BT Security Operational Technology & Threat Management Visualise & Detect Service Schedule

Part B - Service Description

Section A – The Service

1. GRADED SERVICES AND STANDARD COMPONENTS

1.1 BT will provide the Customer with one of following graded services in accordance with the details as set out in the Order:

1.1.1 **"Visualise"** consisting of the following standard components (the "Visualise Service"):

(a) A "Security Platform" containing sensors from a range of suppliers. The sensors are either physical devices or virtual appliances collecting data from the assets to provide threat information, alerts and other asset information in order to gain visibility on the security of Customer's operational technology network. If agreed on the Order that the sensors will be physical devices, these will be sold to the Customer by BT as Purchased Equipment. The Customer may as an option order a Management Console (as defined in paragraph 1.1.2 b)as part of the Security Platform as further set out in this Schedule.

(b) Supplier Software and any Threat Intelligence subscription licenses associated with the Security Platform. BT will procure and deliver this Software and the respective licenses for the subscription term as set out in the Order;

(c) Project managed installation and deployment;

(d) Initial configuration of the appliances on the Security Platform;

(e) Asset discovery and initial tuning;

(f) Training by the selected Supplier for up to ten (10) named Customer contacts; and

(g) Security Platform optimisation and fine tuning.

(h) Set Customer's operational technology environment baseline

1.1.2 **"Detect"** consisting of following standard components (the "Detect Service"):

(a) The standard components as set out with Visualise;

(b) A "Management Console". The Management Console uses feeds from the sensor appliances to provide asset data, threat information; alerts and other information to manage the security on a network. The Management Console is either physical devices or virtual appliances. If agreed on the Order that the Management Console will be physical devices, the Management Console will be sold to the Customer by BT as Purchased Equipment;

(c) "Sentries". The sentries are physical devices that BT deploys into the Customer's environment on the Site in order to aggregate the alerts, and send these to the BT monitoring systems. They are also used to store back-ups. These Sentries will operate in a primary/failover mode and remain BT equipment;

(d) Monitoring and management of the Security Platform, and Cyber Security threats;

(e) Continuous improvement; and

(f) Incident management

2. SERVICE OPTIONS

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

2.1.1 If the Customer selected only the Visualise Service; a Management Console as set out in paragraph 1.1.2 (b);

2.1.2 An additional "SaaS Management Console". A SaaS Management Console is a cloud based Management Console which is deployed as software as a service (SaaS), rather than being a physical deployment and enables the Customer to consolidate all its security management within a single application;

2.1.3 Integrate the operational technology alerts with Customer systems. If the Customer orders the integration of the operational technology alerts with Customer systems BT will configure the Security Platform to forward alerts into the Customer's ServiceNow ticketing system (managed by the Customer);

2.1.4 Forwarding of operational technology alerts to Customer-owned SIEM. If the Customer has their own SIEM, BT will configure the Security Platform to forward alerts into the Customer-owned SIEM; and

2.1.5 For the Detect Service only; a spare sensor on Site in the event of an active sensor failure to mitigate the risk of delay in fail-over. BT will provide a field technician to replace the failing sensor with a spare sensor. The spare sensor will be powered on but will not be monitoring the Customer environment.

3. SERVICE MANAGEMENT BOUNDARY

3.1 BT's responsibility to provide and manage the Service is physically and logically limited to the following service management boundary as set out in any applicable Order and this paragraph 3:

3.1.1 For the Visualise Service this is limited to the standard components as set out in paragraph 1.1.1 and any service options selected on the Order as described in paragraph 2. For the Detect Service this is limited to the standard components as set out in paragraph 1.1.2 and any service options selected on the Order as described in paragraph 2.

3.1.2 Where BT deploys shared infrastructure as part of the Service as set out on the Order, BT will manage any Incidents affecting that infrastructure.

3.1.3 BT will have no responsibility for the Service outside the Service Management Boundary, including Customer provided infrastructure and User devices other than when contracted to the Service provided.

3.1.4 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.

3.2 Paragraphs 3.1.1 - 3.1.4 together constitutes the "**Service Management Boundary**". With the exception of items described in paragraphs 1 and 2, BT has no responsibility for any virtual or physical infrastructure or Enabling Services (with the exception of Enabling Services provided by BT which will be provided in accordance with their separate terms).

4. ENABLING SERVICES

4.1.1 The services that the Customer is required to obtain in order to receive this Service ("**Enabling Services**") are :

(a) Remote access connectivity.

