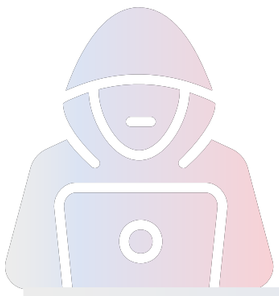
Red Team Assessment : Validate Adversary Resilience

A strategic briefing for executive security leaders.Red Team Assessments validate whether real attackers can compromise your most critical business assets.

CREST Registered Region - Global

VA PEN TEST

certin Empanelled



RED

Team Assessment

What Recent Adversary Campaigns Reveal About Detection Readiness

These are not warnings.
They are shared lessons from organizations that tested their defenses under realistic conditions.

27 SECONDS

AVERAGE ECRIME BREAKOUT TIME
(CROWDSTRIKE)

Attackers move laterally before most SOCs complete initial triage. The lesson: detection speed must match adversary speed.

11 DAYS

MEDIAN DWELL TIME FOR SOPHISTICATED ACTORS

Even organizations with mature SOCs are finding adversaries that evade signature-based detection.

60%

HUMAN ELEMENT IN BREACHES
(VERIZON DBIR)

Phishing, vishing, and social engineering remain the most reliable initial access vector. Technical controls alone do not address this.

$4.88M

GLOBAL AVERAGE BREACH COST
(IBM)

Organizations that discover breaches through red team exercises rather than real incidents reduce this cost by 40–60%.

Key Insight

The pattern across these data points is consistent: organizations investing in compliance-led testing are validating their vulnerability inventory but not their detection and response capability. The gap between what penetration tests measure and what red teams reveal is the gap most boards are now asking about.

The Current Threat Landscape

Adversaries are faster, smarter, and more persistent than ever. Industry benchmarks highlight the urgency to test real-world resilience across people, processes, and technology.

93%

ENTERPRISE NETWORKS COMPROMISED WITHIN 2 DAYS

Attackers gain initial access quickly and move laterally with speed and precision. Perimeter defenses alone are no longer enough.

29 min

AVERAGE ATTACKER BREAKOUT TIME

Once inside, attackers break out of their initial foothold in less than 30 minutes. Detection must be faster than the attacker.

442%

INCREASE IN VISHING ATTACKS

Voice-based social engineering is surging and proving to be one of the most effective ways to bypass technical controls.

6.4:1

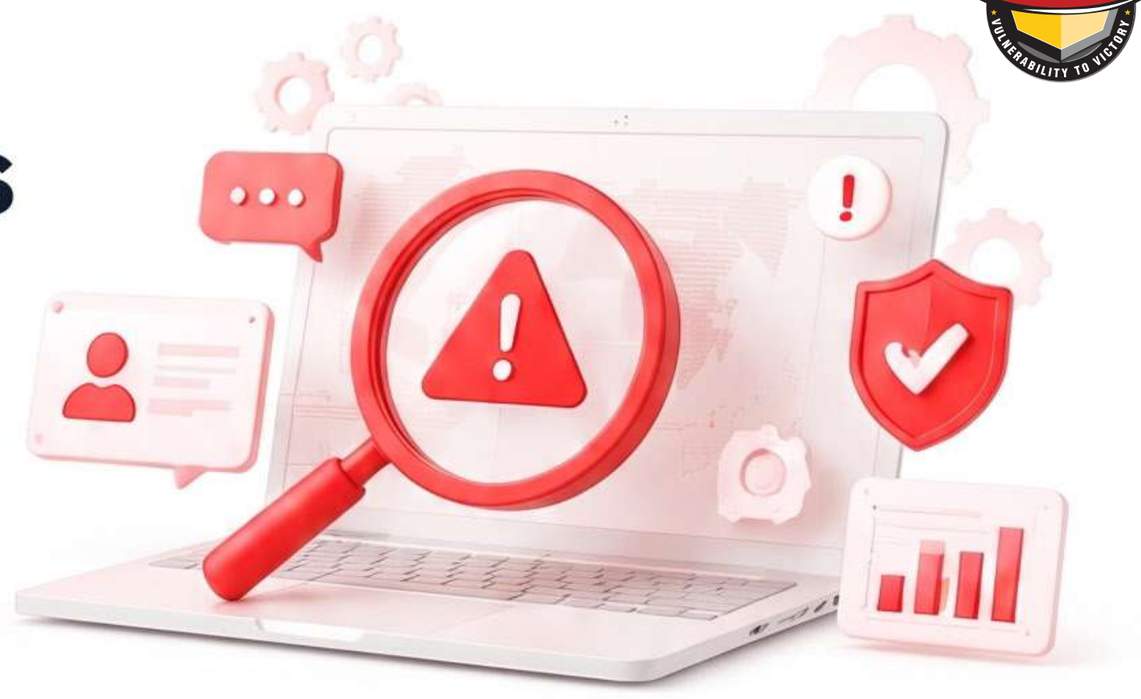
AVERAGE ROI ON RED TEAM INVESTMENTS

Organizations see strong returns by identifying attack paths, closing gaps, and preventing costly breaches before they happen.

