



# Managed Sentinel and Extended Detection and Response (XDR) Service Schedule to the General Terms

## Contents

A note on 'you' .....	2
Words defined in the General Terms .....	2
Part A – The Managed Sentinel / XDR Service .....	2
1 Service Summary .....	2
2 Graded Service Tiers .....	2
Table 2.1: Service Summary by Graded Service Tier .....	2
3 Service Options.....	12
4 Service Management Boundary .....	12
5 Associated Services and Third Parties .....	12
6 Sale of Goods .....	13
7 Specific Terms .....	13
Part B – Service Delivery and Management.....	16
8 BT's Obligations.....	16
9 Your Obligations .....	16
Part C – Service Levels .....	20
10 Service Levels and Service Remediation Advice Targets .....	20
Part D – Defined Terms.....	22
11 Defined Terms .....	22



## A note on 'you'

'You' and 'your' mean the Customer.

## Words defined in the General Terms

Words that are capitalised but have not been defined in this Schedule have the meanings given to them in the General Terms.

## Part A – The Managed Sentinel / XDR Service

### 1 Service Summary

- 1.1 BT will provide you with a security managed service, supporting threat detection, compliance reporting, and incident response and investigation by the collection and analysis of historical data across a variety of sources and this may include the partial or full remediation of an identified threat via the **Managed Sentinel & XDR Service**.
- 1.2 The Managed Sentinel & XDR Service may not be available in all countries.

### 2 Graded Service Tiers

- 2.1 You will choose one of the Graded Service Tiers, Foundation, Foundation Plus or Premium, to use with your Managed Sentinel & XDR Service, as set out in any applicable order.
- 2.2 A summary of the Service activities undertaken / features available for each Graded Service Tier, is set out in Table 2.1 below :

**Table 2.1: Service Summary by Graded Service Tier**

Service Stage	Feature / Service	Graded Service Tier		
		Foundation	Foundation +	Premium
Initial Set Up	Access / Build Customer Azure Log Analytics Workspace(s)	✓	✓	✓
	Access / Build Customer Managed Sentinel Workspace(s)	✓	✓	✓
	Delegated Rights Management Access to Sentinel	✓	✓	✓
	Content Allowance per quarter	5	10	*unlimited
*Note this is subject to agreement with BT and resource availability				
Controlled Deployment	Data Connector Build : Microsoft Cloud Data Connectors	✓	✓	✓
	Data Connector Build : External Non-Microsoft	✓	✓	✓
	Rules Optimisation : Test and tune	✓	✓	✓



Service Stage	Feature/Service	Graded Service Tier		
		Foundation	Foundation +	Premium
Monitoring and Management	1st Line Incident Response: Validation and severity evaluation	✓	✓	✓
	2nd Line Incident Response : Implementation of mitigation procedures to manage validated incidents	✓	✓	✓
	2nd Line Response : In-depth investigation on multi-stage attacks taking appropriate action e.g. threat hunting	✗	✗	✓
	Remediation of an incident / threat short term and longer term action to improve the customers security posture	✗	✗	✓
	Security Optimisation Manager to provide in-life operational support	✗	✓	✓
	Weekly Summary Report	✗	✓	✓
	Monthly Summary Report	✗	✓	✓
	Executive Summary Report	✗	✓	✓
	Security Orchestration Automation Response	✓	✓	✓
	Playbooks : Tailored so that the customer can change BT CySOC action for incident management	✗	✓	✓
	Limited set of threat intelligence feeds	✓	✗	✗
	Integration of a rich and broad set of Threat Intelligence feeds	✗	✓	✓
Continuous Improvement	SOM Quarterly Service Meetings and Tuning Sessions	✓	✓	✓
	SOM Monthly Service Meetings and Tuning Sessions	✗	✓	✓
	Quarterly Review of Security Policy to identify Changes needed for new threats	✗	✓	✓

2.3 BT will facilitate the setup and delivery of the Managed Sentinel & XDR Service in accordance with the Graded Service Tier selected by you, as set out in the Order.

2.4 Unless the context indicates otherwise, the provisions in respect of Foundation will apply to Foundation Plus and Premium and the provisions of Foundation Plus will apply to Premium. If there is a conflict between the provisions of the Graded Service Tiers, the order of priority of the relevant provisions is:

(a) Premium;



- (b) Foundation Plus; and
- (c) Foundation.

### 2.4 Initial Setup & Controlled Deployment

#### 2.4.1 Foundation

- (a) BT will appoint an unnamed SOM to be your single point of contact during the Initial Setup and Controlled Deployment. The SOM will undertake any activity remotely and will not visit your Site.
- (b) You may request that BT, at an additional charge:
  - (i) appoints a named BT Project Manager to be your single point of contact during the Initial Setup. The named BT Project Manager will undertake any activity remotely and will not visit your Site; or
  - (ii) provide a named BT Project Manager who will be available to attend meetings at your Site, depending on your location, for the duration of the Initial Setup.
- (c) You may make up to 5 Simple Service Requests per quarter ("**Content Allowance – Foundation**").
- (d) Note Foundation level Customers will have a Managed Sentinel Service only, the XDR aspect of the Managed Sentinel & XDR Service is not offered at Foundation level.

#### 2.4.2 Foundation Plus

- (a) BT will provide a named SOM and Project Manager for the duration of the Initial Setup and Controlled Deployment.
- (b) BT will provide you with access to a named SOM on a shared basis, for the duration of the Managed Sentinel & XDR Service, to assist with any issues or requests.
- (c) You may request that, at an additional Charge, the named SOM will be available to attend meetings at your Site, depending on your location, for the duration of the Initial Setup and Controlled Deployment.
- (d) You may make up to 10 Simple Service Requests per quarter ("**Content Allowance – Foundation Plus**").
- (e) Note Foundation Plus level Customers will have a Managed Sentinel Service only, the XDR aspect of the Managed Sentinel & XDR Service is not offered at Foundation Plus level.

#### 2.4.3 Premium

- (a) BT will provide a named SOM and Project Manager for the duration of the Initial Setup and Controlled Deployment.
- (b) BT will provide you with access to a named SOM on a dedicated basis, for the duration of the Managed Sentinel & XDR Service, to assist with any issues or requests.
- (c) You may request that, at an additional Charge, the named SOM will be available to attend meetings at your Site, depending on your location, for the duration of the Initial Setup and Controlled Deployment.
- (d) You may make an unlimited number of Simple Service Requests per quarter, subject to agreement with BT and resource availability ("**Content Allowance – Premium**").

#### 2.5.4 All Tiers

During the Initial Setup any existing Customer Sentinel Solution will be migrated to the Managed Sentinel & XDR Service and this may mean a loss of any original content if you have not archived it.

### 2.5 Custom Content Design and Deployment

#### 2.5.1 Foundation

- (i) BT will provide you with the Standard Default Rule Set.
- (ii) You will select additional Custom Content, as set out in the table at Paragraph 2.1, that you have agreed with BT when you place the Order and ensure that the Custom Content you select meets your requirements. Any additional Custom Content will be charged, in addition, on a Professional Services basis.
- (iii) If you have requested changes to your Custom Content during the Controlled Deployment Custom Content Optimisation Period, you will follow the Content Allowance Change Management Process set out in Paragraph 2.9.2.
- (iv) BT may provide you with Professional Services at an additional Charge, at your request, to assist you in the creation of your Custom Content.
- (v) Should BT elect to standardise Custom Content requested by you, the content will be added to the Standard Default Rule Set, made available to BT's wider customer base, in which case the content will cease to count towards your Custom Content allocation and no additional Charges



will apply. In such circumstances, BT will own the Intellectual Property Rights in relation to the content.

- (vi) Subject to receiving acceptable information from the Data Sources, BT will configure the Managed Sentinel & XDR Service to implement the Custom Content agreed with you and in accordance with Paragraph 8.2.
- (vii) Unless otherwise set out in any applicable Order, the Custom Content Design and Deployment activities set out in this Paragraph 2.5.1 will be undertaken remotely by BT.
- (viii) The SOM will work with you in respect of the Custom Content Design and Deployment.
- (ix) BT may apply additional Charges if work cannot be undertaken remotely and BT is required to attend the Site(s).

### 2.5.2 **Foundation Plus**

- (i) You will select additional Custom Content, as set out in the table at Paragraph 2.1, that you have agreed with BT when you place the Order and ensure that the Custom Content you select meets your requirements. Any additional Custom Content will be charged, in addition, on a Professional Services basis.
- (ii) The SOM will assist you with the configuration of the Managed Sentinel & XDR Service in accordance with the agreed Custom Content.

### 2.5.3 **Premium**

- (i) You will select additional Custom Content, as set out in the table at Paragraph 2.1, that you have agreed with BT when you place the Order and ensure that the Custom Content you select meets your requirements. Any additional Custom Content will be charged, in addition, on a Professional Services basis.
- (ii) You will provide a named contact and appropriate technical support to work with BT during the Controlled Deployment Custom Content Optimisation Period.