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 paragraph 8;

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; and

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 that the Customer confirms or BT deems acceptance of the Service in writing in accordance with paragraph 6.2; or

6.3.2 the date of the first day following the Acceptance Test Period.

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. END USER LICENCE AGREEMENT (EULA)

7.1 The applicable EULA depends on the Supplier selected.

7.2 The EULA applicable for Nozomi can be found at: https://www.nozominetworks.com/legal/eula/ and https://www.nozominetworks.com/legal/dpa-addendum/

7.3 The EULA applicable for ForeScout can be found at: https://www.forescout.com/company/legal/eula/ and https://www.forescout.com/wp-content/uploads/2022/04/Forescout-DPA-End-Users_-4.7.22-EM.pdf

7.4 The EULA applicable for Claroty can be fount at: https://www.claroty.com/eula/ and https://claroty.com/dpa

Section C – Service Responsibility Matrix

8. BT RESPONSIBILITIES

8.1 Project managed installation and deployment

BT will:

8.1.1 appoint a project manager to co-ordinate all elements associated with the Service, liaising with the Customer, the installers and the Suppliers. All project management activity will be administered remotely and the project manager will not visit your Site;

8.1.2 appoint a solution architect to conduct a technical workshop to fully understand the Customer requirements;

8.1.3 design a Security Platform to meet the Customer's cyber security requirements and project manage the delivery and deployment of the solution on the Customer operational technology estate in accordance with any applicable Order.

8.1.4 only if the Customer has selected the Detect Service, configure a pair of Management Consoles and a pair of Sentry appliances per solution to give increased resilience against failure.

8.2 Initial configuration of the appliances on the security platform

Following design and deployment of the Security Platform, BT will complete the base configuration of the appliances to include:

8.2.1 deployment of the Threat Intelligence feed, and current Common Vulnerabilities and Exposures (CVE), in accordance with the Customer's Threat Intelligence licence subscription;

8.2.2 discovery of the connected devices that are visible to the Security Platform;

8.2.3 baselining normal behaviour for the assets;

8.2.4 initiation of learning mode to identify communication paths between the assets;

8.2.5 provision of a report on discovered assets, Vulnerabilities and communications profiles;

8.2.6 if the Customer has selected the Visualise Service, creation of up to ten (10) Customer User accounts as administrator.

8.2.7 if the Customer has selected the Detect Service, creation of up to ten (10) local Customer User accounts as read only.

8.3 Initial Security Platform optimisation and tuning

Following initial asset discovery and visualisation, BT will:

8.3.1 for the Visualise Service, assign a technical implementation manager (TM) to work closely with the Customer nominated trained individuals in order to fine tune the platform.

8.3.2 for the Detect Service, appoint a service optimisation manager (SOM) to work closely with the Customer nominated trained individuals in order to fine tune the platform.

8.3.3 tune the Security Platform to provide platform optimisation.

8.3.4 configure the pre-defined dashboards and reports associated with the Service, in accordance with the details as set out in any applicable Order.

8.3.5 work with the Customer in relation to Customer acceptance testing and approval.

8.3.6 for the Visualise Service, provide handover to the Customer, of the Security Platform into Service. Once the handover is done BT's responsibilities will end.

8.3.7 for the Detect Service, manage the Service in-life as set out in paragraphs 8.4-8.6.

8.4 Monitoring and management

8.4.1 **1st Line analyst response**. BT will provide support from a level 1 Cyber Security Operating Centre ("CySOC") analysts to respond to alerts, real time dashboard information or Threat Intelligence on 24 hours a day, 7 days per week basis. The level 1 analyst will investigate the inputs and initiate the appropriate control action as follows:

(a) the analyst will triage the alert to verify the threat;

(b) if the activity is found to be a false positive, the alert will be discarded;

(c) if the alert requires further investigation, the analyst will create a ticket;

(d) if the alert is deemed of a high severity, the analyst will call/e-mail you to inform the Customer;

(e) the analyst will undertake further analysis to give an initial view of the threat;

(f) the Customer will have the ability to Live-monitor the service via the online console.

8.4.2 **2nd Line analyst investigation and verification.** BT will provide support from a Level 2 CySOC analyst responsible for supporting, monitoring, and troubleshooting efforts as it relates to BT SOC operations working with operational technologies. The level 2 analyst determines if a critical system or data set has been impacted and provide support for new analytic methods for detecting threats.

