REDSCAN

ASSESS

Red Team Operations

Test your ability to detect and respond to threats with a real-world cyber-attack simulation

Cybercrime targeting organisations is at an all-time high. A breach caused by a skilled and persistent attacker can result in massive financial loss and damage to your business. To understand how this could happen before it occurs, a Red Team Operation performed by experienced ethical hackers is the only viable option.

CREST

Every **Red Team Operation** from Redscan is an intelligence-led assessment aligned to the security risks your business faces. Our skilled, CREST certified operatives surpass the remit of traditional security testing to challenge the effectiveness of your organisation’s technology, personnel and processes with a highly focussed, multi-faceted attack conducted over weeks or months.

Red Team Operations can be performed to:

- Achieve an agreed objective, such as data exfiltration
- Identify the Most Dangerous Courses Of Action (MDCOA) a persistent aggressor might take
- Review physical and virtual security controls
- Test employees’ response to cyber-attacks and breaches
- Validate incident response plans
- Simulate the latest adversarial tactics, techniques and procedures, including:
    - Social Engineering
    - Phishing
    - Physical Intrusion
    - Spoofing

Redscan’s Red Team assessments have a 100% success rate.

Business benefits

- ✓ Assess and evaluate the capability of technology, people and processes to detect the latest complex attacks
- ✓ Reveal gaps in security architecture, training and policies so that new investments deliver verifiable improvements
- ✓ Test cyber defences with realistic intrusions that mimic genuine attacks from persistent and determined attackers
- ✓ Uncover and address vulnerabilities before they are exploited by malicious actors
- ✓ Receive help remediating complex security vulnerabilities, no matter the root cause
- ✓ Inform risk management decisions from boardroom to shop floor

Key features

- + Operational objectives and scope agreed with client ahead of time
- + Customisable engagements designed to mirror common attack scenarios
- + Cutting-edge tools and techniques to ensure that systems and controls are challenged
- + Experienced ethical hackers: CREST CRT, CCT APP, CCT INF, CCSAM, CCSAS, OSCP, TIGER CTM, CEH
- + Controlled and confidential engagements conducted without the knowledge of all employees
- + ‘Need to Know’ communication throughout each engagement
- + Clear and detailed summary reports suitable for technical and non-technical stakeholders

CREST

SC 2018 awards EUROPE
Winner
BEST CUSTOMER SERVICE

2018 Computing Security Awards
WINNER
Pen Testing Solution of the Year

The value of Red Team Operations

- Discover the vulnerabilities that criminals could use to obtain login credentials for IT systems
- Learn how easy it is for a hacker to access privileged client data
- Identify methods that could be used to disrupt business continuity
- Map exploitable routes and processes which provide access to IT systems and facilities
- Expose gaps in surveillance which allow criminals to operate for an extended period without detection

Our methodology

Redscan's Red Team Operations are based on a systematic and intelligence-driven methodology that mirrors the tactics and procedures of determined cybercriminals.

1. **Reconnaissance** – Collecting information about the target organisation and employees via publicly available sources.
2. **Staging** – Establishing the specialist resources necessary to conduct an attack.
3. **Attack delivery** – Compromising a network to establish a foothold.
4. **Internal compromise** – Lateral movement, privilege escalation and command and control activity.
5. **Reporting and analysis** – Presenting the lessons from the exercise in order to remediate and mitigate risks and provide advice on future improvements and investments.

Reasons to choose Redscan

- ✓ One of the highest accredited ethical hacking companies in the UK
- ✓ Complete post-test care for effective risk remediation
- ✓ In-depth threat analysis and advice you can trust
- ✓ We think and operate like genuine cybercriminals, whilst doing none of the damage

2018 Computing Security Awards WINNER

Pen Testing Solution of the Year

Safeguard your business today

Talk to our experts about a custom security assessment

EMAIL US
✉ info@redscan.com

CALL US
☎ 0800 107 6098

ONLINE
redscan.com

FAQs

What is a Red Team?

A team of ethical hackers who possess and leverage the skills, resources and mindset of cybercriminals. Thankfully they're on your side and use their wealth of experience to test the effectiveness of your organisation's security by performing a simulated cyber-attack.

How long does a Red Team Operation last?

The duration of a Red Team Operation is dependent upon the scope and objective(s) of the exercise. A full end-to-end red team engagement is typically performed over one to two months, however specific scenario-based operations with a narrower focus can be performed over 11-18 days. Shorter operations, such as those designed to simulate insider threats, are usually based on an assumed compromise.

How does a red team assessment differ from a pen test?

A penetration test is a form of ethical hacking focussed on identifying security vulnerabilities that could allow an attacker into your network at a given point in time. A red team assessment is a longer, more extensive engagement that simulates a genuine cyber-attack, and is focussed on validating the effectiveness of organisations' breach detection and response capabilities.

How often should a Red Team Operation be conducted?

At key junctures in the development of your organisation; if one has never been conducted before and if there have been significant changes in policy, personnel or structure.

What happens after the operation is completed?

A full report on the engagement is presented, detailing the success of the operation and all vulnerabilities observed and exploited. Advice is given via an included telephone debrief. Upon request, debriefing sessions can be provided to key stakeholders.

CREST

SC awards 2018 EUROPE Winner BEST CUSTOMER SERVICE

2018 Computing Security Awards WINNER Pen Testing Solution of the Year