### 2.5.4 **All Tiers**

BT will provide further policies tailored to your specific requirements to use as your Custom Content.

## 2.6 **Data Source Connection**

### 2.6.1 **All Tiers**

- (i) BT will configure the Managed Sentinel & XDR Service to receive Event Log Data from the Data Sources agreed with you and set out in the CEP Form attached to any applicable Order.
- (ii) You will configure the Data Sources to send Logs to the Managed Sentinel & XDR Service or provide BT with the requisite details and consents to enable BT to configure the Data Sources directly, as set out in any applicable Order.
- (iii) You will connect the Data Sources to the Managed Sentinel & XDR Service unless BT provides the Data Source, in which case, BT will connect the Data Source to the Managed Sentinel & XDR Service.
- (iv) BT will not be liable for any failure of the Managed Sentinel & XDR Service to process Logs sent to the Managed Sentinel & XDR Service from Data Sources not set out in the CEP Form or set out in any applicable Order.
- (v) BT will only undertake threat correlation or threat monitoring from Data Sources that are set out in the CEP Form.
- (vi) BT may apply additional Charges if work cannot be undertaken remotely and requires BT to attend the Site(s).

## 2.7 **Controlled Deployment - Content Optimisation & Training**

BT will work with you during the Controlled Deployment Custom Content Optimisation Period in accordance with the Graded Service Tier selected by you, as follows:

### 2.7.1 **General**

#### (a) **Foundation**

- (i) The provisions of Paragraph 9.2 will apply.
- (ii) BT will provide you with User Guides.
- (iii) You will comply with the User Guides.
- (iv) Both of us will direct all communication to the other via e-mail.
- (v) If the Controlled Deployment Custom Content Optimisation Period is extended for any reason beyond 90 days from the date you receive Notice from BT in accordance with Paragraph 8.2.2, BT may apply additional Charges.

#### (b) **Foundation Plus and Premium**

Both of us will direct all communication to the other via the SOM.



### 2.7.2 Customer Training

#### (a) Foundation

No Customer training is offered for the Foundation level Service.

#### (b) Foundation Plus and Premium

- (i) BT may deliver training to a specified group of Users, via a conferencing service, if requested by you.
- (ii) Additional training may be offered at BT's sole discretion.

#### (c) All Tiers

You may communicate with BT directly via the SOM or email.

### 2.8 Monitoring and Management

The Monitoring and Management will commence on the Service Start Date.

#### 2.8.1 Proactive Monitoring

##### (a) Foundation

- (i) BT will monitor the performance of the Managed Sentinel & XDR Service at intervals set by BT and, where possible, provide advance incident alert warning to you through the Managed Sentinel & XDR Service, or via email, of impending issues that may affect the Managed Sentinel & XDR Service and that BT identifies as a result of the monitoring. BT may not identify all impending issues.
- (ii) You are responsible for resolving the issues that BT provides you advance warning of in Paragraph 2.8.1(a)(i).
- (iii) You will ensure that you or third parties, as required, configure routing/permissions on platforms or Enabling Services to allow BT to carry out the monitoring.

##### (b) Foundation Plus

- (i) Both of us will agree a process for BT to contact you when it identifies an issue that impacts the Managed Sentinel & XDR Service.
- (ii) BT will use historic and current metrics, captured via the monitoring of the Managed Sentinel & XDR Service, to forecast issues that may impact the performance of the Managed Sentinel & XDR Service and recommend by e-mail to you, mitigating actions which should be taken to address the threat that has been reported.

##### (c) Premium

###### (i) Automated Remediation

Automated Remediation is provided as part of Premium. Following the provision to you of an enhanced incident alert, as specified in Paragraph 2.8.1(a)(i), the SOC support team will automatically implement any Remediating Action necessary, on those managed devices/services, which you have identified as being within scope of the Automated Remediation service ("**Managed Devices/Services**") in respect of the identified threat which has been highlighted by the identified security incident, subject to Paragraphs 2.8.1(c)(ii) and 2.8.1(c)(iii) below.

- (ii) You must have agreed with BT at the outset of the Order that BT can automatically take Remediating Action in relation to managing specific incidents which are in-scope of the BT Managed Sentinel & XDR Service. You must fulfil your obligations, both before and during the Service, as detailed in Paragraph 9 of this Schedule, in order for BT to take any Remediating Action. These obligations include but are not limited to identifying to BT in advance of commencement of the Services (as well as keeping BT informed during the Services) of the specific services, in respect of which, BT is authorised to automatically take Remediating Action. BT shall not be responsible for any impact on any Devices, Customer Equipment, or your wider Network as a result of taking Remediating Action.
- (iii) Where you wish for BT to take Remediating Action, but do not wish for BT to automatically take such Remediating Action, you may specify that BT is to instead seek your prior approval before implementing any Remediating Action.

###### (iv) Deselection of Automated Remediation

- (a) If, prior to the Customer Committed Date, you do not wish for BT to automatically take Remediating Action for any incident as part of the Service, you may give written notice to BT that you do not wish for the Automated Remediation component of the Service to be included in your Order.



- (b) If, during the term of the Services, you do not wish for the Automated Remediation component of the Service to be included in your Order, you may also elect to remove the Automated Remediation by giving written notice to BT. Where you have given written notice during the term of the Service that you no longer wish for Automated Remediation to be included in the Service, BT shall confirm in writing that it has received your request and confirm the date from which Remediating Action shall no longer be taken by BT.
- (c) For the avoidance of doubt, where you give BT written notice of your deselection of the Automated Remediation component of the Service, either before the Service is commenced by BT (as per Paragraph (a) above) or during the operation of the Service (as per Paragraph (b) above), this shall not result in any reduction to the Charges which are payable in line with the selected Service Tier. Furthermore, by giving written notice to deselect Automated Remediation from the Service, you hereby confirm that you shall be responsible for implementing any Remediating Action which BT recommends and that BT shall not be responsible for taking any such Remediating Action, nor liable for the results of any Remediating Action undertaken by you.
- (d) BT does not make any representations or warranties, whether express or implied, as to any outcomes of Remediating Action (whether taken by: (i) BT; or (ii) you (where you have deselected Automated Remediation as per Paragraph 2.8.1(c)(iv)(a) or (b) above)) in respect of specific services, including but not limited to any reduction in the threat impact on any specific Device, any Customer Equipment or your wider Network.

### 2.8.2 Managed Sentinel & XDR – Managed Sentinel BT MSSP Tenant Technical Incident Monitoring

#### (a) All Tiers

BT will proactively monitor and manage the Managed Sentinel BT MSSP Tenant 24x7x365 ("**Managed Sentinel BT MSSP Tenant Technical Incident Monitoring**").

### 2.8.3 Upgrades

#### (a) All Tiers

- (i) BT may from time to time upgrade any Software or firmware used to deliver the Managed Sentinel & XDR Service to ensure that BT remains within the supplier's supported software specification. The dates and times of any Software or firmware upgrades will be notified to you in advance if, in the view of BT, it affects the Managed Sentinel & XDR Service.
- (ii) You will confirm to BT any change in the number of devices / log sources and Data Sources you are adding in to your Managed Sentinel & XDR Service.

### 2.8.4 Capacity Management

#### (a) All Tiers

- (i) If BT identifies that changes in your usage volumes could result in the Managed Sentinel & XDR Service being unable to process the data effectively, or BT identifies that your usage volumes are higher than those agreed, BT will contact you to discuss any recommended changes to the data that is collected, or change in Charges, as a result of your increased usage.
- (ii) If you do not agree to make changes to the data collected, following advice from BT in accordance with Paragraph 2.8.1(a)(i), BT will not be liable for any performance issues of the Managed Sentinel & XDR Service.

### 2.8.5 Technical Incident and Fault Management

#### (a) Foundation

- (i) You will notify all Technical Incidents to the Service Desk.
- (ii) All communications with the Service Desk will be in English.
- (iii) The Service Desk that will action the Technical Incident notifications is available 24x7x365 and is staffed by security trained professionals.
- (iv) BT will give you a Ticket.
- (v) BT will assess the Technical Incident in accordance with the criteria set out in the table below:





Priority	Description
P1	Serious impact and Technical Incident cannot be circumvented, typically where the Managed Sentinel & XDR Service is completely down / unavailable; for example: the Managed Sentinel BT MSSP Tenant is isolated or there is a complete loss of service to your Tenant or critical business functions are prevented from operating.
P2	Large impact on a portion of the Managed Sentinel & XDR Service and cannot be circumvented, causes significant loss of the Managed Sentinel & XDR Service, but the impacted business function is not halted; for example: there are a number of data connectors unavailable.
P3	Small impact on the Managed Sentinel & XDR Service or where a single User or component is affected and it causes some impact to your business; for example there is an intermittent or occasional disturbance which does not have a major impact on the Managed Sentinel & XDR Service or where a temporary work around has been provided.
P4	Minor or intermittent impact to a non-operational element of the Managed Sentinel & XDR Service; for example a temporary failure of reporting or billing.
P5	Incident has no direct impact on the Managed Sentinel & XDR Service. Records normally kept for Technical Incidents are used for information purposes. Example: to track upgrades, for planned outages or for enquiries as well as customer provoked Technical Incidents.