8.4.3 **Security optimisation manager (SOM).** BT will provide support from a security optimisation manager (SOM) to provide the Customer with cyber support in relation to the Service.

8.4.4 **Notifications of changes.** BT will provide the Customer with notification of changes within the Customer security environment and visibility of any new devices which have been added.

8.4.5 **Management of account user policies and user account access control.** BT will manage account user policies and user account access control on Customer's behalf.

8.4.6 **Detection and notification of anomalous asset behaviours.** BT will notify you of any Security Incidents in accordance with the security incident notification process set out at paragraph 8.6 below.

8.4.7 **Visibility of the assets and new devices on Customer's network.** BT will provide the Customer with read only visibility of the assets and any new devices on the Customer's network.

8.5 Continuous Improvement

8.5.1 **Monthly summary report.** BT will provide the Customer with a monthly Service summary report, focussing on the performance of the Service against any applicable targets and service levels set out in this Schedule. Such reports will be made available to the Customer first by email and then subsequently on the "MyAccount Portal" via the SOM. The MyAccount Portal provides the Customer with a report for each security service the Customer has purchased from BT.

8.5.2 **Quarterly Security Solution Review.** The SOM will carry out a quarterly review of Customer's security configuration to further tune and amend the rules applied to the business environment in order to optimise the Service.

8.5.3 **Ongoing End of Life Review.** BT will provide the Customer with an end-of-life review on an ongoing basis, whereby the SOM will provide a report summarising any forthcoming service replacements or upgrades that may be required to any equipment, applications and/or software for the products within the scope of the Order form that will reach end-of-life status within the following six (6) months. The report will also include notifications of equipment, applications and/or software advised to the Customer previously that are past their end-of-life date and require immediate action by the Customer.

8.5.4 **Supplier software release management.** As Suppliers regularly release new software versions (typically between 2 – 4 times per annum); BT will provide software updates and upgrades, patch fixes, provided that the Customer has a valid Supplier support contract, and the Customer's usage is consistent with any terms and conditions of use provided by the Supplier as set out in the applicable EULA. BT will test and validate the latest Supplier software releases within its reference environment prior to contacting the Customer to raise a change request to deploy the validated software. BT will support the latest major or minor software releases (N, N-1, and N-2) in accordance with any applicable support terms and conditions provided by the Supplier.

8.5.5 **Vulnerability management and patching of BT managed appliances.** BT will identify and apply a secure coordinated process for implementing patches to reduce risk of known Vulnerabilities on the BT managed appliances whereby BT will rank all patch updates as priority ranking in accordance with the Common Vulnerability Scoring System ("CVSS") and aims to have the patches ready for implementation as follows:

CVSS Score	Target notification to the Customer that the patch is available from Supplier, BT has tested the patch and the patch is ready for implementation
0	Discretionary
1 – 3	Discretionary during next Patch cycle (3 – 6 months)
4 – 6	28 days
7 – 10	14 days

Vulnerability management and patching of appliances will only be available while the appliance software version is supported by the Supplier. All communications in respect of Vulnerability and patching of appliances will be through the BT SOM and will follow the security platform service request process set out at paragraph 8.5.6 below.

8.5.6 **Security Platform service request process.** BT will provide the Customer withthe ability to request changes , to respond to Customer's changing business requirements, whilst maximising value and reducing disruption to the Service. The SOM will provide the Customer with a Customer handbook, when the Service goes live, setting out the service request catalogue and how the Customer can submit theserequests. BT will implement changes to the Security Platform in response to Customer's requests, subject to the following process:

(a) the authorised Customer contact will submit requests to change the Security Platform via BT's portal providing sufficient detail and clear instructions as to any changes required;

(b) BT will check each request for its complexity and assess whether the change should be completed via the Security Platform service request process or not;

(c) Only requests for policy configuration changes can be made via this method and will be qualified as either Simple, Standard or Complex service requests. BT will apply the following "reasonable use" restrictions ("**Reasonable Use Policy**") for such changes to the Security Platform:

(i) Simple service requests by the Customer are limited to ten (10) per month. A list of the Simple service requests is set out in Appendix 1 to this Part B. When the Customer issues Simple service requests more frequently than as set out the Parties shall, in good faith, discuss the following remedies:

- Aggregating the request over a period of time, so that they may be implemented more efficiently. In this event there may be some implementation delays;
- Reviewing the requirements and agreeing on a new Order either:
  - an appropriate alternative implementation process and any associated charges for this; or
  - a charge per additional Simple service request.

