Managed Cyber Security Services

Service Schedule

June 2026 Edition

Effective from 15 June 2026

Lanmark Limited
Company number 02977539
Registered office: West Hill House, West Hill, Dartford, DA1 2EU
lanmark.com/terms-of-business

Part of the Lanmark Terms of Business suite, published 15 June 2026.

Document control

Field	Value
Document title	Lanmark Limited Managed Cyber Security Services Schedule
Document reference	Lanmark Service Schedule: Managed Cyber Security
Version	June 2026 Edition
Document date	Effective from 15 June 2026
Status	Published (June 2026 Edition)
Supersedes	Lanmark Managed Cyber Security Services Terms of Service (in respect of MDR, ITDR and Managed SIEM only)
Layer	Layer 2 (Service Schedule) of the Lanmark T&C suite
Sits under	Lanmark Master Services Agreement (as in effect from time to time, published at lanmark.com/terms-of-business)

Revision history

Date	Version	Reason
15 June 2026	June 2026 Edition	First publication of the Lanmark Terms of Business suite (June 2026 Edition).

1. Purpose and scope

1.1 This Service Schedule sets out the service-specific terms on which Lanmark provides Managed Cyber Security to the Client. It supplements, and is to be read with, the Lanmark Master Services Agreement (MSA) and the Order Form.

1.2 The Service is a managed cyber security service that combines three capabilities, delivered on a 24x7x365 basis through a Third Party Provider's tooling and Security Operations Centre (SOC):

(a) Managed Detection and Response (MDR) for endpoint devices;

(b) Identity Threat Detection and Response (ITDR) for the Client's Microsoft 365 tenant and Entra identity environment;

(c) Managed SIEM for the Client's infrastructure assets (servers, firewalls, switches, wireless access points and similar).

1.3 Lanmark delivers the Service on a Service and Solution basis: Lanmark deploys, configures and operates the Third Party Provider's tooling on the Client's environment, and the Third Party Provider's SOC analysts deliver 24x7x365 monitoring, alert handling and remediation. Lanmark does not offer a monitor-existing-tooling variant of this Service; where the Client wishes to retain a different cyber tooling stack, the Service does not apply.

1.4 The Service aims to reduce, not eliminate, cyber security risk. No cyber security service can guarantee detection of every threat or prevention of every cyber incident. This Schedule should be read with that limitation in mind throughout, and in particular with Clause 9 (Disclaimers and no guarantee of security).

1.5 Subject to Clause 1.3 of the MSA (order of precedence), this Schedule prevails over the MSA only in respect of the specific Service detail it covers and only where this Schedule explicitly states an override.

2. Definitions

The following definitions apply in this Schedule. Defined terms in the MSA have the meanings given to them in the MSA and are not redefined here.

EDR means endpoint detection and response: the security tooling deployed by the Third Party Provider on in-scope endpoint devices to detect, analyse and respond to threats on those devices.

Entra ID means Microsoft Entra ID, being the identity and access management service for the Client's Microsoft 365 tenant (previously known as Azure Active Directory).

ITDR means identity threat detection and response: the Service capability described at Clause 3.2.

Managed SIEM means the managed security information and event management capability described at Clause 3.3.

MDR means managed detection and response: the Service capability described at Clause 3.1.

Security Event means any observable occurrence in the in-scope environment that is logged or processed by the Third Party Provider's tooling, including routine events such as user sign-ins and policy changes as well as anomalous events.

Security Incident means a Security Event, or a chain of Security Events, that the Third Party Provider's SOC determines to require investigation, response or remediation.

Service means in this Schedule, Managed Cyber Security as described in this Schedule.

SOC means the Third Party Provider's Security Operations Centre, comprising the security analysts and operational infrastructure that deliver 24x7x365 monitoring, alert handling and remediation activity for the Service.

Support Hours means Monday to Friday, 8.00am to 6.00pm UK time, excluding English bank holidays. Support Hours apply to Lanmark's Client-side engagement management for the Service. They do not apply to the SOC, which operates 24x7x365.

Third Party Provider Terms means the terms published by the Third Party Provider from time to time governing the use of its tooling and SOC, including any service level commitments, acceptable use restrictions, processing terms and data protection particulars.

