OnDefend

Purple Teaming

Understand why your controls fail and how to fix them

Penetration testing shows whether you can be compromised. Purple teaming goes further to identify why detection and response controls fail and how to measurably improve them in real time.

Powered by OnDefend BlindSPOT, our program strengthens detection and response through collaborative, intelligence-driven attack simulations that unite red team operators and blue team defenders.

Testing Capabilities

Attack Simulations
Run simulated attacks against live security controls using BlindSPOT and manual red team techniques.

Hands-on Keyboard Activities
Execute manual attacker techniques from assumed breach to evaluate detection across key adversary behaviors.

Results Correlation
Identify which controls worked, where detection failed, and how response processes performed in practice.

Detection Engineering
Design MITRE ATT&CK-mapped detections, tune alert thresholds, and aligns with response playbooks.

Continuous Validation via BlindSPOT
Automate attack simulation for ongoing detection and response validation as environments evolve.

Defensive Maturity Assessment
Evaluate whether security tooling and response processes are operationally effective - not just deployed.

Outcomes

- Detection and response gaps identified across tooling, monitoring, and response workflows
- Root cause analysis of control failures with actionable tuning and engineering recommendations
- Measurable improvement in detection coverage, alert fidelity, and response speed
- Continuous validation via BlindSPOT as environments, threats, and controls evolve

Purple teaming transforms attack simulations into defensive improvements and enables teams to detect faster, respond better, and prove controls work against real adversaries.

OnDefend.com