



# PROACTIVE PROTECTORS



# RED TEAM RISING


The Subtle Art of  
Successful Red Teaming



# Table of Contents

---

- 1 The True Value of Red Teaming**
- 2 The Art of Crafting a Red Team Scenario**
- 3 Compliance-Based Testing vs. Scenario-Based Testing vs. Red Teaming**
- 4 7 Steps to Prepare for a Red Team Engagement**
- 5 Checklist: Getting Ready for Red Teaming**



**Conducting a red team exercise offers significant benefits to enhance your company's security resilience.**


# The True Value of Red Teaming

At its core, red teaming is a controlled, intelligence-led simulation designed to emulate the tactics, techniques, and procedures (TTPs) of real-world adversaries. Conducting a red team exercise offers significant benefits to enhance your company's security resilience, but only if it's planned and executed with tenacity.

For companies with less mature security fundamentals, such as fluctuating asset visibility or underdeveloped detection and response capabilities, a red team exercise may be too advanced. Think of it like putting a new boxer in the ring with a world champion; the fight is mismatched, resulting in few practical lessons and no clear path toward improvement. The key is to calibrate the challenge to the current state of your security. To derive real value, you must have functional security protocols and a team capable of responding to a real-world event.

The true value of red teaming lies not in a simple pass/fail report, but in its ability to validate assumptions about your security program in a real-world context. It goes beyond traditional audits or compliance checks, which often verify the presence of a control but not its effectiveness under duress. A well-executed engagement can prove the effectiveness of your security investments and provide your team with invaluable practice for a genuine breach. We created this guide to equip you with essential mindset and planning strategies to gain the most value from red teaming by using the results to drive long-term digital resilience for your business.





To conduct red teaming successfully is to embrace it as an art form rooted in realism and collaboration.

# The Art of Crafting a Red Team Scenario

A red team scenario is structured to prove or disprove the assumptions your organization holds about its security posture. To conduct red teaming successfully is to embrace it as an art form rooted in realism and collaboration.

It answers the critical business question: **“How resilient are our people, processes, and technology when faced with a dedicated, skilled attacker?”**

This type of testing is not about “stunt hacking” or achieving a technical feat for its own sake.

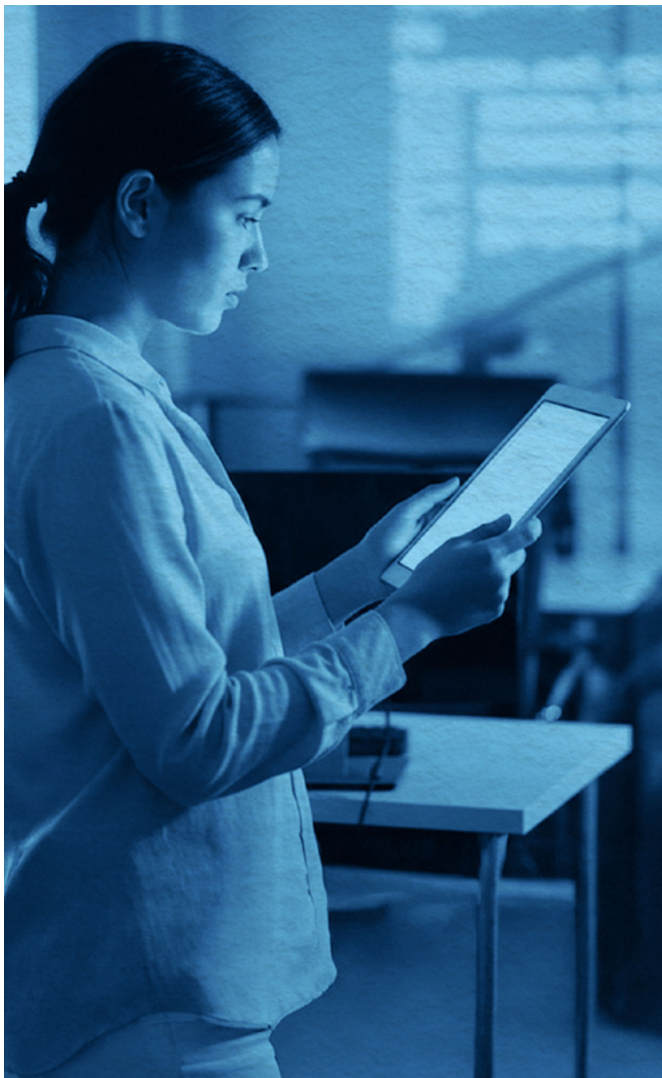
Instead, a valuable red team engagement aligns its scenarios with the threat actors most likely to target your industry. The goal is to create a scenario that mirrors an actual risk, allowing you to practice your response in a safe environment before a real breach occurs. This proactive approach enables you to identify and fix issues before they can be exploited, ultimately driving digital resilience and justifying security investments.

