RED TEAMING: KEY QUESTIONS FOR PLANNING SUCCESS

PLAN SMARTER. **TEST BETTER. STAY AHEAD.**

Before launching a Red Team engagement, use this form to clarify your objectives, define scope, and align stakeholders. The more intentional your planning, the more valuable the insights you'll gain.

1 DEFINING OBJECTIVES: WHAT ARE WE TRYING TO ACCOMPLISH?

Red teaming isn't just about finding vulnerabilities—it's about testing your defenses against meaningful threats. The clearer your goals, the more strategic the outcome.

What are our desired outcomes from this Red Team engagement?

WHY THIS MATTERS	**TIPS FOR SUCCESS**
Every successful Red Team starts with a concrete objective—from testing detection capabilities to simulating a specific threat actor.	Be specific. Identify measurable or observable outcomes (e.g. "Test if a Red Team can access customers' payment data," not just "Find weaknesses.")

What trophies (objectives) should the Red Team target? What are your 'crown jewels' (high-value assets)?

WHY THIS MATTERS	**TIPS FOR SUCCESS**
Clarifying which systems, data, or access points represent the biggest wins for attackers helps you align test efforts with real-world threats.	Involve both business and security stakeholders to identify what attackers would value most, such as sensitive data, intellectual property, or control of business-critical systems. The 5/5/20/X planning framework is useful here.

What known threats or adversaries are we most concerned about?

WHY THIS MATTERS

Tailoring the engagement to mimic a real threat to your specific business, industry, or region helps shape meaningful test scenarios with actionable outcomes.

TIPS FOR SUCCESS

Leverage your threat intel or incident history to inform realistic adversary profiles. Don't guess—use data.

What scenarios or tactics should be tested? (e.g. ransomware, insider threats, backdoors in code)

WHY THIS MATTERS

Choosing the right tactics ensures the test reflects likely attack paths and pressures the controls that matter most.

TIPS FOR SUCCESS

Avoid overly broad scenarios. Prioritize tactics relevant to your environment and adversary profiles; be realistic about what can be tested safely.

2 SCOPING THE ENGAGEMENT: WHAT'S IN, WHAT'S OUT?

Scope defines the boundaries of your Red Team—where it starts, what's fair game, and how deep it will go.

What is the time frame for the engagement?

WHY THIS MATTERS

When you schedule the Red Team can make a big difference. It affects how prepared your team is, who is available to support the engagement, and how quickly you can act on what you learn. Planning ahead helps everything run more smoothly.

TIPS FOR SUCCESS

Try to avoid Q4 – it's the busiest time for Red Teaming vendors; Q1 or Q2 often offer better availability and give you more breathing room to address issues.

Should the Security Operations Center (SOC) be aware of the test? If so, should they have zero, partial, or full knowledge?

WHY THIS MATTERS

This decision shapes the entire exercise. If the SOC doesn't know a test is happening, you're evaluating how well they detect and respond in real time. If they do know, the focus shifts to how well teams coordinate under pressure.

TIPS FOR SUCCESS

Want to test detection and response? Go for zero or partial knowledge. Want to focus on cross-team coordination? Full knowledge might make more sense. There's no wrong choice—just make it intentional.

Are we simulating an external attack or an assumed breach?

WHY THIS MATTERS

Assumed breach scenarios can test lateral movement and internal detection—a different challenge than perimeter defense.

TIPS FOR SUCCESS

Choose based on your security priorities. External attacks test prevention; assumed breaches focus on detection and containment.

What parts of our attack surface should be included? (e.g. cloud infrastructure, physical premises, social engineering targets)

WHY THIS MATTERS

Your attack surface could include a wide range of entry points beyond IT systems – from cloud environments to physical locations to employees themselves. Being deliberate about what you include ensures the test is focused, realistic, and aligned with your goals.

TIPS FOR SUCCESS

Think beyond firewalls. If phishing, tailgating, or cloud misconfigurations are concerns, include them. Tailor the scope to your real-world risks – not just what's easiest to test.

Are any systems or attack types off-limits?

WHY THIS MATTERS

It's common (and reasonable) to exclude production systems or critical business operations. Just make sure the limits are clear.

TIPS FOR SUCCESS

Define these exclusions up front and make sure the Red Team understands them to avoid business disruption.

3

ALIGNING STAKEHOLDERS: WHO NEEDS TO KNOW?

A Trusted Insider Group (TIG) will ensure the test stays controlled, confidential, and connected to the right people.

Who needs to be informed about the Red Team exercise?

WHY THIS MATTERS	TIPS FOR SUCCESS
Not everyone should know – but a few key leaders or points of contact in relevant business units must be looped in to coordinate response and mitigate risk.	Limit knowledge to those with a need-to-know role in managing the test. Over-sharing reduces realism.

Have we briefed all necessary stakeholders?

WHY THIS MATTERS	TIPS FOR SUCCESS
Clarity before kickoff prevents confusion mid-operation, especially for SOC leaders or department heads.	Use a briefing template to align everyone on goals, scope, and their responsibilities before the engagement begins.

Have we clearly communicated the need for confidentiality?

WHY THIS MATTERS	TIPS FOR SUCCESS
Leaking test details can compromise the realism and integrity of the exercise.	Emphasize confidentiality in stakeholder briefings and written documentation. Include it in your kickoff checklist.

4

SETTING THE RULES: HOW WILL THE ENGAGEMENT WORK?

Rules of engagement keep the test realistic and safe – and make sure everyone knows how to handle surprises.

What risks should we mitigate in advance?

WHY THIS MATTERS	TIPS FOR SUCCESS
Think legal clearance, business continuity, and production system impact. Planning prevents panic.	Work with legal, compliance, and operations teams ahead of time to identify and document risks and mitigation plans.

What are the hours for testing?

WHY THIS MATTERS	TIPS FOR SUCCESS
Define whether testing will occur during business hours, off-hours, or 24/7; this affects realism and detection.	Ensure SOC and key responders are aligned on expected testing hours and how to escalate if needed.

How will initial access be attempted?

WHY THIS MATTERS	TIPS FOR SUCCESS
Phishing, credential stuffing, tailgating – each tactic tests different controls.	Select methods that match your top threat concerns and are safe to execute in your environment.

How and how often will the team communicate?

WHY THIS MATTERS	TIPS FOR SUCCESS
Regular check-ins help avoid confusion, manage risk, and adjust scope if needed. Knowing which channel to use (e.g. Slack or Teams) helps prevent missed messages.	Define primary and backup communication channels. Set expectations for check-in cadence before the test begins.

What's the deconfliction process if the Red Team is detected?

WHY THIS MATTERS

You need a safe, agreed-upon process to handle real-time detection or escalation, especially in zero-knowledge tests.

TIPS FOR SUCCESS

Have a predefined deconfliction protocol to prevent disruptions and avoid confusion with real incidents.

Are legal authorization letters in place for physical testing?

WHY THIS MATTERS

Don't get your testers arrested. Legal documentation is essential for physical intrusions.

TIPS FOR SUCCESS

Prepare letters in advance – ink signed by appropriate executives – and ensure the Red Team has them onsite during physical tests.

READY TO PUT YOUR DEFENSES TO THE TEST?

Contact Bishop Fox today
to start planning your **Red Team engagement**.

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.**

LEARN MORE AT BISHOPFOX.COM