REDSCAN
A KROLL BUSINESS

Assessment services

SCENARIO-BASED TESTING

Assess the effectiveness of your security operations to defend against the latest threats

Understand how effective your security controls really are

Measuring the success of security operations on efficiency metrics alone can fail to address a key question all security leaders need to answer: how good are people and controls at preventing, detecting and responding to cyber threats?

Scenario-based testing performed by Redscan's experienced team of consultants, can help to validate the true effectiveness of your organisation's capabilities. This is achieved by simulating a wide range of adversarial tactics and providing recommendations to enhance the protection of key assets.

Evaluate against the latest tactics

A scenario-based test is designed to emulate a specific adversarial tactic, technique or procedure (TTP) that could pose a risk to the security of your organisation.

Engagements are narrower in scope than full red team operations and performed on the basis of an assumed compromise which means they're completed in days rather than weeks.

KEY SERVICE FEATURES

- Flexible engagements designed to simulate the latest adversarial tactics
- Performed by offensive security experts
- Testing aligned to phases of the MITRE ATT&CK framework
- Clear summary reports and actionable insights to improve your security
- A well defined scoping process with clear testing parameters and objectives
- Conducted to the highest technical and ethical standards

Business benefits

Identify gaps in threat visibility

Discover how prepared your organisation is to detect and respond to specific adversarial tactics and techniques.

Better understand security risks

Learn whether systems, data and other critical assets are at risk and how easily they could be targeted by attackers.

Enhance threat hunting

Improve detection of existing and emerging threats by leveraging insights to aid use case development and optimise toolsets.

Measure security effectiveness

Measure threat coverage and resilience, as well as the impact of changes to security controls and processes.

Optimise response plans

Identify improvements to incident response procedures to respond more quickly and effectively to threats.

Prioritise future investments

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

The assessments we offer

Redscan scenario-based tests are aligned to MITRE ATT&CK, a framework which outlines the methods cybercriminals use to compromise networks, escalate privileges and achieve their objectives.

Our experts will work with you to identify the TTPs that pose the greatest risk to your organisation and build the testing strategy best aligned to them. Example scenarios include:

- **A supply chain compromise**
- **Data exfiltration by an employee or contractor**
- **A spear phishing attack to harvest credentials**
- **Installation of malware**

A continuous cycle of improvement

Conducted regularly, scenario-based testing can help you to continually enhance the security of your organisation to defend against the latest threats.

"By assessing the effectiveness of our security controls to detect to a phishing attack, Redscan helped us to identify a range of improvements."

IT DIRECTOR
FSE 250 FIRM

SC 2020 awards highly commended

CYBER SECURITY EXCELLENCE AWARDS WINNER 2021

teiss Awards2020 WINNER

2020 Computing Security Awards

WHY REDSCAN?

- **A CREST-accredited cyber security company**
- **A deep understanding of how hackers operate**
- **In-depth threat analysis and advice you can trust**
- **Complete post-test care for effective risk remediation**

REDSCAN
A KROLL BUSINESS

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