
# Red Team Assessment

## Service Definition Document

January 2026

HM Government
G-Cloud
Supplier

# Document Control

| | | | |
|---|---|---|---|
| **Document Type** | Confidential - Customer Facing | | |
| **Company** | Maple Networks | | |
| **Address** | The Print Rooms<br>164/180 Union Street<br>London<br>SE1 0LH | | |
| **Primary Contact** | Graham Tetley | **Role** | CTO/Lead Consultant |
| **Phone Number** | 020 3858 0048 | **Email address** | gt@maple-networks.com |



# Revision History

| Issue Date | Author | Version | Revision Description |
|---|---|---|---|
| 24/06/2025 | Jonny Zammer | 0.1 | Initial Draft |
| 29/10/2025 | Jasmine Gillard | 0.2 | Updates for G-Cloud 15 |
| 29/01/2026 | Tim Luck | 0.3 | Updates for G-Cloud 15 |
| 30/01/2026 | Jonny Zammer | 1.0 | QA & Release |

HM Government
G-Cloud
Supplier

# Table of Contents

## Contents

HM Government
G-Cloud
Supplier

# Services Overview

The growing speed, scale, and sophistication of cyber threats mean that traditional testing methods are no longer enough. Adversaries today use complex, multi-stage operations that exploit weaknesses across people, process, and technology.

Red Teaming provides organisations with a proactive, high-fidelity way to understand their true defensive readiness. By emulating real-world attackers and their tactics, Maple's Red Teaming exercises expose the *actual* paths an adversary could take to achieve business-critical objectives—helping you strengthen your defences before a real attack occurs and provides you with a unique insight into how your security and IT teams would perform under pressure.

Unlike standard penetration testing, which focuses on finding and reporting vulnerabilities, Red Teaming aims to answer broader business questions:

- *If we were targeted by a sophisticated adversary, what could they achieve?*
- *Are we truly protecting the Crown Jewels?*
- *Would we detect and respond effectively?*
- *What is the real-world impact of a successful attack?*

What Red Teaming can achieve that a traditional penetration testing cannot is the human element of your security infrastructure. Red Teaming will evaluate how your security and IT staff respond to subtle or evolving threats in a realistic scenario, to uncover gaps in awareness, coordination, and endurance that traditional infrastructure tests cannot. This highlights areas for training or process refinement, and gives organisations direct data to address performance issues, or reward quality work.

HM Government
G-Cloud
Supplier

# Service Description

Red Teaming is an end-to-end attack simulation designed to evaluate your organisation's susceptibility to cyber attack. It spans the full lifecycle of an intrusion—from reconnaissance through exploitation to achieving defined objectives such as data exfiltration or operational disruption.

Key characteristics of a Red Team exercise:

- Objective-focused: Designed around realistic business-relevant goals (e.g., gaining access to sensitive financial data or critical systems).
- Threat-led: Uses tactics, techniques, and procedures (TTPs) observed in real threat actors targeting your industry.
- Adversarial and covert: Conducted from the perspective of an external attacker, operating stealthily to test detection and response.
- Authentic and realistic: Designed to simulate the pressure and ambiguity of a real-world cyber incident.

Maintaining the covert element of a Red Team assessment is crucial for valid results, and the organiser for the assessment should assume the role of an *insider threat* for the purposes of authenticity, limiting communication and the spread of information to a very limited amount of people.

Effective Red Teaming mirrors real adversaries. Maple's approach models diverse threat actors, including:

- Nation-state actors – intelligence, sabotage, espionage
- Organised crime groups – ransomware, extortion, fraud
- Hacktivists and competitors – reputation or IP-driven attacks
- Insiders – accidental or malicious misuse

Each simulation is tailored to your threat landscape, aligning testing priorities with business risk.

**High-Level Engagement Models:**

Depending on your maturity, Maple offers several Red Teaming models:

| *Approach* | *Description* | *Best suited for* |
|---|---|---|
| Black Box Testing | A fully covert, external simulation without prior knowledge of your systems. Tests real-world exposure and external resilience. | Mature organisations with established security monitoring. |
| Scenario-Based Testing | A controlled, goal-oriented simulation based on defined attack scenarios. | Organisations ready to test specific business processes or assets. |
| Assumed Breach Testing | Starts with the premise that an attacker already has limited access. Focuses on internal movement, escalation, and detection. | Teams wanting to measure internal detection and containment capability. |
| Threat Intelligence-Led Testing | Simulations based on current, sector-specific threat intelligence (aligned to DORA, TIBER-EU, and other frameworks). | Regulated or high-risk organisations seeking compliance and assurance. |

HM Government
G-Cloud
Supplier

## *Service Package*

| | |
|---|---|
| **Objective** | To identify and safely exploit security weaknesses to improve an organisation's resilience and validate the effectiveness of its people, process, technical controls and overall security of its wider attack surface. |
| **Description** | Maple Networks' Red Team service provides a practical, goal-orientated assessment of an organisation's full attack surface. Our consultants emulate real-world adversary techniques to discover weaknesses across infrastructure, applications, cloud environments, social engineering and physical security to identify and demonstrate the business impact of those weaknesses. Every engagement is tailored to the client's environment, technology stack and objectives, so the exercise delivers meaningful validation rather than a tick-box exercise. |
| **Supported from** | Remotely, or on-site. |
| **Testing Areas** | Our Red Team engagements simulate goal orientated adversaries against an organisation's full attack surface. Typical in-scope areas include external facing assets, internal networks reached via pivoting, web applications and APIs, cloud platforms (such as AWS, Google, Azure, O365), wireless and IoT, social engineering (including phishing, vishing and physical intrusion tests) leading to insider threat assessments. |
| **Process** | All engagements start with a scoping exercise to define and agree the objectives, goals, scope, and identify constraints and exclusions. A statement of work and/or Rules of Engagement is issued and signed, these documents cover the agreed scope, exclusions, communication plan, testing window, escalation and emergency contacts, permitted techniques and abort procedures. A technical call prior to the engagement confirms readiness to avoid any delays to the assessment.<br><br>Red teaming engagements start with detailed reconnaissance against the agreed scope to gather and build a complete picture of the target environment. Reconnaissance includes mapping the external footprint and service exposure, harvesting publicly available details on staff, suppliers, offices and any relevant information for targeted social engineering attacks or to help identify likely entry points and escalation opportunities. This phase informs the operational phase and helps prioritise the most realistic and impactful attack paths. Once the reconnaissance phase is over, a call is arranged between the technical staff and the client to ensure all identified targets remain in scope.<br><br>The next stage would largely depend on the results from the reconnaissance phase and what types of testing are in-scope. Initial access may be attempted through targeted phishing, vishing or physical intrusion. Exploitation of exposed services, such as public-facing infrastructure, web applications, API and/or cloud services would be tested extensively to identify exploit paths toward a foothold. Once a foothold is established the assessment moves into attempting persistent access, lateral movement and privilege escalation to emulate attacker progression. |
| **Output** | **Report**<br>Upon conclusion, Maple delivers a concise executive summary and a detailed technical report that documents the timeline of the engagement, evidence, MITRE mappings, IoCs and remediation actions. Every finding |

HM Government
G-Cloud
Supplier

| | |
|---|---|
| | includes a detailed technical summary, impact, proof of concept, reproduction steps and remediation advice.<br><br>**Debrief**<br>The testing team provide a debrief to provide clarity to the technical team and allow for any questions or queries from the client.<br><br>**Retest**<br>On request, Maple can provide a focused retest to verify remediation of critical gaps of previously exploited paths. |