3. Service description

3.1 Managed Detection and Response (MDR)

3.1.1 MDR provides a managed cyber security service for endpoint devices in scope of the Order Form. The Third Party Provider deploys a lightweight EDR agent to each in-scope endpoint. The agent collects forensic and behavioural data and analyses suspicious activity to detect persistent footholds, malicious software and other endpoint security threats. SOC analysts action and remediate alerts generated by the EDR tooling, applying threat intelligence and incident response practice.

3.1.2 MDR is delivered on a per-endpoint subscription basis. The unit of charge is per installed EDR agent. The Order Form identifies the agreed number of in-scope endpoints at the Service Start Date and the per-agent Fee.

3.2 Identity Threat Detection and Response (ITDR)

3.2.1 ITDR provides continuous, real-time monitoring of the Client's Microsoft 365 tenant and Entra ID environment. Monitored activity includes user sign-ins, application sign-in patterns, mailbox configuration changes (including malicious inbox and forwarding rules), privilege escalation, suspicious application consent, and similar identity-layer events. SOC analysts investigate identity-related Security Incidents and apply remediation, including (with the Client's permission, expressly granted or contemplated by the Client responsibilities in this Schedule) account disablement, session revocation and credential reset.

3.2.2 ITDR is delivered on a per-licensed-user subscription basis. The unit of charge is per Microsoft 365 licensed user with identity activity monitored under the Service. The Order Form identifies the agreed number of in-scope identities at the Service Start Date and the per-identity Fee.

3.3 Managed SIEM

3.3.1 Managed SIEM provides centralised collection, retention and correlation of logs from the Client's infrastructure assets (including, without limitation, firewalls, network switches, wireless access points, servers and other in-scope infrastructure devices). The Third Party Provider's SIEM tooling correlates the collected events to detect anomalies, threats and policy breaches. Alerts arising from the SIEM are passed to the SOC analysts for investigation and response.

3.3.2 Managed SIEM is delivered on a per-asset subscription basis. The unit of charge is per in-scope infrastructure asset. The Order Form identifies the agreed number of in-scope assets at the Service Start Date and the per-asset Fee.

3.4 Combined Service operation

3.4.1 Where the Client subscribes to two or more of the capabilities at Clauses 3.1 to 3.3, the Third Party Provider correlates Security Events across the capabilities (so that, for example, an endpoint-detected anomaly may be linked to an identity-layer event or to an infrastructure log entry) and the SOC handles the combined picture. The unit-based subscription Fees at

Clauses 3.1.2, 3.2.2 and 3.3.2 apply in addition to each other, in accordance with the Order Form.

3.4.2 The Service is delivered 24x7x365. The Third Party Provider's SOC operates continuously. Lanmark's Client-side engagement management for the Service (including reporting, service reviews, response to Client queries and escalation routing) is delivered during Support Hours.

4. In scope and out of scope

4.1 In scope

The Service includes:

(a) deployment, configuration and operation of the Third Party Provider's tooling on the in-scope environment;

(b) 24x7x365 monitoring, alert triage and remediation activity by the SOC, in accordance with the Third Party Provider Terms;

(c) Lanmark Client-side engagement management during Support Hours, including response to Client queries about the Service, routine routing of issues between the Client and the SOC, and the monthly threat and activity report described at Clause 6.5;

(d) periodic service review activity for Retainer Support clients, in accordance with Clause 6.7 of the IT Support Services Schedule where the Client subscribes to that Service in parallel.

4.2 Out of scope

The following are out of scope of the Service and are not provided as part of the Service Fees. Where any of the following is required, it is provided (where Lanmark is able to provide it) as separately-quoted work or under a separate Service Schedule:

(a) forensic investigation, evidence preservation, chain-of-custody handling or expert witness work in connection with a Security Incident;

(b) regulatory breach notification preparation or submission (to the Information Commissioner's Office or any other supervisory authority), other regulatory reporting, and engagement with law enforcement;

(c) invocation, coordination or execution of the Client's business continuity or disaster recovery arrangements;

(d) detection, monitoring or response for endpoints, identities, tenants, applications, infrastructure assets or environments that are not in scope under the Order Form;

(e) vulnerability assessment, penetration testing or any related cyber assessment activity (covered by the Cyber Assessments Services Schedule);

(f) phishing simulation, security awareness training, Cyber Essentials assessment or certification, and Microsoft Intune configuration to Cyber Essentials standards (covered by the Cyber Compliance and Training Services Schedule);

