Service Description

Managed Extended Detection and Response (MXDR)

May 2025

transparity

Contents

1. Service Overview

The Transparity Managed Detection and Response (MDR) service delivers a proactive cybersecurity solution that combines advanced technology, expert analysis, and rapid response. The service incorporates proactive threat hunting and mitigation using advanced detection and rapid incident response.

Managed Extended Detection and Response (MXDR) enhances and expands on our Managed Detection and Response (MDR) service by including platform maintenance and log ingestion from the Microsoft Defender XDR and related security products. It scales with your business, allowing you to add any or all the core Microsoft security products to the service. Optional third-party log file ingestion can be added for comprehensive visibility into your organisation's security activities.

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

2. Service Features

Feature
Managed Detection and Response (MDR)
Security Information and Event Management (SIEM)
Endpoint Detection and Response (EDR)
Platform Maintenance
Threat Hunting
Attack Disruption
Threat Intelligence (TI)
Threat Advisories
Security Reporting Dashboards
Service Delivery Management
Rules of Engagement (RoE)
Log Ingestion
Third-Party Log Ingestion
Inclusive Security Advice
Rapid Onboarding
Microsoft Security Tooling
Phishing Detection and Response
Identity Threat Detection and Response (ITDR)

2.1 Managed Detection and Response (MDR)

- Around the clock monitoring, alert triage, analysis, attack disruption, and guided remediation delivered by our security operations centre.
- 24/7 Expert-level security support provided by our security team located across the globe to provide true follow-the-sun support.

- Our SOC analysts will work in collaboration with your technical team to provide guided remediation
- Alert tuning, detection and management including managing false and benign positives and out of scope resources.

2.2 Security Information and Event Management (SIEM)

This service utilises Microsoft's Sentinel SIEM, which will 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 for the existing platform configuration, and product support for Microsoft Sentinel.

2.3 Endpoint Detection and Response (EDR)

This service utilises Microsoft's Defender for Endpoint P2 / Defender for Servers EDR, which will 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 for the existing platform configuration, and product support for Microsoft Defender for Endpoint P2 / Defender for Servers.

2.4 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 Microsoft for their security tooling. The results of these reviews drive our security blueprints.

This service ensures that Microsoft Sentinel, Defender for Endpoint P2 / Defender for Servers, and any Microsoft Security tooling[1] deployed are continually aligned to our Secure by Default blueprints[2] 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.

2.5 Threat Hunting

This service provides human-operated threat hunting by leveraging Microsoft Sentinel and Defender XDR.

We use the ABCD framework of threat hunting to systematically detect and counter adversaries:

- **Authentication:** Identifying malicious sign-in activities, such as credential theft, adversary-in-the-middle attacks, and brute force attempts.
- **Backdoors:** Detecting unauthorized remote access via malware, web shells, or misconfigurations.
- **Command & Control (C2) Communication:** Identifying attacker-controlled infrastructure used for persistence and lateral movement.
- **Data:** Preventing data theft, ransomware encryption, and destruction.

[1] In scope Microsoft Security tooling / products are listed in section 2.16 below.

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

Threats that are surfaced through the act of Threat Hunting will be addressed as follows:

- Confirmed incidents will be logged and escalated to you as per the rules of engagement.
- Security advisories or recommendations will be logged as risks in the Risk Register and reported on.

2.6 Attack Disruption

Transparity will take decisive, pre-emptive action on your behalf using the Microsoft security tooling available to us in the event of a confirmed cyber-attack, with the aim of disrupting the attack and slowing the attacker until such time we can work with your technical team to provide guided remediation and advice.

The Attack Disruption actions will be determined by the pre-agreed Rules of Engagement (RoE) and can be different for business hours to non-business hours.

2.7 Threat Intelligence (TI)

Threat intelligence is detailed, actionable information about potential and existing cyber threats, which helps organisations prevent, detect, and respond to cybersecurity incidents.

Transparity's MDR service enriches alert investigations and analysis by leveraging Microsoft Sentinel and Defender's automated threat intelligence (TI).

2.8 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.

Threats that are surfaced through Threat Advisories will be addressed as follows:

- An ad-hoc Threat Hunt will be performed if required and any recommendations will be logged as risks in the Risk Register and reported on.
- Confirmed incidents will be logged and escalated to you as per the rules of engagement.