- (vi) BT will review the status of the Technical Incident and amend the priority level assigned initially if necessary.
- (vii) BT will keep you informed throughout the course of the Technical Incident resolution at regular intervals via automated e-mails to the Customer Contact in accordance with Paragraph 10.1.
- (viii) BT will inform you when it believes the Technical Incident is cleared and will close the Ticket when:
  - i. you confirm that the Technical Incident is cleared within 24 hours after having been informed; or
  - ii. BT has attempted unsuccessfully to contact you, in the way agreed between both of us in relation to the Technical Incident, and you have not responded within 24 hours following BT's attempt to contact you.
- (ix) If you confirm that the Technical Incident is not cleared within 24 hours after having been informed, the Ticket will remain open, and BT will continue to work to resolve the Technical Incident.
- (x) Where BT becomes aware of a Technical Incident, Paragraphs 2.8.1(a)(iv) to 2.8.1(a)(ix) will apply.

(b) **Foundation Plus**

- (i) You will notify all Technical Incidents to the Service Desk directly via email.
- (ii) If you notify the Technical Incident to the Service Desk directly, you will have the option of communicating in the languages agreed with BT. If the Service Desk is required to escalate the Technical Incident within BT or to a third-party vendor, then you may be required to communicate in English only.

(c) **Premium**

You will agree with BT whether you report Technical Incidents directly to the Service Desk or to the regional BT SOC.

### 2.8.6 Missing Log Source Monitoring and Reporting





- (a) **All Tiers**
  - (i) BT will notify you, as soon as possible, if one or more of your Data Sources, fails to forward Event Log Data to the Managed Sentinel & XDR Service.
  - (ii) BT will investigate the Technical Incident to determine if the Software or firmware collecting the data is working and functioning correctly. If the Software or firmware is functioning correctly, BT will advise you of the Data Sources that have stopped forwarding and you will investigate and restart the forwarding of the Event Log Data to the Software or firmware delivering the Managed Sentinel & XDR Service.
- 2.8.7 **Event Searches**
  - (a) **Foundation**
    - (i) Logs will be stored in relevant tables. BT will run Scheduled Rules against the relevant tables and categorise each Alerting Incident raised according to its severity for inspection by the BT SOC.
    - (ii) BT will search Events in accordance with the Standard Default Rule Set and the Custom Content selected by you and set out in any applicable Order.
    - (iii) BT may agree to use additional Custom Content in the search of Event Log Data, as set out in any applicable Order.
    - (iv) BT may apply additional Charges if you exceed the applicable Content Allowance set out in the table at Paragraph 2.1.
  - (b) **Foundation Plus**
    - (i) Logs will be stored in relevant tables. BT will run Scheduled Rules against the relevant tables and categorise each Alerting Incident raised according to its severity for inspection by the BT SOC.
    - (ii) BT may apply additional Charges if you exceed the applicable Content Allowance set out in the table at Paragraph 2.1
  - (c) **Premium**
    - (i) Logs will be stored in relevant tables. BT will run Scheduled Rules against the relevant tables and categorise each Alerting Incident raised according to its severity for inspection by the BT SOC.
    - (ii) BT may apply additional Charges if you exceed the applicable Content Allowance set out in the table at Paragraph 2.1
- 2.8.8 **Security Event Management**
  - (a) **All Tiers**

BT will:

    - (i) Analyse Event / Incident data generated by the Managed Sentinel & XDR Service.
    - (ii) Assess appropriate remediation actions to be taken.
    - (iii) If necessary, alert you via email to any potential threats and/or action to be taken by you.
- 2.8.9 **Workbooks and Reports**
  - (a) **Foundation**

BT will provide you with workbooks and standard reporting for the Managed Sentinel & XDR Service via your Tenant or secure email.
  - (b) **Foundation Plus and Premium**

BT will provide you with workbooks and custom reporting for the Managed Sentinel & XDR Service via your Tenant or secure email.
- 2.8.10 **Security Incident Management**
  - (a) **Foundation**
    - (i) **Case Registration**
      - i. BT will notify you of possible Security Incidents, including details of the relevant underlying Event and threat intelligence.
      - ii. BT will raise a Case for each Security Incident that is notified to you.
    - (ii) **Case and Security Incident Management**

Where a Case has been raised by BT in respect of any Security Incident, the BT SOC will contact your nominated customer service teams to notify them of the Security Incident following which BT will close the Case. Such communication may be managed by the BT ticketing system, if this has been selected as part of the Service. If your nominated customer service team does not take any necessary remedial action, BT is not responsible for the ongoing effects of the Security Incident.



(b) **Foundation Plus**

(i) **Case Registration**

- i. BT will notify you of possible Security Incidents, including details of the relevant underlying Event and threat intelligence.
- ii. Mitigation planning: the SOM will provide you with guidance on preventing the recurrence of Security Incidents. This advice may include:
  - (a) advising on malware related to a botnet, known to use command and control servers, that your devices have attempted to connect to; and
  - (b) advising on blocking certain defined network traffic or specific Twitter feeds, at firewall, proxy, or other appropriate control point.

(ii) **Case and Security Incident Management**

Where a Case has been raised by BT in respect of any Security Incident, the BT SOC will contact your nominated customer service teams to:

- i. advise of any necessary remedial action they need to take; and
  - ii. confirm that they have completed any necessary remedial action,
- following which BT will close the Case. If your nominated customer service team does not take the necessary remedial action, BT is not responsible for the ongoing effects of the Security Incident.

(c) **Premium**

(i) **Case Registration**

- i. BT will notify you of possible Security Incidents, including details of the relevant underlying Event and threat intelligence.
- ii. The SOM will provide RCA Support and Ad Hoc Post Security Incident Activity Support in relation to all P1 Security Incidents.

(ii) **Case and Security Incident Management**

The provisions for Premium are as per Foundation Plus, as set out at paragraph 2.8.10 (b)(ii) above.

## 2.9 Continuous Improvement

### 2.9.1 Reviews

(a) **Foundation**

- (i) The SOM will carry out a quarterly review as follows:
  - i. A Managed Sentinel & XDR Service review, focusing on the performance of the Managed Sentinel & XDR Service.
- (ii) The SOM will provide you with a report on the review via email.
- (iii) If requested by you and if agreed to by BT, both of us may hold a conference call to discuss the report.
- (iv) If BT has agreed to participate in a conference call, you will ensure that any report the SOM provides you with will be reviewed by your suitably qualified personnel who are participating in the conference call prior to the conference call taking place.
- (v) You will take appropriate action to address issues as recommended by the SOM in respect of the Managed Sentinel & XDR Service, including implementing security improvements as agreed with the SOM, or as advised by the SOM as your responsibility.

(b) **Foundation Plus**

- (i) The SOM will carry out a review monthly as follows:
  - i. a Managed Sentinel & XDR Service review focusing on the performance of the Managed Sentinel & XDR Service against any Service Targets; and
  - ii. a review of the effectiveness of the Custom Content applied to your Managed Sentinel & XDR Service and the need to fine tune or amend the Custom Content.
- (ii) In addition to taking the action set out in Paragraph 2.9.1(a)(v), you will take appropriate action to address issues in respect of fine tuning or amending your Custom Content as recommended by the SOM.

(c) **Premium**

- (i) The SOM will carry out a review at intervals agreed by both of us but not less than monthly as follows:



- i. a Managed Sentinel & XDR Service focussing on the performance of the Managed Service;
  - ii. a review of the effectiveness of the Custom Content applied to your Managed Sentinel & XDR Service and the need to fine tune or amend the Custom Content.
- (ii) The SOM will also carry out a six-monthly Security Posture review. The SOM will create an action plan with the aim of improving your Security Posture.
- (iii) In addition to taking the action set out in Paragraph 2.9.1(a)(v), you will take appropriate action to address issues in respect of fine tuning or amending your Custom Content as recommended by the SOM.

