PRAETORIAN

DATA SHEET

Assumed Breach Exercise

Test your security program's ability to prevent an initial breach from turning into unfettered access that compromises mission-critical assets or capabilities.

CONTENTS

Key Benefits

- **Assess Security Assumptions:** Test your security capabilities in a controlled scenario to validate your defensive posture.
- **Gain Objective Insights:** Understand your current security posture and risk exposure in relation to relevant threats.
- **Inform Future Investment:** Determine potential business impacts from a successful breach to guide security investment planning.

Why Praetorian

Praetorian Assumed Breach engagements subject your organization to a cyber-attack that exercises your Prevention, Detection, and Response capabilities across People, Processes, and Technology.

Our security engineers provide your team with the opportunity to exercise defensive playbooks under realistic conditions, without the negative impact of a real-world breach. We put your security assumptions to the test and provide factual information regarding your current security maturity posture.

Approach

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

Threat-Driven Scenarios: Our team works with you to create a high-level threat model, which we leverage to create scenarios most probable for your organization to encounter.

Common Scenarios

Malicious Insiders
Threats from employees or contractors with authorized access

Compromised Supply Chain
Attacks through third-party vendors or software dependencies

Compromised Public Facing Service
Exploitation of externally exposed applications or services

Compromised Contractors
Attacks through external consultants or service providers

Compromised Employee
Credential theft or social engineering of staff members

Attack Lifecycle

The Praetorian team leverages both public and private attacker tactics, techniques, and procedures (TTPs) to accomplish a predetermined business impact objective. From our beachhead in your network, we incorporate each stage of the attack lifecycle:

ATTACK STAGING
Prepare infrastructure and tooling required to orchestrate the attack

RECONNAISSANCE
Obtain information about people, process, and technology to identify attack surfaces

LATERAL MOVEMENT & PRIVILEGE ESCALATION
Compromise additional assets and gain privileges strategically

ACTIONS ON OBJECTIVES
Perform necessary steps to achieve the predetermined goal

Workflow

A Praetorian Assumed Breach exercise is not the wild west. We are your security partner and the safety of your environment is the primary driver behind each decision.

1. **PROJECT KICKOFF**
Practice Manager sets up kickoff call with client stakeholders

2. **RULES OF ENGAGEMENT**
Determine scope and collaboratively define attack objective

3. **EXERCISE EXECUTION**
Engineers execute end-to-end attack lifecycle

4. **REPORTING**
Compile draft report upon completion of exercise

5. **DEBRIEF**
In-depth discussion of exercise narrative with stakeholders

Attack Objectives

The defined attack objectives drive every engagement. These goals align with your business risks and focus on demonstrating impact. Examples include:

- Demonstrate direct financial loss through transfer of monetary funds to a nominated bank account
- Emulate ransomware deployment and impact
- Demonstrate control over a critical capability such as power supply to a geographic location
- Demonstrate access to VIP mailbox, data, or workstation
- Demonstrate ability to exert control over an ICS device/environment
- Perpetrate theft of customer data and personally identifiable 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
- **Organizations** needing to demonstrate resilience against cyber-attacks and/or demonstrate resolution of audit findings as part of regulatory requirements
- **Clients** desiring an adversarial experience without the additional hours required for a Red Team engagement

Deliverables

Executive Summary

Includes project goals, potential business risks highlighted by the exercise, 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

Comprehensive narrative-style report of actions and outcomes, granular documentation of significant findings, and 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
98 San Jacinto Blvd, Suite 500
Austin, TX 78701 USA

Ready to Test Your Security Posture?

Contact us today to discuss your Assumed Breach exercise and discover how Praetorian can help you validate your security assumptions.