BT Managed CySOC Service for Splunk Schedule
Part A – Service Terms

Section A Service Terms

1. SERVICE SUMMARY

1.1 BT's Managed CySOC Service for Splunk supports Customers with threat detection, Incident investigation and reporting through the collection and analysis of data across a variety of sources, which may include Remediation Advice relating to Security Incidents identified via the Splunk SIEM Platform. BT's Managed CySOC Service for Splunk comprises:

1.1.1 the standard components of the Service set out in Part B; and

1.1.2 any optional components described in Part B and set out in any applicable Order,

up to the point of the Service Management Boundary ("**Service**").

1.2 This Part A sets out the specific terms and conditions applicable to the Service, and Part B sets out the service description and the terms relating to how BT manages the Service.

1.3 This Schedule will not apply for the provision of any other services provided by BT (including the Enabling Services) as such services will be governed by their separate terms and conditions.

2. MAINTENANCE, CHANGES AND SUSPENSION TO THE SERVICE

2.1 BT may carry out Planned Maintenance on the components of the Service managed by BT from time to time. BT will inform the Customer at least seven (7) calendar days in advance.

2.2 BT may change the Service provided the performance and quality of the Service is not materially adversely affected. Prior to introducing any change to the Service BT shall provide the Customer with as much notice as is reasonably practicable. Such changes may include:

2.2.1 introducing or removing features of the Service; or

2.2.2 replacing the Service with a materially equivalent Service.

2.3 BT may occasionally suspend the Service in an event of emergency and/or to safeguard the integrity and security of the Service, and/or repair or enhance the performance of the Service. Where possible, BT shall inform the Customer without undue delay in advance. Where it is not possible to inform the Customer in advance of restriction or suspension of any affected Service BT shall explain as soon as is reasonably practicable afterwards why such restriction or suspension was required.

3. GENERAL CUSTOMER OBLIGATIONS

3.1 The Customer will:

3.1.1 provide BT access at the appropriate security level to the Splunk SIEM Platform interface;

3.1.2 be responsible for downloading and deploying the Customer's third-party software responsible for the Splunk SIEM Platform;

3.1.3 ensure that the Customer or third parties, as required, configure routing/permissions on platforms or Enabling Services to allow BT to carry out the provision of the Service;

3.1.4 maintain and monitor the Splunk SIEM Platform;

3.1.5 provide BT with the names and contact details of the relevant Customer Contacts;

3.1.6 without undue delay provide BT with any information or assistance reasonably required by BT to enable it to comply with Applicable Law and perform its obligations with respect to the Service;

3.1.7 undertake all aspects of security policy configuration, including setting up any User groups that may be required on Customer's authentication server which the Customer will reflect in the Customer security policy. The Customer will do this using the Portal/s;

3.1.8 use the Incident reporting procedures notified to the Customer by BT and ensure that the Customer Contact is available for all subsequent Incident management communications;

3.1.9 complete any preparation activities that BT may request to enable the Customer to receive the Service promptly and in accordance with any agreed timescales;

3.1.10 carry out activities required to complete the Controlled Deployment as promptly as possible;

3.1.11 submit any Service Request/s for Custom Rules through the Service Request Management Process before the Operational Service Date;

3.1.12 procure services that are needed to permit the Service to operate, including Enabling Services as defined in Part B, and ensure they meet the minimum technical requirements specified by BT;

3.1.13 where the Customer has provided its own or a third-party Enabling Service, ensure and confirm to BT that the Enabling Service is working correctly before reporting Incidents to BT;

3.1.14 inform BT of any planned maintenance on any third party provided Enabling Service;

3.1.15 provide service assurance support to BT, where reasonably requested, to progress the resolution of Incidents for any BT Service installed on an Enabling Service that is not being provided by BT;

3.1.16 in jurisdictions where an employer is legally required to make a disclosure to its Users and employees in relation to the Service:

(a) inform Users (individually or via local workers councils depending on Applicable Law) that as part of the Service being delivered by BT, BT may monitor and report the use of any targeted applications;

(b) ensure that Users have consented or are deemed to have consented to such monitoring and reporting (where such consent is legally required);

3.1.17 share with BT any relevant internal processes or policies that may affect delivery of the Service, and operations, and BT will advise where these are not compatible with the Service;

