

• ADVERSARY SIMULATION

Red Team Exercises

Test your defences.
Challenge your response.

Realistic, objective-based exercises that test how your people, processes and technology detect and respond to sophisticated attacks.

01 Emulate

Use relevant adversary scenarios.

02 Validate

Test detection and response.

03 Improve

Expose gaps in your defences.



TRUSTED SECURITY ADVISOR

Test resilience. Build confidence.

• 01 / SERVICE OVERVIEW

How would your defences handle a real adversary?

Traditional security testing does not always show how an organisation would fare against a determined attacker targeting its most valuable assets. Cyber360 Red Team Exercises emulate relevant adversaries and their tools, techniques and procedures (TTPs) to evaluate security resilience across people, processes and technology.

Objective-based

Focus on realistic attacker goals and the business assets that matter most.

Threat-led

Shape scenarios around adversaries, campaigns and techniques relevant to your industry.

Detection-focused

Evaluate how effectively your teams identify, investigate and contain attacker activity.

• 02 / ASSESSMENT FOCUS

What we evaluate

01**People**

Employee exposure, social engineering scenarios and the response of your security team.

02**Processes**

Escalation, investigation, incident handling and containment decisions during an exercise.

03**Technology**

External defences, monitoring tools, access controls and internal security boundaries.

04**Attack paths**

How controlled initial access could lead to lateral movement and elevated privileges.

05**Critical assets**

Whether an adversary could reach agreed high-value systems, information or crown jewels.

06**Detection & response**

What is detected, what is missed and how your defenders respond to the simulated threat.

CONTROLLED AND AUTHORISED

Realistic testing. Agreed boundaries.

Scope, objectives, prohibited activities, safety measures, communication protocols and emergency procedures are agreed before exercise activity begins.

• 03 / OUR APPROACH

A structured path to real insight.

A threat-led exercise, from scenario design to evaluation of your defenders.

01 Threat intelligence & profiling

Research relevant threat actors, campaigns and attack techniques to build the adversary profile for your exercise.

02 Attack scenario development

Define realistic objectives, constraints and success criteria around your organisation and its most valuable assets.

03 Rules of engagement

Agree scope boundaries, prohibited activities, safety measures, communication protocols and emergency procedures.

04 Reconnaissance & OSINT

Identify exposed assets, potential entry points and publicly available organisational, employee and technical information.

05 Initial access simulation

Test agreed entry routes, such as external vulnerabilities, phishing scenarios or simulated supply chain compromise.

06 Perimeter security testing

Evaluate firewalls, VPNs, email gateways and web filtering against techniques relevant to your threat scenario.

07 Internal reconnaissance & lateral movement

After controlled access, identify high-value targets and test internal movement while evaluating detection.

08 Privilege escalation attempts

Test whether credentials, misconfigurations or trust relationships could allow an attacker to gain higher-level access.

09 Controlled persistence

Within agreed boundaries, evaluate techniques that could maintain access across system reboots or credential changes.

10 Crown jewel targeting

Attempt to reach agreed high-value systems or data to demonstrate the potential impact of the simulated attack.

11 Detection & response evaluation

Document detection events, security-team responses and containment actions to assess monitoring, incident response and threat hunting.

THE OUTCOME

A clearer view of your actual resilience, the gaps exposed by the exercise and priorities for improvement.

Let's test your resilience.

cyber360.coinfo@cyber360.co

UK +44 20 3286 1927

UAE +971 55 768 7199