2.9 Security Reporting Dashboards

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

- Executive summary
- Security incidents
- Exposure management
- Service activity
- Service metrics
- Response SLAs
- Risk Register

Reports available monthly and the content, recommendations or requirements can be discussed with your Service Deliver Manager (SDM) as part of the monthly service reviews.

2.10 Service Delivery Management

As part of your account team, you will be allocated a Service Delivery Manager. They will serve as your primary contact(s) for day-to-day management and interaction for this Service. In addition, the

Service Delivery Manager will act on your behalf to ensure we adhere to our processes and standards to meet contracted obligations and provide advice and guidance on your Cyber Security Service.

Your aligned Service Delivery Manager will host monthly service review meetings with your nominated contacts to run through the following activities:

- Provide you with your monthly service report.
- Discuss your service and run through the report content.
- Discuss and agree actions on any outstanding service tickets, change requests or risks.
- Review the Risk Register backlog.
- Any other business.

2.11 Rules of Engagement (RoE)

As part of this service, a Rules of Engagement (RoE) document will be completed and maintained which clearly defines the scope, objectives, escalation paths, and procedures for security operations, ensuring all parties are aligned and aware of their responsibilities.

2.12 Log Ingestion

This service can ingest and correlate signals and telemetry from your organisation for the following log sources into Microsoft Sentinel:

- Microsoft Entra
- Microsoft Azure
- Microsoft Active Directory
- Microsoft Defender for Endpoint P2 / Microsoft Defender for Servers
- Microsoft Azure Firewall, or a third-party Firewall[3]
- Any / all the following:
  - Microsoft Defender for Office 365 P2
  - Microsoft Entra Identity Protection
  - Microsoft Defender for Endpoint P2
  - Microsoft Defender for Cloud Apps
  - Microsoft Defender for Identity
  - Microsoft Defender for Enterprise IoT
  - Microsoft Defender for Cloud – Cloud Workload Protection (CWP)
    - Microsoft Defender for Servers
    - Microsoft Defender for Storage
    - Microsoft Defender for Azure SQL Databases
    - Microsoft Defender for SQL servers on machines
    - Microsoft Defender for Open-source relational databases
    - Microsoft Defender for Azure Cosmos DB
    - Microsoft Defender for Containers
    - Microsoft Defender for App Service
    - Microsoft Defender for Key Vault
    - Microsoft Defender for Resource Manager
    - Microsoft Defender for AI Workloads
    - Microsoft Defender for APIs
  - Microsoft Defender for IoT

Certain data sources require parsing of Syslog or CEF data through a Syslog Server prior to being ingested into Microsoft Sentinel, for example most firewalls or SaaS applications. If this is required

[3] Where possible.

for the solution, then the requirements will be scoped and a Syslog Server deployed[4] and configured to ingest this data prior to sending to Microsoft Sentinel.

2.13 Third-Party Log Ingestion

This service can ingest and correlate signals and telemetry from third-party security products into Microsoft Sentinel, providing all our MDR capabilities from section 2.1 above against these log sources. However, they will not be subject to Platform Maintenance, and Attack Disruption capabilities will only be leveraged where feature parity exists.

Certain data sources require parsing of Syslog or CEF data through a Syslog Server prior to being ingested into Microsoft Sentinel, for example most firewalls or SaaS applications. If this is required for the solution, then the requirements will be scoped and a Syslog Server deployed[5] and configured to ingest this data prior to sending to Microsoft Sentinel.

2.14 Inclusive Security Advice

Delivered by our SOC to give you peace of mind should you need security advice beyond the scope of the guided remediation.

This service includes up to five (5) hours of advice per month.

2.15 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 Security Consultants and follows the below high-level process:

- Scoping and analysis
  - Understand your environment
  - Review your current security products, data sources / connectors, 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 Microsoft Sentinel, or realign to our security blueprint if already deployed
  - Enable and configure the framework for Defender for Endpoint P2 / Microsoft Defender for Servers, or realign to our security blueprint if already deployed
  - Deploy and configure a Syslog server if required
  - Deploy / enable and configure the frameworks for any / all in scope Microsoft Security tooling, or realign to our security blueprint if already deployed
  - Perform initial alert tuning
- Documentation and operational handover
  - Complete rules of engagement (RoE) documentation

[4] Transparity will deploy a headless Ubuntu Linux server hosted in Microsoft Azure, due to its small compute footprint and reduced attack surface compared to Windows. Data sent to this device from on-premises devices should be secured in transit using a VPN tunnel, which will be the customer's responsibility to facilitate.

