Adversary Simulation

Red Team

CSRG

Making it safer to do business.

WHAT IS AN ADVERSARY SIMULATION?

This is not a normal assessment. We simulate a determined, sophisticated, and patient Advanced Persistent Threat (APT).

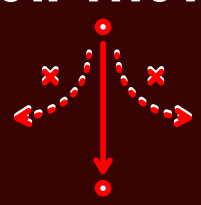
REALISTIC AND BUSINESS DRIVEN

We operate as a true attacker whose goal would be to disrupt your business operations. We do not operate with an 'assumed breach' – you would not give that to an APT, why should you provide to us as part of our assessment?

When we begin our assessment, your business is a 'black box'. We focus on ensuring our evaluation of your detection and response capabilities is as realistic as possible.

From the outset, we develop rules of engagement with you to identify high-value targets that could be most problematic to your company if compromised.

OUR TACTICS



Stealth
Realistic time constraints (e.g., 1-6 months). We simulate attackers who try to avoid detection.

Path of Least Resistance
Simulate adversary focused on achieving objectives, not a total compromise of your systems.

Beyond Domain Admin
We simulate hackers not just looking for access, but also APTs looking to exploit monetary or other business-related advantages.

Social Engineering & Open Source Intelligence (OSINT)
We patiently deploy complex, layered campaigns focused on abusing your existing security processes with publicly available information.

BENEFITS

01. REAL WORLD RESULTS
Our assessments provide you a real-world picture of the weakest areas of your security posture.

02. COLLABORATIVE LEARNING
We work closely with your security team to quickly develop defenses for your infrastructure.

03. CUTTING EDGE
Our methods to penetrate your systems remain dynamic and creative.

04. ACTIONABLE
Results include prioritized, specific, and detailed recommendations to better defend your systems and your company.

INTERESTED? CONTACT US: INFO@CSR.GROUP