3.1.18 make available to BT sufficient resources to facilitate ordering, design, and implementation of the Service;

3.1.19 ensure the Customer's system configurations and network settings allow the traffic types necessary for BT to provide the Service;

3.1.20 work with BT to ensure that the Splunk SIEM Platform is set up and live in readiness before Service onboarding activities can commence;

3.1.21 where applicable, be responsible for deployment of the Service on Users' Devices and the configuration and management of all settings relevant to the Service;

3.1.22 provide consent to;

(a) BT to use, reproduce, store, modify, and display the information from the Customer Logs for the purpose of providing the Service;

(b) BT to use any information obtained regarding malware, spam, botnets or other information related to the Service for the purpose of:

(i) maintaining and improving the Service;

(ii) complying with all legal or contractual requirements;

(iii) making malicious or unwanted content anonymously available to its licensors for the purpose of further developing and enhancing the Service;

(iv) anonymously aggregating and statistically analysing the content; and

(v) other uses related to the analysis of the Service;

(c) BT to use or act upon any suggestions, ideas, enhancement requests, feedback, recommendations or other information provided by the Customer relating to the Service, to the extent it is not Customer's confidential information;

(d) BT to apply signature updates automatically on components managed by BT;

(e) BT personnel to access the Portal/s set up for the Customer for the purposes of providing the managed service, e.g. implementing Service Requests. If access is not provided or removed, service targets for the managed service will not apply; and

(f) BT to have sole access for the necessary administrator credentials or privileged account where required for configuring applications e.g Standard Default Rule or Custom Rule maintenance.

3.1.23 be responsible for establishing communication between the Customer's internal helpdesk and its Users;

3.1.24 ensure that any Incident notifications include all relevant and available information at the time of reporting to BT;

3.1.25 be responsible for maintaining back-up configurations to allow all the Enabling Services to be restored following a swap of equipment forming part of the Enabling Services; and

3.1.26 As the Customer is deemed to have approved all changes to the Customer security policies that are submitted to BT, BT shall not be liable for any disruption or loss to the Customer's business as a consequence of any misspecification by the Customer's security requirements implemented by BT.

4. CUSTOMER EQUIPMENT

4.1 The Customer will:

4.1.1 provide BT with any information reasonably required without undue delay, and the Customer will ensure that the information is accurate and complete;

4.1.2 monitor and maintain any Customer Devices used in connection with the Service;

4.1.3 ensure that any Customer Devices that the Customer uses, directly or indirectly, in relation to the Service:

(a) are technically compatible with the Service; and

(b) are 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.

4.2 The Customer agrees that BT will not be liable for any failure by the Customer to comply with this Paragraph 4 and the Customer will be liable to BT for any claims, losses, costs or liabilities incurred or suffered by BT due to the Customer's failure to comply with this Paragraph 4.

5. PASSWORDS, AUTHORISED USERS AND SECURITY

5.1 Obligations applicable to any User.

5.1.1 The Customer is responsible for the proper use of any usernames, personal identification numbers and passwords or similar used in conjunction with the Service, and the Customer will take all necessary precautions to ensure that the foregoing are kept confidential, secure and not made available to unauthorised persons.

5.1.2 The Customer will distribute, manage and maintain access profiles, passwords and other systems administration information relating to the control of Users' access to the Service.

5.1.3 The Customer will promptly terminate access of any person who is no longer an authorised User.

5.1.4 The Customer will promptly inform BT 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.

5.1.5 The Customer will change any or all passwords or other systems administration information used in connection with the Service if BT asks Customer to do so in order to help safeguard ensure the security or integrity of the Service.

5.1.6 The Customer will not allow any specific User license to be used by more than one User unless it has been reassigned in its entirety to another User.

5.2 Obligations applicable to Administrator(s).

5.2.1 BT will provide the Customer Administrator access rights to the Portal/s as set out in Part B. The Customer must:

(a) not remove or alter the Administrator account without BT's prior consent;

(b) avoid unauthorised access to the Administrator account;

(c) keep the Administrator account password secure, change the password if the employee who has access to the Administrator account leaves the business, changes role and/or no longer requires access;

(d) pay all remedial costs if there is an Incident which is a direct result of authorised or unauthorised access to the Administrator account and BT is requested to restore Service to the prior configuration;

(e) where the Customer allows multiple Administrators to access the Portal/s, give each of the Administrators a unique login and provide management access or read only privileges specific to each of them and inform any additional Administrator Users of their responsibilities set out in this Schedule;

(f) keep personnel access to the Administrator account up to date; and

(g) keep records of any changes and make these available to BT where required.

