Managed Sentinel and XDR Service
Annex to the Managed Service Schedule

Application of this Annex

This Annex sets out the additional terms that will apply where BT provides you with the Managed Sentinel and XDR Service. The terms of this Annex apply in addition to the terms set out in:

(a) the Schedule; and

(b) the General Terms.

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 Annex have the meanings given to them in the General Terms and the Schedule.

Part A – The Managed Sentinel and XDR

1 Service Summary

1.1 BT will provide you with a security information and event management service, supporting threat detection, compliance reporting, and incident response and investigation by collection and analysis of historical data across a variety of sources ("**Managed Sentinel and XDR Service**").

2 Managed Service Packages

2.1 You will choose one of the Managed Service Packages, some of the features of which are set out in the table below, to use with your Managed Sentinel and XDR Service as set out in any applicable Order. The Managed Service Package you have chosen for the Managed Sentinel and XDR Service must align with the Managed Service Package you have chosen for your overall Managed Service, as set out in the Schedule:

Service Stage	Feature / Service	MS1 Package	MS2 Package	MS3 Package
Initial Set Up	Access / Build Customer Azure Log Analytics Workspace(s)	✓	✓	✓
	Access / Build Customer Managed Sentinel Workspace(s)	✓	✓	✓
	Delegated Rights Management Access to Sentinel	✓	✓	✓
Controlled Deployment	Data Connector Build: Microsoft Cloud Data Connectors	✓	✓	✓
	Data Connector Build: External Non-Microsoft	✓	✓	✓
	Rules Optimisation: Test and tune	✓	✓	✓
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 Customer's 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	TAM Quarterly Service Meetings and Tuning Sessions	✓	✓	✓
	TAM Monthly Service Meetings and Tuning Sessions	×	✓	✓
	Quarterly Review of Security Policy to identify Changes needed for new threats	×	×	✓

2.2 The provisions in respect of MS1 will apply to MS2 and MS3 and the provisions of MS2 will apply to MS3. If there is a conflict between the provisions of the Managed Service Packages, the order of priority of the relevant provisions is:

2.2.1 MS3;

2.2.2 MS2; and

2.2.3 MS1.

2.3 **Delivery Model**

2.3.1 **Customer-Led**

(a) If you select the Customer-Led Delivery Model, you are responsible for purchasing and managing your access to the Microsoft Sentinel platform.

2.3.2 **BT SOCaaS for Microsoft Sentinel**

(a) If you have selected BT SOCaaS for Microsoft Sentinel, BT will, as a Microsoft Cloud Solution Provider, provide you with a Subscription to Microsoft Sentinel and the required Azure Resources that are hosted by the Supplier.

(b) BT will provide you with a Consumption-Based Subscription in which the price is calculated based on cloud resource consumption.

(c) BT will provide escalations to the Supplier on your behalf for any Incidents found with the Microsoft Sentinel platform.

(d) To be eligible for BT SOCaaS for Microsoft Sentinel, you must not already have a Microsoft Sentinel Subscription. If you have already procured a Microsoft Sentinel Subscription, you may select one of the Managed Service Packages to use as part of the Managed Sentinel and XDR Service in accordance with the Customer-Led Delivery Model.

(e) As part of BT SOCaaS for Microsoft Sentinel, BT will provide you with the capability to place Orders for your Subscription via BT sales agents.

(f) The Microsoft Sentinel Data Lake functionality is excluded from BT SOCaaS for Microsoft Sentinel, unless otherwise set out in the applicable Order.

2.4 **Initial Setup**

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

2.4.1 **MS1**

(a) BT will appoint a TAM to be your single point of contact during the Initial Setup and Controlled Deployment. The TAM 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) provides 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 – MS1"**).

(d) Note MS1 level Customers will have a Managed Sentinel Service only, the XDR aspect of the Managed Sentinel and XDR Service is not offered at MS1 level.

(e) **Custom Rule Design and Deployment**

(i) BT will provide you with the Standard Default Rule Set.

(ii) You will select additional Custom Content that you have agreed with BT when you place the Order and ensure that the Custom Content you select meet 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 Custom Content Change Management Process set out in Paragraph 2.7.2.

(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 a Custom Rule requested by you, the rule will be added to the Standard Default Rule Set, made available to BT's wider customer base, in which case the rule 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 rule.

(vi) Subject to receiving acceptable information from the Data Sources, BT will configure the Managed Sentinel and XDR Service to implement the Custom Content agreed with you.

(vii) Unless otherwise set out in any applicable Order, the Custom Rule Design and Deployment activities set out in this Paragraph 2.4.1(e) will be undertaken remotely by BT.

(viii) The TAM will work with you in respect of the Custom Rule Design and Deployment.

(ix) BT may apply additional Charges if work cannot be undertaken remotely and BT is required to attend the Site(s).

(f) 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.

(g) Subject to receiving acceptable information from the Data Sources, BT will configure the Managed Sentinel and XDR Service to implement the Custom Content agreed with you.

(h) Unless otherwise set out in any applicable Order, the Custom Content Design and Deployment activities set out in Paragraph 2.4.1(e) will be undertaken remotely by BT.

(i) The TAM will work with you in respect of the Custom Content Design and Deployment.

(j) BT may apply additional Charges if work cannot be undertaken remotely and BT is required to attend the Site(s).

2.4.2 **MS2**

(a) BT will appoint a TAM and a BT Project Manager during the Initial Setup and Controlled Deployment. The TAM will undertake any activity remotely and will not visit your Site.

(b) BT will provide you with access to a named TAM on a shared basis, for the duration of the Service, to assist with any issues or requests.

(c) You may request that BT, at an additional Charge, provides a named TAM who 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 – MS2**").

(e) Note MS2 Service Package level Customers will have a Managed Sentinel Service only, the XDR aspect of the Managed Sentinel and XDR Service is not offered at MS2 Service Package level.

(f) **Custom Rule Design and Deployment**

(i) You will select 5 additional Custom Content that you have agreed with BT when you place the Order and ensure that the Custom Content you select meet your requirements. Any additional Custom Content will be charged, in addition, on a time and materials basis.

(ii) The TAM to assist you with the configuration of the Managed Sentinel and XDR Service in accordance with the agreed Custom Content.

2.4.3 **MS3**

(a) You may make an unlimited number of Simple Service Requests per quarter, subject to agreement with BT and resource availability ("**Content Allowance – MS3**").