## Moving Beyond Initial Access to Test True Resilience

A common misconception is that a red team's success is defined by whether it can breach the perimeter. In reality, this view is short-sighted. Real-world threats are persistent and have more time and resources than any scoped engagement. An over-emphasis on initial access creates a false sense of security. Placing all your resources and controls at the perimeter means that if one thing slips through, everything inside is fair game. You need defense in depth. This means visibility, detection, and containment capabilities inside your organization, too.

Effective red teaming evaluates the full attack chain. We want to know: can you find all the touch points? Can you contain the threat? Can you fully eradicate it, with certainty and efficiency?

This includes assessing the advanced techniques of lateral movement and organizational mobility. Phishing to gain access is common, but phishing again internally to move laterally is something we don't see often enough in testing, even though it happens in real attacks. It's a great way to test trust boundaries within the organization. Person-to-person movement and exploiting relationships are very effective. Once inside, all the fancy perimeter filtering is irrelevant.



### Assumed Breach: Doing It Realistically, Not Lazily

Sometimes, the most valuable insights come from an "assumed breach" model, where the test begins from a point of compromise. How we set that up matters. Historically, people just created a test account, gave it access to a clean machine, and said, "Go," but that's not good enough. That's what farmers would call "fallow earth." A new user account with no activity history, no realistic group memberships, and none of the messiness of a real corporate identity falls short of proving much.

Security products relying on abnormality and heuristic analysis treat such accounts differently from real users, pulling us further away from reality. In contrast, a real compromised user has baggage—aged accounts, old permissions, logon patterns—all of which matter when testing whether a threat actor would be caught or not, as well as the impact of their compromise.



## A Collaborative Path to Growth

The most productive red team engagements move beyond an adversarial “us versus them” mentality. The ultimate objective is mutual learning. As we say a lot to clients, red teaming is like a counseling session. We all go in with our strengths and weaknesses on display, because that’s the only pathway to acceptance and growth that works.

The red team should not be a fire meant to burn down your defenses, but a fire that motivates urgency and improvement. This requires a collaborative partnership where both sides can be transparent. We must be able to discuss failures and near-misses honestly.

The post-engagement review should be brutally honest, not just, “Here’s what we got,” but “Here’s what we tried, here’s what almost worked, here’s what failed.” Sometimes a control works not by design, but by luck, and understanding that distinction is critical for building true resilience.

This approach also demands strict ethical boundaries and a focus on operational safety. Everything we do as red teamers must be seen through an ethical lens. Just because we can exploit something doesn’t mean we should. Maybe we find a critical Remote Code Execution (RCE) in building management software. Do we exploit it? What if that software controls the HVAC system for a high-heat facility? We could create a safety risk. We need to simulate real threats, but we cannot become the threat ourselves.

By balancing realism with operational safety and stealth with learning outcomes, red teaming becomes a powerful tool. It tests not just whether you spot an attack, but whether your team has the processes in place to hunt for threats, contain them, and eradicate them with confidence.



