Simulate the Adversary. Strengthen the Defender.

Red Team Operations

RKON's Red Team Operations mimics real-world attackers to measure your organization's true ability to detect, respond, and recover. Our controlled, intelligence-informed red teaming exercises expose critical gaps in people, processes, and technology, enabling you to build a stronger, more resilient security posture.

Our Approach

- Human-led red team operators with deep adversary simulation expertise
- Aligned with MITRE ATT&CK, NIST, and industry best practices
- Scenario-driven engagements mapped to your business priorities
- Knowledge transfer to defenders for lasting improvement

Benefits

- Test true readiness, not just controls
- Identify critical detection gaps
- Strengthen processes and defensive playbooks
- Increase resilience against advanced persistent threats
- Align security investments to the highest risk

Why RKON

- **75% fewer** critical exposures identified post-engagement
- RKON operates with speed and adaptability, aligning operations to business drivers like M&A
- Executive and technical reporting
- Controlled, rules-of-engagement-based execution
- Debriefing with detection gaps, incident response scoring, and recommendations

What We Deliver

Adversary Emulation

- Simulate realistic attack chains targeting your environment
- Test detection, response, and containment capabilities

Full Kill Chain Simulation

- Execution from social engineering to initial access, lateral movement, privilege escalation, and data exfiltration
- Realistic end-to-end campaigns

Covert Operations

- Test your security team's ability to detect and respond to real attacker movements
- Identify dwell time and detection gaps
- Measure incident response maturity

Purple Team Collaboration (Optional)

- Partner with your defenders during or after exercises
- Share findings to enhance detections and response
- Validate SIEM/EDR rules and playbooks