(b) **Custom Rule Design and Deployment**

(i) You will select 10 additional Custom Content that you have agreed with BT when you place the Order and ensure that the Custom Content you select meet your requirements. Any additional Custom Content will be charged, in addition, on a time and materials basis.

(ii) You will provide a named contact and appropriate technical support to work with BT during the Controlled Deployment Custom Content Optimisation Period.

2.4.4 **Policies and Migration - All Tiers**

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

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

2.4.5 **Data Source Connection – All Tiers**

(a) BT will configure the Managed Sentinel and XDR Service to receive Event Log Data from the Data Sources agreed with you and set out in the CEP Form attached to the applicable Order.

(b) You will configure the Data Sources to send Logs to the Managed Sentinel and 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.

(c) You will connect the Data Sources to the Managed Sentinel and XDR Service unless BT provides the data source in which case BT will connect the Data Source to the Managed Sentinel and XDR Service.

(d) BT will not be liable for any failure of the Managed Sentinel and XDR Service to process Logs sent to the Managed Sentinel and XDR Service from Data Sources not set out in the Data Capture Form or otherwise set out in any applicable Order.

(e) BT will only undertake threat correlation or threat monitoring from Data Sources that are set out in the Data Capture Form.

(f) BT may apply additional Charges if work cannot be undertaken remotely and requires BT to attend the Site(s).

2.5 **Controlled Deployment**

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

2.5.1 **General**

(a) **MS1**

(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 the TAM.

(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) **MS2 & MS3**

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

2.5.2 **Customer Training**

(a) **MS1**

(i) No customer training is offered for the MS1

(b) **MS2 & MS3**

(i) BT may deliver training to a specified group of Users, via a conferencing service, if requested;

(ii) Additional training may be offered at BT's sole discretion.

2.5.3 You may communicate with BT directly via the TAM or email.

2.6 **Monitoring and Management**

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

2.6.1 **MS1**

(a) **Proactive Monitoring**

(i) BT will monitor the performance of the Managed Sentinel and XDR Service at intervals set by BT and, where possible, provide advance warning to or via email of impending issues that may affect the Managed Sentinel and 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 2.6.1(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) **Managed Sentinel and XDR Service Managed Sentinel BT MSSP Tenant Technical Incident Monitoring**

BT will:

(i) proactively monitor and manage the Managed Sentinel BT MSSP Tenant 24x7x365 ("**Managed Sentinel BT MSSP Tenant 24x7x365**").

(c) **Workbook and Reports**

(i) BT will provide you with reporting for the Managed Sentinel and XDR Service via your Tenant or secure email

(d) **Security Incident Management**

(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.

(e) **Event Searches**

(i) **Standard Service Package**

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 for your selected Managed Service Package.

2.6.2 **MS2**

(a) **Proactive Monitoring**

(i) Both of us will agree a process for BT to contact you when it identifies an issue that impacts the Managed Sentinel and XDR Service.

(ii) BT will use historic and current metrics captured via the monitoring of the Managed Sentinel and XDR Service to forecast issues that may impact the performance of the Managed Sentinel and XDR Service and make recommendations to you by e-mail, as agreed by you, mitigating actions which should be taken to address the threat that has been reported.

(b) **Workbook and Reports**

(i) BT will provide you with workbooks and custom reporting for the Managed Sentinel and XDR Service via your Tenant or secure email.

(c) **Security Incident Management**

(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 TAM 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.

(d) **Event Searches**

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 for your selected Managed Service.

2.6.3 **MS3**

(a) **Workbook and Reports**

(i) BT will provide you with workbooks and custom reporting for the Managed Sentinel and XDR Service via your Tenant or secure email.

(b) **Security Incident Management**

(i) **Case Registration**

i. BT will notify you of possible Security Incidents, including details of the relevant underlying Event and threat intelligence.

ii. The TAM 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 MS3 are as per MS2, as set out at Paragraph 2.6.2(c)(ii) above.

(c) **Event Searches**

(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 for your selected Managed Service Package.

(d) **Automated Remediation**

(i) Automated Remediation is provided as part of MS3. Following provisioning to you of an enhanced incident alert, the BT 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 2.6.3(d)(ii)and 2.6.3(d)(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 and XDR Service. You must fulfil your obligations, both before and during the Service, as detailed in Paragraph 9 of this Annex, 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***

i. 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.

ii. 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.

iii. 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 2.6.3(d)(i) above) or during the Operation of the Service (as per Paragraph 2.6.3(d)(iv)ii above), this shall not result in any reduction to the Charges which are payable in line with the selected Managed Service Package. 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.

iv. 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 2.6.3(d)(iv)iii 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.

2.6.4 **Upgrades**

(a) BT may from time to time upgrade any Software or firmware used to deliver the Service to ensure that they remain 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 and XDR Service.

(b) You will confirm to BT any change in the number of devices/log sources you are adding in, to your Managed Sentinel and XDR Service.

2.6.5 **Capacity Management**

(a) If BT identifies that changes in your Usage Volumes could result in the Managed Sentinel and 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.

(b) If you do not agree to make changes to the data collected, following advice from BT in accordance with Paragraph 2.6.5(a) BT will not be liable for any performance issues of the Managed Sentinel & XDR Service, and you may be charged accordingly.

2.6.6 **Technical Incident and Fault Management**

(a) **All Service Packages (MS1, MS2 & MS3)**

(i) You will report all Technical Incidents through MyAccount. An Incident Ticket will be automatically created in ServiceNow and assigned to CySOC. Alternatively, customers may call CySOC for triage; if required, CySOC will direct you to raise the incident via MyAccount > ServiceNow (SNOW).

(ii) All communications with CySOC and the Service Desk must be conducted in English.

(iii) The Service Desk and CySOC operate 24x7x365, staffed by security-trained professionals who will action Technical Incident notifications.

(iv) You will receive a ticket reference upon incident creation.

(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 and 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 and XDR Service and cannot be circumvented, causes significant loss of the Managed Sentinel and 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 and 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 and 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 and XDR Service; for example: a temporary failure of reporting or billing.

(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, 2.6.6(a)(iv) to 2.6.6(a)(ix) will apply.

2.6.7 **Missing Log Source Monitoring and Reporting**

(a) **All Service Packages (MS1, MS2 & MS3)**

(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 and 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 and XDR Service.