# Compliance-Based Testing vs. Scenario-Based Testing vs. Red Teaming

As you shift from how red teaming should be practiced to which testing method is most beneficial for your business today, carry this mindset forward: the right test for your security maturity will give you the most valuable results.

Choosing the right testing approach depends on your security stance, objectives, and regulatory obligations. Use this side-by-side comparison to determine whether compliance-based testing, scenario-based testing, or red teaming best aligns with your goals.

Criteria	Compliance-Based Testing	Scenario-Based Testing	Red Teaming
<b>Primary Purpose</b>	Satisfy regulatory requirements; verify presence of controls.	Validate specific “what if” threats and defensive functions.	Assess true resilience by emulating real-world adversaries.
<b>Core Question</b>	“Do we meet the mandated testing criteria?”	“Can we detect and respond to this specific attack?”	“How do our people, process, and tech perform under attack?”
<b>Scope and Depth</b>	Broad, checklist-driven, and defined by the framework.	Focused scope with depth on chosen systems or processes.	Narrow but deep; follows an objective-driven attack narrative.
<b>Output</b>	Findings list, control validation, and evidence pack for auditors.	Scenario report with gaps, detections, and targeted improvements.	Attack narrative, response quality, and strategic security gaps.
<b>Intelligence &amp; Realism</b>	Aligned to framework; not always tailored to current threats.	Threat-informed within a chosen scope; uses practical methods.	Industry-relevant TTPs; realism is prioritized.
<b>Readiness Prerequisite</b>	Baseline security program; established governance and policies.	Solid fundamentals; some detection and response maturity.	Mature security operations, asset visibility, and IR capability.
<b>When to Perform</b>	Required by regulators.	Building toward red teaming or validating a critical risk path.	Seeking strategic assurance and validation of program investments.
<b>Time and Planning</b>	Structured timelines with heavy coordination and documentation.	Moderate planning; typically requires 4–8 weeks.	Significant planning; allow 1–3 months for scoping and intel.
<b>Social/Physical Engineering</b>	Included only if prescribed by the framework and scope.	Included when threat-justified for the specific scenario.	Included when intelligence supports it as a realistic vector.
<b>Decision Support</b>	Governance and audit assurance.	Operational decisions for specific capability gaps.	Executive strategy and investment decisions.
<b>Measurement Focus</b>	Control effectiveness against a static compliance mandate.	Scenario-specific detection time and response quality.	MTTD, MTTR, detection gaps, and containment effectiveness.
<b>Vendor Due Diligence</b>	High; regulatory alignment and evidence handling are critical.	Medium; focuses on data handling and scoping controls.	High; vendor holds sensitive data; GDPR/DORA alignment required.
<b>Typical Next Step</b>	Remediate control gaps; maintain certification posture.	Tune detections, refine processes, and re-test targeted paths.	Blameless post-mortems and a multi-year maturity roadmap.

No single testing method fits every situation. Start with the option that matches your current readiness, risk priorities, and regulation requirements, then evolve your program over time. This can start with validating controls with compliance-based testing, then moving into pressure-testing specific pathways through scenario-based exercises. Then ultimately, using red teaming to assess real-world resilience end-to-end.



# 7 Steps to Prepare for a Red Team Engagement

---

A successful red team engagement depends on rigorous preparation rooted in technical maturity, collaborative planning, and business priorities. Use the following steps to ensure your organization is ready to maximize the value of the exercise and avoid common pitfalls.

## 1 Assess Foundational Readiness

**Goal: Verify that your organization has strong foundational security capabilities in place.**

- Confirm up-to-date asset visibility, functional security controls, and a defined incident response process.
- Ensure past penetration test findings have been addressed and security hygiene is maintained.
- If you lack these elements, consider scenario-based testing as an interim step before proceeding with a full red team exercise.

## 2 Secure Executive Sponsorship and Stakeholder Alignment

**Goal: Obtain executive buy-in at the earliest stage.**

- Red teaming is not just a security test; it requires attention and support from senior leadership and cooperation across departments.
- Identify a “control group” of key stakeholders who are informed of the engagement, but maintain strict confidentiality to preserve the test’s integrity.