(ii) Standard service requests by the Customer are chargeable in accordance with rates as agreed on an Order. A list of Standard service requests is set out in Appendix to this Part B.

(iii) Complex service requests are any requests for changes other than a Simple or Standard service request e.g. changes requiring additional hardware and/or licenses. Other examples are set out in the Appendix to this Part B. Complex service requests are subject to a new Order to be agreed between the Parties and agreement on the additional Charges. The Customer will not raise more than two (2) Complex service requests per month.

8.6 Incident Management

8.6.1 Technical incident management

(a) A technical incident means an unplanned interruption to, or a reduction in the quality of, the Service or a particular element of the Service ("**Technical Incident**"). Technical Incidents will be handled by the BT Security Service Desk which is available via telephone 24 hours a day seven days per week and staffed by security trained professionals. All communications with the BT Service Desk will be in English. Only Customer Contacts are allowed to report a Technical Incident to the BT Service Desk.

(b) When the Customer identifies a Technical Incident associated with the BT managed appliances (sensors, Sentries and/or the Management Console) or where BT becomes aware of such a Technical Incident, the BT Service Desk will action the Technical Incident as follows:

(i) BT will give the Customer a Ticket.

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

Priority	Description
P1- High	Total loss of Service. Customer experiences a total loss of Service which cannot be circumvented. Fault affecting multiple Users.
P2– Medium	Service degraded. Customers' Service is partially interrupted or impaired and cannot be circumvented. Fault affecting multiple Users.
P3– Low	Loss of primary service – resilience successful. Low service impact. Medium impact on customer business that can be circumvented. A large % of the customers' business is functioning normally.
P4– Low	No Service impacts. Problem circumvented Little or no business impact on the customer. General requests for information. i.e. Intermittent connectivity problem.

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

(iv) BT will keep the Customer informed throughout the course of the Technical Incident resolution at regular intervals via the BT Service Desk to the Customer Contact however BT will not provide a progress update while BT is waiting on Customer's input or feedback.

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

- The Customer Contact confirms that the Technical Incident is cleared within 24 hours after having been informed; or
- BT has attempted unsuccessfully to contact the Customer Contact and the Customer Contact has not responded within 24 hours following BT's attempt to contact the Customer Contact.

(vi) 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.

(c) BT will aim to provide the Customer with an initial response and a resolution in relation to a Technical Incident in accordance with following table:

Priority	Initial response	Further updates	Resolution time frames
P1	1 hour	Every 4 hours	1 day
P2	6 hours	Every 8 hours	2 days
P3	12 hours	Every 12 hours	3 days

(d) The response times and availability targets shown in the tables above are targets only and BT will have no liability for failure to meet them.

8.6.2 Security Incident Management

(a) A 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"). Security Incidents will be handled by the BT SOC. All communications with the BT SOC will be in English. Only Customer Contacts are allowed to report a security incident to the BT SOC.

(b) Where BT becomes aware of a Security Incident, the BT SOC will action the Security Incident as follows:

(i) The BT SOC will notify the Customer of possible Security Incidents, including details of the relevant underlying issue and Threat Intelligence in accordance with the target response times set out below.

(ii) BT will raise a case for each Security Incident that is notified to the Customer.

(iii) Where a case has been raised by BT in respect of any Security Incident, the BT SOC will contact the Customer nominated customer service teams to:

- advise of any necessary remedial action they need to take; and
- confirm that they have completed any necessary remedial action,
- following which BT will close the Security Incident,

(c) BT will not provide a progress update while BT is waiting on Customer's input or feedback.

(d) BT will aim to provide the Customer with an initial response in relation to a Security Incident in accordance with following table:

Priority	Security Incident Investigation response targets
P1	within 4 hours
P2	within 8 hours
P3	within 24 hours
P4	N/A used to capture other requests

(e) The response times shown in the table above are targets only and BT will have no liability for failure to meet them.

9. CUSTOMER RESPONSIBILITIES

The Customer will be responsible for completing the following actions:

9.1 Preparation

9.1.1 Prior to provision of the Service by BT, the Customer will:

(a) Complete the Service information capture form which includes:

(i) providing BT with the name and contact details of the individuals who would assist and input with the network design;

(ii) listing the number of Customer Sites and their location;

(iii) providing approximate numbers of manufacturing zones and cell areas within the Sites;

(iv) advising BT of any compliance or regulatory framework/data sovereignty requirements;

(v) providing the expected number of nodes (assets) per Site; and

(vi) confirming if the industrial control system/network is air-gapped.

