BT Managed CrowdStrike Falcon XDR Service 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 Supplier Security Modules. The following security modules of the Supplier will be provided and supported by BT:

CrowdStrike Security Modules	Description – Standard Modules
Falcon Prevent	Next generation anti-virus that uses a combination of artificial intelligence, behavioural detection and machine learning algorithms so known and unknown threats can be anticipated and prevented. Falcon Prevent protects against threats, from malware and ransomware to sophisticated attacks on endpoints.
Falcon Insight XDR	Extended detection and response capability. Falcon Insight XDR enriches and prioritises security data collection with embedded threat intelligence and MITRE ATT&CK mappings. AI-powered protections are used to surface and prevent sophisticated threats, without any prior knowledge of the threat.
Falcon Intelligence	Threat intelligence that enriches detected security events and incidents to enable faster and more accurate security incident management decisions.
Falcon Threat Graph Standard (7 days)	CrowdStrike's cloud-scale platform used for advanced threat intelligence and analytics of Customer's security data. Threat Graph stores (7 days) and correlates endpoint and other security activity data. A costed option can be selected to extend the standard 7-day period.
Falcon Device Control	USB device control provides the visibility and control to enable safe usage of USB devices across the organisation.
Falcon Firewall Management	Host firewall control capability delivering a single, host firewall management solution for centralised policy control.
Falcon Discover	IT hygiene capability used to identify unauthorised accounts, devices and applications in real time, enabling faster remediation and improved security coverage.
Falcon Spotlight	Vulnerability insights using the Falcon Sensor to provide scan less vulnerability assessment, delivering automated vulnerability information to help prioritise cyber risks associated with known vulnerabilities.

1.1 CrowdStrike Falcon Sensor Software: This is Supplier Software for use during the licence period as set out in the Order for the Customer to download and install on the required endpoints. This software enables the Customer to use the Service.

1.2 CrowdStrike Falcon Security Modules Software: This is Supplier Software for the licence period as set out in the Order for the use of monitoring and protecting the Customer's devices, information, and infrastructure.

1.3 CrowdStrike Falcon Portal: This is the CrowdStrike provided secure portal that provides BT and the Customer with a right to access and use the Service. The CrowdStrike Falcon Portal allows the detection and response service to be performed for the devices and infrastructure being protected.

1.4 CrowdStrike Falcon Platform: This is the software as a service platform that processes the security telemetry from the Falcon Sensor Software in line with the CrowdStrike Security Modules allowing the Customer to protect the selected devices and infrastructure.

1.5 BT Security Portal: the BT Security Portal used to provide a secure mechanism for service requests and incident management.

1.6 **BT support**. BT will provide the Foundation Graded Service Tier as standard. The features of Foundation are as follows:

BT Support	Description – Foundation Features
Implementation Support	BT's Cyber Design and implementation team will provide support and be responsible for the setup, configuration and optimisation of the CrowdStrike XDR platform in line with the Customer's requirements.
BT Cyber Security Operations Centre ("**CySOC**") support	The CySOC is responsible for any Security Incident detected by the Service. The CySOC uses Customer data traffic in pursuit of the Service's detection and response capability. Where an alert is detected by the CySOC, a warning will be raised and reported to the Customer via the BT Security Portal. The Customer can access the BT Security Portal to confirm and initiate any corrective investigation. Once the Security Incident is resolved, the Customer will respond with confirmation to BT via the BT Security Portal, telephone or email that the Security Incident is closed.
Advise the Customer of high impact Incidents and Security Incidents	Generate the following types of incidents from the Service: Proactive – The CySOC reports the Security Incident to the Customer based on the initial severity and priority. 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. The CySOC will provide the details of the Security Incident to the Customer.
Service availability monitoring	BT will monitor the availability of the CrowdStrike Falcon platform in conjunction with CrowdStrike using the CrowdStrike service emails.
Service request management	In accordance with the Service Request Process set out in Paragraph 8.5, the Customer may request via the BT Security Portal to implement 10 Simple Service Requests (SSRS) per quarter.
Reporting	On a bi-annual basis BT will do a review and send a report to the Customer as further detailed in Paragraph 8.4.1.
Security Incident log retention	BT will keep a log of all Security Incidents detected on the BT Security Portal. The Security Incident log will be retained for 7 days.