2.6.8 **Security Event Management**

(a) **All Packages (MS1, MS2 and MS3)**

BT will:

(i) analyse Event / Incident data generated by the Managed Sentinel and XDR Service;

(ii) assess appropriate remediation actions to be taken; and

(iii) if necessary, alert you via email to any potential threats and/or action to be taken by you.

2.7 **Continuous Improvement**

2.7.1 **Reviews**

(a) **MS1**

(i) The TAM will carry out a review every two months per annum as follows:

i. a Managed Sentinel and XDR Service review, focussing on the performance of the Managed Sentinel and XDR Service.

(ii) The TAM 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 TAM 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 TAM in respect of the Managed Sentinel and XDR Service including implementing security improvements as agreed with the TAM or as advised by the TAM as your responsibility.

(b) **MS2**

(i) The TAM will carry out a review monthly as follows:

i. a Managed Sentinel and XDR Service review focussing on the performance of the Managed Sentinel and XDR Service against Service Targets;

ii. a review of the effectiveness of the Custom Content applied to your Managed Sentinel and XDR Service and the need to fine tune or amend the Custom Content; and

(ii) In addition to taking the action set out in Paragraph 2.7.1(a)(v), you will take appropriate action to address issues in respect of fine tuning or amending your Custom Content as recommended by the TAM.

(c) **MS3**

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

i. a Managed Sentinel and XDR Service focussing on the performance of the Managed Sentinel and XDR Service against Service Targets;

ii. a review of the effectiveness of the Custom Content applied to your Managed Sentinel and XDR Service and the need to fine tune or amend the Custom Content;

(ii) The TAM will also carry out a six-monthly Security Posture review. The TAM will create an action plan with the aim of improving your Security Posture;

(iii) In addition to taking the action set out in Paragraph 2.7.1(a)(v), you will take appropriate action to address issues in respect of fine tuning or amending your Custom Content as recommended by the TAM.

2.7.2 **Custom Content Change Management Process**

(a) 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 TAM, providing sufficient detail and clear instructions as to any changes required;

(ii) BT will check each request for its complexity and assess whether the change should be completed via the Custom Content 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 Custom Content Change Management Process; and

(iv) BT may provide you with Professional Services at an additional Charge, at your request, to assist you in writing your change request.

(b) **MS1**

(i) BT will provide contact details for the BT SOC or TAM 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 2.7.2(b)(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.

(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. five per quarter in respect of MS1; and
   b. ten per quarter in respect of MS2.

In respect of MS3 there is no limit on the amount of requested Standard Changes, but their implementation is subject to agreement with BT and resource availability.

ii. you will not raise Urgent Change requests more frequently than:
   a. one per quarter in respect of MS1;
   b. three per quarter in respect of MS2; and
   c. three per quarter in respect of MS3.

iii. where BT's measurements show that change requests are being raised more frequently than as set out in Paragraph 2.7.2(b)(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.

(vi) 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.

(vii) BT may implement an Emergency Change without your approval.

(viii) You are deemed to have approved all changes to the Custom Content that you submit to BT.

(ix) 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.

(c) **MS2**

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

(d) **MS3**

(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 Rule.

3 Service Options

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

4 Service Management Boundary

4.1 BT will provide and manage the Managed Sentinel and XDR Service in accordance with Parts A, B and C of this Annex and as set out in any applicable Order ("**Service Management Boundary**").

4.2 BT will have no responsibility for the Managed Sentinel and XDR Service outside the Service Management Boundary.

4.3 BT does not make any representations, whether express or implied, about whether the Managed Sentinel and 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 and XDR Service, or any part of the Managed Sentinel and 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 and XDR Service will detect or block all malicious threats.

4.4.3 The Managed Sentinel and 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 and XDR Service, or any degradation of the Managed Sentinel and XDR Service, if you do not have and maintain the appropriate logs and functionality.

4.4.4 Where you have selected BT SOCaaS for Microsoft Sentinel, the Microsoft Subscription(s) is provided solely for your own use, and you will not resell the Microsoft Subscription(s) (or any part or facility of it) to any third party.

5 Associated Services

5.1 You will have the following services in place that will connect to the Managed Sentinel and XDR Service and are necessary for the Managed Sentinel and XDR Service to function (dependent upon which Manged Service Package has been selected) and will ensure that these services meet the minimum technical requirements that BT specifies:

5.1.1 Microsoft Sentinel and Log Analytic Workspace(except where you select BT SOCaaS for Microsoft Sentinel, in which case BT will procure these on your behalf);

5.1.2 Microsoft 365 Defender;

5.1.3 Microsoft Defender for Cloud;

5.1.4 Microsoft Defender XDR Portal; and

5.1.5 Access to the Marketplace,

(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 and XDR Service.

5.4 If BT provides you with any services other than the Managed Sentinel and XDR Service, this Annex will not apply to those services and those services will be governed by their separate terms.

6 BT Equipment

6.1 No BT Equipment is provided by BT as part of the Managed Sentinel and XDR Service.

7 Specific Terms

7.1 **Customer Committed Date**

7.1.1 If you request a change to the Managed Sentinel and XDR Service or any part of the Managed Sentinel and XDR Service, then BT may revise the Customer Committed Date to accommodate that change.

7.1.2 BT may expedite delivery of the Managed Sentinel and XDR Service for operational reasons or in response to a request from you, but this will not revise the Customer Committed Date.

7.2 **Right to Use**

7.2.1 BT gives you a non-exclusive, non-transferable and limited right to use the Managed Sentinel and XDR Service for your internal business purposes only.

7.2.2 You will not resell or otherwise transfer the Managed Sentinel and XDR Service granted under this Contract.

7.3 **Invoicing**

7.3.1 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 and XDR Service is provided for less than one month, the full monthly charge will be applied;

(c) Consumption Charges, monthly or quarterly in arrears (depending on your billing frequency), calculated at the then current rates; and

(d) Professional Services Charges.

