Red Team Assessments

A RICOH Company

With cyber security threats intensifying all the time, organisations cannot afford to be complacent about their security environment. Even if they have undergone regular IT health checks and are confident their systems are up to date and policies are secure, there is always room for improvement.

Red Team testing is designed to test the security infrastructure and processes of your organisation as a whole. It is not restricted to cybersecurity but also applies in areas outside of the traditional technical security arena, utilising a variety of techniques including penetration testing, social engineering and physical security testing.

The Service

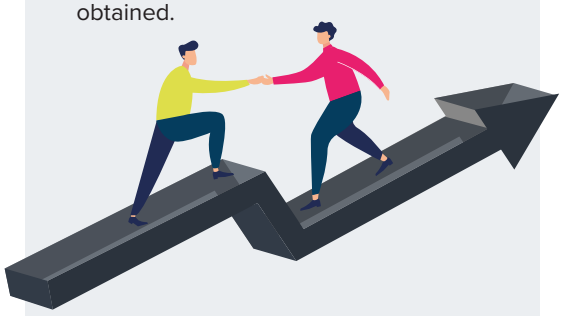
Conducted by seasoned penetration testers, our Red Team Tests are designed to probe your organisation for areas where a malicious user could gain trust where none should be given, access areas or materials intended for restricted groups and exert control over privileged processes and systems.

The tests accurately replicate the techniques, tactics and procedures used by criminal gangs, opportunist attackers and nation states. We test your overall security from the perspective of a malicious threat actor, including the use of home-grown techniques and customised scenarios developed over many years in red teaming and social engineering.

Stage 1
Reconnaissance

The reconnaissance phase of a red team attack seeks to develop an attack profile by locating the weak points in an organisation and uncovering additional information of the highest value attack vectors.

Open-Source Intelligence (OSINT) gathering is conducted to ascertain public domain information on the target organisation. Specific information on staff, such as email addresses and telephone numbers, is useful to an attacker when performing a remote social engineering exercise. Other useful information, such as publicly available information on IP address ranges, software versions, DNS records and the technologies in use on publicly facing applications, will also be obtained.



Stage 2
Gaining Access

Once a profile has been built on your organisation's attack surface, an attacker will attempt to gain access to the organisation physically or remotely.

The attack methodology created by the consultant based on the services and technologies you have in use is likely to include a combination of the following: phishing attacks, Red Team attacks, telephone or physical social engineering attacks, VPN bypass attacks, password guessing, wireless attacks and employee impersonation attacks.

Simulated attacks will cover the five scenarios that comprise the tabletop assessment of your Incident Response Plan (IRP):

Small Ransomware Outbreak: An employee visited a trusted website frequently used within the aerospace and defence industry, and downloaded a file they thought was an information file required for their job.

Phishing campaign and Malware: The Finance Team has been targeted with a Spear Phishing email containing a PDF purporting to show details of a recent payment adjustment.

Data Breach, involving physical intrusion and unauthorised system access: During a review of the system logs, the IT team discovers an employee has been logging into the system at odd times of the night and on days when they should not be working.

Large Ransomware outbreak: Members of the HR team have received a number of emails from an unknown attacker threatening to access systems and steal/encrypt sensitive data. It is not known who the attacker is and how they plan to attack.

Invoice Fraud and Email Compromise: The Finance team is alerted after a customer makes contact querying an email containing new payment directions.

Contact MTI
T: +44 (0) 1483 520 200
E: ukmarketing@mti.com
W: mti.com

Datacentre Modernisation
Data & Cyber Security
Managed Services
IT Transformation

Stage 3
Exploit and Compromise

Once access has been gained, the final phase of the assessment will cover lateral movement within the network, escalation of privilege and account compromise and the installation of an executable representative of ransomware.

MTI uses information from the reconnaissance phase to attack users and services (in a safe and controlled manner) and gain a foothold on the network. We will locate and attempt to exfiltrate data and install safe executable files onto servers and hosts. This will highlight the level of access obtained and the risk if the executable file had been ransomware.

This exercise is designed to test monitoring and alerting to determine if the attack has been detected and that SOC teams carried out the relevant actions and responses. Successfully bypassing monitoring will highlight gaps in coverage and procedures.

Outcomes & Benefits

Red Team Testing delivers the following outcomes:

- Provides intelligence on physical and logical security gaps.
- Identifies and addresses weaknesses in incident response.
- Identifies remediation options to address issues in the most effective manner.

Deliverables

Red Team Testing provides:

• A Phishing/Red Team assessment with the focus on ransomware attacks.

• A full timeline of events outlining every action performed with the date and time to track attacks back to network monitoring tools or SOC/SIEM capabilities and understand why they were or were not detected.

• Full detailed technical findings, evidence and recommendations.

Why MTI?

A longstanding member of global cyber security bodies, CREST and CHECK, MTI has the security expertise and experience to help you deal with a wide-ranging number of threats and attacks. As one of the first companies to provide penetration testing services, we have developed a wealth of knowledge and skills in the tactics used by malicious users to gain access to corporate networks. This enables us to identify risks to your organisation and outline remediation measures to counter those risks.

Our aim is to provide greater security without sacrificing functionality in any given environment.

MTI has supplied penetration testing services to local and central government, Critical National Infrastructure within the NHS and utilities sectors, the Ministry of Defence, the private sector, and companies affiliated with the US Department of Defense.

"MTI have been our cyber security partner for several years. The commercial support they give to allow us to deliver an effective programme of external assurance has been great. Penetration testing engagements are carried out efficiently and to a high standard, with the testers having an impressive range of skills and knowledge. We were particularly impressed with a recent test of one of our web applications where the tester carried out tests which were 'outside of the box' and took time to explain the findings.

In a recent engagement, the team adapted well to our feedback over the design and delivery of some exercising scenarios, providing timely responses and changes to enable a successful outcome."

Josh Evans
Cyber Security Analyst
Anglian Water Services Limited

Contact MTI
T: +44 (0) 1483 520 200
E: ukmarketing@mti.com
W: mti.com

Datacentre Modernisation
Data & Cyber Security
Managed Services
IT Transformation