Further details of these BT support services are set in Paragraph 8 of this Part B.

2. SERVICE OPTIONS

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 **Optional BT Support Services**. The Customer may select the Foundation Plus and Premium Graded Service Tiers. In addition to the standard features as set out in Paragraph 1.7, the standard features of Foundation Plus and the Premium Graded Service Tiers are as follows:

BT Support	Description
BT Cyber Security Operations Centre support ("**CySOC**")	In addition to the standard CySOC support service: For Foundation Plus: • The CySOC will provide the details of the Security Incident to the Customer. • The CySOC can provide suggested measures to mitigate detected threats. For Premium: • The CySOC will provide the details of the Security Incident to the Customer. • The CySOC can provide suggested measures to mitigate detected threats.

Service request management	In accordance the Service request Process set out in Paragraph 8.5; the Customer may request via the BT Security Portal or via e-mail to the TAM to implement per quarter: For Foundation Plus: • 15 SSRs For Premium: • Unlimited SSRs
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. For Foundation Plus: • The CySOC will provide the details of the Security Incident to the Customer. • The CySOC can provide suggested measures to mitigate detected threats. For Premium: • The CySOC will provide the details of the Security Incident to the Customer. • The CySOC can provide suggested measures to mitigate detected threats.
BT Eagle-i	BT Eagle-i is a BT developed security orchestration automation and remediation (SOAR) platform for false positive reduction, threat intelligence enrichment and automated quarantine of at-risk endpoint devices. This Service option is available for Foundation Plus and Premium. For Foundation Plus: Eagle-i provides accurate and guided security case creation to advise the Customers of what action should be taken for endpoint detected threats. For Premium: Where appropriate and in line with the Customer's security policy(ies), auto-contain/quarantine of the affected endpoint(s) to ensure they are disconnected from the corporate network as soon as possible. The devices can still communicate with the Falcon platform for reinstatement to be carried out once the issue has been remediated by the Customer.
Reporting	• For Foundation Plus BT will provide on a quarterly basis; and • For Premium BT will provide on a monthly basis a review and report to the Customer as further detailed in Paragraph 8.4.2

2.2 **Optional Supplier Security Modules.** The Customer may order as a Service option one or more of the following additional Supplier Security Modules:

CrowdStrike Security Modules	Service Description
Falcon Identity Protection	Threat detection and real-time prevention of identity-based attacks using a combination of AI, behavioural analytics and a flexible policy engine to enforce risk based conditional access for users, applications and hosts. This Service option is available only where the Customer has selected a Foundation Plus or Premium Graded Service Tier.
Falcon Cloud Security	Unified agent and agentless platform cloud security capability that protects the Customer's cloud estate with integrated cloud workload protection (CWP), cloud security posture management (CSPM), cloud identity entitlement management (CIEM). This Service option is available only where the Customer has selected a Premium Graded Service Tier.
Falcon Overwatch	Threat hunting service delivered by CrowdStrike's cybersecurity experts to hunt within the Falcon platform for traces of sophisticated intrusions. This Service option is available where the Customer has selected a Foundation, Foundation Plus or and Premium Graded Service Tier.

CrowdStrike Security Modules	Service Description
Falcon Log Scale Cloud for Falcon Extended Retention	Extended storage of Falcon raw sensor data beyond the 7-day standard period. The Customer may select on the Order either 30, 60, 90, 180 or 365-days retention of Falcon raw sensor data. This Service option is available where the Customer has selected a Foundation, Foundation Plus or and Premium Graded Service Tier.
Falcon Sandbox	Dedicated Customer instance and access to Falcon Sandbox. Sandbox enables deep analysis of evasive and unknown threats, enriches the results with threat intelligence and delivers actionable indicators of compromise ("IOCs"), to better understand sophisticated malware attack. This Service option is available where the Customer has selected a Foundation, Foundation Plus or and Premium Graded Service Tier.

