Red Team & Adversary Simulation

Test Your Defenses Against Real-World Threats

AI-powered threat emulation with expert human operators

Powered by MITRE ATT&CK Framework

Pentesting Found Vulnerabilities. Now What?

Mature security programs need to test detection and response, not just find holes

197 days

Average time attackers remain undetected in compromised networks

80%

of organizations that passed pentests still got breached within a year

$4.88M

Average cost of a data breach in 2024

68%

of breaches involved the human element

Penetration Testing vs Red Teaming

Penetration Testing

- > Finds vulnerabilities in systems
- > Defined scope and targets
- > Technical focus
- > Blue team is aware
- > Answer: "What can be exploited?"
- > Compliance-driven

Red Teaming

- > Tests detection & response capabilities
- > Objective-based (e.g., exfil data)
- > People, process, and technology
- > Blue team unaware (realistic)
- > Answer: "Can attackers achieve goals?"
- > Maturity-driven

Red teaming answers: "If a real attacker targeted us, would we detect and stop them?"

AI + Human Expertise

We combine AI-powered threat emulation with expert human operators

Threat Intelligence

Emulate real APT groups targeting your industry using current TTPs

MITRE ATT&CK Mapping

Every technique mapped to the framework for clear coverage reporting

AI Agents

Automated simulation of adversary behaviors at scale

Human Operators

Expert guidance for complex decisions and novel attacks

Multi-Platform

Windows, Linux, macOS, and BSD environments supported

Safe Execution

Controlled operations with rollback capabilities

Service Options

Adversary Simulation

$699

per month

- Monthly threat actor simulations
- MITRE ATT&CK based TTPs
- Windows, Linux, macOS, BSD
- One human operator
- Detailed simulation reports
- 2 months remediation support

Human-Led Simulation

$9,999

per engagement

- One-time targeted simulation
- Specific threat actor emulation
- Two human operators
- Any platform compatibility
- Comprehensive reporting
- 4 months remediation support

Custom Red Team

Custom

engagement

- Bespoke operations
- Objective-based scenarios
- 3+ human operators
- Physical + digital if needed
- Executive briefings
- 6 months remediation support

Deliverables & Outcomes

Attack Narrative

Full timeline of actions, techniques used, and how far the attack progressed

Detection Gap Analysis

What your SOC/EDR missed and specific recommendations to close gaps

MITRE ATT&CK Coverage

Visual heat map of techniques tested and detection rates

Executive Summary

Board-ready report with risk ratings and business impact

Remediation Roadmap

Prioritized action plan to improve detection and response

Ongoing Support

2-6 months of remediation guidance via email/Slack

Is Red Teaming Right for You?

You're Ready If...

- You have a mature pentesting program
- You've invested in EDR/XDR/SIEM
- You have a SOC (internal or MSSP)
- Compliance requires it (some do)
- Board/execs want assurance defenses work
- You've had a breach and rebuilt

Start with Pentesting If...

- You haven't done a pentest recently
- You have known unpatched vulnerabilities
- No detection tools in place yet
- No incident response plan/team
- Still building basic security controls

Not sure? We'll assess your maturity and recommend the right service.

Ready to Test Your Detection Capabilities?

- > Discuss your security maturity and objectives
- > Get a custom threat scenario proposal
- > See sample attack narratives and reports

SCHEDULE A CONSULTATION

integsec.com/redteaming