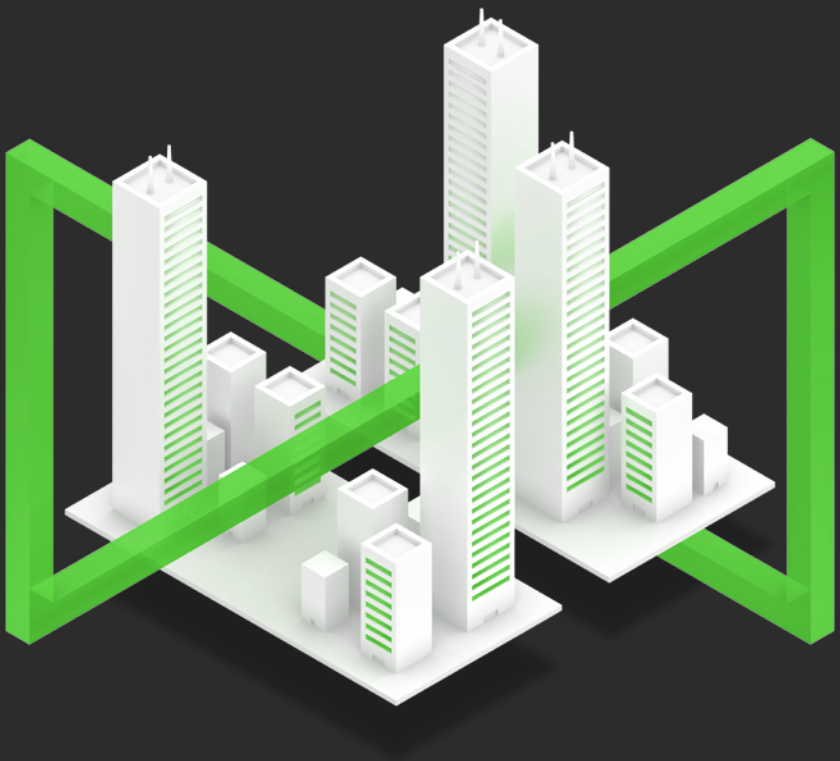
DEVCORE

Red Team Assessment

Safeguard the organization's mission-critical and strategic assets



LEARN MORE

about DEVCORE

DEVCORE is committed to delivering top-tier red team assessment services, simulating real-world adversary attacks to help clients uncover hidden vulnerabilities and enhance their overall defense posture.

DEVCORE

Red Team Assessment

Safeguard the organization's mission-critical and strategic assets

Cybersecurity Under Pressure: Why Red Team Assessments Are More Critical Than Ever

Traditional perimeter defenses can't keep pace with modern threats—from organized threat actors to ransomware and supply chain attacks.

What organizations need instead is a clear, end-to-end understanding of how both systems and personnel respond under active attack. That's precisely why red team assessments have become essential—they expose real-world gaps and strengthen overall cyber resilience.

Red Team Assessment: Simulating Real-World Threats

A red team assessment simulates a realistic cyberattack without disrupting business operations. Acting as adversaries, operators apply diverse tactics within defined time frames to uncover vulnerabilities, gain access, and execute objective-driven attacks.

By emulating advanced, multi-vector threats, red team assessments expose real-world tactics, techniques, and procedures (TTPs), surface system weaknesses, and highlight detection gaps. This enables organizations to validate response capabilities and prepare teams under realistic, controlled conditions.

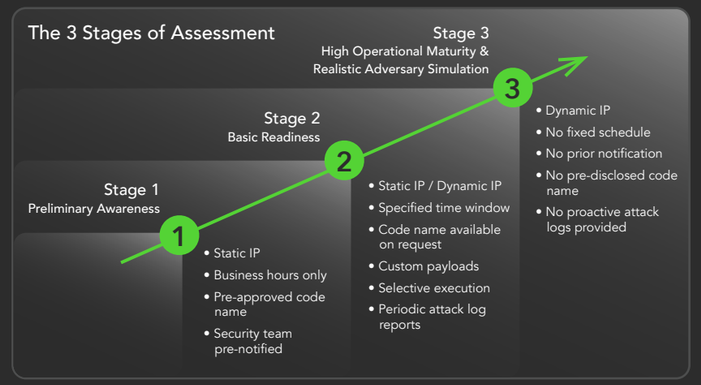
Select the Appropriate Assessment Mode

A red team assessment can be structured in progressive phases, tailored to an organization's security maturity and assessment objectives:

Phase 1 – Identify Initial Weaknesses
Surface critical vulnerabilities and entry points within scope through guided collaboration to reduce exploitation risk.