7.3.2 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 and XDR Service in accordance with Paragraph 8.2, outside of Business Hours;

(c) Charges for expediting provision of the Managed Sentinel and XDR Service at your request after BT has informed you of the Customer Committed Date;

(d) Charges for restoring the Managed Sentinel and XDR Service if the Managed Sentinel and XDR Service has been suspended in accordance with Clause 15 of the General Terms;

(e) Charges for cancelling the Managed Sentinel and XDR Service in accordance with Clause 16 of the General Terms;

(f) additional Charges 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 MS1 Package in accordance with Paragraph 2.4.1(b)

(h) Charges for the named TAM attending meetings at your Site if you have purchased MS2 or MS3 Package in accordance with Paragraph 2.4.2(c);

(i) Charges for additional Custom Content in accordance with Paragraph 2.4.1(e)(ii), 2.4.2(f)(i) and 2.4.3(b)(i);

(j) Charges for the cost of implementing Complex Changes in accordance with Paragraph 2.7.2(b)(iii) and Emergency Changes in accordance with Paragraph 2.7.2(b)(vi)

(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 2.7.2(b)(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 9.1.8;

(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 4.7 of the Schedule upon termination of the relevant Managed Sentinel and XDR Service.

7.3.3 **Usage Volume Reasonable Use Policy**

(a) Where your Usage Volume exceeds the agreed Usage Volume in a given month, BT reserves the right to 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.

7.4 **Upgrade to a Higher Managed Service Package**

7.4.1 You may upgrade to a higher Managed Service Package during the Minimum Period of Service.

7.4.2 No Termination Charges will be payable from the Managed Service Package you are moving from. New Charges for the upgraded Managed Service Package will be set out in the Order.

7.4.3 A new Minimum Period of Service will apply to the upgraded Managed Service Package as set out in the Order.

7.4.4 If you upgrade to a higher Managed Service Package under either this Annex, the Schedule or any other Associated Service, you must upgrade your entire Contract to that higher Managed Service Package.

7.4.5 You cannot downgrade to a lower Managed Service Package.

7.5 **EULA**

7.5.1 BT will only provide BT SOCaaS for Microsoft Sentinel if you have entered into an end user licence agreement with the Supplier in the form set out at https://www.microsoft.com/licensing/docs/customeragreement as may be amended or supplemented from time to time by the Supplier ("**EULA**").

7.5.2 By accepting the terms of the EULA, you agree to observe and comply with it for all use of your Microsoft Sentinel Subscription in relation to BT SOCaaS for Microsoft Sentinel.

7.5.3 In addition to what it says in Clause 15 of the General Terms, if you do not comply with the EULA, BT may restrict or suspend BT SOCaaS for Microsoft Sentinel upon reasonable Notice, and:

(a) you will pay the Charges that are payable for BT SOCaaS for Microsoft Sentinel until the Contract ends; and

(b) BT may charge a restarting Charge to start BT SOCaaS for Microsoft Sentinel again.

7.5.4 You are responsible in accordance with the terms of the EULA for the use of the Software.

7.5.5 You will enter the EULA for your own benefit and the rights, obligations, acknowledgements, undertakings, warranties, and indemnities granted in accordance with the EULA are between you and the Supplier.

7.5.6 You will deal with the Supplier with respect to any loss or damage suffered by you or the Supplier under the EULA and any loss or damage will not be enforceable against BT.

7.6 **Customer Responsibility for Configuration and Use**

7.6.1 You acknowledge that BT SOCaaS for Microsoft Sentinel includes Microsoft Sentinel. To the extent that any configuration, deployment, integration, administration, management or use of Microsoft Sentinel or related Microsoft services is carried out by, on behalf of, you or at your direction, you shall be responsible for the consequences of such activities.

7.6.2 You may de-authorise BT as your Delegated Administrator through your Microsoft Tenant at any time. BT will not be able to administer or support your Microsoft Tenant on your behalf if you de-authorise BT as your Delegated Administrator.

7.6.3 BT shall not be liable for any loss, damage, service degradation, Security Incident, failure or limitation arising from:

(a) any configuration, integration, deployment or use of Microsoft Sentinel or related Microsoft services by you or any third party acting on your behalf;

(b) any inaccurate, incomplete or misleading instructions, information or requirements provided by you; or

(c) your use of Microsoft Sentinel or related Microsoft services in a manner inconsistent with BT's or the Supplier's documentation, guidance or recommendations.

7.6.4 You shall indemnify BT against all Claims, losses, costs or liabilities brought against BT that arise out of or in connection with:

(a) any configuration, deployment, integration, administration or use of Microsoft Sentinel or related Microsoft services by you or any third party acting on your behalf; or

(b) BT's compliance with your instructions, specifications or requirements.

The foregoing indemnification obligation is in addition to any defence obligation and not subject to any limitation of, or exclusion from, liability set out in the Contract.

7.7 **Additional Cancellation, Suspension and Termination Rights**

7.7.1 Where you have taken BT SOCaaS for Microsoft Sentinel:

(a) BT provides the Subscription as a Microsoft Cloud Solution Provider and your Subscription may be modified by Microsoft from time to time. Where any such change affects the Subscription provided to you, BT may amend, replace, cancel or discontinue the affected Subscription, or make corresponding changes to the Contract, by giving you Notice. BT will not be liable to you for any such change, amendment, replacement, cancellation or discontinuance to the extent it results from a change imposed by Microsoft;

(b) BT may terminate the Contract or any part of the Contract immediately if Microsoft terminates your access to Microsoft Sentinel at any time. BT will not be liable to you for such termination; and

(c) BT will not be liable to you if Microsoft temporarily disables your Subscription for legal or regulatory reasons or breach by you of the EULA.

7.8 **Amendments to the Schedule**

7.8.1 Table in Paragraph 2.1 is deleted and replaced with the following:

	Managed Service 1	Managed Service 2	Managed Service 3
Service Desk	Yes	Yes	Yes
Service Management	N/A	Yes	Yes

Maintenance	N/A*	N/A*	N/A*
Configuration Management	Yes	Yes	Yes
Asset Management	N/A**	N/A**	N/A**
Proactive Monitoring	Monitoring & Event Management	Monitoring & Event Management	Monitoring & Event Management
Infrastructure Reporting	Service Reporting	Service Reporting	Service Reporting
Change Management	Service Request Management	Service Request Management	Service Request Management
	5 x Simple Service Requests (SSRs)	10 x Simple Service Requests (SSRs)	Unlimited*** Simple Service Requests (SSRs)
	No Custom Rule Allowance	5 x Custom Rule Allowance The allowance is based on a 12-month rolling basis, Requests outside allowance are chargeable.	10 x Custom Rule Allowance The allowance is based on a 12-month rolling basis, Requests outside allowance are chargeable.

* You are responsible for your own Microsoft Sentinel and XDR portal.