Why It Matters

Traditional security validation shows where you are vulnerable. Red Team Assessments show how an attacker would succeed. In today's threat landscape, that visibility is critical to building real cyber resilience.

Common Assumptions vs Reality



These are not misconceptions to correct.
They are reasonable assumptions
that need updated context.

WHAT YOU THINK	THE REALITY
We run annual pentests, so we know our risk posture. This is the most common starting point, and it is a strong one.	**Pentests identify technical vulnerabilities in a defined scope.** Red teams test whether your people, processes, and technology work together to detect and stop a real adversary. These answer fundamentally different questions.
Red teaming is only for mature security organizations. Understandable, given how the service is often positioned in the market.	**Organizations at every maturity level benefit.** For less mature teams, a red team engagement creates a baseline and shows exactly where detection gaps exist. The earlier you test, the more efficiently you invest.
Our SIEM/SOC would detect a real attack. A reasonable assumption, given the investment that has gone into building that capability.	**In our experience, most SOCs detect red team activity only after the objective has already been achieved.** The value is in revealing these gaps before a real adversary does.
Red teams just try to break in. We already know we can be breached. This is an important reframe, and it is worth taking further.	**A professional red team engagement maps complete attack paths,** tests crisis response procedures, validates detection capabilities, and provides a prioritized remediation roadmap. The goal is organizational learning, not just proving a breach.
This seems disruptive to operations. A legitimate concern, especially in environments with low tolerance for unplanned disruption.	**Red team engagements are designed with explicit rules of engagement,** safety protocols, and real-time coordination. The goal is to test resilience without creating actual risk.

Bottom Line

Red Team Assessments bridge the gap between security assumptions and real-world adversary behavior, giving leadership the evidence they need to make confident risk decisions.

What a Red Team Assessment Really Delivers

A red team assessment is a controlled, goal-driven engagement that simulates a real adversary to uncover gaps that traditional testing misses.

How It Works

01 PLAN

We define objectives, scope, rules of engagement, and success criteria aligned to your business risks.

02 ATTACK

Our team emulates real adversaries to identify, exploit, and escalate across people, processes, and technology.

03 REPORT & STRENGTHEN

We deliver actionable insights, validate impact, and help you strengthen controls where it matters most.

Key Benefits for Your Organization

Expose Hidden Gaps
Find vulnerabilities and attack paths that automated tools and traditional assessments do not uncover.

Prove Real-World Impact
Understand how an attacker could impact your business, not just whether a vulnerability exists.

Improve Detection & Response
Validate your security controls, SOC processes, and incident response against real attacker behavior.

Strengthen Security Investments
Get clear, evidence-based insights to prioritize remediation and maximize security ROI.

Build Board-Level Confidence
Demonstrate proactive risk management and cyber resilience with credible, real-world evidence.

Drive a Security-First Culture
Empower teams with actionable learning to continuously improve and stay ahead of adversaries.

The Outcome

Red Team Assessments give you the clarity to close critical gaps, the confidence to prove resilience, and the advantage to stay ahead in an evolving threat landscape.

Who Should Prioritize Red Team Assessments

Every organization faces risk. These are the teams and industries that benefit the most.

Ideal For

- Organizations handling sensitive customer, financial, or health data
- Enterprises undergoing digital transformation or cloud adoption
- Companies in regulated industries with high compliance requirements
- Organizations with previous security incidents or evolving threat exposure
- Leadership teams seeking evidence-based security assurance

What You Get

Realistic Threat Emulation

Simulates advanced adversaries using real tactics, techniques, and procedures.

Comprehensive Coverage

Tests across people, processes, and technology – not just your network.

Actionable Insights

Delivers clear, prioritized findings that drive measurable improvements.

Stronger Security Posture

Helps close critical gaps and improve detection, response, and resilience.

Board-Level Reporting

Provides executive-friendly reports with risk context and business impact.

Continuous Readiness

Establishes a repeatable engagement model to stay ready for what's next.

Key Takeaway

Red Team Assessments are not just for large enterprises or high-profile targets. They are for any organization that wants to understand its real risk, strengthen its defenses, and earn the confidence to grow securely.

Our Approach.
Your Advantage.

We combine experienced adversaries, proven methodology, and actionable insights to help you stay ahead of tomorrow's threats, today.

Our Red Team Assessment Offerings

External Red Team Assessments

Simulate real-world attacks from outside your network to identify exploitable weaknesses attackers could leverage.

