Red team scoping questions

These are the questions a SilentGrid consultant asks when scoping a red team or adversary simulation. Answering them first makes the call shorter and the plan more accurate.

"Not sure" is a fine answer. Several of these are decided together on the call.

Questions marked **Sizing** help us prepare an accurate quote.

01 Objective

What outcome would worry your board most if an attacker achieved it?

Why we ask: this becomes the exercise objective. "Approve a fraudulent payment" tests far more than "get domain admin".

Is there a threat you want to emulate? A ransomware group, or an actor known to target your sector.

Why we ask: it shapes the tools and techniques used, and how the attack path is mapped to MITRE ATT&CK.

Is the exercise required by a regulator, such as CORIE?

Why we ask: CORIE sets its own phases and reporting, which changes the plan.

What will you do with the result?

Why we ask: a result for an investment case needs different evidence from one used to train the security team.

02 Starting position

Should the exercise include getting in, or start from assumed access?

SIZING

Why we ask: initial access can take weeks. Assumed breach spends that time inside the network instead.

Is social engineering allowed, and are any staff groups excluded?

Why we ask: phishing and phone pretexting need explicit approval.

Is physical access to any site in scope?

SIZING

Why we ask: physical entry needs separate authorisation letters and planning for each site.

Should the scenario start from a compromised supplier, contractor or software dependency?

Why we ask: supply chain scenarios need the right starting access, and sometimes the supplier's agreement.

Roughly how many staff, sites, domains and cloud tenants are in the environment?

SIZING

Why we ask: the size of the environment sets how long reconnaissance and movement take.

03 Control Group

Who needs to know the exercise is running?

Why we ask: that group becomes the Control Group. Everyone outside it, including the security operations team, is part of what is being tested.

Who can pause or stop the exercise at any hour?

Why we ask: a real incident, or a response that goes too far, needs one call to resolve.

If your defenders escalate, how will the Control Group confirm it is the exercise without telling them?

Why we ask: the check has to be quiet, or the defenders learn the answer.

Is detection and response outsourced, and does the provider need notice?

Why we ask: some managed security contracts require notice. Otherwise the provider's response is part of the test.

04 Rules of engagement

Which systems, data or people are off limits?

Why we ask: these become the exclusions in the rules of engagement.

Are there periods when the exercise must not run? Financial close, peak trading or a change freeze.

Why we ask: the exercise is planned around them.

On reaching the objective, how far should the proof go?

Why we ask: demonstrating access, or taking a screenshot or test file, proves the point without touching real data.

Which third parties host systems in scope, and whose approval is needed?

Why we ask: cloud and hosting providers may need notice before testing.

05 Detection and response

What do you most want to learn about the defence? Whether it detects, how fast it escalates, or whether it contains.

Why we ask: it decides which moments are recorded and timed.

What security tooling is in place? Endpoint detection, a SIEM, identity monitoring.

Why we ask: findings can then separate "not logged" from "logged but missed".

Would a purple team session after the exercise be useful?

Why we ask: replaying the attack with defenders turns missed detections into working ones. It is scoped separately.

06 After the exercise

Who needs to hear the result? The board, executives or technical teams.

Why we ask: it shapes the debriefs and the report.

Would you want key fixes retested, or the exercise continued through CAOS (Continuous Adversary Operations Service) or an annual program?

Why we ask: follow-up work is agreed at scoping, not assumed.

Discuss your testing priorities

www.silentgrid.com/contact