** Asset Management is your responsibility.

*** whilst the allowance for SSRs is unlimited in MS3, this is subject to agreement with BT and BT resource availability.

7.8.2 Paragraphs, 2.5 (**Maintenance Care Levels**), 2.6 (**Enhanced Proactive Monitoring for Associated Services**) 2.7 (**Vital Port Monitoring**), 2.8 (**In-Band and Out of Band Management**), 2.9 (**Configuration Management**) and 2.10 (**Software Upgrades**) of the Schedule will not apply.

7.8.3 Paragraph 2.11.3 (**Network Reporting**), 2.11.4 (**IPSLA Reporting**), 2.11.5 (**Application Reporting**) and 2.11.6 (**Vendor Network and Application Reporting**) of the Schedule will not apply.

7.8.4 Paragraph 2.12 (**Capacity Management**) and 2.13 (**Availability Management**) of the Schedule will not apply.

7.8.5 Paragraph 2.16.5 (**WLAN Survey**), 2.16.6 (**Network Assessment Physical Detail Collection Package and Network Assessment Physical Detail Collection Day Rate**), 2.16.7 (**Infrastructure Cabling**) and 2.16.8 (**PDS Installation Services**) of the Schedule will not apply.

7.8.6 The wording of Paragraph 4.1 (**Changes to the Contract**) of the Schedule is deleted and replaced with the following:

4.1.1 BT may propose changes to this Schedule, the General Terms or the Charges (or any of them) by giving you Notice at least 90 days prior to the end of the Minimum Period of Service and each Renewal Period ("**Notice to Amend**").

4.1.2 Within 10 days of any Notice to Amend, you will provide BT Notice:

(a) agreeing to the changes BT proposed, in which case those changes will apply from the beginning of the following Renewal Period;

(b) requesting revisions to the changes BT proposed, in which case both of us will enter into good faith negotiations for the remainder of that Minimum Period of Service or Renewal Period, as applicable, and, if agreement is reached, the agreed changes will apply from the beginning of the following Renewal Period; or

(c) terminating the Contract at the end of the Minimum Period of Service or Renewal Period, as applicable.

4.1.3 If we have not reached agreement in accordance with Paragraph 4.1.2(b) by the end of the Minimum Period of Service or the Renewal Period, the terms of this Schedule will continue to apply from the beginning of the following Renewal Period unless you give Notice in accordance with Paragraph 4.1.2(c) or BT may give Notice of termination, in which case BT will cease delivering the Managed Sentinel and XDR Service at the time of 23:59 on the last day of the Minimum Period of Service or subsequent Renewal Period as applicable.

7.8.7 Regardless of what it may say in Paragraph 4.2 (**Minimum Period of Service and Renewal Periods**) of the Schedule:

4.2.1 You may request an extension to the Managed Sentinel and XDR Service for a Renewal Period by Notice in writing to BT at least 90 days before the end of the Minimum Period of Service or Renewal Period ("**Notice of Renewal**").

4.2.2 If you issue a Notice of Renewal in accordance with Paragraph 4.2.1, BT will extend the Managed Sentinel and XDR Service for the Renewal Period and both of us will continue to perform each of our obligations in accordance with the Contract.

4.2.3 If you do not issue a Notice of Renewal in accordance with Paragraph 4.2.1, BT will cease delivering the Managed Sentinel and XDR Service at the time of 23:59 on the last day of the Minimum Period of Service or Renewal Period.

4.2.4 If the Managed Sentinel and XDR Service is the only Associated Service purchased under the Contract for the Managed Service, Paragraph 4.2 of the Schedule will not apply to the Managed Service and Paragraph 7.7.7 of this Annex will apply; and

7.8.8 4.2.5 If the Managed Sentinel and XDR Service is purchased along with other Associated Services under the Contract for the Managed Service, Paragraph 4.2 of the Schedule will apply to the Managed Service and the other Associated Services and Paragraph 7.8.9 of this Annex will apply only to the Managed Sentinel and XDR Service.

7.8.9 Regardless of what it may say in Paragraphs 4.3.2 and 4.3.3 of the Schedule, if either of us terminates the Managed Service in accordance with Paragraph 4.3.1 of the Schedule, the Managed Sentinel and XDR Service will automatically terminate at the same time and you will pay Termination Charges in accordance with Paragraph 4.7 of the Schedule.

7.8.10 Paragraph 4.10 (**Security**) of the Schedule will not apply.

7.8.11 Paragraphs 5.1.3 (**BT obligations for PDS Installation**) and 5.3 (**BT's obligations During Operation**) of the Schedule will not apply.

7.8.12 Paragraphs 6.1.4 (**providing BT access to any of your Sites**), 6.1.6 (**specialist equipment at your Site**), 6.1.9 (**LAN protocols and applications compatible with the Managed Service and Associated Service**) and 6.2.13 (**your obligations on expiry or termination of the Managed Service**) of the Schedule will not apply.

7.8.13 Paragraphs 6.3 (**UCC Obligations**), 6.4 (**WAN Obligations**) and 6.5 (**LAN Obligations**) of the Schedule will not apply.

7.8.14 The wording in Paragraph 7 (**Notification of Incidents**) of the Schedule is deleted and replaced with the following:

7.1 Where you become aware of an Incident or a Security Incident:

7.1.1 The Customer Contact will report it to the Service Desk or Cyber Security Operations Centre;

7.1.2 BT will give you a Ticket;

7.1.3 BT will inform you when it believes the Incident or Security Incident is cleared and will close the Ticket when:

(a) you confirm that the Incident or Security Incident is cleared within 24 hours after having been informed; or

(b) BT has attempted unsuccessfully to contact you, in the way agreed between both of us in relation to the Incident or Security Incident, and you have not responded within 24 hours following BT's attempt to contact you.

7.1.4 If you confirm that the Incident or Security 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 Incident or Security Incident.

7.1.5 Where BT becomes aware of an Incident or Security Incident, Paragraphs 7.1.2, 7.1.3 and 7.1.4 will apply.

7.1.6 This Paragraph 7 will not apply to Security Incidents if you have selected the MS1 Package.

7.8.15 Part C (**Service Levels**) of the Schedule will be deleted and Part C of this Annex will apply instead.

7.9 **Amendments to the General Terms**

7.9.1 The definition of Force Majeure Event in the General Terms is deleted and replaced with the following:

(a) "Force Majeure Event" means any event that neither of us can control and that stops or delays either of us from doing something, including:
(b) natural event including a flood, a storm, lightning, a drought, an earthquake, or seismic activity; an epidemic or a pandemic;
(c) a terrorist attack, civil war, civil commotion or riots, war, the threat of war, preparation for war, an armed conflict, an imposition of sanctions, an embargo or a breaking-off of diplomatic relations;
(d) cyber terrorism;
(e) any law made or any action taken by a government or public authority, including not granting or revoking a licence or a consent;
(f) collapsing buildings, a fire, explosion, or accident; or
(g) any labour or trade dispute, a strike, industrial action, or lockouts.

