to achieve the goal

WORKFLOW

1

PROJECT KICKOFF

Praetorian's Practice Manager will set up a kickoff call with client stakeholders to introduce the team.

2

RULES OF ENGAGEMENT & THREAT MODEL

We explicitly determine the scope of the exercise and collaboratively define the attack objective.

3

RED TEAM EXERCISE

Our engineers execute the end-to-end attack lifecycle. Communications occur between the predefined teams in a fluid fashion.

4

REPORTING

Upon completion of the live exercise, Praetorian compiles the draft report.

5

DEBRIEF

We hold a debriefing call between all participants and the client's project stakeholders wherein we discuss an in-depth narrative of the exercise.

Collaborative attack objectives. A Praetorian Red Team exercise is not the wild west. The safety of our client's environment is the primary driver behind each decision we make for the duration of the exercise. We are their security partner.

For that reason, we ensure the client provides explicit consent and authorization for every attack action. We work with the client to set attack objectives that align with their specific business risks. The objectives then drive the engagement, informing the technical milestones we set. Finally, they provide a focal point for demonstrating impact.

Sample attack objectives include:

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

WHY PRAETORIAN

Praetorian Red Team engagements subject client organizations to an end-to-end cyber-attack that exercises their Prevention, Detection, & Response capabilities across their People, Processes, & Technology. Our security engineers provide the client's security team with the opportunity to exercise their defensive playbooks under realistic conditions, without the negative impact of a real-world breach. We put clients' security assumptions to the test, and provide factual information regarding the current security maturity posture of their organisation.

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

DELIVERABLES

Executive Summary

Includes project goals, potential business riskshighlightedby 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.

Praetorian Security, Inc.
6001 W Parmer Ln, Ste 370, PMB 2923
Austin, TX 78727 USA
info@praetorian.com

To learn more about Praetorian, visit: www.praetorian.com

ABOUT PRAETORIAN

Praetorian is an offensive security engineering company whose mission is to make the digital world safer and more secure. Through expertise and engineering, Praetorian helps today’s leading organizations solve complex cybersecurity problems across critical enterprise assets and product portfolios.