Service Description

Threat and Vulnerability Management (TVM)
August 2025

transparity

Contents

1. Service Overview

The Transparity Threat and Vulnerability Management service delivers a proactive cybersecurity solution that combines advanced technology, expert analysis and support in prioritising vulnerability patching and risk mitigation. The service scans your public facing and internal digital environments for known vulnerabilities helping you minimise downtime, costs, and improve your compliance requirements - Cyber Essentials and other frameworks.

Additional information may be included in your Order Form or Statement of Work.

2. Service Features

Feature
Threat and Vulnerability Management (TVM)
Platform Maintenance
Threat Advisories
Security Reporting
Rapid Onboarding

2.1 Threat and Vulnerability Management (TVM)

On a monthly cadence, Transparity's expert-level security team will perform the following activities:

- A vulnerability assessment of your network-connected assets across public, private and OT / IoT networks (depending on the agreed scope)
- Vulnerability analysis and prioritisation
- Our Cyber Security Consultants will work in collaboration with your technical team to provide guided remediation of high and critical vulnerabilities on a rolling top 10 basis each month

This service utilises industry standard tooling, which can be deployed using our Secure by Default security blueprints or aligned to our blueprints if already in production and maintained as part of the service.

This service includes change control and product support for our preferred Threat and Vulnerability Management tooling.

2.2 Platform Maintenance

Transparity's security teams constantly review recommendations from industry standard security governing bodies such as the NCSC, CIS, NIST, CISA, and MITRE. They also review and test product enhancements, improvements and features from our preferred Threat and Vulnerability Management tooling. The results of these reviews drive our security blueprints.

This service ensures that the deployed Threat and Vulnerability Management tooling is continually aligned to our Secure by Default blueprints[1] ensuring that your organisation is benefitting from an evergreen security configuration, rather than a set-and-forget approach to product maintenance.

The core product(s) will be enabled / deployed into production (green field) or realigned to our security blueprint framework if already deployed (brown field), enabling you to onboard your devices.

[1] Customer can choose to opt out of the security blueprint alignment if required and will be logged on the Risk Register.

2.3 Threat Advisories

Threat advisories are reports that provide information about significant new trends or developments regarding potential or existing cyber threats, including analytical insights into the tactics, techniques, and procedures (TTPs) of adversaries.

This service offers detailed reports and advisories for impactful and emerging threats being tracked by our SOC.

2.4 Security Reporting

Providing holistic visibility into the status of your organisation's security service through robust reporting (where tooling is deployed and managed within this service) monthly.

2.5 Rapid Onboarding

This service offers rapid deployment of the required security tooling into production (green field), or realignment to our security blueprints if already deployed (brown field), protecting your organisation from cyber threats and providing visibility of threats as quickly as possible.

Onboarding will be performed by Transparity's Cyber Security Consultants and follow the below high-level process:

- Scoping and analysis
  - Understand your environment
  - Review your current security products, use cases, and ensure prerequisite requirements are met
  - Define service architecture and topology
  - Create statement of works (SoW)
- Implementation
  - Enable and configure the framework for our preferred Threat and Vulnerability Management tooling, or realign to our security blueprint if already deployed
  - Perform an initial vulnerability assessment
- Documentation and operational handover
  - Log any observed security risks
  - Perform operational handover to service

3. Service Operations

Please refer to our Operations Manual for further information on incident management, requests for change and information requests.

3.2 Service Maintenance

We will perform platform monitoring and maintenance the following products in line with our Secure by Default security blueprints:

- Our preferred Threat and Vulnerability Management tooling

Where action is required to resolve an incident and to rectify, it requires a change, we will use reasonable effort to make any changes outside of your change freeze periods as notified by you, provided you have given us reasonable prior written notice.

