RED TEAMING: QUESTIONS TO ASK VENDORS

CHOOSE WITH INTENT. **TEST WITH CONFIDENCE. DECIDE WITH CLARITY.**
Before selecting a red team vendor, use this worksheet to evaluate how potential partners think about objectives, realism, and decision-making.

VENDOR EVALUATION MATRIX

HOW TO USE: Complete the evaluation questions (starting on the next page) for each vendor. Then use the Vendor Evaluation Matrix to calculate and compare vendor scores using the Confidence Scoring legend. Add points for each vendor and dimension, then add total. Total points of 20+ indicate strong vendor selections.

Evaluation Dimensions	Vendor #1	Vendor #2	Vendor #3	Vendor #4
Objectives & Intent Alignment				
Scenario Design Approach				
Threat Modeling & Adversary Relevance				
Evidence & Decision Support				
People & Process Consideration				
Modern Environment Coverage				
Reporting & Deliverables				
Engagement Style & Partnership				
TOTAL				

CONFIDENCE SCORING LEGEND

- (3 pts) High confidence: Clear understanding and credible capability supported by specific examples.
- (2 pts) Moderate confidence: General alignment, but depth, clarity, or evidence is limited or uneven.
- (1 pt) Low confidence: Vague, generic, or leaves significant questions unanswered.

1 OBJECTIVES & INTENT ALIGNMENT

EVALUATION PROMPT
Does this vendor help us sharpen intent or do they assume the same engagement works for everyone?

- How does the vendor help us define what “success” looks like for red teaming?
- What questions do they ask to understand our business risk and security priorities?
- How do they distinguish between testing for exposure, detection, and decision-making?
- How do they align testing outcomes to executive or board-level concerns?

2 SCENARIO DESIGN APPROACH

EVALUATION PROMPT
Can the vendor explain what they would test and why, without defaulting to a generic scope?

- How does the vendor describe their approach to building attack scenarios?
- Do scenarios start from attacker goals or from systems and controls?
- How do they tailor scenarios to our environment and maturity level?
- How do they adapt if initial attack paths fail or assumptions change?

3 THREAT MODELING & ADVERSARY RELEVANCE

EVALUATION PROMPT
Does the vendor demonstrate threat fluency or rely on broad, familiar narratives?

- How does the vendor determine which threat actors are most relevant to us?
- What informs their choice of tactics, techniques, and tooling?
- How do they account for identity, cloud, and SaaS-driven attack paths?
- How do they evolve adversary models as threats change?

4 EVIDENCE & DECISION SUPPORT

EVALUATION PROMPT
Would this vendor's output help us explain why decisions were made, not just what was found?

- How does the vendor describe the type of evidence they deliver?
- How do they explain control failure and attack progression to leadership?
- How do they translate technical activity into business impact?
- How would their output support prioritization or investment decisions?

5 PEOPLE & PROCESS CONSIDERATION

EVALUATION PROMPT
Does the vendor treat people and process as first-class parts of security or afterthoughts?

- How does the vendor account for detection and response during testing?
- How are SOC, IR, or MSSP workflows considered?
- How do they evaluate effectiveness without undermining defenders?
- How are people and process gaps framed in results?

6 MODERN ENVIRONMENT COVERAGE

EVALUATION PROMPT
Does the vendor focus where attackers are going or where testing is easiest?

- How does the vendor approach cloud-native and hybrid environments?
- How are SaaS platforms, third parties, and trust relationships handled?
- How do they test identity, automation, and workflow abuse?
- Where do they look for risk between systems, not just within them?

7 REPORTING & DELIVERABLES

EVALUATION PROMPT
Would these deliverables support planning or just prove testing occurred?

- How does the vendor structure final deliverables?
- Are results scenario-driven or finding-driven?
- How do they separate tactical issues from strategic themes?
- How are findings tied to risk rather than vulnerability counts?

8 ENGAGEMENT STYLE & PARTNERSHIP MODEL

EVALUATION PROMPT
Does this feel like a partnership built for improvement or a one-time transaction?

- How does the vendor describe collaboration during scoping and testing?
- How do they handle ambiguity or changing constraints?
- How do they tailor engagements to different maturity levels?
- What does long-term value look like beyond a single engagement?

READY TO TEST YOUR DEFENSES?

ABOUT BISHOP FOX

Bishop Fox is the leading authority in offensive security, providing solutions ranging from continuous penetration testing, red teaming, and attack surface management to product, cloud, and application security assessments.

LEARN MORE AT BISHOPFOX.COM