[5] Transparity will deploy a headless Ubuntu Linux server hosted in Microsoft Azure, due to its small compute footprint and reduced attack surface compared to Windows. Data sent to this device from on-premises devices should be secured in transit using a VPN tunnel, which will be the customer's responsibility to facilitate.

- Log any observed security risks
- Perform operational handover to service

2.16 Microsoft Security Tooling

This service can utilise some or all of Microsoft's Security tooling, any of 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 for the existing platform configuration, and product support for any / all the following Microsoft Security products:

- Microsoft Defender for Office 365 P2
- Microsoft Entra Identity Protection
- Microsoft Defender for Endpoint P2
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity
- Microsoft Defender for Enterprise IoT
- Microsoft Defender for Cloud – Cloud Workload Protection (CWP)
  - Microsoft Defender for Servers
  - Microsoft Defender for Storage
  - Microsoft Defender for Azure SQL Databases
  - Microsoft Defender for SQL servers on machines
  - Microsoft Defender for Open-source relational databases
  - Microsoft Defender for Azure Cosmos DB
  - Microsoft Defender for Containers
  - Microsoft Defender for App Service
  - Microsoft Defender for Key Vault
  - Microsoft Defender for Resource Manager
  - Microsoft Defender for AI Workloads
  - Microsoft Defender for APIs
- Microsoft Defender for IoT

2.17 Phishing Detection and Response

When utilising Microsoft Defender for Office 365 as part of this service, Phishing Detection and Response will be added as a service enhancement.

Phishing Detection and Response adds detection, investigation, quarantine, and mitigation of phishing and business email compromise (BEC) attacks by leveraging the capabilities within Microsoft Defender for Office 365 P2 and the Transparity SOC.

2.18 Identity Threat Detection and Response (ITDR)

When utilising Microsoft Entra Identity Protection P2 and / or Microsoft Defender for Identity as part of this service, Identity Threat Detection and Response (ITDR) will be added as a service enhancement.

Identity Threat Detection and Response (ITDR) adds detection, investigation, and mitigation of identity-based attacks by leveraging the capabilities withing Microsoft Entra Identity Protection P2 and / or Microsoft Defender for Identity and the Transparity SOC.

3. Service Operations

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

3.1 Service Maintenance

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

- Microsoft Sentinel (SIEM)
- Microsoft Defender for Endpoint (EDR) P2 / Microsoft Defender for Servers
- The Linux Syslog server if deployed as part of the Sentinel ingestion requirements
- Any Microsoft Security tooling[6]*

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.

3.2 Alert Response / Triage

On receipt of an alert, our SOC will triage the alerts on your behalf and work with you to identify and mitigate the source of the detected threat – providing expert guidance and proactive support that extends to interfacing directly with your impacted services alongside you until the threat is contained. Where additional remedial activity is required to mitigate reoccurrence (for example, configuration changes or software / hardware device patching) our team will provide guidance and remain on-hand to advise on corrective actions.

Where desired, our Security Operations and Consultancy teams can conduct remedial activity on your behalf via a Retained Security Consultancy service, or a scoped project.

Please note: Alert response / triage is not the same as incident response (IR)

3.3 Attack Disruption

Our Attack Disruption service feature helps you to gain an edge over malicious actors through a combination of proactive manual interventions and automated response actions, designed to disrupt and slow attacks at the earliest stage via decisive action from the Transparity SOC.

Attack Disruption is designed to scale as your organisation grows by replacing response actions with increasingly more targeted countermeasures as your security tooling portfolio matures.

Example interventions and responses of the Attack Disruption add-on:

- Identities (Active Directory, Entra, M365, Linux)
  - Disable or lock the compromised account
- Endpoints (clients and servers)
  - Shutdown or isolate the compromised device
- Network-based threats (C2, Crypto Mining, Botnet, Darknet, DDoS, Proxy, PUA, etc)
- Inject blocking rule into the firewall to disable communications

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).