3. SERVICE MANAGEMENT BOUNDARY.

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

3.1.1 The CrowdStrike Falcon Portal;

3.1.2 The BT Security Portal

3.1.3 The Customers Graded Service Tier level as set out in Part B.

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

4. ENABLING SERVICES

4.1 The Customer will have the following services in place that are necessary for the Service to function:

4.1.1 Internet connectivity between the endpoints and cloud infrastructure covered by the Service and the CrowdStrike Falcon platform.

(the "**Enabling Service**")

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 Service to ensure that it is configured correctly;

5.1.3 connect the Service to each Enabling Service;

5.1.4 on the date that BT has completed the activities in this Paragraph 5.1, confirm to the Customer that the Service is available for performance of any Acceptance Tests.

6. ACCEPTANCE TESTS

6.1 The Customer will carry out the Acceptance Tests for the Service within five (5) Business Days after receiving notice from BT ("**Acceptance Test Period**").

6.2 The Service is accepted by the Customer if the Customer confirms acceptance in writing during the Acceptance Test Period or is treated as being accepted by the Customer if the Customer does not provide BT with notice to the contrary by the end of the Acceptance Test Period.

6.3 Subject to Paragraph 6.4, the Operational Service Date will be the earlier of the following:

6.3.1 the date the Customer confirms, or BT deems acceptance of the Service in writing in accordance with Paragraph 6.2;

6.3.2 the date of the first day following the Acceptance Test Period; or

6.3.3 the date the Customer starts to use the Service.

6.4 If, during the Acceptance Test 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 notice that BT has remedied the non-conformance and inform the Customer of the Operational Service Date.

Section B Supplier Terms

7. EULA

7.1 The applicable EULA will be: https://www.crowdstrike.com/terms-conditions/

Section C Service Management

8. SERVICE MANAGEMENT

8.1 Technical Incidents

8.1.1 Where the Customer or BT becomes aware of a Technical Incident:

(a) it will be reported to the Service Desk;

(b) BT uses structured questions to record the details of the Technical Incident. The BT Service Desk will log the Technical Incident in BT's standard incident management system and generate a Ticket;

(c) 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; 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.

(d) 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.

8.2 Security Incidents

The reporting and resolution of Security Incidents depends on the Service options ordered by the Customer.

8.2.1 Where the Customer has ordered the Foundation Graded Service Tier, BT will only provide first line support on the following basis:

(a) when BT becomes aware of a Security Incident via the CySOC a warning will be raised and reported to the Customer via the BT Security Portal. The Customer will remain responsible for undertaking Mitigation Actions on the Security Incident.

(b) When the Customer reports a Security Incident to BT, BT will only log the Security Incident on the BT Security Portal and provide the Customer some basic advice.

8.2.2 Where the Customer has ordered the Foundation Plus Graded Service Tier, in addition to the first line support:

(a) BT will provide second line support where a cyber analyst within the CySoc will:

(i) provide monitoring and troubleshooting related to the CySOC operations working with the Service technologies and other core network security products;

(ii) determine critical system and data integrity;

(iii) provide for new analytic methods for detecting threats;

(iv) provide by e-mail recommended mitigation or corrective actions to the Customer.

(b) BT will liaise with other BT Service Desks where the Customer has other security products.

(c) The Customer will remain responsible for implementing any required mitigation or corrective actions as recommended by BT.

(d) If the Security Incident is still unresolved, BT will escalate to the third line support (provided by the Supplier), which will deal with escalations from second line support (provided by BT), and use the investigations conducted by BT to support a Security Incident effectively.

8.2.3 Where the Customer ordered the Eagle-i Service option, BT will automatically implement Mitigation Actions.

8.3 Technical and Security Incidents additional terms:

8.3.1 The Customer will ensure that any Technical Incident or Security Incident notification includes all relevant and available logs at the time of contacting BT.