### 2.9.2 Content Allowance Change Management Process

#### (a) All Tiers

BT will implement changes to the Custom Content in response to your request subject to the following process:

- (i) the authorised Customer Contact will submit requests to change the Custom Content via an email service request to the BT SOC or SOM, providing sufficient detail, and clear instructions as to any changes required, are provided;
- (ii) BT will check each request for its complexity and assess whether the change should be completed via the Content Allowance Change Management Process or whether it requires to proceed in accordance with Clause 31 (Service Amendment) of the General Terms;
- (iii) only changes to Custom Content will be completed via the Content Allowance Change Management Process;
- (iv) BT may provide you with Professional Services at an additional Charge, at your request, to assist you in writing your change request; and
- (v) BT will apply the following "reasonable use" restrictions ("**Reasonable Use Policy**") for changes to the Custom Content:
  - i. you will not raise Standard Change requests more frequently than:
    - a. three per quarter per Managed Sentinel & XDR Service in respect of Foundation;
    - b. ten per quarter per Managed Sentinel & XDR Service in respect of Foundation Plus; and
    - c. unlimited per quarter per Managed Sentinel & XDR Service in respect of Premium (subject to agreement with BT and resource availability).
  - ii. you will not raise Urgent Change requests more frequently than:
    - a. one per quarter per Managed Sentinel & XDR Service in respect of Foundation;
    - b. three per quarter per Managed Sentinel & XDR Service in respect of Foundation Plus; and
    - c. three per quarter per Managed Sentinel & XDR Service in respect of Premium;
  - iii. where BT's measurements show that change requests are being raised more frequently than as set out in Paragraph 2.9.2(a)(v) BT may, either:
    - a. aggregate your requests over a period of time, so that they may be implemented more efficiently. In this event there may be some implementation delays; or
    - b. review your requirements and agree with you an appropriate alternative implementation process and any associated charges.
  - iv. BT will use reasonable endeavours to implement an Emergency Change as quickly as is reasonably practicable. BT may charge you the cost of implementing an Emergency Change.
  - v. BT may implement an Emergency Change without your approval.
  - vi. You are deemed to have approved all changes to the Custom Content that you submit to BT.



- vii. You are responsible for the impact of BT implementing the changes and BT is not liable for any consequences arising from the impact of the implementation of the changes.

(b) **Foundation**

- (i) BT will provide contact details for the BT SOC or SOM to all pre-agreed and authorised Customer Contacts to enable you to submit your change requests.
- (ii) Simple Changes subject to the Reasonable Use Policy set out in Paragraph 2.9.2 (a)(v) are included in the Charges.
- (iii) Complex Change requests will proceed in accordance with Clause 31 (Service Amendment) of the General Terms and BT will charge you the cost of implementing Complex Changes.
- (iv) BT will communicate the status of change requests via e-mail to the Customer Contact requesting the change.

(c) **Foundation Plus**

- (i) The authorised Customer Contact may submit requests to modify the Custom Content, via email to the BT SOC or direct to the SOM.

(d) **Premium**

- (i) BT will use reasonable endeavours to identify errors or potential unforeseen consequences of your requested Simple Changes and Complex Changes and advise you appropriately and will not be liable for any consequence arising from:
  - i. your miss-specification of your security requirements in relation to the Custom Content; or
  - ii. unforeseen consequences of a correctly specified and correctly implemented Custom Content.

### 3 Service Options

There are no Service Options available for the Managed Sentinel & XDR Service.

### 4 Service Management Boundary

- 4.1 BT will provide and manage the Managed Sentinel & XDR Service in accordance with Parts A, B and C of this Schedule and as set out in any applicable Order ("**Service Management Boundary**").
- 4.2 BT will have no responsibility for the Managed Sentinel & XDR Service outside the Service Management Boundary.
- 4.3 BT does not make any representations, whether express or implied, about whether the Managed Sentinel & XDR Service will operate in combination with any Customer Equipment or other equipment and software.
- 4.4 **Service Restrictions**
  - 4.4.1 BT will not be liable if BT is unable to deliver the Managed Sentinel & XDR Service, or any part of the Managed Sentinel & XDR Service, due to a failure of any Customer Equipment, including any Customer Log sources and Data Sources.
  - 4.4.2 BT does not guarantee that the Managed Sentinel & XDR Service will detect or block all malicious threats.
  - 4.4.3 The Managed Sentinel & XDR Service assumes standard Logs and functionality, as communicated to you by BT. BT will not be liable for any inability to provide the Managed Sentinel & XDR Service, or any degradation of the Managed Sentinel & XDR Service, if you do not have and maintain the appropriate Logs and functionality.

### 5 Associated Services and Third Parties

- 5.1 You will have the following services in place that will connect to the BT Managed Sentinel & XDR Service and are necessary for the Managed Sentinel & XDR Service to function (dependent upon which contract tier has been signed) and will ensure that these services meet the minimum technical requirements that BT specifies:
  - 5.1.1 Microsoft Sentinel and Log Analytic workspace;
  - 5.1.2 Microsoft 365 Defender ;
  - 5.1.3 Microsoft Defender for Cloud



(each an “**Enabling Service**”).

- 5.2 In order to provide our Sentinel and or XDR service, BT will also require access to your tenants that provide your user and infrastructure protection using the Microsoft Defender suite of services.
- 5.3 You will allow BT access to the appropriate services within your Tenant to enable the creation and ongoing management of the Managed Sentinel & XDR Service.
- 5.4 If BT provides you with any services other than the Managed Sentinel & XDR Service (including, but not limited to any Enabling Service) this Schedule will not apply to those services and those services will be governed by their separate terms.

## 6 Sale of Goods

- 6.1 The UN Convention on Contracts for the International Sale of Goods will not apply to the Contract.

## 7 Specific Terms

### 7.1 Changes to the Contract

- 7.1.1 BT may amend the Contract (including the Charges) at any time by either:
  - (a) publishing the amendment online at [www.bt.com/pricing](http://www.bt.com/pricing) or [www.bt.com/terms](http://www.bt.com/terms) (or any other online address that BT advises you of); or
  - (b) by giving Notice to you.
- 7.1.2 In the event that the amendments cause you material detriment, BT will give you Notice at least 30 days before the change is to take effect and, in the case of any other amendments, at least one day before the change is to take effect.
- 7.1.3 If BT makes any amendment to the Contract that causes you material detriment, you will not have to pay any Termination Charges if you give Notice to terminate the affected Service in accordance with Clause 17 of the General Terms within:
  - (a) 90 days after the date of notification if BT has only published the amendment online in accordance with Paragraph 7.1.1(a); or
  - (b) 30 days after the date of the Notice if BT has given you Notice in accordance with Paragraph 7.1.1(b).

### 7.2 Minimum Period of Service

- 7.2.1 At the end of the Minimum Period of Service, unless one of us has given Notice to the other of an intention to terminate the Managed Sentinel & XDR Service in accordance with the Contract, BT will continue to provide the Managed Sentinel & XDR Service and each of us will continue to perform our obligations in accordance with the Contract.
- 7.2.2 If either of us gives Notice to the other of an intention to terminate the Managed Sentinel & XDR Service, BT will cease delivering the Managed Sentinel & XDR Service at the time of 23:59 on the last day of the Minimum Period of Service.

### 7.3 Customer Committed Date

- 7.3.1 If you request a change to the Managed Sentinel & XDR Service or any part of the Managed Sentinel & XDR Service, then BT may revise the Customer Committed Date to accommodate that change.
- 7.3.2 BT may expedite delivery of the Managed Sentinel & XDR Service for operational reasons or in response to a request from you, but this will not revise the Customer Committed Date.

### 7.4 Right to Use

- 7.4.1 BT gives you a non-exclusive, non-transferable and limited right to use the Managed Sentinel & XDR Service for your internal business purposes only.
- 7.4.2 You will not resell or otherwise transfer the Managed Sentinel & XDR Service granted under this Contract.

### 7.5 Invoicing

- 7.5.1 Unless set out otherwise in any applicable Order, BT will invoice you for the following Charges in the amounts set out in any applicable Order:
  - (a) Installation Charges, in advance once you have placed the Order;
  - (b) Recurring Charges, monthly in arrears (depending on your billing frequency). For any period where the Managed Sentinel & XDR Service is provided for less than one month, the full monthly charge will be applied; and
  - (c) Professional Services Charges.
- 7.5.2 BT may invoice you for any of the following Charges in addition to those set out in any applicable Order:

- (a) Charges for investigating Technical Incidents that you report to BT where BT finds no Technical Incident or that the Technical Incident is caused by something for which BT is not responsible under the Contract;
- (b) Charges for commissioning the Managed Sentinel & XDR Service in accordance with Paragraph 8.2, outside of Business Hours;
- (c) Charges for expediting provision of the Managed Sentinel & XDR Service at your request after BT has informed you of the Customer Committed Date;
- (d) Charges for restoring the Managed Sentinel & XDR Service if the Managed Sentinel & XDR Service has been suspended in accordance with Clause 10.1.2 of the General Terms;
- (e) Charges for cancelling the Managed Sentinel & XDR Service in accordance with Clause 16 of the General Terms;
- (f) additional Charges in accordance with Paragraph 0(v) if the Controlled Deployment Custom Content Optimisation Period is extended for any reason beyond 90 days after receiving Notice from BT in accordance with Paragraph 8.2.2;
- (g) Charges for appointing and providing a named BT Project Manager if you have purchased Foundation in accordance with Paragraph 2.4(c)(b);
- (h) Charges for the named SOM attending meetings at your Site if you have purchased Foundation Plus or Premium in accordance with Paragraph 2.4.2(c) or Paragraph 2.4.3(c);
- (i) Charges for additional Custom Content in accordance with Paragraphs 2.5.1(ii), 2.5.2(i) and 2.5.3(i);
- (j) Charges for the cost of implementing Complex Changes in accordance with Paragraph 2.9.2(b)(iii) and Emergency Changes in accordance with Paragraph 2.9.2(b)(iii);
- (k) Charges associated with an appropriate alternative implementation process if you have raised change requests more frequently than allowed by the Reasonable Use Policy in accordance with Paragraph 2.9.2(a)(v);
- (l) Charges to cover any costs reasonably incurred by BT as a result of any non-conformity of the Customer Equipment in accordance with Paragraph 7.5.2(l);
- (m) any other Charges as set out in any applicable Order or as otherwise agreed between both of us; and
- (n) any Termination Charges incurred in accordance with Paragraph 7.6 upon termination of the relevant Managed Sentinel & XDR Service.

