Service Definition
Red Team Assessment

Introduction

Organisations across commercial, government, and critical national infrastructure (CNI) sectors face increasingly sophisticated cyber threats. Traditional testing is essential, but true resilience depends on how effectively your organisation can detect, respond, and recover from a real adversary.

Intertek's Red Teaming service provides a controlled, intelligence-driven simulation of real-world cyber attacks, giving a complete assessment of your organisation's security posture and readiness.

Scoping

Although Red Teaming is related to penetration testing, there are fundamental differences between the two disciplines: Red Teaming is not simply a more thorough or in-depth penetration test, and organisations conducting Red Teaming should already be conducting regular penetration tests and implementing the agreed remediation plans to gain the most benefit from the exercise. A Red Team exercise may start with an initial threat intelligence phase in conjunction with the organisation and uses this information to develop scenarios and draft a test plan; depending on the requirements of the organisation.

This threat intelligence information is passed to the Red Team who will then use it to attempt to penetrate the organisation's defences using the agreed scenarios and test plans. This provides a realistic simulation of an actual attack which gives an accurate assessment of the organisation's defences and their detection and response capability. This test of the organisation's detection and response to an incident is just as important as the test of the defences because the ubiquity of data breaches across all sectors shows that relying on good defences to stop all attacks is naive; rapidly detecting and responding to a breach is essential to robust cyber security.

Service Overview

Realistic Adversary Simulation

Intertek emulates the tactics, techniques, and procedures (TTPs) of genuine threat actors. Our experts conduct OSINT (Open-Source Intelligence) to identify publicly available information that could be leveraged. This intelligence drives targeted phishing and vishing campaigns, leading to covert intrusion—through external compromise, assumed breach scenarios, or insider-threat pathways—followed by lateral movement and data exfiltration.

The engagement mirrors the full adversary kill chain, showing how an attacker would plan, progress, and operate within your environment.

Common techniques tested include:

- Reconnaissance and OSINT collection
- Phishing and vishing campaigns
- Compromise, escalation, and persistence
- Lateral movement and data exfiltration

Test Your Detection and Response

Only a small group of senior stakeholders are made aware of a Red Team engagement, ensuring your SOC, blue team, and wider IT functions respond authentically.
Intertek evaluates your organisation's ability to:

Service Definition
Red Team Assessment

- Detect malicious activity and anomalies
- Escalate incidents through proper channels
- Coordinate rapid and effective response
- Contain and recover from attacker activity

Tailored Threat-Led Scenarios
Intertek offers Red Teaming in two formats:

- **Consultative** – collaboratively shaping scenarios based on threat intelligence and organisational risk
- **Black-box** – fully covert assessment with zero prior knowledge for the most realistic testing

Evidence-Based Reporting
Our reporting provides actionable insights, documenting every Red Team action and mapping activity directly to **MITRE ATT&CK**. This highlights detection gaps, defensive blind spots, and priority areas for improvement across the kill chain.

Strengthening Organisational Resilience
Intertek's Red Teaming equips organisations with the insight needed to strengthen defences, improve incident response capability, and build confidence that they are prepared for real cyber attacks.

Take the next step in cyber resilience today, to explore a Red Teaming assessment and see how your organisation performs under simulated real-world attacks.

Deliverables
Throughout the duration of the exercise, Intertek NTA will provide regular updates to appropriate staff with relevant findings, summary of activities to date, progress/completion status of phase tasks/activities together with further details of any significant vulnerabilities identified.

Upon completion of all phases, a formal report will be provided with full details of the tasks outlined in the initial penetration test plan, the activities performed against these tasks, success status against defined objectives/threat scenarios, vulnerabilities identified with risk severity classification (High/Medium/Low) and supporting evidence (such as the cyber kill chain) plus recommendations and solutions for fixing issues identified. The report will also provide comment on the responsiveness of the organisation's detect and response team (Blue Team).

The engagement will conclude with a final presentation of findings to senior management with anecdotal evidence of findings easily interpreted by a non-technical audience and detailing business and operational impact with clear suggestions for addressing problems found.

Service Management
You will be appointed a dedicated account manager and provided with points of contact for commercial and technical questions, to ensure that the service is properly executed.

Service Definition
Red Team Assessment

Intertek NTA has a Service Level Agreement that is monitored by a R.A.G system to ensure that delivery standards are met on all projects. The SLA includes timeframes for project delivery with technical staff working to targets to ensure that deadlines are met.

Additionally, Intertek NTA has a customer services department that is responsible for the key administrative aspects of delivery such as liaising with you to confirm site details, scheduling the test, ensuring reports are sent out in a timely manner, scheduling follow up tests and debriefs etc. This is documented and monitored through the use of an internal database system, and links into other key processes regarding the correct method of sending the report according to the protective marking of the contents.

Information Assurance
Intertek NTA is security cleared to perform information security testing services on infrastructure, platforms or software containing data protectively marked up to OFFICIAL-SENSITIVE

Ordering and Invoicing Process
Once the scope of work and number of units/days required has been agreed between the customer and Intertek NTA, a valid purchase order is required to enable scheduling and delivery.

An invoice will then be raised upon delivery of the service.

Customer Responsibilities
The customer is responsible for engaging with Intertek NTA to discuss perceived threat vectors, actors/agents and agreeing targets of interest for the engagement.