CREST Accredited | certin Empanelled

BriskInfosec — VULNERABILITY TO VICTORY

10 Questions to ask

BEFORE HIRING A RED TEAM

Read before you sign anything →

sales@briskinfosec.com

CREST Accredited | certin Empanelled

BriskInfosec — VULNERABILITY TO VICTORY

START WITH SCOPE, OBJECTIVES AND METHODOLOGY.

These three questions define the entire engagement.
Get them wrong and nothing else matters.

1

What is the exact scope – and what is explicitly out of scope?

Every asset, system, environment, and network segment must be clearly defined. Ambiguous scope is how engagements go off the rails – or miss your most critical attack surfaces entirely.

SCOPE

2

What are the specific business objectives of this engagement?

Are you testing ransomware resilience? Insider threat scenarios? Crown jewel access paths? A Red Team without defined objectives is just an expensive network scan.

OBJECTIVES

3

What threat actor profile will the Red Team simulate?

Nation-state APT? Opportunistic cybercriminal? Malicious insider? The simulated adversary should reflect your organization's actual threat landscape – not a generic attacker profile.

THREAT MODELING

sales@briskinfosec.com

CREST Accredited | certin Empanelled

BriskInfosec — VULNERABILITY TO VICTORY

VALIDATE THE TEAM, THE RULES, AND THE REPORTING.

Who is doing the testing and what they're allowed to do is just as important as what they find.

4

What are the credentials and certifications of the Red Team operators?

Ask for OSCP, CRTO, CRTE, or CREST-certified professionals. A Red Team is only as good as the operators running it. Don't let vendor branding substitute for individual competence.

TEAM QUALITY

5

What are the rules of engagement — and who can call a halt?

Define what actions are permitted, what requires pre-approval, and who the emergency contact is if something goes wrong. Without a clear abort protocol, a simulated attack can become a real incident.

RULES OF ENGAGEMENT

6

What does the final report look like — and who is it written for?

A good Red Team report has an executive summary for leadership, a technical findings section for your security team, and a risk-ranked remediation roadmap. Ask for a sample report before you sign anything.

REPORTING

sales@briskinfosec.com

CREST Accredited | certin Empanelled

BriskInfosec™ — VULNERABILITY TO VICTORY

REMEDIATION, RETESTING, COMPLIANCE AND COMMUNICATION.

These are the questions most organizations forget to ask – and regret not asking.

7

Does the engagement include remediation guidance - not just findings?

A list of vulnerabilities without fix guidance is a problem statement, not a solution. Your team needs clear, prioritized, actionable steps — mapped to effort and business impact.

REMEDIATION

8

Is retesting included after you remediate the critical findings?

Fixing vulnerabilities without verifying the fix is wishful thinking. Insist on at least one retest cycle for critical and high-severity findings - it should be part of the engagement, not an add-on invoice.

RETESTING

9

How does this engagement map to your compliance requirements?

If you need to demonstrate Red Team activity for ISO 27001, PCI-DSS, DPDPA or CERT-In compliance, confirm the methodology and deliverables align to those frameworks before the engagement begins.

COMPLIANCE

10

How will progress and findings be communicated during the engagement?

Will there be weekly check-ins? Real-time critical finding alerts? A secure channel for sharing evidence? Communication cadence during a live Red Team engagement matters - especially if something critical is discovered early.

COMMUNICATION

REMEDIATION RETESTING COMPLIANCE COMMUNICATION

sales@briskinfosec.com

CREST Accredited | certin Empanelled

BriskInfosec — VULNERABILITY TO VICTORY

RED FLAGS - WALK AWAY

IF THEY CAN'T ANSWER THESE, FIND ANOTHER VENDOR.

Not every firm that offers Red Teaming actually delivers it. These are the warning signs that separate real operators from checkbox vendors.

They can't name the individual operators or their certifications

If they say "our team is highly experienced" but can't tell you who specifically will run your engagement - that's a red flag. You're paying for individual expertise, not a brand name.

Their methodology is vague or proprietary with no explanation

Legitimate Red Teams follow recognized frameworks - MITRE ATT&CK, TIBER-EU, CBEST, PTES. If they won't explain their methodology, they probably don't have a rigorous one.

The proposal looks identical to a VAPT report outline

Red Teaming and VAPT are different disciplines. If their Red Team deliverable looks like an automated vulnerability scan report with a different cover page - it probably is.

No rules of engagement document or legal authorization letter

Any professional Red Team will insist on documented legal authorization before touching a single system. If they're willing to start without it - that's not confidence, it's a liability for you.

A vendor that pushes back on these questions is telling you everything you need to know.

The right team will welcome them.

sales@briskinfosec.com

CREST Accredited | certin Empanelled

BriskInfosec — VULNERABILITY TO VICTORY

WHY THIS MATTERS

A BAD RED TEAM ENGAGEMENT COSTS MORE THAN NO ENGAGEMENT AT ALL.

Most organizations treat Red Teaming as a checkbox.
The ones who get real value treat it as a strategic exercise -
and that starts before the engagement even begins.

WITHOUT THE RIGHT QUESTIONS	WITH THE RIGHT QUESTIONS
You get a generic report	You get real intelligence
Vague scope leads to shallow testing	Scope is tight, targeted, and purposeful
Findings don't map to your actual risk	Findings align to business-critical assets
No remediation guidance - just a list of vulnerabilities	Actionable remediation with clear priorities
Can't retest. Can't track progress.	Retesting included. Improvement tracked.

VS

The quality of your Red Team engagement is decided in the briefing room – not during the test itself.

These 10 questions are your briefing checklist.

sales@briskinfosec.com

CREST Accredited certin Empanelled

BriskInfosec
VULNERABILITY TO VICTORY

RED TEAM · OFFENSIVE SECURITY

PLANNING A RED TEAM ENGAGEMENT? START HERE.

Don't let a poorly scoped engagement
give you a false sense of security.
The right Red Team asks **hard questions** -
and so should you before you hire one.

Book a Meeting

sales@briskinfosec.com