#### 7.5.3 Usage Volume Reasonable Use Policy

- (a) Where your monthly usage volume exceeds the agreed Usage Volume, as determined by the average usage volume measured over a consecutive three-month period, BT may increase the monthly Charges to reflect the increase in usage volumes.
- (b) BT will notify you at least one month in advance before any changes in the Charges are applied.

7.5.4 BT is not responsible for any increases to charges between you and Microsoft where you have requested BT modify the Managed Sentinel & XDR Service.

### 7.6 Termination Charges

7.6.1 If you terminate the Contract or the Managed Sentinel & XDR Service for convenience in accordance with Clause 17 of the General Terms you will pay BT:

- (a) all outstanding Charges or payments due and payable under the Contract;
- (b) any other Charges as set out in any applicable Order; and
- (c) any charges that BT has to pay a supplier as a result of early termination of the Managed Sentinel & XDR Service.

7.6.2 In addition to the Charges set out at Paragraph 7.6.1 above, if you terminate during the Minimum Period of Service, you will pay BT:

- (a) for any parts of the Managed Sentinel & XDR Service that were terminated during the first 12 months of the Minimum Period of Service, Termination Charges, as compensation, equal to:
  - (i) 100 per cent of the Recurring Charges for any remaining months of the first 12 months of the Minimum Period of Service;
  - (ii) 20 per cent of the Recurring Charges for the remaining months, other than the first 12 months of the Minimum Period of Service;
  - (iii) any waived Installation Charges; and
- (b) for any parts of the Managed Sentinel & XDR Service that were terminated after the first 12 months of the Minimum Period of Service, Termination Charges, as compensation, equal to 20 per cent of the Recurring Charges for any remaining months of the Minimum Period of Service.

### 7.7 Upgrade to a Higher Graded Service Tier



- 7.7.1 You may upgrade to a higher Graded Service Tier during the Minimum Period of Service.
- 7.7.2 No Termination Charges will be payable from the Graded Service Tier you are moving from. New Charges for the upgraded Graded Service Tier will be set out in the Order.
- 7.7.3 A new Minimum Period of Service will apply to the upgraded Graded Service Tier as set out in the Order.
- 7.7.4 You may not downgrade to a lower Graded Service Tier.





### Part B – Service Delivery and Management

#### 8 BT's Obligations

##### 8.1 Service Delivery

Before the Service Start Date and, where applicable, throughout the provision of the Managed Sentinel & XDR Service, BT:

- 8.1.1 will provide you with contact details for the Service Desk;
- 8.1.2 will comply with all reasonable health and safety rules and regulations and reasonable security requirements that apply at the Site(s) and that you have notified to BT in writing, but BT will not be liable if, as a result of any such compliance, BT is in breach of any of its obligations under this Contract;
- 8.1.3 will, once the requirements of the Managed Sentinel & XDR Service have been confirmed and agreed, and, where applicable, you provide the details set out in Paragraph 7.3.1, provide you with a Customer Committed Date and will use reasonable endeavours to meet any Customer Committed Date;
- 8.1.4 will not be responsible for any:
  - (a) delay in providing;
  - (b) interruption to; or
  - (c) degradation of,the Managed Sentinel & XDR Service caused by errors or omissions in any information, instructions or scripts provided to BT by you in connection with the Managed Sentinel & XDR Service, or any actions taken by BT at your direction.

##### 8.2 Commissioning of the Service

Before the Service Start Date, BT will:

- 8.2.1 conduct a series of standard tests on the appropriate tenants that are used as part of the Managed Sentinel & XDR Service to ensure that the Service is configured correctly; and
- 8.2.2 on the date that BT has completed the activities in this Paragraph 8.2, confirm that the Managed Sentinel & XDR Service is available for Controlled Deployment Custom Content Optimisation and performance of any Acceptance Tests in accordance with Paragraph 9.2.

##### 8.3 During Operation

On and from the Service Start Date, BT:

- 8.3.1 will respond and use reasonable endeavours to remedy a Technical Incident without undue delay if BT detects or if you report a Technical Incident;
- 8.3.2 will respond to Security Incidents as set out in Paragraph 10.1;
- 8.3.3 may, in the event of a security breach affecting the Managed Sentinel & XDR Service, require you to change any or all of your passwords;
- 8.3.4 will use secure protocols or provide a secure management link to connect to the Software or firmware at your Site(s) via the Internet or other agreed network connection, in order to monitor the Managed Sentinel & XDR Service proactively and to assist in Technical Incident diagnosis; and
- 8.3.5 may carry out Maintenance from time to time and will use reasonable endeavours to inform you at least five Business Days before any Planned Maintenance on the Managed Sentinel & XDR Service. However, BT may inform you with less notice than normal where Maintenance is required in an emergency. BT may carry out the Maintenance remotely or by visiting the Site as appropriate.
- 8.3.7 will implement and take the appropriate Remediating Action required to manage the incident / threat identified as part of the Managed Sentinel & XDR Service, via automatic remediation where agreed with the customer as quickly as is technically practicable.

##### 8.4 The End of the Service

On termination of the Managed Sentinel & XDR Service by either of us, BT:

- 8.4.1 may delete any Content, including stored Logs or any configuration data relating to BT's management of the Managed Sentinel & XDR Service; and
- 8.4.2 may remove the Managed Sentinel & XDR Service from your Tenant.

#### 9 Your Obligations

##### 9.1 Service Delivery

Before the Service Start Date and, where applicable, throughout the provision of the Managed Sentinel & XDR Service, you will:



- 9.1.1 provide BT access at the appropriate security level to your Tenant;
- 9.1.2 nominate suitably empowered and informed customer service teams that will interact with the BT SOC when raising Technical Incidents and when responding to Security Incidents;
- 9.1.3 provide BT with information reasonably requested (including business and technical information accurate in all respects) in a timely manner and promptly notify BT, in writing, of any changes to the information you have provided;
- 9.1.4 provide BT with a copy of your security policies;
- 9.1.5 ensure that you have the capabilities, Log Forwarders and supported protocols in place to be able to forward Event Log Data to the Managed Sentinel & XDR Service;
- 9.1.6 provide BT with the ability to install any Microsoft Sentinel & XDR Software or firmware inside your network on a network segment where Customer Equipment Log Data Sources being monitored can deliver Event Log Data to the Managed Sentinel & XDR Service;
- 9.1.7 attend integration meetings to discuss further tuning and configuration of the Managed Sentinel & XDR Service;
- 9.1.8 complete any preparation activities including installation and maintenance of any software or hardware that is not included as part of the Managed Sentinel & XDR Service, that BT may request to enable you to receive the Managed Sentinel & XDR Service promptly and in accordance with any reasonable timescales;
- 9.1.9 in jurisdictions where an employer is legally required to make a disclosure to its Users and other employees:
  - (a) inform your Users that as part of the Managed Sentinel & XDR Service being delivered by BT, BT may monitor and report to you the use of any targeted applications by them;
  - (b) ensure that your Users have consented or are deemed to have consented to such monitoring and reporting (if such consent is legally required); and
  - (c) agree that BT will not be liable for any failure by you to comply with this Paragraph 9.1.9, you will be liable to BT for any Claims, losses, costs or liabilities incurred or suffered by BT due to your failure to comply with this Paragraph 9.1.9;
- 9.1.10 if applicable, ensure that the LAN protocols and applications you use are compatible with the Managed Sentinel & XDR Service;
- 9.1.11 where applicable, prepare and maintain the Site(s) for the supply of the Managed Sentinel & XDR Service, in accordance with any instructions from BT, including:
  - (a) complying with any Site accommodation requirements as set out in any applicable Order;
  - (b) providing a secure, continuous power supply at the Site(s) for the operation and maintenance of the Managed Sentinel & XDR Service at such points and with such connections as BT specifies, and, in order to mitigate any interruption to the Managed Sentinel & XDR Service resulting from failure in the principal power supply, provide back-up power with sufficient capacity to conform to the standby requirements of the applicable standards.
- 9.1.12 give Notice to BT, five Business Days in advance, and provide details, of any changes to your network, that may affect the functioning of the Managed Sentinel & XDR Service. If this information is not provided, or is provided less than five Business Days before a change, then BT will not be liable for any Technical or Security Incidents or incorrect functioning of the Managed Sentinel & XDR Service as a result of the change;
- 9.1.13 ensure that your WAN or Internet access circuit bandwidth is sufficient to meet your requirements and for the management access by BT;
- 9.1.14 manage, and provide BT with, accurate details of your internal IP Address design;
- 9.1.15 ensure that the Managed Sentinel Devices are able to receive updates, such as vulnerability signatures, directly over the Internet, or over an alternative path agreed with BT for that purpose;
- 9.1.16 if BT has agreed to provide any part of the Managed Sentinel & XDR Service using Customer Equipment, ensure that the relevant Customer Equipment:
  - (a) complies with any minimum specification given to you by BT;
  - (b) will comply with the requirements of Paragraph 9.3.4;
  - (c) is fully functional; andif the relevant Customer Equipment does not comply with this Paragraph 9.1.16 then BT may raise an additional Charge to cover any costs reasonably incurred by BT as a result of the non-conformity, and any agreed installation dates and the Customer Committed Date(s) may no longer apply;
- 9.1.17 ensure that your network and all applications conform to relevant industry standards and provide written confirmation to BT upon reasonable request;



