

**IntegSec Red Teaming** goes beyond vulnerability discovery to test your organization's ability to detect, respond to, and contain real-world attacks. Using AI-powered threat emulation combined with expert human operators, we simulate adversary behaviors from the MITRE ATT&CK framework to identify gaps in your detection and response capabilities.

## WHAT WE TEST

- > Detection capabilities (EDR, XDR, SIEM)
- > SOC alerting and triage effectiveness
- > Incident response procedures
- > Lateral movement detection
- > Data exfiltration controls
- > Privilege escalation monitoring
- > Persistence mechanism detection
- > Human response under pressure

## DELIVERABLES

- > Complete attack narrative with timeline
- > Detection gap analysis report
- > MITRE ATT&CK coverage heat map
- > Executive summary for leadership/board
- > Prioritized remediation roadmap
- > SOC improvement recommendations
- > Post-engagement support (2-6 months)
- > Optional purple team debrief

## Service Options

### Adversary Simulation

**\$699/mo**

Subscription

- > Monthly threat actor simulations
- > MITRE ATT&CK based TTPs
- > All major platforms supported
- > One human operator
- > Detailed simulation reports
- > 2 months remediation support

### Human-Led Simulation

**\$9,999**

Per Engagement

- > Targeted threat actor emulation
- > Custom scenario development
- > Two human operators
- > Any platform compatibility
- > Comprehensive reporting
- > 4 months remediation support

### Custom Red Team

**Custom**

Engagement

- > Bespoke objective-based operations
- > Physical + digital if needed
- > 3+ human operators
- > Executive briefings included
- > Purple team option
- > 6 months remediation support

# Our Approach

## Threat Intelligence

Emulate APT groups that target your industry with current TTPs

## MITRE ATT&CK

Every technique mapped for clear coverage and gap reporting

## AI + Human

AI agents for scale, human experts for complex decisions

## Safe Execution

Controlled operations with rollback and safety rails

## Multi-Platform

Windows, Linux, macOS, BSD environments supported

## Realistic Scenarios

Blue team unaware for authentic response testing

# Best For Organizations With

Mature Pentest Programs

EDR/XDR Deployed

SOC or MSSP

Incident Response Plans

Board Reporting Needs

# Ready to Test Your Defenses?

Discuss your security maturity and get a custom threat scenario proposal.

[INTEGSEC.COM/REDTEAMING](https://integsec.com/redteaming)