Service Definition

Ransomware Resilience Assessment

Introduction
Ransomware Resilience Testing is a specialist cyber security service designed to assess an organisation's ability to detect, prevent, respond to, and recover from a real-world ransomware attack.

Scoping
Each Ransomware Resilience Testing engagement is individually scoped to ensure it reflects the organisation's risk profile, operating environment and business priorities, while remaining safe, controlled and proportionate.

Service Overview
Unlike traditional penetration testing or compliance-driven assessments, this service actively simulates modern ransomware operations across the full attack lifecycle. Using real attacker techniques, tactics and procedures (TTPs), the service provides clear evidence of whether security controls work in practice, under pressure, rather than in theory.

The service focuses on proving organisational resilience by replicating the behaviour of known ransomware groups, from initial access through lateral movement, data exfiltration and attempted encryption, while working closely with defensive teams to maximise learning and improvement.

The service delivers a targeted, intelligence-led ransomware simulation, including:

- Bite-sized red team testing using a CBEST-aligned approach, focused specifically on ransomware threats
- Realistic replication of current ransomware group techniques based on detailed threat intelligence
- End-to-end testing of the ransomware kill chain, from initial compromise to attempted impact
- Active testing of technical controls, people and processes — not policy review or consultancy
- Close collaboration with the organisation's SOC and security teams using a purple team approach
- Clear identification of where defences successfully prevented attack progression and where controls failed

The outcome is a practical, evidence-based assessment of ransomware resilience.

Benefits
- Provides proof of resilience, not assumptions or theoretical risk
- Identifies real attacker paths through complex, layered security environments
- Focuses security investment on controls that materially reduce ransomware risk
- Improves detection and response capability through hands-on defender collaboration
- Reduces the likelihood and impact of ransomware-related downtime, data loss and recovery costs
- Strengthens organisational confidence against sector-specific ransomware threats

Service Definition

Ransomware Resilience Assessment

Deliverables

- Delivered by experienced offensive security specialists using current threat intelligence
- Testing is scoped collaboratively to align with business priorities and risk appetite
- Conducted safely to avoid disruption to live services
- High levels of engagement with internal security teams throughout the exercise
- Findings are validated and discussed in real time where appropriate

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.

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.