Penetration Testing as a Service (PTaaS)

Service Definition Document

January 2026

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**	gtetley@maplenetworks.co.uk

Revision History

Issue Date	Author	Version	Revision Description
14/05/2022	Rebecca Gilmour	0.1	Initial Draft
18/05/2022	Rebecca Gilmour	1.0	Final Release
01/05/2024	Jonny Zammer	1.01	Updates for G-Cloud 14
05/05/2025	Jonny Zammer	1.02	Updates for G-Cloud 15
19/08/2025	Graham Tetley	1.02	Updated for PTaaS
08/01/2026	Jasmine Gillard	1.03	QA

Table of Contents

Contents

Service Overview

Maple's Penetration Testing as a Service (PTaaS) supports the delivery of continuous, on-demand security testing. Unlike traditional point-in-time pen tests, Maple's PTaaS provides continuous security testing, identifying exploitable weaknesses, providing proof of impact, prioritising remediation by attack path, and verifying fixes through instant retesting.

Maple's service supports the delivery of recurring autonomous and human-assisted testing, integrated reporting, exploit proof, remediation guidance, and re-test validation. To deliver these capabilities, Maple Networks leverages the Horizon3 NodeZero platform, enabling autonomous, repeatable security validation that identifies real-world attack paths and supports continuous assurance throughout the year.

The service enables organisations to:

- Continuously validate security posture against evolving threats.
- Prove compliance with frameworks such as UK NCSC CAF v4.0, NIST CSF, and PCI DSS.
- Reduce mean time to remediate (MTTR) vulnerabilities.

All penetration testing activity is delivered by CREST-certified consultants, and all Maple Penetration Testing services are accredited by CREST. Ensuring recognised industry standards of technical assurance and reporting quality.

Service Scope

This chapter identifies and describes the high-level components that make-up the service, which comprise the:

- Service package – which defines the service, capabilities and options
- Service platform infrastructure - which defines the service delivery mechanism
- Supporting services - any processes or resources that support the delivery of the service

Service Package

Objective	• Identify and validate exploitable vulnerabilities across external, internal, cloud, and identity surfaces. • Provide exploit proof and risk-context reporting to prioritise remediation. • Support compliance assessments (CAF 4.0, NIST, PCI DSS, ISO 27001) through structured evidence packs. • Continuously validate that fixes are effective using the fix-verify loop. • Reduce reliance on point-in-time pen testing and enable continuous assurance.
Description	Maple's service delivers recurring autonomous and human-assisted testing, integrated reporting, exploit proof, remediation guidance, and re-test validation. The service enables organisations to: • Continuously validate security posture against evolving threats. • Prove compliance with frameworks such as UK NCSC CAF v4.0, NIST CSF, and PCI DSS. • Reduce mean time to remediate (MTTR) vulnerabilities.
Service Scope	• External Infrastructure: Internet-facing assets, SaaS, and third-party exposures. • Internal Infrastructure: Privilege escalation, lateral movement, segmentation validation. • • Cloud & Identity: IAM roles, misconfigurations, MFA resilience, overprivileged accounts. • Detection Validation: Mapping activity to MITRE ATT&CK to test SOC detection and alerting. • Web Applications: OWASP Top 10 Testing including SQLi, XSS, CSRF, IDOR. Authentication and Session Handling Testing. Business Logic Abuse and Input Validation. API and Microservice Endpoint Security Review. • AI Penetration Testing • Autonomous Penetration Testing • Horizon3 NodeZero Platform
Hosted-in	Remote
Supported from	All support and management are delivered remotely from the Maple Networks 24x7x365 Security and Network Operations Centre

Support level	The Maple Networks service includes the following support levels on the platform: • Onboarding • Training on how to use the platform • Review of testing outputs (including manual testing verification by a certified Penetration Tester). • Support with remediation guidance • Support with remediation delivery (service Uplift) The level of support per customer will be customised and specific to each individual customer.
Required connection types	The Maple Networks service requires internet connectivity. Maple will establish a remote session to customer environments by a pre-determined method suitable for both parties. All connections are encrypted over the public internet.

