itps

intelligent technology. practical solutions.

ITPS Managed Detection & Response (MDR)

Service Definition (G-Cloud)

IASME CYBER BASELINE

CYBER ESSENTIALS PLUS

Crown Commercial Service Supplier

bsi

ISO 9001 Quality Management Systems CERTIFIED

ISO/IEC 20000-1 IT Service Management CERTIFIED

ISO/IEC 27001 Information Security Management CERTIFIED

Technology for a brighter tomorrow.

Registered Office:

IT Professional Services Ltd
Angel House
Unit 5
Angel Park
Drum Industrial Estate
Chester-Le-Street
DH2 1AQ

http://www.itps.co.uk

Contents

1. Service description

ITPS provides a comprehensive, fully Managed Detection and Response (MDR) service delivered by the ITPS Security Operations Centre (SOC). This service combines 24x7x365 security monitoring with advanced SIEM analytics, proactive threat hunting, and governed incident response.

The service is designed to ingest and correlate telemetry across the customer's entire estate - endpoint, identity, cloud, network, and email - to identify complex threats that evade single-point solutions. It filters out noise to enable a timely, proportionate response based on technical risk, scope, and confidence.

Service Operations

- 24x7x365: Continuous monitoring, correlation, and triage of in-scope telemetry.
- Severity-Driven Handling: All incidents (P1-P4) are triaged and progressed 24x7, prioritised by severity.

2. Business Benefits and Outcomes

The MDR service provides measurable business value by reducing cyber risk, improving operational resilience, and supporting informed decision-making during security incidents.

Key Service Benefits:

- 24x7 Threat Detection & Response: Continuous monitoring ensures threats are identified and acted upon regardless of time zone, operational hours, or local staffing availability.
- Reduced Dwell Time: Automated containment and rapid SOC analyst actions minimise the window between compromise and containment, reducing the likelihood of data loss or service disruption.
- Comprehensive Visibility: By correlating telemetry across endpoint, identity, cloud, email, and network domains via a SIEM, the service provides visibility across the full attack chain, identifying lateral movement and complex attack paths.
- Proactive Threat Hunting: Beyond automated alerts, the service includes human-led threat hunting to identify dormant attackers and sophisticated threats that bypass standard rules.
- Security Expertise on Demand: Access to highly trained SOC analysts, detection engineers, and threat hunters without the cost or retention risks of building an in-house function.
- Evidence-Based Governance: Structured reporting and service reviews provide clear insight into security activity, threat trends, and recurring risks to support governance and investment decisions.

Predictable Costs: Consolidates people, processes, SIEM technology, and tooling into a single, predictable operating model.

3. What Is Included

The MDR service is a single, integrated offering comprising the following components:

Advanced Detection & Investigation

- 24x7 Monitoring: Continuous surveillance of all in-scope telemetry sources.
- SIEM Correlation: Multi-domain analytics to correlate weak signals across endpoints, identity, and cloud into high-fidelity incidents.
- Analyst-Led Investigation: Human validation of alerts to determine "escalate vs. close" decisions.
- Threat Hunting: Scheduled, hypothesis-driven sweeps looking for indicators of compromise (IOCs) and behavioural anomalies.
- Enrichment: Application of threat intelligence and contextual analysis to every case.

Containment and Response (Within Agreed Authority)

- Playbook-Driven Response: Consistent, auditable handling aligned to internal playbooks.
- Governed Containment: Active containment actions for endpoint and identity (e.g., host isolation, account disablement) where supported.
- Incident Management: Full lifecycle management of the incident from detection through to containment and handover for remediation.

Continuous Improvement & Governance

- Detection Tuning: Continuous tuning of rules to improve signal-to-noise ratios and adapt to the changing threat landscape.
- Vulnerability Reporting: Exposure reporting where supported by the contracted platform (e.g., via Defender for Endpoint).
- Service Reviews: Monthly reviews covering activity, trends, SLA performance, and improvement actions.