- 9.1.18 for any Customer Equipment used in the Managed Sentinel & XDR Service, be responsible for ensuring compliance with Applicable Law, including obtaining (if required) local import and User licenses and the written authority from all respective authorities, particularly for countries where the use and import of encryption Software and devices may be restricted by Applicable Law, or the export and re-export of the encryption Software or devices may be subject to the United States of America export control law and not act to misuse the Managed Sentinel & XDR Service as provided by BT to contravene or circumvent these laws. BT may treat any contravention of these laws as a material breach and:
- (a) suspend the Managed Sentinel & XDR Service and BT may refuse to restore the Managed Sentinel & XDR Service until BT receives an acceptable assurance from you that there will be no further contravention; or
  - (b) terminate the Managed Sentinel & XDR Service upon Notice in accordance with Clause 18 of the General Terms;
- 9.1.19 provide BT with any information that is reasonably requested by any regulatory body, legal authority or government entity in any country in connection with regulatory, administrative, legal or lawful interception requests;
- 9.1.20 be responsible for any issues on Users' machines or your servers (e.g. operating system, coding languages and security settings) making sure all issues are dealt with in a timely manner and ensure that any repaired devices are configured correctly to send data to the Managed Sentinel & XDR Service; and
- 9.1.21 ensure that your network or Internet connectivity performs correctly and will send Logs to the Managed Sentinel & XDR Service;

### 9.2 **Controlled Deployment Custom Content Optimisation and Acceptance Tests**

- 9.2.1 You will carry out the Controlled Deployment Custom Content Optimisation within the Controlled Deployment Custom Content Optimisation Period.
- 9.2.2 In respect of Foundation Plus and Premium, both of us will jointly carry out the Controlled Deployment Custom Content Optimisation. You will use reasonable endeavours to complete the Controlled Deployment Custom Content Optimisation as early into the Controlled Deployment Custom Content Optimisation Period as possible.
- 9.2.3 You will submit any changes you require to the Custom Content as a result of the Controlled Deployment Custom Content Optimisation through the Custom Content Change Management Process.
- 9.2.4 You will carry out the Acceptance Tests for the Managed Sentinel & XDR Service during the Controlled Deployment Custom Content Optimisation Period and use reasonable endeavours to complete the Acceptance Tests as early into the Controlled Deployment Custom Content Optimisation Period as possible.
- 9.2.5 The Managed Sentinel & XDR Service is accepted by you if you confirm acceptance in writing during the Controlled Deployment Custom Content Optimisation Period or is treated as being accepted by you if you do not provide BT with Notice to the contrary by the end of the Controlled Deployment Custom Content Optimisation Period.
- 9.2.6 Subject to Paragraph 9.2.7, the Service Start Date will be the earlier of the following:
- (a) the date that you confirm or BT deems acceptance of the Managed Sentinel & XDR Service in writing in accordance with Paragraph 9.2.5; or
  - (b) the date of the first day following the Controlled Deployment Custom Content Optimisation Period.
- 9.2.7 If, during the Controlled Deployment Custom Content Optimisation Period, you provide BT Notice that the Acceptance Tests have not been passed, BT will remedy the non-conformance without undue delay and provide you Notice that BT has remedied the non-conformance and inform you of the Service Start Date.

### 9.3 **During Operation**

On and from the Service Start Date, you will:

- 9.3.1 ensure that Users report Technical Incidents to the Customer Contact and not to the Service Desk;
- 9.3.2 ensure that the Customer Contact will take Technical Incident reports from Users and pass these to the Service Desk using the reporting procedures agreed between both of us, and is available for all subsequent Technical Incident management communications;
- 9.3.3 monitor and maintain any Customer Equipment connected to the Managed Sentinel & XDR Service or used in connection with the Managed Sentinel & XDR Service;
- 9.3.4 ensure that any Customer Equipment that is connected to the Managed Sentinel & XDR Service or that you use, directly or indirectly, in relation to the Managed Sentinel & XDR Service is:



- (a) connected using the applicable BT Network termination point, unless you have BT's permission to connect by another means;
  - (b) technically compatible with the Managed Sentinel & XDR Service and will not harm or damage BT Equipment, the BT Network, or any of BT's suppliers' or subcontractors' network or equipment; and
  - (c) approved and used in accordance with relevant instructions, standards and Applicable Law and any safety and security procedures applicable to the use of that Customer Equipment;
- 9.3.5 immediately disconnect any Customer Equipment, or advise BT to do so at your expense, where Customer Equipment does not meet any relevant instructions' standards or Applicable Law and redress the issues with the Customer Equipment prior to reconnection to the Managed Sentinel & XDR Service;
- 9.3.6 submit a request to BT if you want to change any Managed Sentinel Device's IP Address or change, add or remove any Data Source;
- 9.3.7 notify BT of any planned work that you intend to undertake that may cause a Technical Incident;
- 9.3.8 ensure that all Enabling Services are maintained throughout the provision of the Managed Sentinel & XDR Service;
- 9.3.9 be responsible for any conclusions drawn from, and rectification of, any issues identified by use of the Managed Sentinel & XDR Service, supported by BT in accordance with the Graded Service Tier selected by you and set out in any applicable Order;
- 9.3.10 maintain a written list of current Users and provide a copy of such list to BT within five Business Days following BT's written request at any time;
- 9.3.11 ensure the security and proper use of all valid User access profiles, passwords and other systems administration information used in connection with the Managed Sentinel & XDR Service and:
  - (a) immediately terminate access for any person who is no longer a User;
  - (b) inform BT immediately if a User's ID or password has, or is likely to, become known to an unauthorised person, or is being or may be used in an unauthorised way;
  - (c) take all reasonable steps to prevent unauthorised access to the Managed Sentinel & XDR Service; and
  - (d) satisfy BT's security checks if a password is lost or forgotten;
- 9.3.12 ensure that appropriate Log level auditing is turned on for all Data Sources monitored by the Managed Sentinel & XDR Service. If the Log level auditing is not turned on, this will impact the Managed Sentinel & XDR Service;
- 9.3.13 attend review meetings, as required by BT;
- 9.3.14 prior to the meeting referred to in Paragraph 9.3.13, provide the most up to date network diagram of your existing IT network;
- 9.3.15 if you fail to attend the review meetings referred to in Paragraph 9.3.13 regularly, BT has the right to refuse your requests for tuning of the Managed Sentinel & XDR Service;
- 9.3.16 in the event of a Technical Incident requiring your technical support, provide BT with the necessary support and timely authorisation for any necessary changes notified by BT to your Customer Contact; and
- 9.3.17 provide 60 days' Notice prior to termination, if you require your Logs to be transferred.
- 9.3.18 For the XDR element of the Managed Sentinel & XDR Service, you will explicitly point out the Managed Devices/Services (those devices/services in respect of which BT is authorised to automatically implement any Remediating Action) and those managed devices/services for which BT must seek your approval before implementing any Remediating Action; and
- 9.3.19 update the policies for any Managed Devices/Services, so that BT may access and automatically implement any Remediating Action in respect of those Managed Devices/Services. For the avoidance of doubt, BT shall not be liable for the impact of any Remediating Action taken in respect of a specific managed device/service where you have not communicated clearly to BT that no Remediating Action should be taken automatically by BT in respect of that specific managed device/service.
- 9.3.20 promptly notify BT in writing where you no longer wish for Automated Remediation to form part of your Service (in line with Paragraph 2.8.1 (c)(iv)(b) above) and acknowledge that, where you undertake any Remediating Action, BT shall not be liable for the results of such Remediating Action (as per Paragraph 2.8.1 (c)(iv)(c)).

