BT Managed CySOC Service for Splunk Schedule
Part B – Service Description

Section A The Service

1 STANDARD COMPONENTS OF THE SERVICE

BT will provide the Customer with the following Services in accordance with the details as set out in the Order:

1.1 BT Portal: This is the BT Portal used to provide a secure mechanism for Service Requests.

1.2 BT Monitoring and Management Support. BT will provide the following standard monitoring and management features:

BT Monitoring and Management Support	Description
Implementation Support	BT will provide the Customer with access to a named TAM as BT's security support on a shared basis, for the duration of the Service, to assist with any issues or requests.
Cyber Security Operations Centre support ("**CySOC**")	The CySOC uses Customer data traffic coming from the Splunk SIEM Platform in pursuit of the Service's threat detection capability. Where a Security Incident is detected by the policies applied to the CySOC, a Case will be raised and reported to the Customer via the BT Portal or email. The CySOC will provide the details of the Security Incident and remediation advice to mitigate detected threats to the Customer. Once the Security Incident is resolved, the Customer will respond with confirmation to BT via the BT Portal or email that the Customer has taken the necessary remediation action and that the Security Incident is closed. If no confirmation is received by the Customer, the case will be closed after a period of approximately 72 hours.
Advise the Customer of high impact Security Incidents	The CySOC reports the Security Incident to the Customer based on BT's initial severity and priority assessment. The Security Incident is then passed to the Customer for them to assess the impact to their business and a priority will be assigned based on the Customer feedback.
Service Request Management	In accordance with the Service Request Management Process set out in Paragraph 8.5; the Customer may submit a Service Request via the BT Portal or by e-mail to the TAM.
Security Incident triage	In addition to the standard CySOC support service, BT will also provide proactive management of detection of and response to security related events/incidents. The CySOC will provide the details of the Security Incident to the Customer and can provide suggested measures to mitigate detected threats.
BT SOAR	BT uses a Security Orchestration Automation and Remediation platform to correlate events, enhanced by BT threat intelligence data lake to report a Security Incident/s to the Customer.
Reporting	BT will share monthly reports and review meetings will be held between the TAM and Customer.
Security Incident log retention	BT will keep a log of all Security Incidents detected on the SOAR. The Security Incident log will be retained for 90 days and used for reporting purposes.

Further details of BT Monitoring and Management Support services are set out in Paragraph 8 of this Part B.

2 SERVICE OPTIONS

2.1 BT will provide the Customer with any of the following chargeable options as set out in any applicable Order and in accordance with the details as set out in that Order:

2.1.1 delivery of Complex Service Requests;

2.1.2 delivery of Simple Service Requests that are outside of the Customer's quarterly allowance as set out in Paragraph 8.5.3;

2.1.3 Custom Rules and Playbooks that are not covered by the existing BT Standard Default Rule Set and are outside of the Customer's allowance as set out in Paragraph 6. Any additional Custom Rules and Playbooks will be charged as One-Time Charges and must follow the defined Service Request Management Process; and

2.1.4 bespoke Customer training.

3 SERVICE MANAGEMENT BOUNDARY

3.1 BT's responsibility to provide and manage the Service is limited to the following service management boundary:

3.1.1 the standard Service elements as set out in Paragraph 1 including the BT Portal; and

3.1.2 any ordered optional Service elements set out in Paragraph 2.

3.2 Paragraph 3.1 constitutes the "**Service Management Boundary**".

3.3 BT will have no responsibility for the Service outside the Service Management Boundary.

3.4 BT does not make any representations, whether express or implied, about

3.4.1 whether the Service will operate in combination with any Customer Equipment or other equipment and software; or

3.4.2 the ability of the Service to detect, block and mitigate all malicious threats or attacks from the Internet.

3.5 BT will not be liable if BT is unable to deliver the Service, or any part of the Service due to a failure of any Customer Equipment, including any Customer Logs.

3.6 The Service assumes Customer Logs and functionality is available from the Customer's Splunk SIEM platform. BT will not be liable for any inability to provide the Service, or any degradation of the Service if the Customer does not have and maintain the appropriate licences, Customer Logs and functionality to the Customer's Splunk SIEM Platform.

4 ENABLING SERVICES

4.1 For the duration of the Subscription Term, the Customer will have the following services in place that are necessary for the Service to function:

4.1.1 Splunk SIEM Platform licences that will allow BT to provide the Service; and

4.1.2 access for BT to the Splunk SIEM Platform user interface.

(the "**Enabling Services**")

5 COMMISSIONING OF THE SERVICE

5.1 Before the Operational Service Date, BT will:

5.1.1 deliver and configure the Service as set out in the Order;

5.1.2 conduct a series of standard tests on the Splunk SIEM Platform to ensure that it is configured correctly to provide the Service;

5.1.3 connect the Service to each Enabling Service; and

5.1.4 on the date that BT has completed the activities in this Paragraph 5, confirm that the Service is available for Controlled Deployment and performance of any Acceptance Tests in accordance with Paragraph 7.

