PRAETORIAN

DATA SHEET

Purple Team Engagements

Collaborative security exercises that improve your ability to prevent, detect, and respond to attacks through tailored attack scenarios and interactive workshops.

CONTENTS

Key Benefits

- **Assess Security Assumptions:** Evaluate capabilities through collaborative, controlled attack scenarios
- **Improve Attack Readiness:** Prepare for the threats most relevant to your organization
- **Enhance Detection & Response:** Improve ability to detect attacks, triage security events, and execute response procedures

Your Challenge

Your organization has invested significant financial and human resources in developing a cybersecurity strategy that aims to prevent, detect, and respond to threats. You need to know how effective your people, process, and technology are at maintaining a robust security posture.

> **Collaborative Improvement:** Your internal team wants to collaborate on refining your approach wherever gaps might exist.

Capabilities Overview

Praetorian Purple Team engagements encompass two primary variants plus an optional supplemental offering. Regardless of variant, the goal is to identify gaps in your security strategy and provide detailed strategies tailored specifically for your environment and defensive controls.

DETECTION & RESPONSE ANALYSIS

Can be standalone or follow-on from Red Team exercises. Involves collaborative workshops to discuss prevention, detection, and response opportunities across attack chains.

CONTROLS VALIDATION

Tests effectiveness of security controls through attack chain simulations. Includes EDR testing, policy evaluation, and MITRE ATT&CK Framework TTPs.

DEFENSE ENABLEMENT

Optional supplemental offering where Praetorian engineers implement detection engineering logic within your existing security technology stack.

Service Variants

Standalone Detection & Response

Praetorian engineers develop and perform an attack scenario with TTPs based on your risk profile, then conduct interactive workshops with your security teams.

Follow-On Detection & Response

The same engineers who conducted a Red Team engagement replay the original attack chain execution in a collaborative, interactive fashion with your teams.

Why Praetorian

Praetorian Purple Team engagements provide collaborative exercises with the objective of improving your ability to prevent, detect, and respond to attacks against your organization.

Through the execution of tailored attack scenarios, we evaluate the effectiveness of your organization's defenses and provide actionable recommendations for improving security. Our engineers put your security assumptions to the test and work interactively with you to close the gaps that expose your organization to risk.

> **Expertise:** All Praetorian Purple Team engineers have demonstrated expertise across multiple industries with intimate knowledge of enterprise technologies and modern environments, including Cloud, DevOps stacks, and SaaS deployments.

Who Needs This Service

- **Boards of Directors** looking to bolster their organization's resilience to cyber-attacks
- **Security teams** wanting to derive additional value from previous engagement types and ensure attack readiness across a range of TTPs
- **Organizations** needing to demonstrate resilience against cyber-attacks and/or demonstrate resolution of audit findings as part of regulatory requirements

Workflow

Detection & Response Analysis - Standalone Workflow:

2-3 WEEKS OUT	WEEK 1	WEEK 2	WEEK 2+
Engagement Setup	**TTP Creation**	**TTP Execution**	**Documentation**
Kickoff, finalize objectives, create schedule, setup meetings	Confirm access, environment familiarization, create and tune TTPs	Collaborative sessions, real-time execution, replay and walkthrough	Reporting, client verification, technical and executive debrief

> **Both approaches involve collaboration** between Praetorian and the client to discuss opportunities for prevention, detection, and response across each step of the executed attack chains. Praetorian also tests the efficacy of any improvements the client implements throughout the engagement.

Deliverables

At the completion of the engagement, Praetorian experts provide the following:

Executive Summary

Includes project goals, potential business risks highlighted by the 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.

Interactive Workshops

Tailored workshops that nurture internal collaboration, provide training and experience, and improve overall attack readiness against cyber-attacks.

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.

Website
www.praetorian.com

Email
info@praetorian.com

Address
6001 W Parmer Ln, Ste 370, PMB 2923
Austin, TX 78727 USA

Ready to Strengthen Your Defenses?

Contact us today to discuss your Purple Team engagement and discover how Praetorian can help you improve your security posture through collaborative testing.