INTEGSEC

Red Teaming Sales Cheat Sheet

Internal Quick Reference Guide

30-Second Elevator Pitch

"Most companies test their security with traditional pentests - but real attackers don't follow a checklist. **IntegSec's Red Team** uses the same tactics as nation-state hackers to find the vulnerabilities that matter most. We combine **AI-powered reconnaissance** with **certified experts** to simulate real-world attacks across your entire organization - not just your network. Whether you need **ongoing threat simulation for $699/month** or a **comprehensive engagement starting at $9,999**, we help you find and fix critical weaknesses before attackers do. **What's your biggest concern about your current security posture?**"

Common Objections & Responses

"We already do penetration testing."

Pentests check boxes - red teams find real risk. **Pentests focus on known vulnerabilities**, while red teams simulate how actual attackers would chain together weaknesses across people, process, and technology. **70% of breaches involve techniques pentests don't cover.**

"It's too expensive."

A single breach costs **$4.45M on average**. Our subscription starts at **$699/month** - less than one day of breach response. Plus, red team findings often reveal issues that would otherwise require expensive incident response later.

"We're not a target / too small."

43% of breaches target SMBs - attackers see them as easy targets. If you have customer data, financial info, or intellectual property, you're already a target. Our flexible pricing makes enterprise security accessible.

"Our security team can handle it."

Even great teams have blind spots. **External red teams bring fresh perspectives** and adversary tradecraft your team may not see daily. We actually **help train your team** through realistic scenarios.

"What if you cause damage?"

We use **non-destructive techniques** with careful scope control. Every engagement has clear rules of engagement, and our team has **zero incidents** across hundreds of engagements. We carry full liability insurance.

Qualification Questions

- ? When was your last security assessment? What did it cover?
- ? Have you ever tested how your team responds to a real attack?
- ? Do you have compliance requirements (SOC 2, PCI, HIPAA)?
- ? What's your biggest security concern right now?
- ? How do you currently measure security effectiveness?
- ? Has your organization experienced a breach or close call?
- ? Do you have a security operations team or MSSP?
- ? What would a breach cost your business in terms of reputation?
- ? Are you looking to satisfy board/executive security requirements?
- ? What's your timeline for improving security posture?

Pricing Quick Reference

Subscription	Per Engagement	Enterprise
$699/mo	**$9,999+**	**Custom**
Ongoing threat simulation, quarterly assessments	Full red team exercise, comprehensive report	Multi-site, ongoing, advanced scenarios

Key Differentiators

AI	ATT	$
AI + Human	**MITRE ATT&CK**	**Flexible Pricing**
AI recon with expert exploitation	Framework-aligned TTPs	$699/mo to custom enterprise

Ideal Customer Profile

Finance	Healthcare	Legal	Manufacturing
High-value targets	PHI protection	Client confidentiality	IP protection

Competitive Comparison

Capability	IntegSec	Big 4 Consultants	Traditional Pentest Firms	Automated Tools Only
AI-Enhanced Reconnaissance	**Yes**	Limited	No	**Yes**
Certified Operators	**Yes**	**Yes**	Varies	No
Social Engineering Included	**Yes**	Extra Cost	Extra Cost	No
Physical Security Testing	**Yes**	Extra Cost	No	No
Subscription Option	**$699/mo**	No	No	**Yes**
Executive Reporting	**Yes**	**Yes**	Basic	No

Key Talking Points

For Executives

"We help you understand real business risk, not just technical vulnerabilities. Our reports translate security findings into business impact."

For IT Leaders

"We test your defenses the way real attackers would - giving you actionable intelligence to improve your security program."

For Compliance

"Our MITRE ATT&CK-aligned assessments satisfy requirements for SOC 2, PCI DSS, HIPAA, and cyber insurance policies."

For Security Teams

"We partner with your team - every engagement includes knowledge transfer so you can improve detection and response."

Disqualification Signals

- ! No budget authority or security budget under $10K/year
- ! Looking for automated scanning only (point to Vuln Assessment)
- ! Needs immediate compliance checkbox (point to PTaaS)
- ! No executive buy-in for realistic attack simulation
- ! Expecting guarantees of "unhackability"
- ! Unwilling to sign rules of engagement