(g) general IT support, including endpoint configuration, user administration and tenant administration unrelated to the Service (covered by the IT Support Services Schedule);

(h) backup, archival or recovery of data, including data lost or rendered unavailable as a result of a Security Incident (covered by the Backup Services Schedule);

(i) remediation activity that goes beyond the standard SOC remediation practice published by the Third Party Provider. Standard SOC remediation includes, for

example, isolating an affected endpoint, terminating a malicious process, removing a foothold where the tooling allows, disabling a compromised user session and applying identity containment steps such as account disablement or credential reset. Activity that is not standard SOC remediation (for example, large-scale environmental rebuild, manual eradication of advanced persistent threats requiring custom tooling, or remediation requiring extensive engineer time outside the Service operating model) is out of scope of the standard Service Fees;

(j) broader identity hygiene work, including (without limitation) multi-factor authentication rollout, conditional access redesign, privilege model review, legacy authentication cleanup, tenant hardening and similar identity programme activity. This work is out of scope of the Service except where required as immediate SOC remediation for a Security Incident, or where expressly included in the Order Form or in a separate Service Schedule;

(k) anything stated as out of scope in the Order Form.

5. Service Levels

5.1 SOC Service Levels (Third Party Provider passthrough)

5.1.1 The 24x7x365 monitoring, alert triage, investigation, response and remediation activity that comprise the substantive cyber security work of the Service are delivered by the Third Party Provider's SOC. The applicable Service Levels for those activities are the Service Levels published by the Third Party Provider from time to time.

5.1.2 Lanmark does not commit to Service Levels different from, or more onerous than, those published by the Third Party Provider for the SOC activity. Where the Third Party Provider's SOC fails to meet its published Service Levels, Lanmark's obligation and liability in respect of that failure is limited to using reasonable endeavours to pass through, or assist the Client in pursuing, any remedies available under the Third Party Provider Terms. This Clause 5.1.2 is a Service-specific application of Clause 17.4 of the MSA.

5.1.3 The current Third Party Provider is identified in the Sub-Processors List published at lanmark.com/terms-of-business. The Client may request a copy of, or a reference to, the Third Party Provider's currently-published Service Levels from Lanmark.

5.2 Lanmark engagement Service Levels

5.2.1 Lanmark provides Client-side engagement management for the Service during Support Hours. Engagement management includes responding to Client queries about the Service, routing matters between the Client and the SOC where this is helpful, producing the monthly threat and activity report at Clause 6.5, and (for Retainer Support clients) participating in periodic service reviews.

5.2.2 Lanmark engagement management is delivered on a reasonable endeavours basis within Support Hours. Lanmark does not commit to a fixed Initial Response Time for engagement queries under this Schedule. Where the Client subscribes to the IT Support Services Schedule in parallel, engagement queries for the Service that are logged in the Service Tooling as Service Tickets are handled in accordance with the priority classification and Support Hours response model of the IT Support Services Schedule.

5.2.3 Cyber Security Incidents themselves are not handled through the Lanmark engagement channel. They are handled directly by the SOC in accordance with the Third Party Provider Terms. The Lanmark engagement channel is for queries about the Service, reporting and escalation routing, not for incident response.

5.3 Service Level measurement and exclusions

5.3.1 The Third Party Provider's records of SOC activity (alerts, responses, remediations) are the authoritative record of SOC Service Level performance, save in the case of manifest error. Lanmark's records in the Service Tooling are the authoritative record of Lanmark engagement activity.

5.3.2 Time spent waiting for Client action, Client information, third-party action (other than action by the SOC), or any other matter outside the reasonable control of Lanmark or the Third Party Provider does not count towards any applicable Service Level.

5.3.3 The Service Levels at this Clause 5 are service management targets. They do not give rise to service credits, fee reductions, repayment of Fees or any similar monetary remedy. Where the SOC fails to meet a Third Party Provider published Service Level, Lanmark's obligation and liability in respect of that failure is limited to using reasonable endeavours to pass through, or assist the Client in pursuing, any remedies available under the Third Party Provider Terms, in accordance with Clauses 11.2 and 17.4 of the MSA. Where Lanmark fails to meet a reasonable endeavours engagement standard under Clause 5.2, the Client's remedy is service review and escalation through the IT Support Services Schedule (where the Client subscribes to it in parallel) or through Lanmark's commercial contact for the engagement. Subject to Clause 18 of the MSA, this Clause 5.3.3 states the Client's full and exclusive remedy, and Lanmark's only obligation and liability, for non-performance or non-availability of the Service Levels at this Clause 5.

