COGNISYS

PENETRATION TESTING

Purple Team assessment

Improve your security by bringing together offensive and defensive teams with our purple team assessment.

Why conduct a purple team assessment?

Organisations need proactive security assessments to navigate the cyber security landscape effectively, especially in high-risk sectors. The purple teaming assessment is crucial for strengthening your defences against targeted attacks. It involves a hands-on attack simulation and collaborative knowledge sharing to enhance cyber security competencies and skills.

Organisations must move beyond relying solely on perimeter or endpoint security products to achieve faster and more reliable detection at all cyber-a reliable detection at all cyber-attack stages.

Methodology

Define objectives

We collaborate with your security teams to determine the focus of the purple team assessment, ensuring it aligns with your organisational objectives. Whether you want to test specific attack vectors, improve response to insider threats, or evaluate the efficiency of your detection tools, our methodology is tailored to address your key concerns.

Requirements

Before the assessment, we work with the defensive (blue team) to gather relevant network and security infrastructure details. This includes collecting information about your existing security tools, detection mechanisms, and critical assets. We ensure that the test is planned to meet your specific needs.

Collaborate approach

Our approach to purple teaming is flexible and adaptable. As testing progresses, we adjust our strategies based on real-time insights, creating opportunities for learning and enhancing both offensive tactics and defensive measures. The assessment includes continuous collaboration between the red and blue teams to develop an ongoing learning cycle.

Attack simulation

Our (red team) initiates the assessment by simulating advanced attack scenarios, including common and emerging threats. The goal is to test your network's resilience, probe for vulnerabilities, and understand how threat actors might attempt to breach your defences.

Detection and response testing

The assessment provides an opportunity to test incident response procedures. We evaluate how your team responds to different attack stages, such as lateral movement or privilege escalation, and identify areas where the incident response can be optimised.

Knowledge transfer and improvement

A significant aspect of purple teaming is continuous learning. Our experts work closely with your teams throughout the assessment, providing actionable insights and guidance to improve the overall security process. We highlight areas of improvement in both detection and response mechanisms.

Why choose Cognisys' purple team assessment?

Enhance your security strategy with our purple team assessment services. We offer a collaborative approach that empowers red and blue teams to work together in identifying and addressing security gaps. Our certified experts have a proven track record of successfully combining offensive and defensive techniques to improve network security.

With comprehensive reporting and actionable insights, we help you build a resilient, proactive defence system. Our tailored methodology ensures that the assessment aligns with your organisation's security goals and helps you stay ahead of the evolving threats.

BACK TO CONTENTS