8.3.2 The progress update times, and restoration times are targets only and BT will have no liability for failure to meet them.

8.3.3 BT may require additional data during the investigation of the Technical Incident or Security Incident that may include:

(a) Windows preprocessor (WPP) logs; providing debugging information at developer level;

(b) complete dumps (not mini dumps);

(c) packet captures - required to investigate firewall, application control, Device control issues;

(d) machine image - when issue cannot be reproduced;

(e) performance monitor logs;

(f) process monitor logs;

(g) Microsoft Windows performance analyser;

(h) Filemon logs; and

(i) remote access to the Customer's endpoint Devices.

8.4 Reviews and reporting

8.4.1 Foundation

(a) The TAM will carry out a review on the performance of the Service bi-annually and send a report to the Customer Contact.

(b) The Customer will take appropriate action to address issues as recommended by the TAM, including implementing security improvements as agreed:

8.4.2 Foundation Plus & Premium

(a) The TAM will carry out a review on the performance of the Service quarterly where the Customer has selected Foundation Plus and monthly where the Customer has selected Premium and send a report to the Customer Contact with the following actions:

(i) a review focusing on the performance of the Service;

(ii) a review of the Customer's security policy(ies) focusing on the effectiveness of the rules applied to the Customer's security policy(ies) and the need to fine tune or amend the rules of the Customer's security policy(ies).

(b) Unless the Customer has ordered Eagle-i, the Customer will be responsible for initiating the appropriate change requests in accordance with the Change Management Process to address issues in respect of fine tuning or amending the Customer's security policy(ies) as recommended by the TAM.

8.5 Service request management process

8.5.1 BT will implement changes to the Customer's security policy(ies) in response to service requests submitted by the Customer via the Security Portal, subject to the following process:

(a) BT will provide secure access to the Security Portal to all pre-agreed and authorised Customer contacts to enable service requests to be submitted. Timeframes will be standard, with target timescales of one Business Day, except during periods of Planned Maintenance.

(b) SSRs are upgrades and modifications needed because of planned developments and security improvements. SSRs will be executed subject to the Customer submitting the request and in accordance with a timing agreed with the Customer. SSRs are applicable to the following catalogued items:

Change Title	Change Description
Falcon Console User(s)	Add/Modify/Delete user account's roles permissions or access to features and functionality in the CrowdStrike Falcon console. Maximum of four users per request.
Falcon Host Group(s)	Add/Modify/Delete endpoints to/from Falcon Groups. Maximum of ten hosts per request.
Falcon Exclusions	Manage folders, files, and file types to exclude from detections, blocking, and file extraction. Maximum of ten exclusions and/or folders per request.
Falcon API	Manage the API key that applies to Customer Falcon environment. This request is for a single API secret key only.
Falcon IOC Management	Upload Customer specific IOCs to Allow-lists or block-lists. Maximum of 10 IOCs per request.
Falcon Sandbox	Configure Falcon Sandbox, which enables suspicious files or URL is submitted to the Falcon Sandbox.
Falcon Endpoint-Containment	Control the network isolation of the endpoints. Misconfiguration of these polices can isolate the endpoints from the network. Containment of one host per request is allowed. Please raise a new request if more than one host is to be contained.
Falcon Endpoint - Inactive	Delete endpoint from Falcon console, please note that deleting a Windows, Mac, or Linux host does not uninstall or deactivate its sensor. Maximum of ten endpoints removed/restored per request.
Falcon Custom Alerts	Request custom alerts to configure email alerts using predefined CrowdStrike templates. Maximum of ten custom alerts per request.
Falcon Identity - Subnets	Label the Customer's environment IP segments in falcon under Identity modules to have more granular control over the Identity rules. Maximum of ten subnets per request.
Falcon Identity - Compromised passwords Passphrases	The Compromised Password Detection feature identifies passwords on Microsoft AD that the system determines were previously compromised. Maximum of one file per request.
Falcon Complex Change Request	Use this request if the requirement falls outside of the available change requests.