(b) Notify BT of any environmental considerations BT should be aware of e.g., heat, power availability, altitude, humidity, lighting etc.

9.1.2 Remote Connectivity; the Customer will:

(a) for the Visualise Service, confirm the remote network access mechanism e.g., Citrix, will be provided (enabling BT to complete device configuration remotely).

(b) for the Detect Service:

(i) confirm the IP Addresses to be used by BT to establish secure remote access in order to monitor and manage the in-scope appliances;

(ii) outline any proprietary protocols that need to be supported; and

(iii) confirm the physical BT Sentries installation locations.

9.2 Pre-delivery

9.2.1 As soon as practicable, following signature of the Order, the Customer will:

(a) fill in the Customer Enrolment Package form ("CEP").

(b) provide BT with high level design information, which includes:

(i) Copy of customer network diagram;

(ii) Switches and routers make and model;

(iii) Rack positions, rack space and cabinet numbers; and

(iv) Network time protocol source for the Management Console access.

(c) attend a kick-off call to confirm scope of works;

(d) appoint a single point contact / project manager, to work with BT to coordinate deployment activities within Customer's organisation;

(e) A Customer contact per Site to work with BT to undertake the tuning activites within the Customers Site

(f) sign off on the high level design;

(g) provide BT with low level design information which include:

(i) Physical appliances information; being:

- Hostnames (including naming conventions);
- IP Addressing, including domain name system and network time protocol settings;
- Power source and plug type;
- Switches and router configuration e.g., firmware version, average CPU utilisation, bandwidth utilisation, low level monitoring ports and networks to mirror;
- for the Detect Service only, separate rack and power sources for the Management Console;

- for the Detect Service only, BT Sentries' information to include IP addresses, subnet mask, and default gateway.

(ii) Virtual appliances information; being:

- the compute platform/infrastructure on which the virtual deployment is to take place
- Hostnames (including naming conventions;
- IP Addressing, including DNS & NTP settings;
- Performance stats from hypervisor when requested;
- Console access to the Virtual Machine (VM) when required;
- Resolution of hypervisor related incidents.

9.2.2 To enable access to Cloud SaaS (SaaS Management Console, and associated Threat Intelligence) the Customer will:

(a) ensure management servers and/or sensors have reliable network access to Cloud SaaS where applicable; and

(b) manage firewall changes required for on-premises appliances to communicate with Cloud SaaS.

9.2.3 For the Visualise Service only, in order to configure devices remotely, the Customer will provide to BT remote network access mechanism details as follows:

(a) A description of the remote access solution and share Customer's security policy

(b) Remote Access software agent details, if required; and

(c) Remote Access credentials

9.2.4 The Customer will provide to BT the following cabling information:

(a) Provide the necessary cabling and patching cables to complete the installation of the BT managed appliances

(b) Provide media type, speed, and duplex settings

(c) Provide switch name and port numbers used by the BT appliances

(d) Switch location (Room/Rack/RU)

9.2.5 The Customer will assist BT to complete the pre installation survey activity for each Site. This may be by telephone, email, or on-site visit.

9.3 IMPLEMENTATION AND ACCEPTANCE INTO SERVICE (AIS)

9.3.1 Prior to installation the Customer will:

(a) provide BT, and BT's employees, agents, consultants, and subcontractors, with access to sites during Business Hours, or as otherwise agreed, to enable BT to set up, deliver and install the Purchased Equipment; and

(b) provide safe and secure storage of equipment when delivered, before the installation field agent technician arrives to undertake installation.

9.3.2 During installation the Customer will:

(a) show the installation agent field technician where such devices need to be installed;

(b) ensure that there is a method of communication for the installation agent field technician to use when on site i.e., internet, mobile, PSTN;

(c) provide the necessary cabling and patching cables to complete the install;

(d) for virtual appliance installation only:

(i) provide the compute platform/infrastructure on which the virtual deployment is to take place;

(ii) download and run the virtual image provided by BT

(iii) provide BT remote access to the console of the virtual machine for BT to complete the installation; and

(iv) configure switches, routing, and firewall to provide IP level communication between the sensors back to the Management Console.

9.3.3 Following installation the Customer will:

(a) dispose of, or provide suitable storage of, all packaging.

