REDSCAN
A KROLL BUSINESS

Assessment services

RED TEAM OPERATIONS

Fully assess your organisation's threat detection and response capabilities with a simulated cyber-attack

A fully simulated cyber-attack

A breach by a skilled and persistent attacker could result in serious financial and reputational damage to your organisation.

A Red Team Operation from Redscan is a simulated cyber-attack designed to help you prevent this scenario by challenging the effectiveness of your technology, people and processes, and detecting gaps in threat detection and response.

What is red teaming?

An extended type of security assessment, a Red Team Operation accurately replicates the approach a sophisticated attacker could take to target your organisation and achieve their objective, such as exfiltration of sensitive data.

To be as true to life as possible, engagements are conducted over a period of weeks, and often without the knowledge of all security personnel. However, unlike malicious attacks, they are conducted to obtain insight rather than cause disruption.

KEY SERVICE FEATURES

- Intelligence-led operations designed to replicate the latest adversarial approaches
- Performed by experienced offensive security experts
- Custom engagements with a clearly defined scope and objectives
- Can include both physical and virtual intrusion attempts
- Often conducted without the knowledge of all employees
- Clear summary reports with actionable insights to enhance your security

Business benefits

Evaluate your response to attack

Learn how prepared your organisation is to respond to a targeted attack designed to test the effectiveness of people and technology.

Identify and classify security risks

Discover if systems, data and other critical assets are at risk and how easily they could be targeted and compromised by adversaries.

Uncover hidden vulnerabilities

By mirroring the latest adversarial tactics, red teaming can help identify hidden vulnerabilities that attackers might seek to exploit.

Receive help to address exposures

Benefit from post-operation support to address any weaknesses identified and mitigate the risk of real-life attacks.

Enhance blue team effectiveness

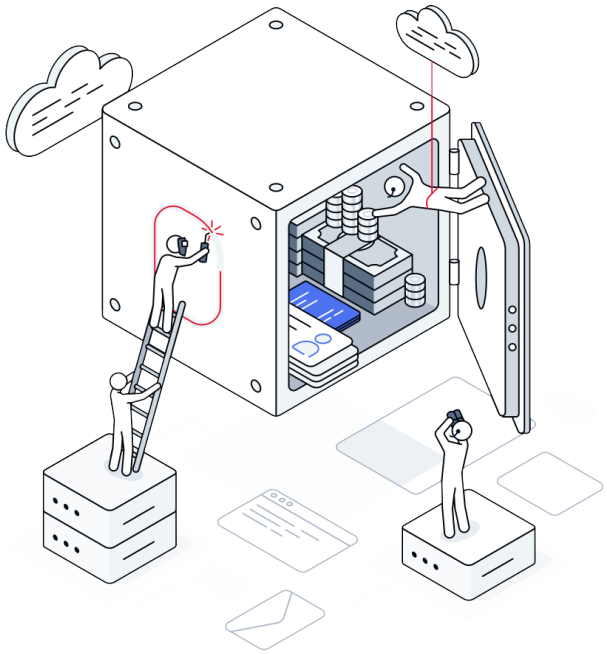
Gain insight to help your security team better identify and address gaps in threat coverage and visibility.

Prioritise future investments

Better understand your organisation's security weaknesses and ensure that future investments deliver the greatest benefit.

Example objectives of a Red Team Operation

- Gaining access to sensitive data stored in an on-premises or cloud network
- Taking control of an IoT device or critical asset
- Hijacking the account of a C-level executive
- Obtaining physical access to a server room and installing malware



Redscan's red team identified ways an attacker could breach our defences and provided help to minimise future risks."

HEAD OF IT
FTSE 250 ORGANISATION

Our intelligence-driven approach

Redscan Red Team Operations follow a systematic and intelligence-driven methodology that mirrors the latest adversarial tactics, techniques and procedures.

01 Reconnaissance	Utilising a variety of tools, techniques and resources to collect information about the target organisation and employees via publicly available sources.
02 Staging	Setting up and concealing the infrastructure and resources needed to launch attacks and can include social engineering activity and setting up servers.
03 Attack delivery	Compromising and obtaining a foothold on the target network to exploit discovered vulnerabilities.
04 Internal compromise	Achieving the objectives of the operation with activities such as lateral movement across the network, privilege escalation and data exfiltration.
05 Reporting & analysis	A final report provides an overview of vulnerabilities and attack vectors, as well as recommendations on remediating and mitigating risks.

SC 2020 awards highly commended

CYBER SECURITY EXCELLENCE AWARDS WINNER 2021

teiss Awards2020 WINNER

2020 Computing Security Awards

REDSCAN
A KROLL BUSINESS

0800 107 6098 info@redscan.com www.redscan.com