6. Operational arrangements

6.1 Service hours

6.1.1 The Third Party Provider's SOC operates 24x7x365. The Service is delivered continuously by the SOC, in accordance with the Third Party Provider Terms.

6.1.2 Lanmark Client-side engagement management for the Service is delivered during Support Hours.

6.2 Support channels

6.2.1 Communications with Lanmark in connection with the Service (engagement queries, reporting requests, service reviews) are routed through the standard support channels at Clause 6.2 of the IT Support Services Schedule (the self-service portal in the Service Tooling, the published service desk email address and the published service desk telephone number).

6.2.2 Communications with the SOC about a Security Event or Security Incident handled by the SOC are routed through the channels published by the Third Party Provider, which may include in-tool messaging, the Third Party Provider's portal or other channels identified during onboarding.

6.3 Onboarding and deployment

6.3.1 Onboarding for the Service includes:

(a) deployment of the EDR agent to in-scope endpoints (Clause 3.1);

(b) connection to the Client's Microsoft 365 tenant and Entra ID environment for ITDR (Clause 3.2);

(c) configuration of log forwarding from in-scope infrastructure assets to the Managed SIEM (Clause 3.3);

(d) baseline tuning of detection rules and notification thresholds for the Client's environment;

(e) documentation of the in-scope environment, authorised contacts and escalation routes.

6.3.2 Onboarding requires Client cooperation, including granting Lanmark and the Third Party Provider the access, permissions and information identified in Clause 7. The expected duration of onboarding is identified in the Order Form. Where onboarding requires significant remediation of the Client's pre-existing environment before the Service can operate safely (for example, large-scale identity hygiene work, mass agent push to legacy endpoints, or extensive log source configuration on legacy infrastructure), that remediation work is identified in the Order Form and may be charged separately.

6.4 Incident escalation

6.4.1 Where direct SOC channels are made available to the Client during onboarding: where the SOC detects a Security Incident that requires Client action, the Third Party Provider's SOC contacts the Client directly through the channels established at onboarding; and where the

Client first becomes aware of a suspected Security Incident, the Client should contact the SOC through those channels. The Client should not delay contacting the SOC by routing the matter through Lanmark; the Lanmark engagement channel is for engagement queries, not for incident reporting. Where the Third Party Provider's operating model does not provide direct SOC channels to the Client (so that SOC communications with the Client are routed through Lanmark), Lanmark will act as the routing channel during Support Hours and on a reasonable endeavours basis Out of Hours, in each case in accordance with the Third Party Provider's escalation model in force from time to time.

6.4.2 Where the Client requires Lanmark's assistance in routing communications to the SOC, in clarifying SOC instructions, or in coordinating any Client-side response action that falls outside the Service (for example, IT Support engineer work), Lanmark provides that assistance during Support Hours where the Client subscribes to the IT Support Services Schedule, and on a reasonable endeavours basis otherwise.

6.5 Reporting

6.5.1 Lanmark provides the Client with a monthly threat and activity report covering: SOC activity in the reporting period, Security Events and Security Incidents observed, remediation actions taken, indicators of compromise (where applicable), and trends or recommendations arising. The report is provided through the Service Tooling or by email, as agreed at onboarding.

6.5.2 Where Lanmark and the Client agree a periodic service review under Clause 6.7 of the IT Support Services Schedule, Service performance is included in that review by reference to the monthly threat and activity report.

7. Client responsibilities

To enable Lanmark and the Third Party Provider to deliver the Service, the Client will:

(a) grant Lanmark and the Third Party Provider the access, credentials, permissions and information they reasonably require to deploy, operate and tune the Service, including administrative access to in-scope endpoints, the Microsoft 365 tenant and Entra ID environment, and in-scope infrastructure assets;

(b) permit and facilitate the deployment of the EDR agent to in-scope endpoints, the connection to the Microsoft 365 tenant and the configuration of log forwarding from in-scope infrastructure;

(c) provide accurate and complete information about the in-scope environment (including the inventory of endpoints, identities, applications, infrastructure assets, supplier relationships and connectivity patterns) at onboarding and on a continuing basis;