Service Features

	Description	Standard / Optional / Customisations
Rapid onboarding	A key pillar of the **Maple PTaaS** service is for organisations to be able to take advantage of, and gain value from the service as quickly as possible. Upon completion of signature of the support contract and all prerequisites (identified in onboarding documentation) being completed. Maple will aim to have the platform up and running within 3 working days.	Standard
Account Test Lead	**Maple PTaaS** will provide each organisation with access to a pool of experts as well as an aligned Account Test Lead. The A ccount Test Lead will be there for multiple purposes which includes: • A dedicated Maple contact in the event of a major test being carried out • A technical escalation point for remediation • Direct point of contact for any queries and guidance regarding major changes and projects with the customer The Account Test Lead will be assigned during the onboarding.	Standard
Portals	All customers will be provided with access to an online custom portal where tests can be scheduled and outputs reviewed. An ITSM support portal where incidents, changes and service requests can be logged will also be provided. The portal will be available 24x7 and calls will be handled 24x7 in accordance with their priority and the aligned SLA.	Standard
Escalation Path	**Maple PTaaS** comes with multiple escalation paths as standard within the service. **Technical Escalation Path** • Testers • Account Test Lead • CTO **Commercial and Operational Escalation Path** • Account Manager • CEO Escalation paths and contact details will be clearly defined and onboarding. A Service Operations Manual will be defined with contact details, escalation path for both parties. It will also include any pre-authorised remediation activities. This will be review during regular	Standard

	service reviews.	
Support	**Maple PTaaS** is a service delivered by highly skilled and certified testers. Every organisation is different therefore the service can be customised to meet the requirements of each individual organisation. This can include: - **Subject Matter Expert (SME) Tester Review** • Maple PTaaS becomes an extension of the internal team and delivers an additional layer of review and contextualisation of the report output. • Maple will review all outputs and provide advice and guidance on prioritisation of remediation activity. • Maple will, where required, complete additional manual testing to complement the PTaaS offering. **<u>Optional Uplift</u>** **Proactive Remediation Support** • Maple PTaaS will provide remediation support, upon approval from the internal team Maple will carry out remediation activities on behalf of the internal team. • Upon completion of remediation, Maple will carry out any retests on Critical and High vulnerability remediations. • Maple PTaaS proactive support will also include SME support in the event escalation is required. Operational processes and procedures will be agreed and documented during the onboarding process, allowing for a bespoke service for each organisation.	Customisation

Technical Features

	Description	Standard / Optional / Customisations
Autonomous Pentesting	PTaaS runs safe, repeatable tests without requiring custom payloads or agents.	Standard
Exploit Proof	Safe evidence (screenshots, captured tokens, impact demonstration).	Standard
Fix-Verify Loop	Automated retesting validates remediation success.	Standard
Risk Prioritisation	Attack-path context ranks issues by exploitability and impact.	Standard
Executive Dashboards	Board-ready reporting with trending and compliance mapping.	Standard
SOC Validation	Test SOC performance against real-world attacks mapped to MITRE ATT&CK framework.	Standard
CAF 4.0 Alignment	PTaaS results mapped to CAF principles and contributing outcomes.	Standard

Supporting Services

Maple Networks Service Desk	• Provides 24x7x365 support and management of the service and supporting infrastructure. • Handles events, requests, queries and incidents raised by authorised users only, whether by phone, e-mail or self-service support portal. • Handles Change Requests (CR) in accordance with Maple Networks' Change Management process. • Resolves problems with, applies changes to and maintains the patch state of, the service platform in accordance with Maple Networks' change management process. • Makes configuration changes on request (for example, changes to in scope infrastructure).
Maple Networks Self Service Support Portal	Maple Networks will provide customer-nominated administrators with access to a Self-service support portal through which they can: • Request additional scope to be configured. • Create new and update existing incidents for investigation. • Create new and update existing changes from a change catalogue. • See additional services that can be onboarded.

Roles and Responsibilities

The following chapter identifies the high-level roles and responsibilities of the service; all responsibilities are subject to change throughout the term of the service and will be mutually agreed by both Maple and the partnering organisation:

Item	Maple / Partner Organisation / Shared
Scope Definition	Partner Organisation
Testing Windows	Partner Organisation
Test Scheduling	Shared
Change Controls	Shared
Initial Output Review	Shared
Detailed Output Review	Maple
Additional Testing (Manual)	Maple
Maintenance of Platform	Maple
Remediation Action	Shared (Depending on Maple's access to environment)

Available Service Levels

This chapter identifies the service level measures applicable to the service.

Test Frequency	• On-demand • Scheduled (monthly/quarterly) • Continuous
Report Delivery	• Initial results within 24 hours post-test • Fully review reports within 5 business days
Critical Findings Alerts	• High-severity exploit notifications delivered within 24 hours
Tester Support Hours	• Standard business hours (09:00–17:00) • 24/7 available on premium tier

Incidents, Service Request and Changes

Customers should consider these measures in the context of the general terms and conditions described in full in the Maple Networks Service Level Agreement document (available on request).

Response time	**Incidents** • P1 • P2 • P3 • P4 **Changes** • Standard • Normal • Emergency **Service Request**