#### 9.4 The End of the Service

On termination of the Managed Sentinel & XDR Service by either of us, you will:

- 9.4.1 provide BT with all reasonable assistance necessary to remove BT Equipment from the Site(s);



## Managed Sentinel & XDR Service Schedule

- 9.4.2 disconnect any Customer Equipment from BT Equipment located at the Site(s);
- 9.4.3 not dispose of or use BT Equipment other than in accordance with BT's written instructions or authorisation;
- 9.4.4 arrange for any BT Equipment located at the Site(s) to be returned to BT or, if BT has elected to disconnect and remove the BT Equipment located at the Site(s) in accordance with Paragraph 8.4.2 above, arrange access for BT to carry out such disconnection and removal; and
- 9.4.5 be liable for any reasonable costs of recovery that BT incurs in recovering the BT Equipment.

### Part C – Service Levels

#### 10 Service Levels and Service Remediation Advice Targets

##### 10.1 Managed Sentinel & XDR – Service Targets

Priority	Graded Service Level	Security Incident: Notification Target	Target Time: Remediation Advice	Target Time: Commencement of Remediation Action
P1	Foundation	whenever a progress update is available	4 hours	N/A
	Foundation Plus	within 30 minutes from the Security Incident being reported	4 hours	N/A
	Premium	within 30 minutes from the Security Incident being reported	4 hours	*4 hours
P2	Foundation	whenever a progress update is available	8 hours	N/A
	Foundation Plus	within 2 hours from the Security Incident being reported	8 hours	N/A
	Premium	within 2 hours from the Security Incident being reported	8 hours	*8 hours
P3	Foundation	whenever a progress update is available	24 hours	N/A
	Foundation Plus	within 4 hours from the Security Incident being reported	24 hours	N/A
	Premium	within 4 hours from the Security Incident being reported	24 hours	*24 hours
P4	Foundation	whenever a progress update is available	Weekly/Monthly in agreed reporting	N/A
	Foundation Plus	within 5 hours from the Security Incident being reported	Weekly/Monthly in agreed reporting	N/A
	Premium	within 5 hours from the Security Incident being reported	Weekly/Monthly in agreed reporting	*Weekly/Monthly as agreed
P5	Foundation	whenever a progress update is available	Weekly/Monthly in agreed reporting	N/A



## Managed Sentinel & XDR Service Schedule

	Foundation Plus	within 6 hours from the Security Incident being reported	Weekly/Monthly in agreed reporting	N/A
	Premium	within 6 hours from the Security Incident being reported	Weekly/Monthly in agreed reporting	*Weekly/Monthly as agreed
* Note as the length of time to complete any remediation will vary according to the nature of the incident, this figure represents the time to start the remediation action				

- 10.1.1 From the Service Start Date, BT will aim to provide you with an initial response in relation to a Security Incident ("**Security Incident Notification**") in accordance with the target response times as set out in the table above for the Graded Service Tier selected by you and set out in any applicable Order.
- 10.1.2 BT will not provide a progress update while BT is waiting on your input or feedback.
- 10.1.3 BT will not provide a Target time for Security Incident resolution because the mitigation responsibility rests with you.
- 10.1.4 The Target Response Times shown in the table above are targets only and BT will have no liability for failure to meet them.
- 10.1.5 No Service Credits apply to the provision of the Security Incident target response times in the table above or the Target Time for Remediation Advice.

### 10.2 Service Level Availability

- 10.2.1 There is no standard Service Level Availability for this Managed Sentinel & XDR Service.





### Part D – Defined Terms

#### 11 Defined Terms

In addition to the defined terms in the General Terms, capitalised terms in this Schedule will have the below meanings (and in the case of conflict between these defined terms and the defined terms in the General Terms, these defined terms will take precedence for the purposes of this Schedule). BT has repeated some definitions in this Schedule that are already defined in the General Terms. This is to make it easier for you to find the definitions when reading this Schedule.

**"Acceptance Tests"** means those objective tests conducted by you that when passed confirm that you accept the Managed Sentinel & XDR Service and that the Managed Sentinel & XDR Service is ready for use in accordance with Paragraph 9.2.5.

**"Ad Hoc Post Security Incident Activity Support"** means ad hoc activity, requested by you, following a previously reported Security Incident.

**"Alerting Incident"** means a Security Incident created by the Managed Sentinel & XDR Service as a result of a Scheduled Rule, MS Rule or Fusion Rule meeting its alerting threshold.

**"Automated Remediation"** means the Service component outlined at Paragraph 2.8.1(c).

**"Azure Active Directory"** means Microsoft's cloud based identity and access management system.

**"Azure Lighthouse"** means a control panel that integrates with portals, IT service management tools, and monitoring tools to let service providers view and manage Azure deployments for customers.

**"BT Project Manager"** means the delivery manager BT appoints to liaise with you on Initial Setup and Controlled Deployment matters as set out in this Schedule.

**"BT SOC"** means BT's security operations centre where BT's team of security analysts and specialists use various security technologies to monitor and protect people, processes and assets across an organisation.

**"Business Hours"** means between the hours of 0800 and 1700 in a Business Day.

**"Case"** means an issue that is "opened" and "closed" over a period of time to achieve resolution of a Security Incident that has been identified by the Managed Sentinel & XDR Service.

**"CEP Form"** means the customer enrolment package form attached to any applicable Order.

**"Complex Change"** means a change that is not a Simple Change. Examples of Complex Changes are set out in the document titled Simple and Complex Changes which will be shared with you on completion of Initial Setup.

**"Content"** means applications, data, information (including emails), video, graphics, sound, music, photographs, software or any other material.

**"Content Allowance"** means the allowance of Custom Content as set out in the table at Paragraph 2.1.

**"Content Allowance Change Management Process"** means the process in relation to changes to the Custom Content as set out in Paragraph 2.9.2.

**"Content Allowance – Foundation"** means the Foundation allowance for Simple Service Requests per quarter as specified in paragraph 2.4.1 (c).

**"Content Allowance – Foundation Plus"** means the Foundation Plus allowance for Simple Service Requests per quarter as specified in paragraph 2.4.2 (d).

**"Content Allowance – Premium"** means the Premium allowance for Simple Service Requests per quarter as specified in paragraph 2.4.3 (d).

**"Continuous Improvement"** means the continuous improvement phase of the Managed Sentinel & XDR Service as set out in Paragraph 2.9.

**"Controlled Deployment"** means the controlled deployment phase of the Managed Sentinel & XDR Service as set out in Paragraph 2.7.

**"Controlled Deployment Custom Content Optimisation"** means the fine tuning of your Custom Content, conducted by you or in respect of Foundation Plus or Premium only both of us jointly.

**"Controlled Deployment Custom Content Optimisation Period"** means up to 90 Business Days after receiving Notice from BT in accordance with Paragraph 8.2.2. This period may be extended by BT depending on various parameters including number of Logs, creation of rule sets and wider activities running and testing associated Playbooks.

**"Custom Content"** means custom Scheduled Rules or workbooks as applicable specific to your requirements and individual deployment that are created in the Managed Sentinel & XDR Service and set out in any applicable Order.

**"Custom Content Design and Deployment"** means the Custom Content design and deployment services set out in Paragraph 0.





**"Customer Equipment"** means any equipment including any Purchased Equipment and any software, other than BT Equipment, used by you in connection with the Managed Sentinel & XDR Service.

**"Customer Sentinel Solution"** means your original Sentinel Solution before contracting with BT to provide the Managed Sentinel & XDR Service .

**"Customer Service Description"** means the document that describes the Managed Sentinel & XDR Service and includes, for instance, the Standard Default Rule Set. This document is not legally binding.

**"Data Sources"** means data from network and security devices and host systems that are compatible with the Supported Device List.

**"Delegated Rights Management"** means BT can sign into your Tenant and have authorisation to work in delegated customer subscriptions and resource groups.

**"Emergency Change"** means a highly critical, Simple Change that must be implemented as soon as possible specifically to address an issue having an adverse impact to business operations, or to prevent or resolve a P1 Technical Incident or a P1 Security Incident.

**"Enabling Services"** has the meaning given in Paragraph 5.1.

**"Event"** means an event that is generated by your network, security or IT systems that is then forwarded to the Managed Sentinel & XDR Service for processing, analysis and storage.

**"Event Search"** means scheduled analysis of normalised Event Log Data, to track threats, monitor User activity and track related transactions and data access and categorise each Event according to its severity for inspection by the BT SOC.

**"Event Log Data"** means the data that is generated by your network, security or IT system in response to events or activity on the Data Sources.