(d) promptly notify Lanmark of any material change to the in-scope environment that may affect the Service (including additions or removals of endpoints, identities or infrastructure assets, changes to suppliers, changes to remote-working patterns, changes in Microsoft 365 licensing, and changes that introduce previously-unmonitored systems);

(e) implement or authorise Lanmark or the Third Party Provider to implement reasonable security recommendations made in writing where those recommendations affect the security or supportability of the in-scope environment;

(f) respond promptly (and in any event within timescales appropriate to the Priority Level of the matter) to Lanmark or SOC requests for information, approval or Client-side action in connection with a Security Event or Security Incident;

(g) comply with the Third Party Provider Terms to the extent those terms apply to the Client's use of the Service;

(h) ensure that the Client maintains, independently of this Service, its own backup arrangements (Lanmark recommends backup Services under the Backup Services Schedule) and its own cyber insurance arrangements appropriate to the Client's risk exposure;

(i) not introduce or continue to operate, in the in-scope environment, software, hardware or services that the Client knows or ought reasonably to know create vulnerabilities the Service cannot reasonably mitigate, without first agreeing the position with Lanmark. For this purpose, 'ought reasonably to know' is assessed by reference to: (i) the vendor's published end-of-life or end-of-support status; (ii) any written warning given by Lanmark or the Third Party Provider; (iii) any critical vulnerability published by the vendor, by a recognised security authority (such as the National Cyber Security Centre or the Cybersecurity and Infrastructure Security Agency), or by the Third Party Provider; and (iv) any operating system, application or component that is unsupported by its vendor or that has not received security updates within a reasonable period;

(j) cooperate fully with the SOC's response to any Security Incident, including authorising the actions reasonably required to contain and remediate the Incident.

(k) on termination or expiry of the Service, promptly remove (or permit Lanmark or the Third Party Provider to remove) all Third Party Provider software, agents, connectors, integrations and configuration items from the Client's systems and Microsoft 365 tenant. Where the Client does not effect or facilitate such removal within thirty (30) days of the termination or expiry date, the Client indemnifies Lanmark against any Third Party Provider Fees, claims or third-party regulatory action arising from the continued operation of the Third Party Provider software, agents, connectors, integrations or configuration items after the termination or expiry date.

Where the Client does not meet a responsibility under this Clause 7, and that failure causes or materially contributes to a Security Incident, a failure of the Service or a Client loss arising in connection with the Service, Lanmark and the Third Party Provider are not liable for the consequent loss or damage, and the Client's indemnity at Clause 8 applies to the extent set out in Clause 8.

8. Indemnification

8.1 The Client will indemnify Lanmark against any third-party claim made against Lanmark (including regulatory action by any regulator or supervisory authority and including claims by employees, customers or counterparties of the Client), and against Lanmark's reasonable costs and expenses (including reasonable legal fees) incurred in connection with such third-party claim or regulatory action, where the claim or action arises out of or in connection with:

(a) the Client's breach of any obligation under this Schedule, the MSA or the Third Party Provider Terms;

(b) the Client's misuse of any access, credentials or permissions granted to Lanmark or to the Third Party Provider for the purpose of delivering the Service;

(c) the Client's provision of inaccurate, incomplete or misleading information about the in-scope environment, or the Client's failure to notify a material change to that environment as required under Clause 7(d);

(d) the Client's failure to act on a security recommendation made by Lanmark or the Third Party Provider in writing in accordance with this Schedule;

(e) the Client's introduction or continued use of software, hardware or services in the in-scope environment that the Client knew or ought reasonably to have known created vulnerabilities the Service cannot reasonably mitigate.

8.2 The indemnity at Clause 8.1 does not apply to the extent that the matter giving rise to the third-party claim or regulatory action is caused by the gross negligence or wilful misconduct of Lanmark, or by Lanmark's breach of a non-excludable obligation under the Data Protection Legislation, the MSA or applicable law. For the avoidance of doubt, the indemnity is given without prejudice to, and does not narrow, the non-excludable carve-outs at Clause 18.1 of the MSA (death or personal injury caused by negligence, fraud or fraudulent misrepresentation, and any other liability which cannot be limited or excluded under applicable law).

