COGNISYS

PENETRATION TESTING

Red Team assessment

Strengthen your cyber defences with a comprehensive red team assessment.

Why conduct a red team assessment?

A red team assessment is essential for organisations committed to strengthening their defence systems against advanced cyber threats. This assessment rigorously tests your people, processes and technologies, revealing vulnerabilities that routine penetration testing may miss.

The simulation of sophisticated attack vectors delivers essential insights into your organisation's ability to detect, mitigate, and recover from real-world breaches. Investing in a red team assessment is vital to maintaining a resilient and adaptive security posture in an increasingly hostile digital landscape.

Scoping and planning

Define objectives

We begin by collaborating with your team to establish the objectives of the red team assessment. Whether your focus is testing specific attack vectors, evaluating incident response capabilities, or assessing overall organisational resilience, we tailor our approach to meet your unique security goals.

Scoping and engagement parameters

We define the full scope of the red team assessment, covering all potential attack vectors—from phishing and social engineering to network infiltration and data exfiltration. With client permission and a "get out of jail free" card in place, our red team is authorised to simulate a broad range of adversarial tactics. This comprehensive approach ensures that every aspect of your organisation's defences is thoroughly tested.

Threat modelling

Based on the identified scope, we develop a threat model that outlines potential adversaries, attack vectors, and scenarios most relevant to your organisation. This modelling helps us simulate realistic attack scenarios aligned with the threats your business is most likely to face.

Rules of engagement

Establishing clear rules of engagement is essential to ensure that the red team assessment is conducted safely and effectively. We define the scope, constraints, and guidelines for the assessment, including how far the red team can go in their attack simulations and which systems are in-scope or out-of-scope.

Logistics and preparation

We plan the logistics of the assessment, including scheduling, resource allocation, and ensuring all necessary tools and environments are in place. This phase also involves briefing key stakeholders and ensuring that communication channels are established for incident reporting during the assessment.

Stakeholder communication

We maintain ongoing communication with your key stakeholders throughout the planning process to ensure alignment and transparency. Regular updates and briefings help keep everyone informed and prepared for the assessment, minimising potential disruptions to normal operations.

SmartView takes care of your reporting

Cognisys' SmartView Portal provides a centralised platform for clients to manage their projects and vulnerabilities efficiently. Through the portal, clients can track the status of each identified issue, assign tasks to team members, and monitor the progress of remediation efforts.

A detailed report is prepared once the red team assessment is complete, prioritising findings and providing strategic, actionable recommendations to strengthen your security posture through our SmartView portal.

Why choose Cognisys' red team assessment?

Our red team assessment offers expertise in advanced threat simulation and security strategy. Our certified professionals emulate sophisticated adversaries to assess and fortify your defences rigorously. We provide a customised assessment tailored to your organisation's needs to evaluate potential vulnerabilities and map them with the MITRE ATT&CK framework.

Our insights enhance your incident response capabilities and refine your overall security posture, ensuring your organisation can effectively counter advanced cyber threats.

BACK TO CONTENTS