DATA SHEET

Assumed Breach Exercise

KEY BENEFITS

- **Assess** security assumptions and capabilities in a controlled scenario
- **Gain** objective insights on current security posture to understand risk exposure in relation to the relevant threats to your organization
- **Determine** the potential business impacts that may result from a successful breach, to inform future security investment planning

WHY PRAETORIAN

Praetorian Assumed Breach engagements subject client organizations to a 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 organization.

praetorian

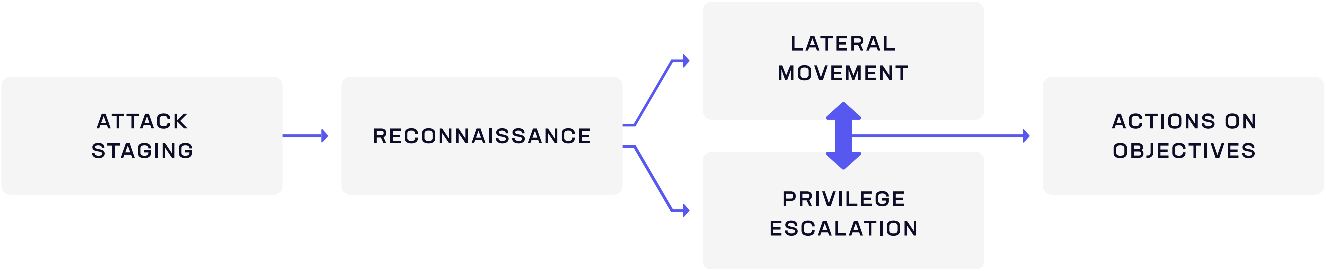
Approach

Praetorian bases Assumed Breach engagements on the assumption that an initial breach of the client environment has occurred, and so we begin within the internal client network. Therefore, the client's defensive goal is to prevent an initial breach of their environment from turning into unfettered access that results in the compromise of mission critical assets or capabilities.

Our team works with the client to create a high-level threat model, which we then leverage to create scenarios that are most probable for the client to encounter. Common scenarios include:

- Malicious insiders
- Compromised contractors
- Compromised supply chain
- Compromised employee
- Compromised public facing service

The Praetorian team leverages both public and private attacker tactics, techniques, and procedures (TTPs) in an attempt to accomplish a predetermined business impact objective. From our beachhead in the client's network, we incorporate each stage of the 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.

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.

All Praetorian 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.

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.

Attack Objectives

A Praetorian Assumed Breach exercise is not the wild west. We are our clients' security partner and the safety of the client's environment is the primary driver behind each decision. For that reason, the Rules of Engagement ensure explicit consent and client authorization is provided for every attack action. The defined attack objectives drive every engagement. These attack goals align with the business risks of each client's specific organization and focus on demonstrating impact. This information also directly informs the technical milestones we set for the engagement.

Examples include:

- Demonstrate direct financial loss through the transfer of monetary funds to a nominated bank account
- Demonstrate access to VIP mailbox, data, or workstation
- Emulate ransomware
- 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

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
- **Clients** desiring an adversarial experience without the additional hours required for a Red Team engagement

Deliverables

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

Executive Summary

Includes project goals, potential business riskshighlighted by 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.

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.
98 San Jacinto Blvd, Suite 500
Austin, TX 78701 USA
info@praetorian.com

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