6 CUSTOM RULE DESIGN AND DEPLOYMENT PERIOD

6.1 BT will provide the Customer with the Standard Default Rule Set and relevant Playbooks which are applied to the Splunk SIEM Platform.

6.2 The Customer will have a Custom Rule Allowance of 15 Custom Rules per Subscription Term.

6.3 The Customer can request additional Custom Rules and Playbooks that are not covered by the existing BT Standard Default Rule Set as a Service option.

6.4 Any Custom Rules/requirements that are needed before the Operational Service Date may extend the standard delivery timelines. The timeline will be agreed with the Customer in advance.

6.5 If the Customer has requested Custom Rules or any changes to Custom Rules during the Deployment Period, this will be taken from the Customer's Custom Rule Allowance and must follow the Service Request Process set out in Paragraph 8.5 below. Should BT elect to standardise Custom Rules requested by the Customer, the rule will be added to the Standard Default Rule Set, and made available to BT's wider customer base, in which case the rule will cease to count towards the Customer's Custom Rule allocation and no additional Charges will apply. In such circumstances, BT will own the Intellectual Property Rights in relation to the rule.

6.6 Subject to receiving acceptable information from the Customer Logs, BT will configure the Service to implement the Custom Rules agreed with the Customer in accordance with Paragraph 5.

6.7 The TAM will assist the Customer with the configuration of the Service in accordance with the agreed Custom Rules.

7 CONTROLLED DEPLOYMENT AND ACCEPTANCE TESTS

7.1 BT and the Customer will jointly carry out the Controlled Deployment. The Customer will use reasonable endeavours to complete the Controlled Deployment as soon as possible and within agreed project timescales.

7.2 The Customer will submit any changes it requires to the Custom Rules as a result of the Controlled Deployment through the Service Request Management Process.

7.3 The Customer will carry out the Acceptance Tests for the Service during the Controlled Deployment Period and use reasonable endeavours to complete the Acceptance Tests as early into the Controlled Deployment Period as possible.

7.4 The Service will undergo the Acceptance Tests prior to the Service going live. Acceptance Tests are considered successful:

7.4.1 if the Customer confirms acceptance in writing to BT during the Controlled Deployment Period; or

7.4.2 if the Customer does not provide BT with notice to the contrary by the end of the Controlled Deployment Period.

7.5 Subject to Paragraph 7.7, the Operational Service Date will be the date that the Customer confirms, or BT deems acceptance of the Service in writing in accordance with Paragraph 7.4.

7.6 If, during the Controlled Deployment Period, BT provides the Customer notice that the Acceptance Tests have not been passed, the Customer will remedy the non-conformance without undue delay.

7.7 If, during the Controlled Deployment Period, the Customer provides BT notice that the Acceptance Tests have not been passed, BT will remedy the non-conformance without undue delay and provide the Customer with notice that BT has remedied the non-conformance and inform the Customer of the Operational Service Date.

Section B Service Management

8 SERVICE MANAGEMENT

8.1 Technical Incidents

8.1.1 Where the Customer becomes aware of a Technical Incident which may impact the Service:

(a) The Customer will report the Technical Incident to the TAM during Business Hours or the CySOC outside of Business Hours and a Ticket will be raised;

(b) all communications with the TAM will be in English;

(c) BT will assess the Technical Incident in accordance with the criteria set out in the table below:

Priority	Description
P1	Service is inoperative resulting in total loss of Service. Priority shall be reduced to P2, on a work effort basis, by the successful implementation of a workaround acceptable to the Customer.
P2	Service is partially inoperative reducing the availability of Service.
P3	Minor disruption of Service.
P4	Non-Service affecting query relating to the product

(d) BT will review the status of the Technical Incident and amend the priority level assigned initially if necessary.

(e) BT will inform the Customer when it believes the Technical Incident is cleared and will close the Ticket when:

(i) The Customer confirms that the Technical Incident is cleared within 24 hours after having been informed by BT; or

(ii) If BT is unable to reach the Customer to confirm Technical Incident resolution, BT will attempt to contact the Customer three times in total, at regular intervals, before automatically closing the Technical Incident Ticket.

(f) If the Customer confirms 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.

(g) BT will notify the Customer of any Technical Incidents on the BT side which may affect the Service.

8.2 Event Searches and Management

8.2.1 Customer Logs will be stored in relevant Splunk SIEM Platform tables. BT will run the Standard Default Rule Set against the relevant tables and categorise each Alerting Incident raised according to its severity for inspection by the BT CySOC.