8.3 The Client's indemnity at this Clause 8 is subject to the limitations and exclusions of liability at Clause 18 of the MSA (including the per-Service per-Contract Year cap at Clause 18.2 and the exclusions at Clause 18.3 of the MSA). Clause 18.2.2 of the MSA applies.

8.4 Lanmark will give the Client prompt written notice of any third-party claim or regulatory action that may give rise to an indemnity under Clause 8.1, and will not settle or admit liability without the Client's prior written consent (such consent not to be unreasonably withheld or delayed). The Client may take conduct of the defence of the claim at the Client's cost where Lanmark gives its prior written approval, such approval not to be unreasonably withheld. Lanmark may refuse approval where, in Lanmark's reasonable opinion, the claim or regulatory action concerns Lanmark's own legal, regulatory, confidentiality or reputational interests, including (without limitation) any matter involving Lanmark's confidential information, security tooling, SOC procedures, other clients of Lanmark, or any direct investigation of Lanmark by a regulator or other authority. Where Lanmark refuses approval, Lanmark will assume conduct of the defence and will keep the Client reasonably informed.

9. Disclaimers and no guarantee of security

9.1 The Service aims to reduce, not eliminate, the Client's exposure to cyber security risk. The Service does not constitute a guarantee of any specific security outcome. In particular, and without limitation, Lanmark and the Third Party Provider do not warrant or guarantee that:

(a) the Service will detect every Security Event or Security Incident that affects the in-scope environment;

(b) the Service will prevent any specific cyber-attack or category of cyber-attack;

(c) the Service will be free of false positive or false negative detections;

(d) the Third Party Provider's tooling, agents or platform will operate without interruption, error or downtime;

(e) the Client will not suffer a cyber-related loss while the Service is in operation.

9.2 The Third Party Provider's tooling, agents, SOC services and any other software or service made available by the Third Party Provider in connection with the Service are supplied to the Client under the Third Party Provider Terms. Lanmark does not give any separate warranties (express, implied or statutory) in respect of the Third Party Provider's tooling, agents, SOC services or any other Third Party Provider product, save to the extent that any such warranty cannot be excluded under applicable law. This Clause 9.2 does not exclude any warranty or other obligation that cannot be excluded under applicable law, and does not affect Lanmark's own obligation to deploy, configure and manage the Service in accordance with the MSA and this Schedule.

9.3 Subject to Clause 18 of the MSA, Lanmark is not liable to the Client for any Security Incident or cyber-related loss that occurs while the Service is in operation, to the extent that the Service has operated in accordance with this Schedule and the Third Party Provider Terms. The Service is designed to reduce risk; it does not transfer the Client's residual cyber risk to Lanmark.

9.4 The Client acknowledges that cyber security is a shared responsibility between the Client and Lanmark, that the Client retains ultimate responsibility for the security of its own systems, data and operations, and that the Service is one element of a broader cyber resilience posture that the Client should maintain (including its own internal policies, training, backup arrangements, business continuity arrangements and cyber insurance).

10. Data protection particulars

This Clause 10 supplements Clause 13 (Data protection) of the MSA and sets out the Article 28 processing particulars for the Service. Defined terms in Clause 13 of the MSA apply in this Clause.

Article 28 particular	Value for the Managed Cyber Security Service
Subject matter of the processing	Provision of the Managed Cyber Security Service to the Client, including endpoint monitoring (MDR), identity monitoring (ITDR), infrastructure log monitoring (Managed SIEM), Security Event detection, Security Incident investigation, remediation activity, threat intelligence application and Service reporting.
Duration of the processing	For the duration of the Service, plus reasonable retention periods after the end of the Service. The Third Party Provider's tooling and SOC retain Security Event and Security Incident records (including for forensic, audit, regulatory and threat intelligence purposes applicable to the Third Party Provider's operation of the Service) in accordance with the Third Party Provider Terms. Lanmark-held records are governed by Lanmark's Data Protection and Retention Policy.
Nature and purpose of the processing	Collection, storage, organisation, structuring, retrieval, consultation, analysis, alignment, combination, restriction, use and (where applicable) erasure of Personal Data for the purpose of cyber security monitoring, threat detection, incident response and Service operation.
Types of Personal Data	Authorised User identification data (name, role, sign-in identifiers, email address); user behavioural and activity data (sign-in times, sign-in locations, application usage, session and device metadata); endpoint device data (device identifiers, operating system, software inventory, running processes, behavioural telemetry); identity and access data (group membership, permission changes, multi-factor authentication events); infrastructure log data (firewall traffic, switch events, server logs, security tool outputs); incidental Personal Data that appears in monitored activity or incident records.
Categories of data subject	Authorised Users, Client employees and contractors, third parties whose Personal Data appears incidentally in monitored activity (for example, in email subjects, traffic destinations or identity-related events), and where applicable Client customers or counterparties whose identifiers appear in Security Event or Security Incident records.
Documented instructions for processing	Set out in the MSA, this Schedule, the Order Form, the Lanmark service documentation produced during onboarding, and any further written instructions the Client gives Lanmark from time to time. The Third Party Provider Terms inform the processing operations required to deliver the Service through the Third Party Provider's tooling and SOC; the Client's instructions to Lanmark remain governed by the MSA and the Data Protection Legislation.

