What is Red-Teaming?

The term “red team” is derived from traditional military war games: red teams are the attackers (“blue teams” are the defenders). In relation to cyber security, Red Teams are external entities brought in to test the effectiveness of an organisations security program (or a particular part of it).

Red teaming is a thorough and hands-on approach to security testing that puts your organization’s defences to the test by simulating real-world attack scenarios. This process involves analysing the tactics, techniques, and procedures (TTPs), used by potential adversaries to replicate the kinds of strategies attackers are likely to use. The primary objective in red teaming is to see how well your organization can detect, respond to, and recover from these advanced threats, by adopting the perspective of a determined adversary.

Red Teaming vs Penetration Testing

Think of Red Teaming as the next evolution of Penetration Testing. In fact Penetration Testing could even be considered a subset of a Red Team engagement, but with much differing approaches and goals.

Red teaming is a simulated attack on a company, it’s employees or systems and is based on a scenario with identified goals. Penetration testing is focused on a set of defined systems and the outcome is usually a list of confirmed vulnerabilities in those systems. Whereas the outcome of a red team engagement could be if a given objective was achieved (such as taking control of a certain system, obtaining specific data, etc) and then establishing the route (or routes!) on how that goal was reached.

Also penetration testing is usually a noisy affair, which takes place with the wider organisations knowledge. Part of the benefits of a red team test, is that it is carried out stealthily over a much longer period, without the knowledge of the blue team (the organisations defenders). The idea is to also test how an organisation detects and responds to attacks.

Features	Penetration Testing	Red Teaming
Objective	Find all vulnerabilities in the target systems in scope	Achieve stated goals using an array of real-world TTPs
Timeframe	Typically short to medium effort, from days to a few weeks, depending on the scope	Longer effort, usually more than a month
Testing Approach	Manual and automated testing	More manual testing focused, with some automation. Includes non-technical testing techniques
Techniques	Commercial, open-source, bespoke tools and manual techniques, using a static methodology.	Commercial, open-source, bespoke tools and manual techniques. Flexible methodology and creative testing approach. Use of other techniques such as social engineering, physical tests, etc.
Organisational Awareness	Defenders are usually aware. Testing is noisy	Defenders are not aware. Testing is quiet and stealthy
Targets	Predefined	Exclusions can be defined, but targets are typically wide-ranging.
Outcome	A list of validated vulnerabilities, prioritised by risk, with remediation advice.	Achievement (full or partial) of goal and identification of route(s) to obtain goal. Provides insight into overall security capabilities and response (strengths & weaknesses)
Cost	Limited testing window is agreed, typically costing from a few days to weeks.	Usually more expensive as more security experts are involved and the duration is much longer.

Our Red Teaming Service

Our Red Teaming methodologies are based on leading industry practice, using the most modern testing frameworks such as TIBER-EU, MITRE ATT&CK, CREST and OWASP. Testing can be broken into the below distinct phases.

Scoping: Every organization is unique, and so are our red team engagements. We collaborate with your organization to define goals, objectives and rules of engagement, from open-scope engagements, to 'assumed breach', to narrow-focused tests.

<Example of objectives?>

Intelligence: Intelligence and information in relation to your organisation is gathered which might influence the testing approach. Open-source intelligence (OSINT) and third-party threat intelligence sources may be used.

Reconnaissance: Leveraging any intelligence gathered, passive and active research is undertaken against the organisation, including cataloguing potential targets, be they digital, physical or social. Enumeration of systems can also take place.

Initial Access: Our team simulates real-world attacks to gain unauthorized access, leveraging methods such as:

- Phishing campaigns (email, SMS, or voice-based).
- Exploiting publicly exposed hosts and misconfigurations.
- Leveraging social engineering tactics and weak credentials.

 | Copyright© 2025 Edgescan. All rights reserved.

Exploitation: Upon achieving initial access, we simulate advanced threat actor behaviour by:

- Exploiting vulnerabilities to escalate privileges.
- Establishing persistence in the environment.

Lateral Movement / Pivot: Once a foothold is established, use this as a bridgehead to penetrate further into the organisation

- Mapping and navigating through your systems to identify high-value assets.