(b) make necessary firewall changes for BT technical teams to communicate with the appliances.

(c) provide BT with a secure remote access mechanism to commission devices and carry out asset discovery, baselining and fine tuning of the customer network.

(d) provide BT with a list of up to ten (10) nominated individuals (name, email, role and telephone) to partake in manufacturer training.

(e) For the Detect Service, provide BT with a list of up to ten (10) nominated individuals to have read only access to the Security Platform (note: with Visualise the Customer will have full access).

(f) allocate the appropriate resource to collaborate with BT with fine tuning of the sensors/network. Typically, this should be an individual per installation Site.

(g) for the Visualise Service only, in order to complete the acceptance into service document; provide BT the details of Customer's Contact responsible for:

(i) monitoring the health of the Security Platform

(ii) receiving Security Platform alerts

(iii) problem and change management process

(iv) admin user/read only on-boarding process i.e., how and who would approve and authorise the user's requirement to access the system.

9.4 IN-LIFE

9.4.1 For the Detect Service only, the Customer will assign named resources to:

(a) receive operational alert tickets and provide response back to BT in a timely manner;

(b) support BT in its investigation activities into security related alerts;

(c) take appropriate action to address issues as recommended by the SOM in respect of the Service including implementing security improvements as agreed with the SOM or as advised by the BT SOM as Customer's responsibility.

(d) ensure that each Customer site has at least one (1) designated representative to assist BT with any investigations and requests for information we may have;

(e) participate and feedback in monthly service reviews; and

(f) support BT with its continuous improvement activities e.g., creation of new detections.

10. APPENDIX 1 - LIST OF SIMPLE AND STANDARD CHANGE REQUESTS

Simple Service Requests

Operational Technology Threat Management provides an allocation of up to ten (10) Simple Service Requests (SSR) per month free of charge.

The SSRs are categorised by duration – up to 30 minutes or up to four (4) hours.

All SSRs defined as 30 minutes or less, will be consolidated into a single service request (8 to 1 ratio). BT will keep a running total of SSRs and will show utilisation within the BT monthly report. Any additional SSRs above the allocated monthly allowance are chargeable.

Simple Service Requests	Duration
GUI – Create SMS alerts	**Up to 30 minutes**
GUI – Create email alerts	**Up to 30 minutes**
Config – Amend email destinations	**Up to 30 minutes**
Accounts – add, modify or remove	**Up to 30 minutes**
Operational process – amend	**Up to 30 minutes**
Update operational baseline	**Up to 30 minutes**
Add asset or communication flow to baseline	**Up to 30 minutes**
Recalegorise asset	**Up to 30 minutes**
Standard Dashboard – enable	**4 hours**
Standard Dashboard – modification	**4 hours**
Assertions – Create / modify	**4 hours**
Create basic playbook	**4 hours**
Run a basic adhoc query	**4 hours**
Receive additional OT platform scheduled report from an existing template	**4 hours**
Additional OT manufacturer scheduled report from an existing template	**4 hours**
Create new ad-hoc report	**4 hours**
Modify existing OT manufacturer custom report	**4 hours**

Standard Service Requests

Each Standard Service Request is chargeable.

A Standard Service Request is more complex that a SSR however it can still be handled by the BT CySOC with support from the BT Technical Manager.

Standard Service Requests	Duration
Create packet capture	**4 hours**
Config – Amend network/segments	**4hours**
Config – Change Auth and Credentials	**5 hours**
OT trusted certificates	**5 hours**

Activate a new monitoring interface	**1 day**
GUI – Create a customised dashboard	**1 day**
Add a new monitoring interface	**1 day**
Change IP ranges	**1 day**
Run a complex custom query	**1 day**
Create advanced playbook	**2 days**

Complex Service Requests

Each Complex Service Request (CSR) is chargeable

A CSR will require careful planning e.g. an architectural change, therefore the change control process should be adhered to and a request will have to be submitted via the BT Security Hub.

Once the Customer has raised the CSR BT will assess the request and may seek further information information prior to providing a formal quote.

Complex Service Requests	Indicative Duration
Add OT licenses	**4 hours**
Change retention levels	**6hours**
Amend backups	**6 hours**
Add a new network	**1 day**
Config – Add new network segments	**1 day**
Firewall integration – add/change	**3 days**
System/Data integration – add/change	**3 days**
OT Appliances configuration change	**Project specific pricing**