Internal Red Team Assessments

Evaluate the risk of an insider or compromised account to understand lateral movement and crown jewel exposure.

Cloud Red Team Assessments

Test your cloud environments, identities, and configurations to uncover misconfigurations and privilege escalation paths.

Application Red Team Assessments

Assess the security of your web and mobile applications through real attack simulations beyond automated scans.

Why It Matters Now More Than Ever

Threats Are Evolving
Attackers continuously adapt. Your defenses must evolve faster.

Assumptions Create Biind Spots
You can't protect what you don't know is exposed.

Red Teams Provide the Truth
We show you what attackers can do, not just what tools flag.

Prepared Teams Respond Better
Realistic exposure leads to stronger processes and faster response.

Resilience Builds Trust
Demonstrate to customers, partners, and regulators that you take security seriously.

The Impact in Numbers

80% of organizations gain critical insights they did not expect from traditional testing.

70% reduction in identified high-risk exposures after remediation from red team findings.

3x more effective at preventing breaches with proactive red teaming.

60%+ of breaches involve tactics that red team assessments can replicate and help mitigate.

Take the Next Step

Security is not about avoiding risk entirely—it's about understanding it better than anyone else. Let our red team show you what matters most.
Let's build a stronger, more resilient future together.

What Happens Next?

Client Breaches
Post-assessment security record

Start With Zero Commitment

Understanding your unique security challenges begins with a conversation. We offer a no-obligation consultation to assess your current posture and identify immediate risk areas.

Our Team Holds Industry-Leading Certifications

We invest heavily in our team's continuous education because the threat landscape never stops evolving. Neither do we.

OSCP | OSWE | CISSP | CISA | CEH

CREST Accredited
Internationally certified penetration testing excellence

CERT-IN Empanelled
Government-recognized trusted cybersecurity assessment provider

ISO 27001 : 2022 Certified
Our own security practices are independently audited and verified annually

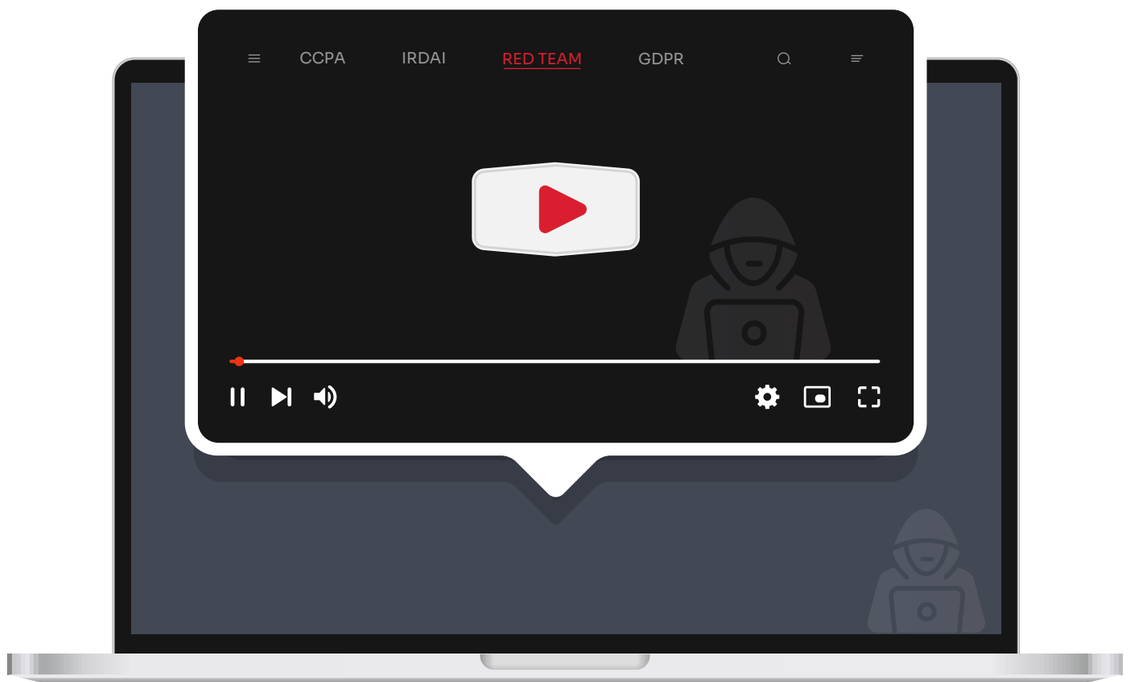
25+
Countries Client Portfolio

67%
Logic flaws missed by bots

98%
Client retention

640+
Successful Customers

5600+
Delivered in 24 countries



Reach us for FREE
consultation

Book Now

sales@briskinfosec.com
www.briskinfosec.com

Our Geographical Presence
India
UAE