[6] In scope Microsoft Security tooling / products are listed in section 2.16 above.

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.
- Microsoft Sentinel is a prerequisite to the delivery of the service and will be deployed and/or configured within Your Microsoft Azure tenant in accordance with the Secure by Design blueprint. You accept that any associated Microsoft consumption costs will be borne by You.
- Where third-party log sources are ingested, we are not responsible for the availability of the 3rd party platforms.
- We will provide a rules of engagement (RoE) document for You to review, this must be approved and signed prior to the service going live.

5.1 Customer Obligations

- 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 provide us with access to the in-scope subscriptions, accounts, and tenants. This access will be used by our support staff and tooling.
- B2B guest access.
    - Azure Lighthouse relationship and delegations.
    - Service Principals.
    - Administration break-glass accounts.
- You will allow us to deploy infrastructure in each public cloud region to handle the collection of activity and diagnostics logs into our monitoring platform.
- You will provide us with reasonable advance notice of any:
    - Intent to perform planned maintenance activities (including upgrades, deployments, patching).
    - Additional resources that you will deploy into the Supported Public Cloud Platform.
    - Penetration tests to be completed and defined rules of engagement during the testing period.
- Guided remediation:
    - You will actively work with our operations team to resolve any raised incidents, 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 incidents 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.
- In the event We determine that an alert generated by the Managed Extended Detection & Response (MDR) Service has evolved from an isolated or contained incident into a security breach we will advise you to invoke your Incident Response procedures.
- You are responsible for configuring the third-party log source to egress logs in the required format to the relevant data connector used by Microsoft Sentinel for log ingestion. If technical assistance is required, Transparity can provide ad-hoc consultancy to assist for an additional charge.

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.
- A Microsoft Exchange Online Plan 1 license is required for the Microsoft Sentinel \ Logic App to facilitate the sending of email to AutoTask.
- Attack Disruption:
  - API for orchestration of security containment actions
  - Supported content hub solution / data connector
  - Any relevant identities such as Service Principals, consent to any relevant Enterprise Applications, API keys, or user accounts to authenticate the workloads

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 VM 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
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
SOC	Security Operations Centre
SIEM	Security Information and Event Management
SOAR	Security Orchestration Automation and Response
UEBA	User and Entity Behavioural Analysis
EDR	Endpoint Detection and Response
SDM	Service Delivery Manager / Management
EPP	Endpoint Protection Platform
TI	Threat Intelligence
TTPs	Tactics, Techniques, and Procedures
APT	Advanced Persistent Threats
RoE	Rules of Engagement
ITDR	Identity Threat Detection and Response

8. Service Level Agreement and Operational Targets

8.1 Response Targets

	P1	P2	P3	P4	P5
Hours of Support	24/7 Mon – Sun	24/7 Mon – Sun	08:00-18:00 Mon – Fri	08:00-18:00 Mon – Fri	08:00-18:00 Mon – Fri
Response	15 mins	Four (4) hours	Eight (8) hours	Twelve (12) hours	Twenty-four (24) hours

8.2 Incident Prioritisation

Priority	Severity	Description
P1	Critical	**Security Incident** • Your organisation has been breached, and malicious activity is in progress – Extremely Urgent • Very high impact in all business areas, extreme impact on users and disruption is excessive. • Evidence that data is being encrypted, deleted, or exfiltrated, user accounts or devices have been compromised, risk that personably identifiable information has been accessed by an attacker, denial of service, supply chain has been compromised. • Business Critical work cannot continue.
P2	High	**High Priority Security Alert** • Potentially or legitimate High impact on significant business areas or specific users. • Individual user cannot complete high priority/business critical work or department or group of users unable to continue with routine work. • Data may be at risk of being encrypted, deleted, or exfiltrated, user accounts or devices may be compromised, personably identifiable information may be accessed by an attacker, denial of service, supply chain may have been compromised.
P3	Medium	**Medium Priority Security Alert** • Potential or legitimate security threat impacting individual User or Group.
P4	Low	**Low Priority Security Alert** • Potential or legitimate security vulnerability which requires investigation Normal work can continue.
P5	Routine	**Non-urgent investigations** • General advice and guidance or agreed scheduled activity.