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 164/180 Union Street London 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 and Release

HM Government
G-Cloud
Supplier

Table of Contents

Contents

Document Control ***2***
Revision History ***2***
Table of Contents ***3***
Services Overview ***4***

Service Description **5**

Maple Networks Penetration Testing Services **5**
Service Overview 5
Service Package 6

HM Government
G-Cloud
Supplier

Services Overview

Maple Networks are next generation Digital and IT service provider in the UK, with skills in various areas across the digital landscape. Maple Networks have developed a range of services to support customers in their digital, data and business transformations.

This Document provides overview service definition information for the Maple Networks Purple Teaming service.

HM Government
G-Cloud
Supplier

Service Description

Maple Networks Purple Teaming

Modern cyber threats evolve faster than most organisations can adapt. Traditional red and blue team exercises – while valuable – often operate in silos: one focused on breaking in, the other on defending. The result is insight without integration, and detection without improvement.

Purple Teaming bridges this gap. It's a collaborative, intelligence-led approach that unites offensive (Red Team) and defensive (Blue Team) experts to continuously test, measure, and enhance an organisation's detection and response capabilities. Purple Teaming represents the next evolution of cybersecurity maturity. It shifts organisations from reactive defence to proactive resilience by combining technical realism with measurable improvement.

At Maple, we believe that true cyber readiness is built through collaboration, transparency, and iteration and our Purple Teaming philosophy focuses on one outcome: turning findings into measurable, repeatable improvement.

In practice, this means:

- Offensive experts simulate real-world attack tactics (mapped to frameworks like MITRE ATT&CK).
- Defensive experts observe, detect, and respond in real-time.

Both teams share insights immediately — adjusting controls, tuning alerts, and refining playbooks as they go. The result is a continuous improvement cycle that makes security measurable and resilient.

Service Overview

Purple Teaming isn't a one-off exercise — it's a continuous learning loop designed to evolve with the threat landscape.

Effective Purple 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.

This is achieved by structuring engagements around:

- Threat-informed defence: Using real adversary tactics to guide testing.
- MITRE ATT&CK mapping: Every attack technique is tied to known TTPs for measurable coverage.
- Automated Breach & Attack Simulation (BAS): To scale and repeat scenarios reliably.
- Continuous feedback: Findings are validated, implemented, and re-tested until the desired outcome is achieved.

HM Government
G-Cloud
Supplier

Service Package

Objective	To collaboratively test, measure, and enhance an organisation's cyber detection and response capabilities by uniting offensive and defensive teams in a structured, intelligence-led improvement cycle.
Description	Purple Teaming combines real-world attack simulation with live defensive monitoring and joint analysis, enabling organisations to validate controls, tune detections, strengthen playbooks, and build measurable resilience against modern threats. Maple's approach aligns attack techniques to MITRE ATT&CK and focuses on continuous improvement rather than one-off testing.
Hosted In	Typically delivered remotely or on-site, with testing conducted against the client's live, staging, or controlled environments depending on scope and risk appetite.
Supported from	Supported by Maple's CREST-accredited Red Team, Blue Team, and 24/7 SOC analysts, leveraging real-world threat intelligence and active incident response experience.
Testing Areas	Scenarios would include (but not limited to): • Phishing and credential theft • Endpoint detection and response validation • Active Directory and privilege escalation • Lateral movement and persistence • Web application/API exploitation • Data exfiltration and loss simulations MITRE ATT&CK technique coverage and detection mapping
Process	• **Scoping & Threat Mapping** – Define goals, adversary profiles, and relevant attack techniques. • **Simulation** – Red Team executes realistic, threat-aligned attack paths. • **Detection & Response** – Blue Team observes, detects, and responds in real time. • **Collaboration & Tuning** – Both teams share insights, adjust controls, and refine playbooks. • **Validation** – Re-test improvements to confirm effectiveness. • **Iteration** – Repeat cycles to drive measurable uplift in detection and response maturity.
Output	**Report** A detailed report including MITRE-mapped findings, validated detections, prioritised remediation actions, measurable improvements (MTTD, MTTR, coverage metrics), and a roadmap for continued capability development. **Debrief** The testing team provide a debrief to provide clarity to the technical team and allow for any questions or queries from the client. **Retest** • On request, Maple can provide a focused retest to verify remediation of critical gaps of previously exploited paths.