

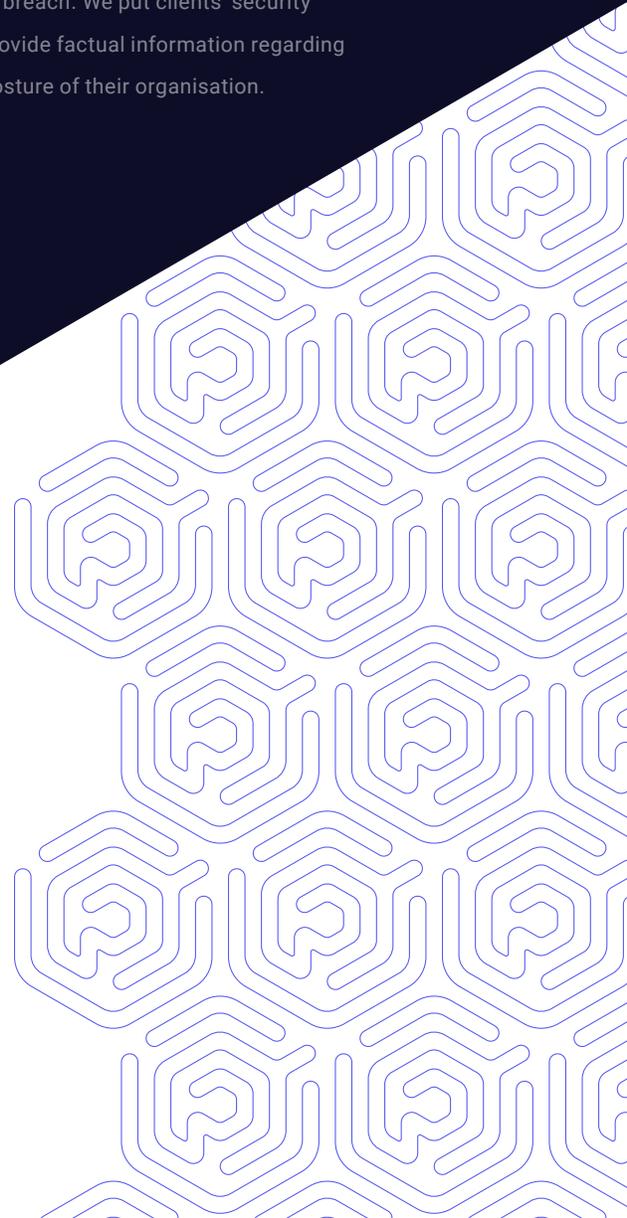
Red Team Exercise

KEY BENEFITS

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

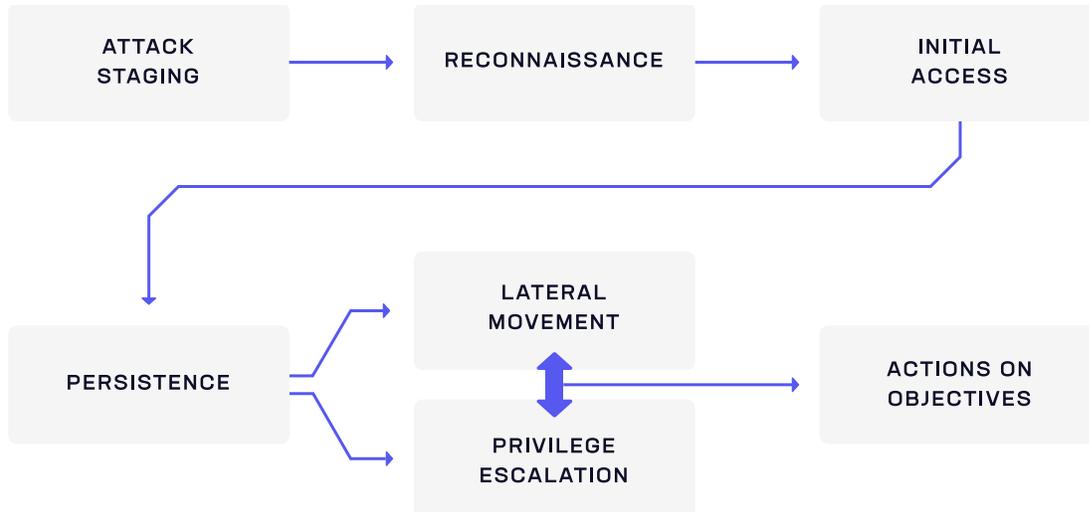
WHY DO A RED TEAM ENGAGEMENT WITH PRAETORIAN

Praetorian Red Team engagements subject client organisations to an end-to-end 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 organisation.



Approach

The Praetorian Red Team leverages both public and private attacker tactics, techniques, and procedures (TTPs) in an attempt to accomplish a predetermined business impact objective. We begin the exercise from a position of zero-prior knowledge, and incorporate each stage of an attack lifecycle:



| | | |
|----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Attack Staging</p> <p>Prepare the infrastructure and tooling required to orchestrate the attack.</p> | <p>Reconnaissance</p> <p>Obtain information about the client’s people, process, & technology to identify attack surfaces and provide intelligence to attacks.</p> | <p>Initial Access</p> <p>Identify and exploit attack vectors to gain initial access to the target environment.</p> |
| <p>Persistence</p> <p>Establish a persistent foothold within the target environment.</p> | <p>Lateral Movement & Privilege Escalation</p> <p>Compromise additional assets and gain additional privileges in a strategic fashion that supports the attack mission.</p> | <p>Actions on Objectives</p> <p>Understand the standard operating procedures surrounding the attack objectives and perform necessary steps to achieve the goal.</p> |

All Praetorian Red 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.

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 Red Team 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 the client provides explicit consent and authorization for every attack action.

The attack objectives align with the business risks of each client's specific organisation, drive the engagement, and provide a focal point for 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
- 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

Deliverables

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



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