Cyber security monitoring may incidentally involve special category Personal Data (for example, where an Authorised User's identity-layer event reveals information about the user's communications) and criminal offence data (for example, where a Security Incident involves alleged

unauthorised access to Client systems by a person whose identity is later established). The Service is not designed for the routine processing of either category of data. Where the Client expects either category to feature in the in-scope environment beyond incidental processing, the Client will inform Lanmark before onboarding so that appropriate technical and organisational measures can be confirmed.

11. Sub-Processors used in delivering this Service

Lanmark uses Sub-Processors to deliver the Service in accordance with Clauses 13.5 to 13.7 of the MSA. The categories of Sub-Processor used in delivering this Service are:

Category	Role in this Service
Third Party Provider	Provision of the EDR, ITDR and Managed SIEM tooling, the agents deployed to the in-scope environment, the SIEM platform, the SOC, the analyst function, the threat intelligence feeds, and the Third Party Provider's portal, support and reporting systems. The SOC operates 24x7x365 and is the principal Sub-Processor for this Service.
Service Tooling provider	Provision of the Lanmark service management system used for Client-side engagement (ticketing, time recording and Lanmark reporting).

The current Sub-Processor in each category (and in particular the identity of the current Third Party Provider), the location of processing for each Sub-Processor, and any applicable international transfer mechanism, are identified in the live Sub-Processors List published at lanmark.com/terms-of-business. The Sub-Processors List is the authoritative source for the identification of current Sub-Processors.

Microsoft 365 tenant dependency

Where ITDR is in scope, the Service monitors activity in the Client's Microsoft 365 tenant and Entra ID environment. Microsoft is not a Lanmark Sub-Processor for this Service. Microsoft's role in respect of the Client's Microsoft 365 tenant is governed by the Microsoft terms applicable to the Client's tenant directly. Lanmark's, and where applicable the Third Party Provider's, access to the tenant for ITDR purposes is exercised under that direct Microsoft relationship and does not change Microsoft's status.

12. Relationship with the Third Party Provider

12.1 The substantive cyber security work of the Service (the SOC monitoring, alert handling, investigation and remediation activity, and the operation of the underlying tooling) is performed by the Third Party Provider. Lanmark deploys, configures, tunes and manages the operational relationship with the Third Party Provider on the Client's behalf, and provides the Client-side engagement management at Clause 5.2.

12.2 The Service is therefore subject to:

(a) the Third Party Provider Terms, including the Third Party Provider's published Service Levels, acceptable use restrictions, processing terms and data protection particulars;

(b) the operational availability of the Third Party Provider's tooling, agents, platform and SOC;

(c) the Third Party Provider's product roadmap, feature set and operating model from time to time.

12.3 Clause 17 of the MSA (Third Party Providers) applies to the Service. In particular, and without limitation, Clause 17.4 of the MSA confirms that Lanmark is not liable for any act or omission of the Third Party Provider, including any failure of the Third Party Provider's product or service to meet a published Service Level or to perform as described in the Third Party Provider's documentation.

12.4 Where the Client requires direct reference to the Third Party Provider Terms (for example, for the Client's own compliance assurance, supplier risk assessment, or regulatory submission), the Client may request a copy or a current URL from Lanmark.