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 and XDR Service, BT:

8.1.1 will provide you with contact details for the Service Desk and/or the CySOC;

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 and XDR Service have been confirmed and agreed, and, where applicable, where you had provided the details set out in Paragraph 7.1.1, 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 and XDR Service caused by errors or omissions in any information, instructions or scripts provided to BT by you in connection with the Managed Sentinel and XDR Service, or any actions taken by BT at your direction.

8.1.5 where you have taken BT SOCaaS for Microsoft Sentinel, will:

(a) create a Marketplace account and single Administrator account for you;
(b) if you do not have a Microsoft Tenant, create a Microsoft Tenant for you and configure the default customersubdomain.onmicrosft.com domain with the information provided by you with the Order;
  (i) where the requested customer subdomain is not available, BT will contact you to supply alternative options;
  (ii) it is not possible to change the customersubdomain.onmicrsoft.com domain once configured;
(c) if you have an existing Microsoft Tenant, send you a Microsoft Partner Relationship Invitation;
(d) assign the Subscription(s) that are detailed on your Order to your Marketplace account; and
(e) provide you with a confirmation email with instructions on how to access the Marketplace account and Microsoft Sentinel.

8.2 **Commissioning of the Service**

Before the Service Start Date, BT will:

8.2.1 conduct a series of standard tests on the on the appropriate tenants that are used as part of the Managed Sentinel and XDR Service to ensure that it 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 and 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 and 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 and XDR Service proactively and to assist in Technical Incident diagnosis;

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 and 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; and

8.3.6 will implement and take the appropriate Remediating Action required to manage the incident/threat identified as part of the Managed Sentinel and XDR Service, via automatic remediation where agreed with you, as quickly as is technically practicable.

8.4 **The End of the Service**

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

8.4.1 may remove the Managed Sentinel and XDR Service from your Tenant and where you have selected SOCaaS, terminate the Microsoft Sentinel service and suspend the Subscriptions.

9 Your Obligations

9.1 **Service Delivery**

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

9.1.1 provide BT access at the appropriate security level to your Tenant;

9.1.2 if BT is creating your Microsoft Tenant, accept that BT will automatically be the Delegated Administrator;

9.1.3 create all individual Users in the Microsoft Tenant that BT creates for you in accordance with Paragraph 9.1.2;

9.1.4 if you receive a Microsoft Partner Relationship Invitation in accordance with Paragraph 8.1.5:

(a) accept the Microsoft Partner Relationship Invitation;
(b) accept BT as your Delegated Administrator to establish the Reseller Relationship;

BT will not be authorised as your Delegated Administrator if you do not accept BT as your Delegated Administrator and the Reseller Relationship will not be established;

9.1.5 if either BT is automatically the Delegated Administrator in accordance with Paragraph 9.1.2 or you accept BT as your Delegated Administrator as part of establishing the Reseller Relationship in accordance with Paragraph 9.1.4(b), consent to Microsoft and its Affiliates (as defined in the EULA) providing BT with Customer Data and Administrator Data (both as defined in the EULA) for the purposes of provisioning, administering and supporting Microsoft Sentinel in accordance with the EULA;

9.1.6 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;

9.1.7 provide BT with a copy of your security policies;

9.1.8 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 and XDR Service;

9.1.9 provide BT with the ability to install any Managed Sentinel and XDR Service 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 and XDR Service;

9.1.10 attend integration meetings to discuss further tuning and configuration of the Managed Sentinel and XDR Service;

9.1.11 complete any preparation activities including installation and maintenance of any software or hardware that is not included as part of the Managed Sentinel and XDR Service, that BT may request to enable you to receive the Managed Sentinel and XDR Service promptly and in accordance with any reasonable timescales;

9.1.12 if applicable, ensure that the LAN protocols and applications you use are compatible with the Managed Sentinel and XDR Service;

9.1.13 where applicable, prepare and maintain the Site(s) for the supply of the Managed Sentinel and 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 and XDR Service at such points and with such connections as BT specifies, and, in order to mitigate any interruption to the Managed Sentinel and 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.

9.1.14 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 and 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 and XDR Service as a result of the change;

9.1.15 ensure that your WAN or Internet access circuit bandwidth is sufficient to meet your requirements and for the management access by BT;

9.1.16 manage, and provide BT with, accurate details of your internal IP Address design;

9.1.17 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;

9.1.18 if BT has agreed to provide any part of the Managed Sentinel and 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 9.2.5;
(c) is fully functional; and

if the relevant Customer Equipment does not comply with this paragraph, 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;

9.1.19 ensure that your network and all applications conform to relevant industry standards and provide written confirmation to BT upon reasonable request;

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 and XDR Service; and

9.1.21 ensure that your network or Internet connectivity performs correctly and will send Logs to the Managed Sentinel and XDR Service;

9.1.22 where you have selected BT SOCaaS for Microsoft Sentinel, you will:

(a) make Microsoft Sentinel available for use within your chosen Microsoft Tenant for the purpose of receiving the Managed Sentinel and XDR Service;
(b) retain full ownership and responsibility of the Microsoft Tenant (including Tenant troubleshooting) and Microsoft Sentinel Subscription, but BT will support you to ensure you have the correct access and permissions necessary for the provision of the Managed Sentinel and XDR Service;
(c) give BT reasonable notice of any planned changes to your Microsoft Sentinel Subscription and validate such changes with BT prior to implementation to prevent any negative impact on BT's ability to provide the Managed Sentinel and XDR Service;
(d) provide BT with the necessary permissions (including Delegated Rights Management, Azure Lighthouse, Azure GDAP, and Azure B2B, where applicable) and any other information that BT reasonably requests to enable BT to procure the Microsoft Sentinel Subscription and establish the Managed Sentinel and XDR Service; and
(e) maintain all prerequisites required for your environment (including supporting licenses outside of BT SOCaaS for Microsoft Sentinel scope, log source configuration, and agent/connector deployment and connectivity), and BT will not be liable for any failure to deliver, or degradation of, the Managed Sentinel and XDR Service to the extent caused by missing prerequisites, unsupported data sources, or changes outside the Service Management Boundary.