## 3 Define Objectives and Rules of Engagement

**Goal: Set objectives that extend beyond generic technical goals.**

- Tie objectives to specific business risks and desired outcomes (e.g., protecting customer data, responding to ransomware).
- Use industry-relevant threat intelligence to ground objectives in realistic risk scenarios.

**Goal: Develop clear Rules of Engagement, covering:**

- Systems/areas in and out of scope.
- Permitted techniques and escalation protocols for critical findings.
- Test timeline and operational boundaries.
- Data handling and vendor security expectations.
- Perform due diligence to ensure red team vendors comply with regulations such as GDPR, DORA, CBEST, or TIBER.



## 4 Invest in Intelligence-Driven Scenario Design

**Goal: Allocate sufficient time for planning—typically at least three months from initial scoping to launch.**

- Use multiple sources of threat intelligence to inform scenario design and stakeholder input.
- Rushing this stage increases the risk of poorly tailored, low-value test results.
- Note that timelines can vary by engagement type (e.g., a compliance-driven test like CBEST may need a more extensive planning phase than an internal assumed breach scenario).

## 5 Select the Scenario and Calibrate Difficulty

**Goal: Collaborate with your vendor to choose the right type and complexity of scenario for your maturity.**

- Balance sophisticated techniques with common methods that remain effective in real attacks.
- Aim for a scenario that challenges but does not overwhelm your defensive capabilities.

**Goal: If using an assumed breach model, ensure realistic execution.**

- Use aged user accounts with genuine activity history rather than new accounts (“fallow earth”) for credible results.

## 6 Establish Communication and Safety Protocols

**Goal: Set up secure communication channels between your control group and the red team vendor.**

- Define a regular cadence for updates, ensuring stakeholders are informed without tipping off defensive teams.

**Goal: Develop robust safety protocols to mitigate risks of business disruption.**

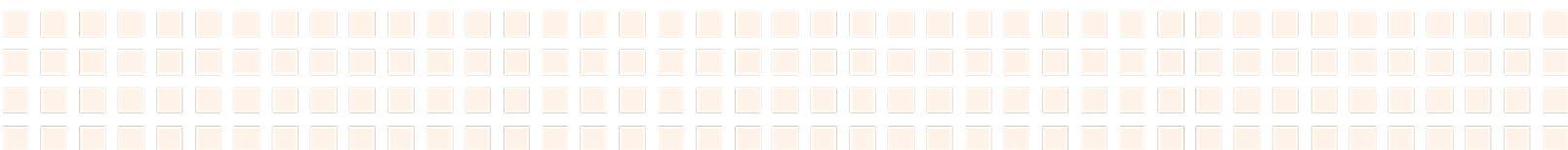
- Carefully define what actions are permitted, especially around operational technology or critical infrastructure.
- Remember: just because a vulnerability can be exploited doesn’t mean it should be. The red team’s role is to simulate threats, not create new risks for the business.

## 7 Plan Post-Engagement Workshops and Continuous Improvement

**Goal: Schedule dedicated time for joint debrief sessions with red and blue teams.**

- Include detection and response workshops, and where possible, purple team exercises to translate findings into tangible improvements.
- Build a feedback loop to update internal threat models, tune detection workflows, and prioritize remediation actions.

By following these steps, your team can plan a red team engagement that is safe, aligns with strategic business goals, and delivers actionable outcomes that strengthen security maturity year over year.



# Checklist: Getting Ready for Red Teaming

---

This checklist distills the essentials of well-planned red team scenarios into clear, actionable steps. Use it to confirm readiness, plan intelligently, and execute safely, so your engagement delivers meaningful, business-aligned outcomes, not just a report.

