PRAETORIAN

DATA SHEET

Attack Path Mapping Assessment

A risk-informed, collaborative approach to assessing your network security posture and reducing available attack paths that expose your organization to compromise.

CONTENTS

Key Benefits

- **Identify Attack Paths:** Discover viable attack paths within your environment using a risk-informed approach
- **Understand Cost:** Understand the cost of each attack path to assist remediation prioritization
- **Improve Resilience:** Reduce available attack paths and improve resilience to cyber-attacks
- **Enhance Perspective:** Gain an offensive perspective through adversarial exercises

Why Do an Attack Path Mapping

Praetorian Attack Path Mapping (APM) assessments take a risk-informed, collaborative approach to assessing your network security posture. We work with you to reduce the available attack paths that expose your organization to compromise.

> **Comprehensive Coverage:** APM assessments leverage a red team offensive mindset and TTPs, with the additional benefit of increased coverage across your estate as opposed to the exploitation of a single attack chain.

Approach

APM assessments evaluate your network security posture through a collaborative process of information gathering, attack planning, and technical execution.

Our risk-informed approach centers on the construction of a threat model. We perform attack surface discovery, interview teams, and establish a deep understanding of high-value assets and relevant threat intelligence.

> **Threat-Driven Testing:** The threat model shapes the direction of the technical execution phase, during which Praetorian engineers identify and exploit vulnerabilities across your environment. Our goal is to maximize value by providing actionable recommendations for improving security.

Workflow

The PASTA (Process for Attack Simulation and Threat Analysis) methodology guides our approach:

1. **SET OBJECTIVES** — Collaborate with client to define attack objectives aligned with business goals
2. **RECONNAISSANCE** — Conduct reconnaissance across environment, engage interviews, review documentation
3. **THREAT MODEL** — Create threat model and propose attack test cases based on findings
4. **EXECUTE TESTS** — Execute attack test cases to identify and validate vulnerabilities
5. **REPORT** — Deliver comprehensive findings with prioritized remediation recommendations

Who Needs This Service

- **Boards of Directors** looking to use ROI analysis to prioritize and maximize their return on investment for security spend
- **CISOs** searching for ways to bolster their organization's resilience to cyber attacks
- **Security teams** looking for a collaborative, risk-informed way to understand their environment from an attacker's perspective
- **Organizations** wanting to improve security testing efficiency to derive maximum value

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.

Engagement Outbrief

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

Technical Findings Report

Comprehensive report of actions and outcomes, granular documentation of significant findings, and actionable recommendations.

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 Map Your Attack Paths?

Contact us today to discuss your Attack Path Mapping Assessment and discover how Praetorian can help you identify and reduce the attack paths exposing your organization to risk.