praetorian

DATA SHEET

Purple Team Engagements

KEY BENEFITS

Assess security assumptions and capabilities through collaborative, controlled attack scenarios

Improve your attack readiness for the threats that are relevant to your organization

Enhance your ability to detect attacks, triage security events, & execute an appropriate response procedure

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. Your internal team also wants to collaborate on refining your approach wherever gaps might exist.

OUR SOLUTION: CAPABILITIES OVERVIEW

Praetorian Purple Team engagements encompass two variants–Detection & Response Analysis and Controls Validation–plus an optional supplemental Defense Enablement offering. Regardless of variant, the goal always is to identify any gaps that might exist in a client's security strategy, and provide detailed strategies tailored specifically for the client's environment and defensive controls.

- **Detection & Response Analysis** engagements can take the form of a standalone exercise or a direct follow-on from a Red Team or similar exercise.

Standalone

Praetorian engineers develop and perform an attack scenario with tactics, techniques & procedures based on the risk profile of the target environment. The Praetorian team then conducts interactive workshops with the client security teams.

Follow-on

The Praetorian engineers who conducted the initial exercise, such as a Red Team, replay the original attack chain execution in a collaborative, interactive fashion with the client security teams.

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

- **Controls Validation** engagements test and evaluate the effectiveness of an organization's security controls through the simulation of attack chain components. They can include testing host-based security controls, such as EDR software and attack reduction rules, as well as testing the effectiveness of policies and procedures, such as incident response plans. This type of engagement may also incorporate a selection of the MITRE ATT&CK Framework TTPs through atomic testing of preventive and detection controls.

- **Defense Enablement** is a supplemental offering to both Detection & Response Analysis and Controls Validation engagements. The Defense Enablement optional phases involve Praetorian engineers implementing the detection engineering logic within the existing security technology stack. This process results in high-fidelity detection logic and response playbooks for client organizations.

WHY PRAETORIAN

Praetorian Purple Team engagements provide collaborative exercises with the objective of improving a client's ability to prevent, detect, & respond to attacks against their organization. Through the execution of tailored attack scenarios, we will evaluate the effectiveness of your organization's defenses and provide actionable recommendations for improving security. Our engineers will put your security assumptions to the test and work interactively with you to close the gaps that expose your organization to the risk of compromise.

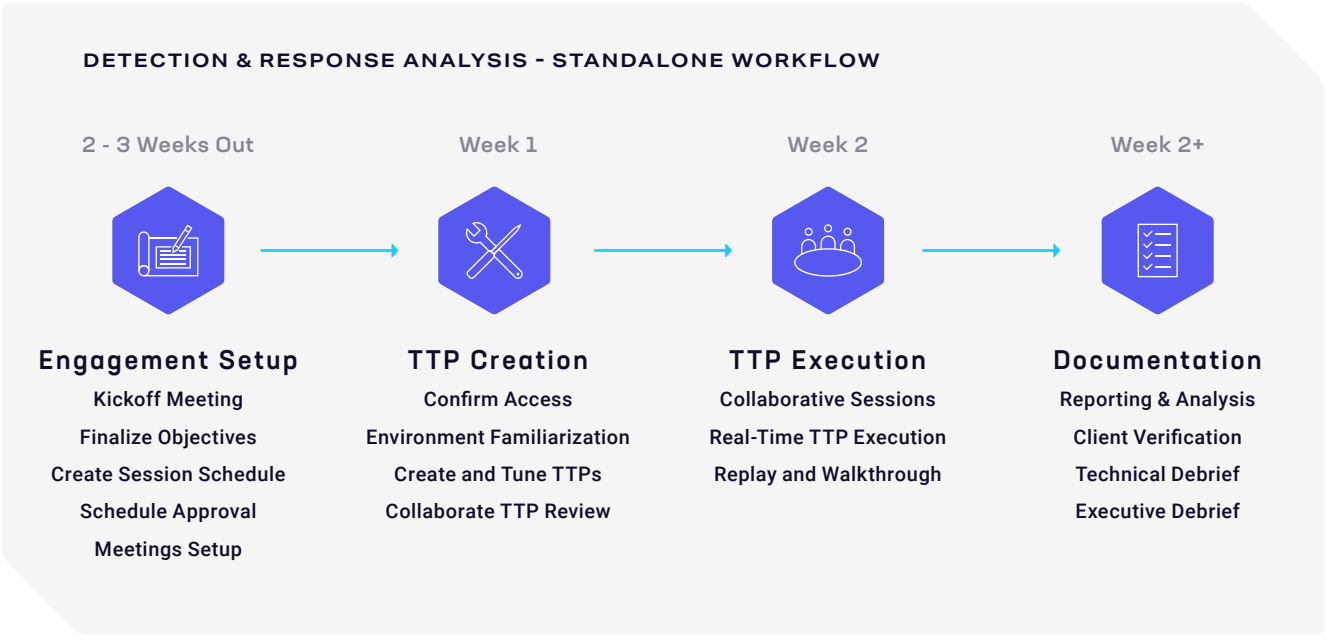
All Praetorian Purple Team engineers have demonstrated expertise across multiple industries with intimate knowledge of enterprise technologies and modern environments, including Cloud environments, DevOps stacks, and modern SaaS focused deployments.

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 their attack readiness across a range of TTPs.
- **Organisations** needing to demonstrate resilience against cyber-attacks and/or demonstrate resolution of audit findings as part of previous engagements or regulatory requirements.

WORKFLOW

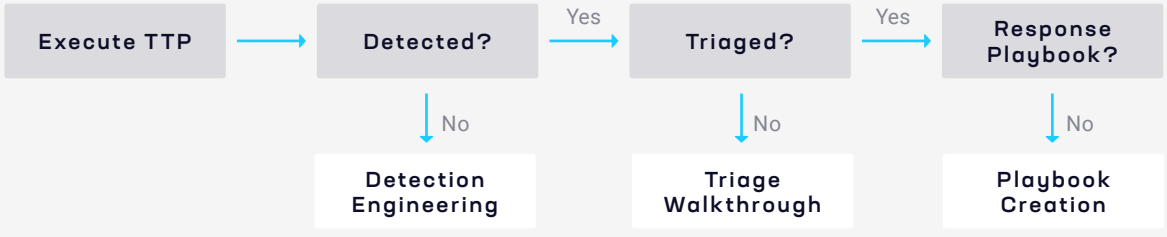
DETECTION & RESPONSE ANALYSIS - STANDALONE WORKFLOW



DETECTION & RESPONSE ANALYSIS - FOLLOW-ON WORKFLOW

CONTROLS VALIDATION WORKFLOW

DEFENSE ENABLEMENT WORKFLOW



DELIVERABLES

Executive Summary

Includes project goals, potential business risks highlighted by the Praetorian 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.

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.