(c) CSRs are any changes not defined as a Simple. BT will check each request for its complexity and will provide a quote for implementing the request, detailing the scope of the CSR and the required additional Charges. Based on BT's quote, the Customer may authorise the CSR from BT.

8.5.2 Where the Customer has selected the Foundation or Foundation Plus Graded Service Tier and SSRs are being raised more frequently than the quarterly allowance; the Parties may either agree:

(a) to aggregate the Customer requests over a period of time, so that they may be implemented more efficiently. In this event there may be some implementation delays;

(b) to review the Customer requirements and agree with the Customer an appropriate alternative implementation process and any associated charges via a new Order; or

(c) to charge such additional SSRs at the rate as set out in the Order.

8.5.3 BT will communicate the status of all service requests via e-mail to the requestor and the status will be available on the BT Security Portal for a period of six months.

8.5.4 The Customer will ensure that any authorised Customer Contact with access to the BT Security Portal will not submit any unauthorised requests.

8.5.5 If the Customer has ordered Foundation Plus or Premium, the authorised Customer Contact may also submit requests directly to the TAM.

8.5.6 If the Customer has ordered Premium, the TAM will use reasonable endeavours to identify errors or potential unforeseen consequences of requested Simple and Complex Change requests and advise Customer appropriately.

8.6 Service targets

8.6.1 Service Availability target:

(a) The CrowdStrike Falcon portal shall be available at least 99.9% of the time, excluding scheduled downtime for Planned Maintenance (not to exceed 4 hours a month) and downtime attributable to force majeure as further detailed at Paragraph 8.6.1(c).

(b) Compliance with the availability target will be measured on a calendar month basis. The Availability will be calculated by dividing (i) by (ii) and then multiplying by 100, where:

(i) is the total number of minutes of up time (i.e., in which there were no Outages) during an applicable calendar month (excluding only downtime occurring during the scheduled maintenance period or attributable to elements of force majeure)

(ii) is the total number of actual minutes in such month minus minutes of downtime occurring during the scheduled maintenance period or attributable to elements of force majeure.

(c) An "Outage" means: (a) for Falcon Insight, or Falcon Intelligence, that substantially all the portal pages are dysfunctional or unavailable, or there is complete unavailability of the portal; and (b) for Falcon DNS, where CrowdStrike servers do not respond to any query. Due to the hierarchical nature of the global DNS system, upstream server blocks or failures that CrowdStrike cannot control or influence, are events of force majeure for the purposes of this schedule.

8.6.2 Service Care target response times and follow-up

(a) Foundation support provides support set out in the table below and will also include email communications, access to the CrowdStrike portal and documented troubleshooting and technical assistance.

(b) Foundation Plus Support provides everything set out in the table below in addition to:

- Access to the CySOC team who will help as required and will provide support for 24 hours a day, seven days per week.
- Quarterly TAM reviews.

(c) Premium Support builds on the Foundation Plus Support as well as:

- Monthly TAM review.

For any P1 or P2 Incident or Security Incident under the Premium Support, the Customer must have a dedicated employee who is available by phone with the necessary access to assist in troubleshooting. If an employee is not available, the Customer will agree with BT on a timeframe for updates.

Priority	Initial Response Target	Next Response Target	Further Responses Target	
P1	Customer will be informed that BT is dealing with their Incident within 15 minutes of receiving it (either via an alert or by the Customer advising us)	First update within 60 minutes from the Incident ticket being opened	Every 60 minutes	
P2	Customer will be informed that BT is dealing with their Incident within 30 minutes of receiving it (either via an alert or by the Customer advising us)		First update within 60 minutes from the Incident ticket being opened	Every 2 hours
P3	N/A		First update within 4 hours from the Incident ticket being opened	Every 4 hours
P4	N/A		First update within 24 hours from the Incident ticket being opened	Every 24 hours