Phase 2 – Validate Defensive Posture
Assess remaining high-risk paths and verify the effectiveness of security controls and blue team response after initial hardening.

Phase 3 – Emulate Realistic Threats
Conduct a no-notice assessment to evaluate true detection and response capabilities, revealing blind spots and unknown attack paths.



Optimizing Red Team Value with Precision Planning

With insights from hundreds of red team assessments, we've found that aligning red and blue team strategies is key to meaningful outcomes.

To maximize value, we provide structured planning options—time-bound execution, dynamic/static IPs, rotating codenames, staged progress disclosure, scoped limits, controlled actions, and alternative approaches for extended engagements.

Through best practices and close collaboration, we help organizations extract the full value of each red team assessment.

Various Assessment Modes

Physical Location	Remote	Designated	Onsite				
Network Vector	Internet	Intranet	Hybrid				
Tactics	Zero-day attack	Threat intelligence emulation	Third-party software	Social engineering	Wi-Fi	Supply chain attack	Extranet attack
Type	Black-box	Grey-box	White-box				
Scope	Full	Partial	Designated				
Objective	Infrastructure	Core system	Elevated privileges	Sensitive data	IoT, OT		
Target	Website	Application	Wireless network	Security appliance	Network segmentation	Cloud security	
Duration	Scheduled time	Blackout date	Anytime				
Defense Evasion	Dynamic IP	Traffic interference	Log tampering	Defense evasion	Race condition		

By the Numbers

60+ enterprise collaborations

110+ red team assessments completed

81% achieved control of targeted systems

82% identified with weak password complexity

77% reached internal network zones via lateral movement

53% resulted in credential or data leaks exposed to public access

Industry Coverage

High-Tech
Semiconductor (design, manufacturing, packaging), computer components, and telecommunications and networking

Financial Services
Assessment delivered for 5 of 6 Domestic Systemically Important Banks (D-SIBs)

Critical Infrastructure
Projects executed across 7 of 8 critical infrastructure sectors, including transportation, energy, and healthcare

Government
Central and local government agencies classified as Tier A and B under national cybersecurity responsibility frameworks

Ongoing Research and Field Contribution

Backed by deep expertise and a commitment to excellence, we continuously integrate cutting-edge research and evolving adversary tactics into our red team assessment and penetration testing methodologies—helping organizations stay ahead of emerging threats.

Our work, trusted by leading enterprises and recognized globally, reflects the forefront of offensive security and advances the cybersecurity community.

13+ International Awards

'24 Top 10 Web Hacking Techniques #1 & #4
'23 Pwn2Own Toronto #3
'22 Pwn2Own Toronto #1
'21 Pwn2Own Austin #2
'21 Pwnie Awards
(Best Server-side Bug)

290+ Vulnerability Disclosure

More than 40 types of products are used by Enterprise.

Microsoft Windows / Exchange / Office / IIS
Linux Kernel, Apache HTTP Server, Exim, PHP
Fortinet, Pulse Secure

60+ International Conferences

Black Hat USA, DEF CON
Black Hat Asia,
Red Team Summit,
CODE BLUE,
HITB, HITCON

50+ Bug Bounty Programs

Amazon,
Meta (Facebook),
GitHub, Google,
LINE, X (Twitter)
Uber

DEVCORE

Fundamentals and Implementation

Clarity on red team fundamentals, use cases, and implementation enables organizations to realize long-term value and prepare effectively.

Q1 What is the difference between a red team assessment and a penetration test?

A penetration test evaluates the security of a specific system or product. In contrast, a red team assessment simulates a full-scope attack against critical assets—within a defined scope and timeframe—to uncover attack paths, emulate adversary techniques, and validate detection and response effectiveness.