3.3 Service Hours

We will provide the following service hours: -

Threat and Vulnerability Management	Business Hours GMT 08:30-17:30	Sat / Sun / Bank Holidays GMT 08:30-17:30	Mon-Sun GMT 17:30-08:30
Consultancy	In-Scope	Out-of-Scope	Out-of-Scope

4. Billing

4.1 Additional Charges

We reserve the right to charge additional fees in the following situations:

- Implementation work carried out outside Business Hours; and
- Any change in your requirements occurring after the implementation of the Service and outside the scope of the contract (as described in the MSA).

5. Dependencies

We will provide the service subject to the following dependencies:

- All professional services required to set up this Service will be subject to separate Statements of Work and Charges and, where applicable, Service Descriptions.
- Our preferred Threat and Vulnerability Management tooling, and any required sensors / agents are a prerequisite to the delivery of the service and will be deployed and/or configured for Your organisation in accordance with the Secure by Design blueprint.

5.1 Customer Obligations

- You will provide us with a list of network-connected resources (FQDN/hosts, IP addresses or CIDR blocks) to perform the vulnerability assessments against.
- It is your responsibility to update us when this provided list changes (additions, deletions, modifications).
- You will provide us reasonable assistance in the performance of the Service(s) including, but not limited to, providing all technical and licence information that we may require to perform the Service(s).
- You will provide named contacts who will be authorised to submit support requests on behalf of your company (“Nominated Contacts”). They will be the designated people with whom all contact is made regarding all requests.
- You will allow us to deploy infrastructure where required to fulfil the requirements to perform the in-scope vulnerability scans.
- You will provide us with reasonable advance notice of any:
    - Intent to perform planned maintenance activities (including upgrades, deployments, patching).
- Guided remediation:
    - You will actively work with our operations team to resolve any raised vulnerability remediation requests, Service Requests, or any activities relating to patching, that require your input or action. For example, you may be required to make any required changes to an OS running within a VM to which we have no access.

    - Some vulnerabilities may require user-impacting remediation activity. You are responsible for distributing and coordinating end-user communications and activity unless agreed otherwise during the planning of the activity.
- It is your responsibility to comply with your data sovereignty controls, policies, and procedures.

5.2 Prerequisites

Transparity's Security Consultants will require access to various systems, resources, and stakeholders within your organisation throughout the course of this engagement to ensure a smooth and successful delivery. The required level of access, permissions and resource alignment for collaboration will be provided ahead of the project commencement.

5.3 Service Restrictions

- We will provide and support the Service on a reasonable endeavours basis only and will not be subject to any availability targets, if:
    - The OS residing on your resources is out of vendor support, or
    - No support contract with the OS provider is in place, or
    - The Supported Public Cloud Environment and or resources are configured in direct contravention of the requirements, best practices, or specific guidelines for support.
- When a ticket is opened with a Public Cloud Vendor the Transparity SLA is paused until a response is received from the respective Public Cloud Vendor.

6. Exclusions

The creation of bespoke code or integrations for 3rd party systems is not included as part of this service; we can provide a separate quotation for any bespoke code or integration work.

6.1 Third Party Related

- Managing incident maintenance for:
    - 3rd party systems,
    - Software, and/or
    - SaaS services.
- Specifically, if the above items are not covered by a third party's warranty, support agreement, or terms of use.
- Management, configuration, maintenance, administration of third-party appliances, Customer applications, and any code used to create, update, or deploy applications from third parties or by the Customer is excluded from this Service.

7. Definitions and Acronyms

In this document "we" or "us" refers to the Supplier, and "you" refers to the Client.

7.1 Terms

The terms listed have the following meanings:

Term	Meaning
Event Management Platform	The tooling Transparity uses to monitor and alert on the Supported Public Cloud Platform

Term	Meaning
Statement of Work	This means a document that defines project-specific or Customer-specific activities, deliverables, and/or timelines for providing services to that Customer.

7.2 Acronyms

Acronym	Meaning
SoW	Statement of Work
TVM	Threat and Vulnerability Management
TTPs	Tactics, Techniques, and Procedures
TI	Threat Intelligence