12.5 Suspension or termination on Third Party Provider discontinuance or material modification. Where the Third Party Provider discontinues its services, materially modifies the substantive functionality or pricing of the tooling on which the Service depends, withdraws from the UK or EU market, or otherwise ceases to be able or willing to deliver the services on which Lanmark relies to provide the Service to the Client, Lanmark may, on written notice to the Client:

(a) suspend the affected element of the Service for a reasonable period to migrate to an alternative Third Party Provider, where commercially reasonable;

(b) modify the Service description and the corresponding Fees to reflect the migrated arrangement, in which case Clause 5.4 of the MSA (material change notice) applies; or

(c) terminate the affected element of the Service on at least sixty (60) days' written notice, in which case the Client's continuing commitment to pay Fees under MSA Clause 20.5 ends with the termination date and any Third Party Provider passthrough Fees due to the Third Party Provider for any unavoidable run-off period are payable by the Client under MSA Clause 20.5.5.

The Client acknowledges that the Service is dependent on the operational continuity of the Third Party Provider, and that the Third Party Provider's commercial decisions are not within Lanmark's control.

13. Service-specific commercial terms

13.1 The Fees for the Service are set out in the Order Form. The unit of charge for each capability is as set out in Clauses 3.1.2 (MDR, per endpoint), 3.2.2 (ITDR, per Microsoft 365 licensed user) and 3.3.2 (Managed SIEM, per infrastructure asset). The Initial Term, the Subsequent Term and the notice period for non-renewal are set out in the Order Form and are governed by the MSA.

13.2 Where the Service depends on the Client maintaining a specific number of in-scope endpoints, identities or infrastructure assets, material changes in the number of in-scope units flow through the unit-of-charge mechanism in the MSA and the Order Form. Pass-through of any Third Party Provider price increase is governed by Clause 7.10 of the MSA.

13.3 Remediation work, environmental rebuild or other significant time-based work that falls outside the standard SOC remediation practice published by the Third Party Provider is provided (where Lanmark agrees to provide it) at Lanmark's published rate card at the time the work is performed, and is invoiced separately.

14. Explicit overrides of the Master Services Agreement

Clause 1.3 of the MSA provides that a Service Schedule prevails over the MSA only in respect of specific service detail and only where the Service Schedule explicitly states an override. The following provisions of this Schedule are explicit overrides of the MSA for the Managed Cyber Security Service:

(a) Clauses 5.1 and 5.3.3 of this Schedule set the Service-specific Service Level position: the substantive cyber security work is delivered by the Third Party Provider under the Third Party Provider Terms; Lanmark passes through the Third Party Provider's published Service Levels and does not commit to its own Service Levels for SOC activity; Lanmark engagement management is delivered on a reasonable endeavours basis during Support Hours; where the Third Party Provider's SOC fails to meet its published Service Levels, Lanmark's liability is limited to any remedies available under the Third Party Provider Terms, and Lanmark will use reasonable endeavours to pass through or assist the Client in pursuing those remedies. This is a Service-specific application of Clauses 17.4 and 18.4 of the MSA and prevails over any inconsistent position the MSA might otherwise be read to allow for this Service;

(b) Clause 8 of this Schedule sets out a Service-specific indemnity from the Client to Lanmark, limited to third-party claims (including regulatory action) and Lanmark's reasonable costs and expenses incurred in responding to such claims or action, with five specified triggers (Client breach, misuse of permissions, inaccurate information, failure to act on recommendations, and knowing introduction of vulnerable software, hardware or services). The indemnity at Clause 8 is subject to the limitations and exclusions of liability at Clause 18 of the MSA, including the non-excludable carve-outs at Clause 18.1;

(c) Clause 9 of this Schedule sets out Service-specific disclaimers, including that no cyber security service can guarantee detection or prevention, that the Third Party Provider's tooling, agents and SOC services are supplied under the Third Party Provider Terms and that Lanmark gives no separate warranties for those Third Party Provider products (save for warranties that cannot be excluded under applicable law), and that Lanmark is not liable for cyber-related loss that occurs while the Service is operating in accordance with this Schedule and the Third Party Provider Terms. These disclaimers do not affect Lanmark's own obligation to deploy, configure and manage the Service in accordance with the MSA and this Schedule, and are Service-specific applications of Clauses 17.4 and 18 of the MSA.

Save as set out above, this Schedule does not override the MSA. Any provision of this Schedule that conflicts with the MSA without expressly stating an override under this Clause 14 is to be read consistently with the MSA in accordance with Clause 1.3 of the MSA.