Q2 When is an organization ready for a red team assessment?

Red team assessments can be tailored to an organization's security maturity.

We recommend initiating them after foundational controls—firewalls, antivirus, network segmentation, and endpoint monitoring—are in place. At this stage, assessments validate defense assumptions, uncover vulnerabilities, and inform future strategy.

Q3 Do organizations with internal red teams still need external assessments?

Yes. External red teams provide a valuable adversary simulation perspective through black-box testing, vulnerability research, and advanced evasion. Operating without prior knowledge of internal systems, they emulate real-world threats to test detection and response under realistic conditions.

Internal red teams bring deep insight into system architecture, business processes, user behavior, and known weaknesses. This enables targeted post-external assessments focused on high-impact paths and critical nodes. Together, internal and external red teams offer complementary strengths that enhance threat readiness and security validation.

Q4 How is a red team assessment priced?

Pricing is based on scope factors—industry, organization size, asset volume, objectives, defensive maturity, and assessment model.

If objectives are met early, we continue identifying additional attack vectors and vulnerabilities to maximize value and threat coverage.

Q5 What is the recommended frequency for conducting a red team assessment?

The frequency of a red team assessment depends on organizational size, defensive maturity, and objectives. We generally recommend conducting one every 12–24 months to validate controls and maintain resilience against evolving threats.

Execution and Impact

Red team assessment details—including duration, coordination with internal IT teams, and safeguards—are structured to ensure business operations remain uninterrupted throughout the engagement.

Q1 How long does a red team assessment take?

All red team assessments are fully customized. A full engagement typically spans 4–6 months and includes intelligence gathering, initial testing, analysis, remediation, hardening, and post-remediation validation. Timelines may vary based on scope and complexity.

Q2 What information should be provided for a first-time red team assessment?

To ensure realistic simulation, first-time red team assessments require only the authorized scope and mission objectives. For organizations with prior red team experience, sharing selected internal context aligned with objectives can enhance engagement depth and effectiveness.

Q3 Should the IT team be notified during the assessment? How should the red team coordinate with the internal blue team?

Assessment models vary by security maturity and objectives—ranging from cooperative mode to coordinated execution to full-scope simulation. Based on realism level, clients may choose to notify blue team members or management. Each model balances realism and control, enabling tailored red-blue collaboration.

Q4 How does the red team simulate insider threats? Can social engineering attacks be included?

Red team assessments can start from a designated host to simulate post-compromise threats. Social engineering may also be included within scope to test detection and response.

Q5 How is business continuity ensured during a red team assessment?

No internal data will be deleted during the assessment. Actions with potential impact are executed only when necessary and approved. No disruptive or visible activity, such as website defacement, is performed.

Benefits and Long-Term Strategic Value

Key long-term impacts of red team assessments include data protection strategies, KPI recalibration, and budget justification through validated risk exposure.

Q1 How is sensitive data protected during a red team assessment?

DEVCORE is ISO 27001 certified, covering all processes and controls for handling customer-sensitive data. Client data is stored in DEVCORE's internal data center, with access restricted to NDA-bound project personnel, and full access logs retained.

Testing data is deleted after assessment completion, with only final reports preserved. Upon client request after the maintenance period, all data can be removed and formal deletion proof provided.

Q2 How can red team assessment results be translated into actionable improvements and budget justification?

Organizations should define red team assessment objectives around critical systems. If attacks succeed, results can quantify business impact by measuring time from compromise to remediation—highlighting operational risk and supporting data-driven security investment.

Q3 How can red team assessments help organizations establish security key performance indicators (KPI)?

Red team assessments establish a foundation for measuring blue team performance via security KPIs. Key metrics include:

- Mean Time to Detect (MTTD):
The average time between the initiation of a red team attack and the blue team's detection.
- Mean Time to Respond (MTTR):
The average time from threat detection to the incident response actions.
- Mean Time to Contain (MTTC):
The time required to fully contain the threat after it has been identified.

These metrics enable organizations to baseline detection and response effectiveness, identify gaps, and guide measurable security improvements.