## Strategy and Mindset

- ✓ Treat red teaming as business enablement, not pass/fail.
- ✓ Calibrate readiness before starting; consider scenario-based testing first if needed.
- ✓ Commit to realism such as industry-relevant TTPs and avoid “stunt hacking.”
- ✓ Embrace collaboration and blameless reviews post-engagement

## Readiness and Planning

- ✓ Confirm asset visibility, SOC maturity, and incident response (IR) capability.
- ✓ Define business-aligned objectives tied to real risks.
- ✓ Establish Rules of Engagement (scope, escalation, data handling, safety).
- ✓ Complete vendor due diligence (GDPR/DORA/CBEST/TIBER; supply chain security).
- ✓ Allocate 1–3 months for scoping, intel, and design.

## Scenario Design and Execution

- ✓ Balance advanced and common techniques; prioritize practicality.
- ✓ Set realistic assumed breach conditions (aged accounts, real activity history).
- ✓ Include internal trust testing and lateral movement where relevant.
- ✓ Maintain a secure communications channel with a control group.
- ✓ Enforce ethics and operational safety; simulate threats without causing harm.



## Measurement and Outcomes

- ✓ Measure beyond initial access: detection quality, response, containment, eradication.
- ✓ Track metrics: MTTD, MTTR, detection gaps, containment completeness, eradication certainty, stakeholder confidence.
- ✓ Document a clear attack narrative and decision points, not just findings.

## Post-Engagement Improvement

- ✓ Run joint red/blue debriefs and blameless post-mortems.
- ✓ Host detection/response and purple team workshops to translate advice into fixes.
- ✓ Involve platform/vendors to tighten rules and configurations live.
- ✓ Prioritize remediation based on business risk and validate fixes.

## 90-Day Action Plan

- ✓ Days 1–30: Analyze, triage, and brief executives; set priorities.
- ✓ Days 31–60: Remediate top issues; run detection/response workshops; update threat models.
- ✓ Days 61–90: Validate fixes (or purple team), finalize business case, and draft multi-year testing roadmap.

## Long-Term Maturation

- ✓ Establish a multi-year cadence (3–5 years) with iterative difficulty calibration.
- ✓ Re-test known weaknesses and expand to new risk areas.
- ✓ Maintain supplier/data security accountability throughout.
- ✓ Regularly report progress and ROI to leadership.

Red teaming creates value when it's realistic, well-governed, and followed by action. Review this checklist before, during, and after your engagement to keep stakeholders aligned, track measurable improvements, and sustain momentum on your multi-year security roadmap.

# PROACTIVE PROTECTORS



## Final Thoughts

Red teaming can become a powerful business enablement tool, but only when approached as a strategic initiative rather than a simple technical audit. By following a modern, intelligence-led approach to red teaming, businesses can validate security investments, drive organizational resilience, and empower strategic decisions. The ultimate goal is not to achieve a pass/fail grade, but to build a more defensible enterprise by safely practicing for a real-world breach. This process enhances the alignment between security programs and business outcomes, ensuring that your protective measures secure what matters most.

Whether you are preparing for a specific compliance mandate or seeking to validate your security posture against emerging threats, the principles of successful red teaming provide a framework for long-term success. By championing this strategic, collaborative, and intelligence-driven approach, you can effectively mitigate risks and build a security program that practices true digital resilience against threats.

The most impactful next step is to initiate these conversations within your company and engage a trusted partner like NetSPI to help guide your journey. **Let's build your plan together. Contact NetSPI.**

### About NetSPI

NetSPI® pioneered Penetration Testing as a Service (PTaaS) and leads the industry in modern pentesting. Combining world-class security professionals with AI and automation, NetSPI delivers clarity, speed, and scale across 50+ pentest types, attack surface management, and vulnerability prioritization. The NetSPI platform streamlines workflows and accelerates remediation, enabling our experts to focus on deep dive testing that uncovers vulnerabilities others miss. Trusted by the top 10 U.S. banks and Fortune 500 companies worldwide, NetSPI has been driving security innovation since 2001. NetSPI is headquartered in Minneapolis, MN, and available on **AWS Marketplace**. Follow us on **LinkedIn** and **X**.