4. What Is Not Included

Unless explicitly contracted, the MDR service excludes:

- Patching, vulnerability remediation, or system hardening implementation.
- Device rebuilds, system restoration, backup/restore, or disaster recovery.
- Day-to-day administration of endpoints, identities, networks, or applications.
- Compliance certification, audit sign-off, or regulatory breach determination.
- Guaranteed prevention of all security incidents.

Note: Operational remediation and recovery remain the responsibility of the customer and/or their appointed IT Managed Service Provider (which may be ITPS under a separate agreement).

5. Service Scope

In-Scope Telemetry

MDR applies to sources formally onboarded and listed as in-scope in the call-off/order form. The service is designed to ingest data from:

- Endpoint: EDR/XDR detections, telemetry, and device context.
- Identity: Sign-in logs, audit trails, and risk signals (e.g., Entra ID).
- Cloud & SaaS: Security and activity logs from agreed tenants/subscriptions (e.g., Azure, M365).
- Email: Security signals and investigative artefacts.
- Network: Log-based network security telemetry (e.g., Firewall/VPN/Proxy/DNS logs).

Minimum Viable Telemetry and Coverage

Service effectiveness is contingent upon meeting the onboarding and coverage expectations agreed at the project outset (e.g., EDR deployment targets). Where telemetry is incomplete, delayed, misconfigured, or materially below agreed coverage, detection quality and SLA applicability may be impacted, and exclusions may apply (see Section 9).

Out of Scope by Default

Unless explicitly included, the following are out of scope:

- Systems not onboarded to the MDR service.
- Non-security monitoring (performance, availability, capacity).
- Unsupported tooling not integrated into the service.
- Bespoke application telemetry or specialist platform logs.
- Manual review of raw logs outside of MDR tooling.

6. Tooling and Integrations

ITPS delivers MDR using an integrated, enterprise-grade toolset centred on SIEM and XDR capabilities. While specific named tooling reflects the current delivery approach, ITPS may substitute equivalent capabilities without reducing agreed service outcomes.

Typical Supported Platforms (As Contracted):

- SIEM & Analytics: Microsoft Sentinel (or equivalent) for central correlation, hunting, and investigation.
- Endpoint Security: Microsoft Defender for Endpoint (or agreed EDR/XDR alternatives).
- SOAR/Orchestration: For enrichment, routing, approvals, and governed response workflows.
- Threat Intelligence: External enrichment sources.
- Communications: Real-time channels (e.g., Microsoft Teams) for P1/P2 coordination.

Note: ITPS does not publish internal playbooks, detection rules, queries, thresholds, correlation logic, or automation implementations as part of this service definition.

7. Definitions

To ensure clarity, the following definitions apply:

- Event: A security-relevant record (e.g., a sign-in log entry).

- Alert: A detection generated by a security control or correlation rule requiring SOC review.
- Incident: Validated or suspected malicious/unauthorised activity requiring containment and incident handling.
- Triage: Analyst review to validate, enrich, assign severity, and determine "escalate vs. close".
- Containment: Actions taken to limit or stop malicious activity within agreed authority.
- Remediation/Recovery: Restoration, rebuilding, patching, and recovery actions (out of scope).
- Core Business Hours: 09:00–17:00 UK time, Monday to Friday, excluding English public holidays.

8. Response Authority Model

MDR response actions are governed by a defined authority matrix agreed during onboarding. All actions are executed proportionately based on severity and technical risk.

Authority Tier	Description	Examples (Non-Exhaustive)	Authorisation
Tier 1 (Limited Impact)	Constrained actions with low blast radius and reversibility.	Isolate a specific endpoint via EDR; revoke named user sessions; block indicators.	Pre-Authorised (If agreed)
Tier 2 (Potential Impact)	Actions that may disrupt users or business services.	Disable user/service account; quarantine server; broader indicator blocks; cloud/email actions.	Approval Required (Default) OR Pre-authorised (For specific high-confidence scenarios agreed at onboarding)
Tier 3 (Potentially Destructive)	High risk or irreversible actions.	Wipe/rebuild; shutdown services; delete data; restore operations.	Customer Execution Only

Customer Responsibilities:

- Maintain named authorised contacts for approval-required actions.
- Ensure availability of contacts for P1/P2 incidents.