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 MS2 and MS3, 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 and 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 and 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 and 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:

9.2.1 where you have selected BT SOCaaS for Microsoft Sentinel, provide support to Users on how to use Microsoft Sentinel and enable Microsoft Sentinel within your business;

9.2.2 ensure that Users report Technical Incidents to the Customer Contact or via MyAccount and not to the Service Desk;

9.2.3 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;

9.2.4 monitor and maintain any Customer Equipment connected to the Managed Sentinel and XDR Service or used in connection with the Managed Sentinel and XDR Service;

9.2.5 ensure that any Customer Equipment that is connected to the Managed Sentinel and XDR Service or that you use, directly or indirectly, in relation to the Managed Sentinel and 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 and 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;

9.2.6 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 and XDR Service;

9.2.7 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;

9.2.8 notify BT of any planned work that you intend to undertake that may cause a Technical Incident;

9.2.9 ensure that all Enabling Services are maintained throughout the provision of the Managed Sentinel and XDR Service;

9.2.10 be responsible for any conclusions drawn from, and rectification of, any issues identified by use of the Managed Sentinel and XDR Service, supported by BT in accordance with the Managed Service Package selected by you and set out in any applicable Order;

9.2.11 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;

9.2.12 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 and 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 and XDR Service; and

(d) satisfy BT's security checks if a password is lost or forgotten;

9.2.13 ensure that appropriate Log level auditing is turned on for all Data Sources monitored by the Managed Sentinel and XDR Service. If the Log level auditing is not turned on, this will impact the Managed Sentinel and XDR Service;

9.2.14 attend review meetings, as required by BT;

9.2.15 prior to the meeting referred to in Paragraph 9.2.14, provide the most up to date network diagram of your existing IT network;

9.2.16 if you fail to attend the review meetings referred to in Paragraph 9.2.14 regularly, BT has the right to refuse your requests for tuning of the Managed Sentinel and XDR Service;

9.2.17 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;

9.2.18 provide 60 days' Notice prior to termination, if you require your Logs to be transferred;

9.2.19 for the XDR element of the Managed Sentinel and 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;

9.2.20 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;

9.2.21 promptly notify BT in writing where you no longer wish for Automated Remediation to form part of your Service (in line with Paragraph 2.6.3(d)(iv)) and acknowledge that, where you undertake any Remediating Action, BT shall not be liable for the results of such Remediating Action

9.2.22 notify BT of any changes to the Tenant or Subscription that could impact the delivery, operations or billing of the Managed Sentinel and XDR Service; and

9.2.23 only use the Microsoft Subscription associated with provision of the Managed Sentinel and XDR Service in accordance with the Contract. You will inform BT 30 days in advance and receive BT consent to any consumption of non-Managed Sentinel and XDR Service-related Resources.

Part C – Service Levels

10 Service Levels and Service Remediation Advice Targets

10.1 **Service Targets Security Incident Management**

Priority	MS Package Level	Security Incident	Target Time: Remediation Advice	Target Time: Commencement of Remediation Action
P1	Standard (MS1)	whenever a progress update is available	4 hours	N/A
	Enhanced (MS2)	within 30 minutes from the Security Incident being reported	4 hours	N/A
	Premium (MS3)	within 30 minutes from the Security Incident being reported	4 hours	*4 hours
P2	Standard (MS1)	whenever a progress update is available	8 hours	N/A
	Enhanced (MS2)	within 2 hours from the Security Incident being reported	8 hours	N/A
	Premium (MS3)	within 2 hours from the Security Incident being reported	8 hours	*8 hours
P3	Standard (MS1)	whenever a progress update is available	24 hours	N/A
	Enhanced (MS2)	within 4 hours from the Security Incident being reported	24 hours	N/A
	Premium (MS3)	within 4 hours from the Security Incident being reported	24 hours	*24 hours
P4	Standard (MS1)	whenever a progress update is available	Weekly/Monthly in agreed reporting	N/A
	Enhanced (MS2)	within 5 hours from the Security Incident being reported	Weekly/Monthly in agreed reporting	N/A
	Premium (MS3)	within 5 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 Managed Service Package 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 Technical Incident resolution because the mitigation responsibility rests with you.

10.1.4 The Target Response Time and Target Time for Remediation Advice 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 Availability**

10.2.1 There is no standard service availability for this Managed Sentinel and XDR Service.

Part D – Defined Terms

11 Defined Terms

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

"**Acceptance Tests**" means those objective tests conducted by you that when passed confirm that you accept the Managed Sentinel and XDR Service and that the Managed Sentinel and XDR Service is ready for use save for any minor non-conformities that will be resolved as a Technical Incident in accordance with Paragraph 9.2.

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

"**Administrator**" means any individual authorised by you responsible for administering Users.

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

"**Analytics Ingest**" means a Microsoft product that enables a customer to send a committed amount of data to Microsoft Sentinel for analysis.

"**Analytics Retention**" means a Microsoft product that enables a customer to store a committed amount of data in the Analytics Tier of Microsoft Sentinel for a set period of time.

"**Analytics Tier**" means a component of Microsoft Sentinel that enables active analysis of logs.

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

"**Azure B2B**" means a multitenant management capability required to manage a service (business to business).

"**Azure GDAP**" or "**Azure Granular Delegated Admin Privileges**" means a multitenant management capability required to manage a service.

"**Azure Lighthouse**" means a multitenant management capability required to manage a service.

"**Azure Resource**" means a manageable entity, component or asset within Azure.

"**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 Annex.

"**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.

"**BT SOCaaS for Microsoft Sentinel**" has the meaning set out in Paragraph 2.3.2(a).

"**BT TAM**" or "**TAM**" means the Threat Analytics Manager BT appoints to be your point of contact for the duration of the Managed Sentinel and XDR Service.

"**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 and XDR Service.

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

"**Microsoft Cloud Solution Provider**" means the Microsoft partner programme that enables BT to sell and support Subscriptions for Microsoft Sentinel.

"**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.

"**Consumption-Based Subscription**" has the meaning given in Paragraph 2.3.2(b).