**"Foundation"** means the Foundation Graded Service Tier as set out in this Schedule.

**"Foundation Plus"** means the Foundation Plus Graded Service Tier as set out in this Schedule.

**"Fusion Rule"** means rules taking Microsoft machine learning and combining various alerts to generate a new alert that may otherwise have been very difficult to detect.

**"General Terms"** means the general terms to which this Schedule is attached or can be found at [www.globalservices.bt.com/en/terms-and-conditions](http://www.globalservices.bt.com/en/terms-and-conditions), and that form part of the Contract.

**"Graded Service Tier"** means Foundation, Foundation Plus or Premium.

**"Initial Setup"** means the facilitation of the setup and delivery of the Managed Sentinel & XDR Service as set out in Paragraph 0.

**"Installation Charges"** means those Charges set out in any applicable Order in relation to installation of the Managed Sentinel & XDR Service or any BT Equipment as applicable.

**"Internet"** means a global system of interconnected networks that use a standard Internet Protocol to link devices worldwide.

**"Internet Protocol"** or **"IP"** means a communications protocol for devices connected to the Internet that specifies the format for addresses and units of transmitted data.

**"IP Address"** means a unique number on the Internet of a network card or controller that identifies a device and is visible by all other devices on the Internet.

**"Local Area Network"** or **"LAN"** means the infrastructure that enables the ability to transfer IP services within Site(s) (including data, voice and video conferencing services).

**"Log"** means an automatically produced and time-stamped file documenting events relevant to a particular program.

**"Log Forwarder"** means a software tool designed to collect event Logs from one or more Data Sources and relay them to an intended destination. Log Forwarders are often used to translate Log messages from one format or protocol to another.

**"Managed Devices/Services"** has the meaning given in Paragraph 2.8.1(c)(i).

**"Managed Sentinel & XDR Service"** has the meaning given in Paragraph 1.

**"Managed Sentinel BT MSSP Tenant"** means the single central Tenant used by BT as a Managed Security Service Provider to view incidents from customer Sentinel Workspaces. It also is the central repository for BT users, rules, workbooks and other content.

**"Managed Sentinel BT MSSP Tenant Technical Incident Monitoring"** has the meaning given in Paragraph 2.8.2(a).

**"Managed Sentinel Device"** means hardware or Virtual Machines that BT uses for the testing or delivery of the Managed Sentinel & XDR Service.

**"Managed Security Service Provider"** means a provider of outsourced monitoring and management of security devices and systems.

**"Microsoft"** means Microsoft Inc., a company registered in the US of One Microsoft Way, Redmond, Washington 98052-6399.

**"Minimum Period of Service"** means a period of 12 consecutive months beginning on the Service Start Date, unless set out otherwise in any applicable Order.

**"Monitoring and Management"** means the monitoring and management phase of the Managed Sentinel & XDR Service as set out in Paragraph 2.8.



**"MS Rule"** means Microsoft rules taking alerts directly from Microsoft security products.

**"Planned Maintenance"** means any Maintenance BT has planned to do in advance.

**"Playbooks"** means a collection of procedures that can be executed once a Security Incident is detected to contain the effects of the Security Incident and restore service.

**"Premium"** means the Premium Graded Service Tier as set out in this Schedule.

**"P1 Security Incident"** means actionable, high risk threat or policy violations that have the potential to cause severe damage or disruption to your environment.

**"P2 Security Incident"** means unauthorised User activities that do not directly impact your system performance or harm data.

**"P3 Security Incident"** means User error, misconfigurations, noncompliance and scanning.

**"P4 Security Incident"** means for information only.

**"P5 Security Incident"** means for information only.

**"P1 Technical Incident"** has the meaning in the table set out in Paragraph 2.8.1(a)(v).

**"P2 Technical Incident"** has the meaning in the table set out in Paragraph 2.8.1(a)(v).

**"P3 Technical Incident"** has the meaning in the table set out in Paragraph 2.8.1(a)(v).

**"P4 Technical Incident"** has the meaning in the table set out in Paragraph 2.8.1(a)(v).

**"P5 Technical Incident"** has the meaning in the table set out in Paragraph 2.8.1(a)(v).

**"Professional Services"** means those services provided by BT which are labour related services and are delivered remotely and charged at day rates unless otherwise set out in any applicable Order.

**"Reasonable Use Policy"** has the meaning given in Paragraph 2.9.2(a)(v).

**"Recurring Charges"** means the Charges for the Managed Sentinel & XDR Service or applicable part of the Managed Sentinel & XDR Service that are invoiced repeatedly in every payment period (e.g. every month), as set out in any applicable Order.

**"Root Cause Analysis"** or **"RCA"** means analysis of data to establish the root cause of a Security Incident or issue.

**"RCA Support"** means assistance in identifying the root cause of a Security Incident or issue and may include support for customer RCA including by reporting on breaks or unwanted actions and recommending fixes or mitigating actions.

**"Scheduled Rules"** means a list of actions or event steps that specifically define the interaction between a role and a system to achieve a goal.

**"Security Case Assessment Notification Target"** means the time from classifying and advising you of a Security Incident to recommending a course of action to you.

**"Security Event Classification Notification Target"** means the time from the BT SOC being made aware of an Event, classifying it and advising you of the classification of such Event.

**"Security Incident"** means a single unwanted or unexpected security event, or series of events, consisting of the actual or potential (attempt underway) exploitation of an existing Vulnerability, and that has a significant probability of compromising business operations and threatening information security.

**"Security Incident Notification"** has the meaning given in Paragraph 10.1.1.

**"Security Posture"** means the overarching approach to security adopted within your company.

**"Sentinel Solution"** means a security information and event management service using Microsoft Sentinel.

**"Sentinel Workspace"** means a container that includes data and configuration information.

**"Service Desk"** means the helpdesk that you will be able to contact to submit Managed Sentinel & XDR Service requests, report Technical Incidents and ask questions about the Managed Sentinel & XDR Service.

**"Service Level Agreement"** means the contractual service levels agreed between BT and you.

**"Service Level Availability"** means target availability corresponding to the Managed Sentinel & XDR Service.

**"Service Management Boundary"** has the meaning given in Paragraph 4.1.

**"Service Option"** has the meaning given in Paragraph 3.

**"Service Start Date"** has the meaning given in Paragraph 9.2.6.

**"Service Target"** means any target that BT aims to meet as set out in this Schedule.

**"Silent Device Alarm"** means that an alarm is triggered when a device does not send any Logs for a set threshold, therefore warranting further investigation.

**"Simple Change"** means the Simple Changes set out in the document titled Simple and Complex Change which will be shared with you on completion of Initial Setup.

**"Site"** means a location at which the Managed Sentinel & XDR Service is provided.

**"SOM"** means the security operations manager BT appoints to be your point of contact for the duration of the Managed Sentinel & XDR Service.

**"Standard Change"** means in respect of a Simple Change upgrades and modifications needed as a result of planned developments and security improvements.

**"Standard Default Rule Set"** means a set of rules that BT can apply to your Managed Sentinel & XDR Service to allow for monitoring by BT, as set out in the Customer Service Description.



**"Supported Device List"** means the list of Event Log Data sources that are readily compatible with the Managed Sentinel & XDR Service as set out in the Customer Service Description (if applicable) attached to any applicable Order, and as may be amended by BT from time-to-time.

**"Target"** means a non contractual threshold that is set to aid the performance of the Managed Sentinel & XDR Service.

**"Target Response Time"** means a non contractual target time to respond to you.

**"Target Time for Remediation Advice"** means a non contractual time to respond to you with remediation advice following an Security Incident.

**"Target Time for Commencement of Remediation Action"** means a non contractual time to commence remediation action following remediation advice in relation to a Security Incident.

**"Technical Incident"** means an unplanned interruption to, or a reduction in the quality of, the Managed Sentinel & XDR Service or particular element of the Managed Sentinel & XDR Service .

**"Tenant"** means an organisation in Azure Active Directory. Each Azure Active Directory Tenant is distinct and separate from other Azure Active Directory Tenants.

**"Ticket"** means the unique reference number provided by BT for a Technical Incident and that may also be known as a **"fault reference number"**.

**"Urgent Change"** means in respect of a Simple Change upgrades and modifications needed as a result of unplanned activities or unforeseen activities, but which are not critical to maintaining the security of the organisation.

**"Usage Volume"** means the agreed usage volume as set out in any applicable Order and calculated on your average gigabytes per day used in the calendar month.

**"User Guides"** means the documents that set out details on how you:

- (a) make changes to the Custom Content(s); and
- (b) access reports.

**"Virtual Machine"** means a computer file, typically called an image, that behaves like an actual computer.

**"Vulnerability"** means a software susceptibility that may be exploited by an attacker.

**"WAN"** means wider area network.

**"Workspace"** means one or more webpages made available to you by BT to provide for one or more specific functions in relation to the Managed Sentinel & XDR Service.