9. Service Levels and Measurement

MDR response actions are governed by a defined authority matrix agreed during onboarding. All actions are executed proportionately based on severity and technical risk.

Severity Classification

Priority	Description	Examples (Non-Exhaustive)

P1 – Critical	Active threat causing or likely to cause a significant business impact	Ransomware execution, domain admin compromise, active data exfiltration
P2 – High	Confirmed malicious activity with limited scope or impact	C2 beaconing, credential dumping, malware execution
P3 – Standard	Suspicious behaviour requiring investigation	Suspicious PowerShell, anomalous login activity
P4 – Low	Informational or policy-related events	Low risk alerts, configuration issues

Incident Handling Targets

"Triage / Initiation" denotes the commencement of analyst-led investigation and/or execution of approved containment actions.

Priority	Triage / Initiation Target	Customer Notification Target	Progression
P1	≤ 15 minutes (24x7)	≤ 30 minutes (Real-time channel + Phone)	Progressed 24x7
P2	≤ 30 minutes (24x7)	≤ 60 minutes (Real-time channel and/or Email)	Progressed 24x7
P3	24x7 Triage (Queue processed alongside P1/P2)	Next Core Business Day (unless reclassified)	Progressed 24x7 (Sequenced after P1/P2)
P4	24x7 Triage (Queue processed alongside P1/P2)	During Core Business Hours	Progressed 24x7 (Sequenced after P1/P2)

SLA Exclusions

Service levels may be paused or voided where delays are caused by factors outside ITPS's reasonable control, including:

- Customer dependency failure (telemetry coverage, access, contacts, approvals).
- Third-party platform outages (cloud providers, telecoms, vendors).
- Connectivity issues outside ITPS control.
- Approved maintenance windows or emergency maintenance.
- Onboarding and baselining periods.
- Incomplete, delayed, suppressed, or misconfigured telemetry.

10. Service Hours and Communications

- 24x7x365: Security monitoring, triage, investigation, and containment aligned to severity.
- Core Business Hours: Service management (onboarding, offboarding, change approvals, reporting).
- Communication Channels:

- P1/P2: Real-time channel (e.g., Teams) with email/phone escalation.
- P3/P4: Service record/ticket channel.

11.Governance and Reporting

- Monthly Service Reviews: Covering incidents, trends, SLA performance, and improvement actions.
- Optional Quarterly Posture Reviews: Strategic insights and long-term recommendations.
- Objective: Governance supports transparency and continual improvement but does not transfer risk ownership or guarantee prevention.

12.Security and Data Handling

ITPS enforces role-based access control, MFA, least privilege access, and auditable logging across all MDR platforms. Customer data is logically separated to prevent cross-customer access.

Data Residency and Retention

- Residency and retention are defined per call-off based on the contracted tier.
- UK-Only processing and storage are supported where required, subject to the delivery model and agreed sub-processors.
- Data protection terms are governed by the applicable Data Processing Agreement (DPA).

13.Dependencies and Customer Responsibilities

To ensure service effectiveness, the customer (and/or their IT MSP) is responsible for:

- Deploying and maintaining endpoint agents to meet agreed coverage targets.
- Enabling required logs and granting API permissions for integrated platforms.
- Maintaining stable connectivity for in-scope sources.
- Maintaining authorised contacts for P1/P2 approvals.
- Executing remediation and recovery actions outside the MDR scope.

14.Onboarding and Offboarding

Onboarding

SLAs apply only after onboarding and baselining are complete and "Go-Live" is formally confirmed. Typical stages include:

- Confirmation of in-scope assets and telemetry.
- Integration and validation of data quality.
- Agreement of response authority and contacts.
- Baselining and tuning to reduce false positives.

Offboarding

Upon termination, offboarding ensures the secure removal of MDR access, integrations, and authority. This includes the closure/handover of in-flight incidents and the secure handling of data in line with regulatory obligations.

15.Optional Bolt-Ons

Where offered, optional add-ons (purchased separately) may include:

- Phishing Simulation
- Security Awareness Training
- Cyber Essentials / Plus Support
- Penetration Testing

These services are distinct from the MDR scope unless explicitly purchased.