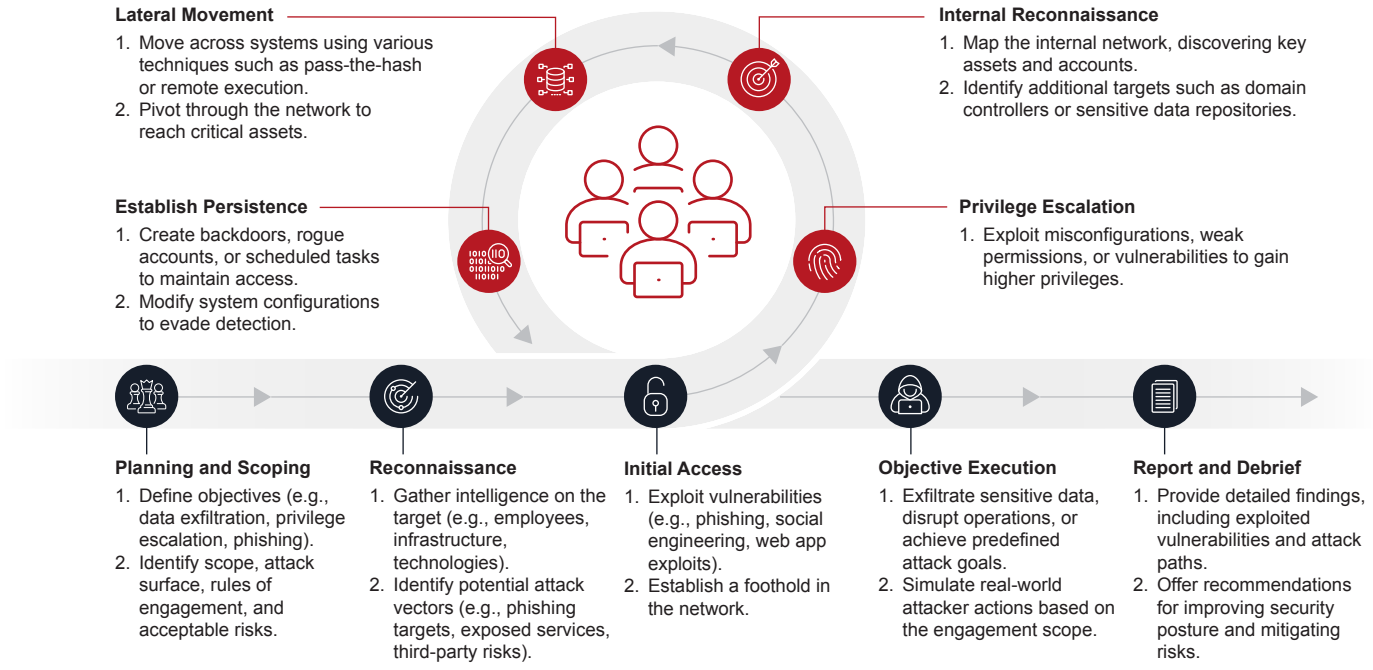
Response Evaluation: Throughout the engagement, we assess your organization's ability to:

- Detect unauthorized activity and suspicious behaviours.
- Respond to simulated threats in a timely manner.
- Identify gaps in monitoring, incident response processes, and security awareness programs.

Reporting and Debriefing: Following the engagement, we provide a detailed report, including:

- A detailed summary of simulated attack scenarios.
- Identified vulnerabilities and weaknesses.
- Identified strengths or any compensating actions by a blue team.
- Actionable recommendations for remediation.
- Strategic insights to strengthen your overall security posture.
- Our Red Team experts are available post-engagement to provide tailored advice and support with remediation efforts, ensuring your organization can implement improvements effectively.

Red-Teaming: How it Works



 | Copyright© 2025 Edgescan. All rights reserved.

Benefits

Organisation View on Defense: Get the bigger picture on your organizations defences

Enhanced Security Posture: Proactively uncover and remediate vulnerabilities before attackers exploit them.

Scalable options: We offer scalable solutions tailored to your needs, whether you require a one-time or continuous assessments to maintain long-term security. (this is to fit edgescan into red team for extra money or sell licences! - see below too)

Improved Detection and Response: Identify gaps in incident monitoring, response times, and playbook effectiveness.

Tailored Insights: Gain recommendations specific to your environment and operational needs.

Regulatory Compliance Support: Align security efforts with industry standards like DORA, NIST, ISO, and GDPR.

Operational Resilience: Strengthen defences against evolving threats through realistic testing and ongoing improvement. Verify the effectiveness of your blue team defences.

Peace of Mind: Leverage the expertise of certified professionals to safeguard critical assets and reduce risk exposure.

