Red Teaming Assessment

Identify vulnerabilities across your organisation

By simulating real-world attack scenarios, this assessment can expose vulnerabilities that may have been overlooked by common security exercises. Output from this assessment can be used to help improve your organisation's defensive capabilities across People, Process and Technology (PPT).

Brochure

Telstra Purple

Your insight into the mind of a hacker

Hackers motivations can range from simple curiosity or seeking financial gain, to top-level sophisticated espionage and state-sponsored attacks.

Red Teaming is all about simulating real-world attacks on your organisation through a controlled exercise, led by our experienced team who can emulate the Tactics, Techniques and Procedures (TTP) of known threat actors.

Identify risk and test your defences

Our service assesses the three pillars of People, Process and Technology (PPT) which underpin your organisation's cyber defence capabilities.

We can help you understand and evaluate your technical vulnerabilities, as well as potential weaknesses in your processes and people.

The Red Team can help provide critical insight into how they targeted your organisation, navigated your defences and how well you responded to their attacks. You can benefit from a wide range of attack scenarios which are detailed in a formal assessment report and walkthrough presentation.

Are you protected against hackers?

Organisations invest significant time, budget and resources to harden their security postures.

Gaining visibility into specific areas where your organisation is vulnerable, across People, Processes and Technologies, can be crucial for evaluating just how resilient you are against current and emerging cyber threats.

The average cost of a data breach to Australian businesses of all sizes is on the rise according to the ASD Cyber Threat Report 2022-2023.

Small
$46,000

Medium
$97,200

Large
$71,600

Reference - ASD Cyber Threat Report 2022-2023

Tailored real-world attack scenarios

The Red Teaming Assessment will simulate a targeted attack against your organisation through a variety of attack vectors including but not limited to digital, physical, and social engineering techniques.

This assessment aims to tailor our attack scenarios to help your organisation improve defensive capabilities by identifying vulnerabilities across People, Process and Technology (PPT).

Goal driven objectives

To provide the most value to your organisation, the goals are tailored to your business needs.

Our service includes seven key phases which aim to achieve the objectives and goals of the assessment.

- Open Source Intelligence (OSINT)
- Attack Surface Mapping
- Social Engineering
- Physical Site Assessment
- Vulnerability Identification and Exploitation
- Assumed Breach Scenario (Optional)
- Post Exploitation (Lateral Movement and Privilege Escalation)

Detailed Reporting & Presentation

Detailed reporting is provided to you at the conclusion of the assessment.

Our Red Team will present the report to your team via a virtual meeting, to help your stakeholders understand your current vulnerabilities and prioritise your next actions. We can cater for a technical or business audience, or both.

The report includes:

- Executive summary
- Business risks
- Strategic recommendations
- Detailed technical findings and recommendations

Clear benefits

Identify Vulnerabilities

Helps identify vulnerabilities that may have been overlooked by typical security exercises.

Improve Response

Helps develop and improve incident response plans, by identifying gaps in processes.

Enhance Awareness

Helps employees in your organisation better understand the impacts of a cyber attack.

Uplift your cyber posture

Helps you identify and prioritise areas of risk, to aid in planning, budgeting and remediation of now known vulnerabilities.

Training Opportunities

Helps provide realistic training opportunities for security personnel. Enable your security team to develop their skills.

Continuous Improvement

Helps organisations identify new vulnerabilities and respond to emerging threats, so defences remain effective over time.

Why us?

We have depth of skills and years of experience managing one of Australia's largest networks.

We are well-positioned to assist your organisation assess your potential vulnerability to a wide range of cyber attack scenarios. Our Red Teaming Assessments help provide a competitive edge against malicious actors.

Want help securing your organisaton?

Contact your Telstra Purple Representative today.

purple.telstra.com/services/cyber-security