8.2.2 BT will search Events in accordance with the Standard Default Rule Set and the Customer's chosen Custom Rule/s.

8.3 Security Incidents

8.3.1 The BT cyber analysts within the CySOC will analyse Security Incidents and Event data generated by the Splunk SIEM Platform and:

(a) assess appropriate remediation actions to be taken;

(b) raise a Case for each Security Incident;

(c) notify the nominated Customer contact by e-mail or via the BT Portal of possible Security Incidents; including details of the relevant underlying Event and recommended mitigation or remediation action to be taken by the Customer.

8.3.2 The Customer will remain responsible for implementing any required mitigation or remediation actions as recommended by BT following a Security Event/Incident. BT is not responsible for the ongoing effects of the Security Incident.

8.4 Reviews and reporting

8.4.1 BT will share standard summary reports and the TAM will conduct meetings with the Customer on a monthly basis.

8.4.2 Meetings entail discussion of Service performance against Service Targets and a review of the effectiveness of the Custom Rules applied to the Service.

8.4.3 The Customer will work with the TAM and take appropriate action to address issues which impact or influence the Service, e.g. fine tuning or amending the Customer's Custom Rules as recommended by the TAM.

8.5 Service Request Management Process

8.5.1 BT will implement changes in response to the Customer's Service Request(s) in accordance with the following process:

(a) the authorised Customer Contact will submit Service Requests from an approved list via an email to the TAM or BT Portal, providing sufficient detail and clear instructions as to any changes required;

(b) BT will check each Service Request for its complexity and assess whether it is a Simple Service Request (SSR) or a Complex Service Request (CSR);

(c) If determined to be simple;

(i) BT will inform the authorised Customer Contact of the Customer's remaining SSR allowance before the Customer decides to proceed; and

(ii) BT will advise the authorised Customer Contact on expected timeline for delivery of the SSR.

(d) If determined to be complex, if eligible;

(i) BT will provide the authorised Customer Contact with costs and timelines to complete the request; and

(ii) BT will not proceed with any CSRs without acceptance of applicable charges from the authorised Customer Contact.

8.5.2 BT may provide the Customer with Professional Services at an additional Charge, at the authorised Customer Contact's request, to assist the Customer in writing the Service Request.

8.5.3 Simple Service Requests:

(a) The Service has an allowance of ten (10) SSRs per quarter.

(b) SSRs outside of the Customer's allowance set out in Paragraph 8.5.3 (a) are subject to an additional Charge.

(c) The initial SSRs are set out on the Order which may be amended from time to time depending on changes by the Supplier subject to BT providing notice to the Customer and, where any changes may have a material impact on the Customer, the Customer's approval will be sought; and

(d) BT will communicate the status of Simple Service Requests via e-mail or BT Portal to the Customer Contact requesting the change.

8.5.4 Complex Service Requests:

(a) CSRs can be ordered in-life and are subject to a one-time Charge.

8.5.5 Custom Rules:

(a) The Service has an allowance of fifteen (15) Custom Rules per Subscription Term and the Customer may request these by submitting a Complex Service Request via e-mail or the BT Portal.

(b) The Customer will not raise Custom Rule requests more frequently than eight (8) per month.

(c) The Customer will not raise Urgent Custom Rules more frequently than two (2) per month.

(d) Where BT's measurements show that Urgent Custom Rules are being raised more frequently than as set out in Paragraph 8.5.5 (c) BT may, either:

(i) aggregate the Urgent Custom Rules over a period of time, so that they may be implemented more efficiently. In this event there may be some implementation delays; or

(ii) review the Customers' requirements and agree with the Customer Contact an appropriate alternative implementation process and any associated charges.

(e) BT will use reasonable endeavours to implement an Emergency Change as quickly as is reasonably practicable. BT may charge the Customer the cost of implementing an Emergency Change.

(f) BT may implement an Emergency Change without the authorised Customer Contact's approval.

(g) The Customer is 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.

8.6 Service Targets and Service Remediation Advice Targets

8.6.1 Service – Security Incident targets

BT Priority	Severity Rating	Security Incident Response Target	Security Remediation Advice Target
P1	Critical (5)	Notify customer in 30 min	Give Remediation Advice in 4 hours
	Very high (4)		
P2	High (3)	Notify customer in 2 hours	Give Remediation Advice in 8 hours
P3	Medium (2)	Notify customer in 4 hours	Give Remediation Advice in 24 hours
	Low/Informational (1/0)		

8.6.2 From the Operational Service Date, BT will aim to provide the Customer 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 in Paragraph 8.6.1 above.

8.6.3 BT will not provide a progress update while BT is waiting on the Customer's input or feedback.

8.6.4 BT will not provide a target time for Security Incident resolution because the mitigation responsibility rests with the Customer.

8.6.5 The Customer has complete responsibility to resolve and carry out any remediation action on the Security Incident.

8.6.6 The target response times shown in the table above are indicative only and BT will have no liability for failure to meet them.

8.6.7 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.