OnDefend

Red Teaming

To stop advanced, persistent adversaries, you need a team that can act like one.

Traditional penetration tests are constrained by scope and time windows. Real adversaries don't have these limits. OnDefend's red team goes beyond those limits with scenario-driven, objective-based attacks executed with minimal scope restrictions to determine whether an organization can detect real-world threats.

Testing Capabilities

Initial Access & Social Engineering

Combines technical intrusion and social engineering to simulate realistic initial access scenarios.

Adversary Emulation

Replicates tactics and behaviors of real threat actors, mapped to MITRE ATT&CK and your risk profile.

Objective-Based Operations

Pursues defined attacker objectives to demonstrate real business and operational impact.

Command, Control & Persistence

Establishes covert access designed to survive monitoring, resets, and credential changes.

Privilege Escalation & Lateral Movement

Exploits misconfigurations and trust relationships to escalate privileges and move across systems.

Evasion & Detection Measurement

Evades controls over extended time to measure true detection capability and response effectiveness.

Outcomes

- Full attack paths validated from initial access through escalation, lateral movement, and impact
- Narrative attack path analysis showing how access was gained, maintained, and expanded
- Measured detection and response effectiveness against realistic adversary campaigns
- Business-level risk findings to support security investment and remediation priorities

Red teaming reveals whether your people, processes, and technology can withstand a real adversary. It gives security leaders the evidence needed to prioritize investment and prove resilience.

OnDefend.com