SERVICE SCHEDULE

BMIT MANAGED DETECTION AND RESPONSE SERVICE

Last Update: 9 January 2026

1. **General.** This is a Service Schedule setting out specific terms of Service in respect of BMIT's MDR Service. The MDR Service shall be considered to constitute a Professional Service, pursuant to Annex A5.

2. **Pre-Requisites.** As a prerequisite to the delivery of the MDR Service, BMIT requires the Customer to implement a BMIT recommended SIEM and/or XDR.

   Any matter whatsoever connected to the licensing or subscription to a SIEM and/or XDR is not covered by the MDR Service and this Service Schedule, including but not limited to the costs covering the use of any SIEM and/or XDR. The SIEM and/or XDR needs to be procured separately by the Customer. Implementation effort for the deployment of any SIEM and/or XDR is expressly excluded from the scope of the MDR Service.

   The Customer may opt to procure the recommended SIEM and/or XDR from BMIT and/or may request BMIT to deploy it, provided that in each case, the Parties agree in terms of a separate Work Order.

3. **Service Description.** The MDR Service is a Service that provides the Customer with the following deliverables:

   a. **Service Scope Document.** BMIT and the Customer shall collaborate to define the scope of the MDR Service Scope which will be documented in an MDR Service Scope Document, and which as a minimum shall include the following information:

      i. The Customer's environment, including networks, endpoints, cloud infrastructure, and other relevant assets to be monitored and protected;

      ii. The types of threats, risks, and security events to be monitored by the MDR Service;

      iii. The agreed-upon response protocols and escalation procedures; and

      iv. Any exclusions or limitations to the MDR Service, such as systems or assets outside the agreed scope.

      Any amendments to the MDR Service Scope must be agreed upon in writing by both Parties and documented in an updated MDR Service Scope Document. Such amendments may result in adjustments to the Service Fees, timelines, or other terms, as mutually agreed by the Parties.

   b. **SIEM Management.** BMIT will manage the Customer's SIEM, including the configuration, identification and creation of rules and the optimisation of the rule set.

   c. **Daily Review of Alerts and Events, Escalation & Recommendations.** During Standard Business Hours BMIT will:

      i. Monitor and review security alerts and events collected by the customer's SIEM and/or XDR as per the MDR Service Scope Document; and

      ii. Conduct triage and prioritise alerts based on severity, impact, and urgency. BMIT will escalate detected critical security events to the Customer with

recommendations on how to respond and shall not take further action unless explicitly requested by the Customer and agreed by BMIT.

d. **Reporting, Assessment & Recalibration.** Involves periodic reporting and solution assessments aimed to systematically adjust and refine the SIEM and/or XDR solution's pre-defined rules to enhance the SIEM's and/or XDR's efficacy in identifying legitimate threats, thereby minimising the incidence of false positives and non-security related recurring alerts.

e. **Managed Response Service.** The Customer shall enter into a Professional Services Agreement and maintain a sufficient number of Service Units for the provision of the Managed Response Service. Where required, the Customer shall purchase additional Service Units to enable BMIT to continue delivering the service. Service units shall be consumed when Professional Services Personnel take remediation actions on the Customer's environment under the Professional Services Agreement. The Customer retains full ownership of, and responsibility for, all security incidents and events, including their resolution. Coverage, initiation, deliverables and other operating terms for the Managed Response Service are set out below:

i. **8x5 Managed Response Service Coverage.** Included by default in the MDR Service at no additional charge. This specifies the time window (i.e. Standard Business Hours) during which BMIT will respond to Security Events and alerts, unless the Work Order specifies 24x7 Managed Response Service Coverage (or other coverage) for the relevant Environment and/or scope.

ii. **24x7 Managed Response Service Coverage.** An add-on to the MDR Service which must be expressly included within the Work Order. Where included, BMIT shall provide the Managed Response Service twenty-four (24) hours a day, seven (7) days a week, including Public Holidays.

iii. **Requesting Managed Response Service.** The Customer shall open a Service Request to initiate Managed Response Service, upon which BMIT will allocate resources to respond to and work on the Security Event. All time spent on response, investigation, containment, remediation, recovery, coordination and reporting will be deducted from the Service Units. BMIT shall provide the Customer with regular updates on the status of the Security Event and the Service Units consumed in performing such activities.

iv. **Reporting and Documentation.** BMIT will provide the Customer with a Security Event report upon completion of each response engagement, which includes a summary of actions taken, the number of Service Units consumed, root cause analysis, identified vulnerabilities and recommendations for future prevention.

v. **Playbooks.** Any playbooks and/or scenarios must be agreed in writing between the parties before they are included within the MDR Service Scope.

4. **Customer Responsibility and Acknowledgment**. The Customer acknowledges that it retains ultimate responsibility for decisions related to its information security posture,

incidents and the management of its IT environment, including, but not limited to, the following obligations:

a. **Notification of IT System Changes**. The Customer is responsible for promptly notifying BMIT of any changes or developments in their IT systems, security controls, or operational environment that may affect the MDR Service Scope or effectiveness of the MDR Service.

b. **Attached Appliances, Hardware, and Software.** The Customer acknowledges and agrees that all appliances, hardware, and software that generate logs and are connected to the SIEM, together with their associated services, are the sole responsibility of the Customer. Such responsibility includes ensuring proper functionality and configuration, maintaining vendor support, subscriptions, licenses, and updates, and preventing interruptions or degradation of such components or their associated services. BMIT shall not be liable for any issues arising from the failure, misconfiguration, or interruption of these components or their associated services, including without limitation failures in log generation or transmission, compatibility issues, or service interruptions.

c. **Access and Permissions**. The Customer shall provide BMIT with the necessary access and permissions to the logs and systems that fall under the MDR Service Scope for the purpose of performing the MDR Service.

d. **Timely Response.** The Customer shall respond to escalated alerts and recommendations in a timely manner to ensure effective mitigation of security risks.

e. **Compliance.** The Customer shall be solely responsible for ensuring that it has all necessary rights, authorisations, and permissions to provide, make available, or otherwise expose any data, systems, or information to the MDR Service. This includes, without limitation, obtaining all required authorisations or consents from data subjects, licensors and third parties whatsoever.

5. **Prerequisite/s or other conditions.** The following are additional conditions applicable to any Service defined in this Service Schedule.

a. **Threat hunting and vulnerability assessments**. Such Services are not included in the MDR Service and must be explicitly scoped and included in a Work Order.

b. **Material, licences, and third-party licences and services**. Unless expressly stated in the Work Order, any additional materials, software licences, or third-party services required for the performance of the services are not included in the Service Fees. BMIT shall notify the Customer in writing of any such requirements and associated costs. Subject to the Customer's prior written approval, the Customer shall bear all related costs.

6. **Service Levels.** The Service Levels defined in Annex 28 – General Service Level Agreement shall apply to the MDR Service subject to the provisions in this section.

The MDR Service requires an onboarding period of up to three (3) months for BMIT personnel to configure, fine-tune, and familiarise with the Customer's specific environment. During this period, adherence to the Service Levels specified in Annex 28 – General Service Level Agreement, may be impacted by onboarding activities. Any deviations from the defined Service Levels during this time shall not be considered a breach provided BMIT acts in good faith and keeps the Customer informed of progress.

Standard Service Levels will apply in full after the initial three (3) months or when both Parties agree that onboarding activities have been completed.

a. **Exclusions.** Remediation or actions performed on endpoints outside the defined MDR Service Scope are excluded from SLA measurement and shall not be counted against Service Level compliance.