Purple Teaming: Bring the red and blue teams together to collaborate on the identification of threats and attack paths.

DORA: Digital Operational Resilience Act

The Digital Operational Resilience Act (DORA) is a regulatory framework introduced by the European Union to strengthen the cybersecurity and operational resilience of financial entities and critical service providers. It establishes a unified approach to managing risks, ensuring that organizations can withstand, recover from, and adapt to operational disruptions and cyber threats.

Our Red Teaming services align with DORA requirements to help organizations in the financial sector and beyond meet these critical compliance standards while enhancing their overall security posture.

DORA specifically highlights the requirement for organisations to undergo a Threat-Led Penetration Test (TLPT) at least once every three years. The TLPT can be thought of as a red team engagement with some scope requirements specific to DORA.

How Our Red Teaming Services Align with DORA

Our Red Teaming services are designed to help organizations achieve compliance with the Digital Operational Resilience Act (DORA) while enhancing their overall operational resilience and cybersecurity capabilities. By focusing on realistic threat simulations, comprehensive testing, and actionable insights, we ensure your organization can meet DORA's requirements effectively.

 | Copyright© 2025 Edgescan. All rights reserved.

Key Alignment Areas

Realistic Threat Simulations: We replicate real-world cyberattacks tailored to your organization's specific threat landscape, validating your defences and resilience against operational disruptions.

Holistic Testing Approach: Our assessments target critical systems, processes, and infrastructures, ensuring alignment with DORA's operational resilience testing requirements.

Intelligence-Led Scenarios: We incorporate threat intelligence into our engagements, ensuring the testing reflects emerging risks and adversary tactics.

Compliance and Reporting: We provide detailed documentation of our findings and testing processes, ensuring you have the evidence required to demonstrate compliance with DORA's incident reporting and operational resilience mandates.

Third-Party Risk Assessment: Our services evaluate the security posture of third-party providers, ensuring compliance with DORA's emphasis on managing ICT-related risks in your supply chain.

Threat-Led Penetration Testing (TLPT): Alignment with the relevant TLTP authority to ensure the full requirements of testing are addressed.

By delivering advanced adversarial testing and detailed insights, we support your organization in meeting DORA's requirements while building a robust and sustainable approach to cybersecurity and operational resilience.

Red Teaming and The Edgescan Platform

Combining Red Teaming with the Edgescan platform provides a comprehensive security strategy that enhances a financial institution's ability to comply with the Digital Operational Resilience Act (DORA). Edgescan's continuous attack surface management (ASM) and full-stack vulnerability management enable real-time identification and prioritization of security gaps, while Red Teaming simulates real-world cyberattacks to test detection and response capabilities.

This integrated approach ensures that financial institutions not only maintain continuous security monitoring but also validate their incident response, threat intelligence, and resilience strategies against sophisticated adversaries. By leveraging Edgescan's automated risk assessments alongside Red Teaming's adaptive, human-driven testing, organizations can proactively address vulnerabilities, strengthen regulatory compliance, and build a robust cyber resilience framework aligned with DORA's stringent requirements.

 | Copyright© 2025 Edgescan. All rights reserved.

The Edgescan Team

With years of experience in penetration testing and security consulting, our experts have the skills and knowledge to help your organization uncover hidden vulnerabilities and build a stronger defence.

Certified Expertise

Edgescan is CREST approved and maintains a robust Information Security Management System (ISMS) which is ISO27001-2022 certified. Additionally, we are a Payment Card Industry Data Security Standard (PCI DSS) Approved Scanning Vendor (ASV).

Our team members are certified through leading organizations such as Offensive Security, CREST, Altered Security, EC-Council and more, ensuring the highest level of expertise and professionalism in every engagement.

Why Choose Us?

Expertise You Can Trust: Our team of seasoned professionals leverages years of experience to deliver actionable insights tailored to your organization's unique environment.

Customizable Engagements: We offer flexible service packages to meet your specific needs, whether it's a one-time assessment or ongoing support.

Proven Methodologies: Using industry-standard frameworks such as TIBER-EU, MITRE ATT&CK, OWASP, and NIST, we ensure thorough and consistent testing.

Seamless Integration: Our Red Team services integrate seamlessly with your existing security operations, enabling swift remediation and long-term resilience.

Contact Us Today

Discover how our Red Team services can fortify your organization's security posture. Contact us at *sales@edgescan.com* for more information on how Edgescan can help secure your business.

edgescan.com | Copyright© 2025 Edgescan. All rights reserved.