QUANTIC

OFFENSIVE SECURITY SERVICES

ADVANCED ADVERSARY SIMULATION

Conducting simulated attacks to evaluate, quantify, and enhance risk detection and incident response capabilities.

Adversary simulation exercises enhance security teams and response protocols by uncovering unnoticed attack tactics and vectors.

Organizations encounter ongoing challenges in adapting to evolving adversary tactics. Maintaining strong security measures alone may not ensure swift breach identification and containment. Inadequate skill refinement within incident response, or "security teams," can significantly impede their effectiveness during real breaches. It's essential for these teams to stay vigilant and adept against increasingly sophisticated attackers.

Service Overview

At Quantic Technologies, we offer cutting-edge "Advanced Adversary Simulation Services" to empower organizations with a proactive and comprehensive approach to fortify their cybersecurity defenses.

Our service combines the expertise of seasoned security professionals with state-of-the-art threat emulation techniques to help you assess, strengthen, and refine your security strategies.

Business Benefits

Demonstrated ROI and Informed Investment

Validating cybersecurity investments via adversary simulations demonstrates ROI and informs further spending decisions.

Tool Optimization and Gap Identification

Adversary simulations reveal tool gaps, enabling precise tuning aligned with MITRE ATT&CK for enhanced security.

Enhanced Incident Detection and Response

Adversary simulations improve synergy among people, processes, and technology for a more effective response to threats.

FEATURES

Capabilities

Red Teaming

Evaluation of Detection and Response Capabilities

Purple Teaming

Collaborative Attack Scenario Execution

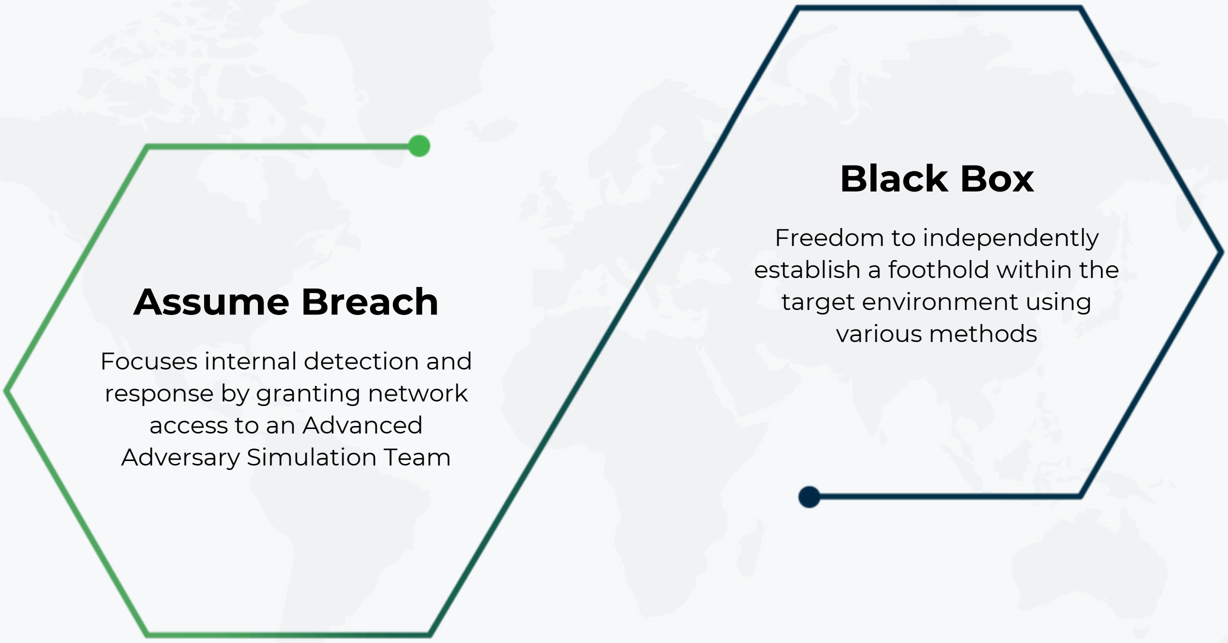
Solution Assessment

Measuring the Effectiveness of your Detection Tools

Penetration Testing Versus Adversary Simulation

Aspect	Adversary Simulation	Penetration Testing
Objective	Emulate real-world cyberattacks, focusing on threat actor behavior and tactics.	Identify and exploit vulnerabilities to evaluate system security.
Focus	Testing security controls and the security team's response to an actual breach.	Identifying and exploiting vulnerabilities in the network, hardware, and applications.
Scope	Extensive understanding of the organization's structure, processes, and units.	Typically limited to vulnerabilities and weaknesses.
Value	Reveals how the organization detects and responds to real-world attacks.	Primarily uncovers technical vulnerabilities.

APPROACH



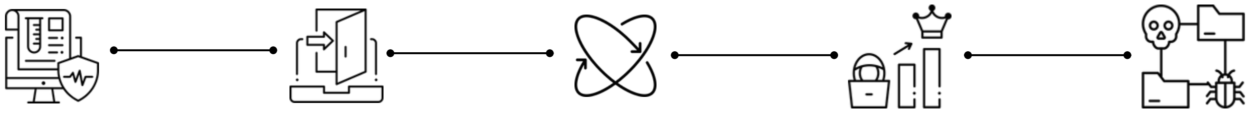
Assume Breach

Focuses internal detection and response by granting network access to an Advanced Adversary Simulation Team

Black Box

Freedom to independently establish a foothold within the target environment using various methods

Methodology



Reconnaissance

Initial Access

Lateral Movement

Privilege Escalation

Persistance

Adversary Simulation Features

- Advanced threat emulation techniques to assess your security operation.
- Collaboration with your team to enhance capabilities.
- Attack scenarios from an attacker's perspective to measure the effectiveness of your detection tools.