"**Consumption Charges**" means the Charges for the Consumption-Based Subscriptions that are based on resource consumption in the preceding month.

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

"**Continuous Improvement**" means the continuous improvement phase of the Managed Sentinel and XDR Service as set out in Paragraph 2.7.

"**Controlled Deployment**" means the controlled deployment phase of the Managed Sentinel and XDR Service as set out in Paragraph 2.5.

"**Controlled Deployment Custom Content Optimisation**" means the fine tuning of your Custom Content, conducted by both of us jointly in respect of MS2 and MS3.

"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 depending on various

parameters including number of Logs, creation of rule sets and wider activities running and testing associated Playbooks.

"**CSP**" means Cloud Solution Provider; a Microsoft-authorised partner that is permitted to procure, manage, support and bill Microsoft cloud services on behalf of a customer.

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

"**Custom Content Change Management Process**" means the process in relation to changes to the Custom Content as set out in Paragraph 2.7.2.

"**Custom Rule Design and Deployment**" means the services set out in Paragraphs 2.4.1(e)2.4.2(f)2.4.3(b).

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

"**Customer-Led Delivery Model**" has the meaning set out at Paragraph 2.3.1.

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

"**Customer Service Description**" means the document that describes the Managed Sentinel and XDR Service and includes the Standard Default Rule Set. This document is not legally binding and does not form part of your Contract.

"CySOC" or "Cyber Security Operations Centre" means BT's cyber 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.

"**Data Capture Form"** means a document that is completed by you to provide detailed information required for service setup and delivery. It forms part of the contractual documentation.

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

"**Delegated Administrator**" means the global administrative access BT must administer and provide support to your Microsoft Tenant. As a Delegated Administrator, BT may perform tasks including but not limited to adding Users, resetting passwords, and adding domains.

"**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 Priority 1 Technical Incident or a P1 Security Incident.

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

"**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.

"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.

"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.

"GDAP" means Granular Delegated Admin Privileges; Microsoft's delegated access model that allows a User to grant a Microsoft partner limited, role-based and time-bound administrative access to the User's Microsoft environment for the purposes of delivering agreed services.

"**Initial Setup**" means the facilitation of the setup and delivery of the Managed Sentinel and XDR Service as set out in Paragraph 2.4.

"**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 Sentinel BT MSSP Tenant 24x7x265" 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 Device**" means hardware or Virtual Machines that BT uses for the testing or delivery of the Managed Sentinel and XDR Service.

"**Managed Service Package"** means Managed Service 1, 2 and 3.

"**Managed Service 1**" or **"MS1"** means the Managed Service 1 Package as set out in this Annex.

"**Managed Service 2**" or **"MS2"** means the Managed Service 2 Package as set out in this Annex.

"**Managed Service 3"** or "**MS3"** means the Managed Service 3 Package as set out in this Annex.

"**Microsoft**" means Microsoft Limited Microsoft Campus Thames Valley Park Reading Berkshire RG6 1WG, UK.
"**Microsoft Sentinel Data Lake**" means a long-term data storage product offered by Microsoft.
"**Microsoft 365 Defender**" means unified security solution that integrates protection across endpoints, identities, email, and cloud apps, providing coordinated threat detection, investigation, and response.
"**Microsoft Defender for Cloud**" means a cloud security platform offering posture management, workload protection, and threat detection across Azure, Amazon Web Services ("**AWS**"), Google Cloud Platform ("**GCP**"), and hybrid environments.
"**Microsoft Defender XDR Portal**" means centralised interface within the Microsoft Defender portal for extended detection and response, consolidating alerts, incidents, and hunting across multiple domains.
"**Microsoft Sentinel**" means a cloud-native Security Information and Event Management ("**SIEM**") and Security Orchestration, Automation, and Response ("**SOAR**") solution. It collects and analyses security data across environments, applies AI for threat detection, and enables investigation and automated response.
"**Monitoring and Management**" means the monitoring and management phase of the Managed Sentinel and XDR Service as set out in Paragraph 2.6.
"MyAccount" means an online customer platform (also referred to as "**Customer Hub**") designed to provide secure, personalized access to your Service allowing case tracking and interactions with BT service teams.
"**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.
"**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.
"**Priority 1 Technical Incident**" has the meaning in the table set out in Paragraph 2.6.6(a)(v).
"**Priority 2 Technical Incident** has the meaning in the table set out in Paragraph 2.6.6(a)(v).
"**Priority 3 Technical Incident**" has the meaning in the table set out in Paragraph 2.6.6(a)(v).
"**Priority 4 Technical Incident**" has the meaning in the table set out in Paragraph 2.6.6(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 2.7.2(b)(v).
"**Resource**" means a Microsoft Azure functionality that enables a service to run.
"**RCA Support**" or "**Root Cause Analysis" 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.
"**Schedule**" means the Managed Service Schedule to which this Annex is attached or can be found at www.bt.com/terms, and which forms part of the contract.
"**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 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.
"**Service Desk**" means the helpdesk that you will be able to contact to submit Managed Sentinel and XDR Service requests, report Technical Incidents and ask questions about the Managed Sentinel and XDR Service.
"**Service Management Boundary**" has the meaning given in Paragraph 4.1.
"**Service Option**" has the meaning given in Paragraph 3.
"**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 Start Date**" has the meaning given in Paragraph 9.2.6.
"**Service Target(s)**" means any target that BT aims to meet as set out in this Annex.
"**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 and XDR Service is provided.
"**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 and XDR Service to allow for monitoring by BT, as set out in the Customer Service Description.

"**Subscription**" means a Microsoft container that is used to provision resources, which for the purposes of BT SOCaaS for Microsoft Sentinel are Analytics Ingest, Analytics Retention, and other Microsoft Sentinel resources required to run the agreed service.
"**Supplier**" means Microsoft Limited Microsoft Campus Thames Valley Park Reading Berkshire RG6 1WG, UK.
"**Supported Device List**" means the list of Event Log Data sources that are readily compatible with the Supplier's Data Sources as set out in the Customer Service Description (if applicable) attached to the applicable Order, and as may be amended by the Supplier from time-to-time.
"**Target**" means a non-contractual threshold that is set to aid the performance of the Managed Sentinel and 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 a 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 and XDR Service or particular element of the Managed Sentinel and 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.
"**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 the 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:

(b) make changes to the Custom Rule(s); and
(c) 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.
"**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 and XDR Service.