DATA SHEET | ATTACK PATH MAPPING

Attack Path Mapping Assessment

KEY BENEFITS

- **Identify** the viable attack paths within your environment using a risk-informed approach
- **Understand** the cost of each attack path, which can assist remediation prioritization
- **Improve** your resilience to cyber-attacks by reducing the available attack paths
- **Enhance** your offensive perspective with an adversarial exercise

WHY DO AN ATTACK PATH MAPPING ASSESSMENT WITH PRAETORIAN

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

Praetorian engineers take the time to understand the client's goals and the target environment before constructing attack paths. Informed by this threat model, we then undertake active testing to identify gaps across the organization's security controls. APM assessments leverage a red team offensive mindset and tactics, techniques, and procedures (TTPs), with the additional benefit of increased coverage across your estate as opposed to the exploitation of a single attack chain.

Our goal throughout is to maximize value to the client by providing actionable recommendations for improving security.

praetorian

Approach

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

Our risk-informed approach to the engagement 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.

The threat model we develop then shapes the direction of the technical execution phase, during which Praetorian engineers identify and exploit vulnerabilities across your environment.

Workflow

1 Set attack objectives in collaboration with client

2 Conduct reconnaissance across environment, engage interviews and review documentation

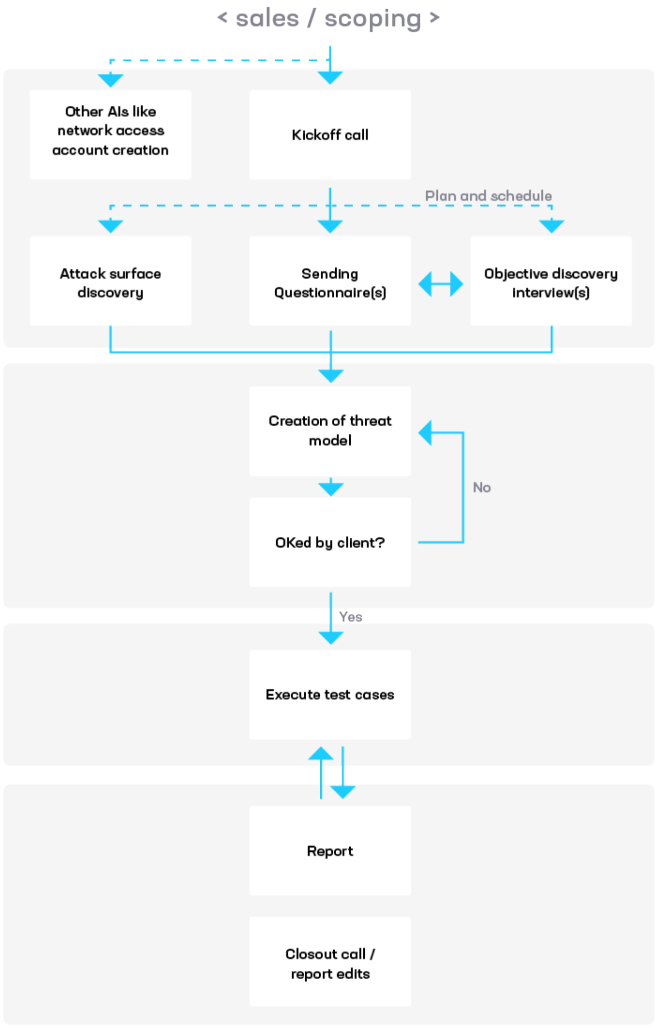
3 Create threat model and propose attack test cases

4 Execute attack test cases

5 Report

PASTA Stage

1. Define Business Functions and Risks
2. Technology Enumeration
3. System Decomposition
4. Threat Analysis
5. Weakness / Vulnerability Identification
6. Attack Simulation
7. Residual Risk Analysis



In the **kickoff call**, determine how attack surface and objectives will be communicated:

- Praetorian-led discovery
- Questionnaires
- Interviews with relevant team(s)

Questionnaires / Interviews- possibly based on PASTA questions in wiki

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 Praetorian team's actions, and strategic recommendations for improving resilience against targeted cyber-attacks.

Engagement Outbrief Presentation

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

Technical Findings Report

Includes comprehensive report of the actions and the outcomes thereof, granular documentation of significant findings, and recommendations from the engagement.

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.

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