5.2.2 If the Customer fails to comply with Paragraph 5.2.1, BT reserves the right to remove the Customer's administration rights.

6. IP ADDRESSES, DOMAIN NAMES

6.1 Except for IP Addresses expressly registered in the Customer's name, all IP Addresses and Domain Names made available by BT with the Service will at all times remain BT's ownership or the ownership of BT's suppliers and are non-transferable.

6.2 All the Customer's rights to use BT IP Addresses or Domain Names will cease on termination or expiration of the Service.

6.3 The Customer warrants that they are the owner of, or are authorised by the owner of, the trademark or name that the Customer wishes to use as Customer's Domain Name.

6.4 The Customer will pay all fees associated with registration and maintenance of the Customer's Domain Name and will reimburse BT for any and all fees that BT pays to any applicable Regional Internet Registry, and thereafter pay such fees directly to the applicable Regional Internet Registry.

7. CUSTOMER LOGS

7.1 The Customer will configure the Splunk SIEM Platform to receive Customer Logs to parse data correctly.

7.2 The Customer will confirm to BT any change in the number of Customer Logs used in connection with the Service.

7.3 BT will not be liable for any failure of the Service due to Customer Logs not being received by the Customer Equipment/Splunk SIEM Platform.

7.4 BT will only undertake threat correlation or threat monitoring from agreed Customer Logs.

8. UPGRADES

8.1 BT may from time to time upgrade any software or firmware used to deliver the Service to ensure that BT remains within the Supplier's supported software specification. The dates and times of any software or firmware upgrades will be notified to the Customer in advance if, in the view of BT, it affects the Service.

8.2 The Customer will confirm to BT any change in the number of Devices or Customer Logs the Customer is adding to the Service.

8.3 The Customer will notify BT of any planned upgrades to the Splunk SIEM Platform.

8.4 The Customer will notify BT of any changes to the Splunk SIEM Platform that may impact the Service.

9. CAPACITY MANAGEMENT

9.1 The Customer is responsible for ensuring that the Splunk SIEM Platform meets the required specifications to ensure sufficient capacity to provide the Service.

9.2 If BT identifies that changes in usage volumes could result in the Service being unable to process the data effectively, or BT identifies that usage volumes are higher than those set out in the Order, BT will contact the Customer to discuss any recommended changes to the Customer Logs, or change in Charges, as a result of the Customer's increased usage.

9.3 If the Customer does not agree to make changes to the Customer Logs following advice from BT in accordance with Paragraph 9.2, BT will not be liable for any performance issues of the Splunk SIEM Platform and Service.

10. SUGGESTIONS, IDEAS AND FEEDBACK

10.1 The Customer agrees that BT will have the right to use or act upon any suggestions, ideas, enhancement requests, feedback, recommendations or other information provided by the Customer relating to the Service, to the extent it is not Customer's confidential information.

Section B Acceptable Use Policy

11. INTRODUCTION

11.1 The Customer acknowledges that it has read and agrees to be bound by and to ensure that any Users will comply with this Section B ("**Acceptable Use Policy**" or "**AUP**").

12. USE OF THE SERVICE

12.1 The Customer will not use the Service in breach of Applicable Law or in any way that is considered to be:

12.1.1 detrimental to any person or in a manner which violates or otherwise encroaches on the rights of others (including rights of privacy and free expression); and

12.1.2 detrimental to the provision of services to the Customer or any other BT customer.

12.2 The Customer will not use the Service to intentionally take, or attempt to take, any action that could:

12.2.1 transfer files that are, contain or are made up of viruses, worms, Trojans, distributed denial of service, any back door or time-bomb or other harmful programmes or software designed to violate the security of BT, any other person or company; or

12.2.2 prevent, block or obstruct access to any programme installed on, or data saved in, any computer or damage or harm the operation of any of these programmes or the reliability or accuracy of any of this data.

13. USE OF MATERIALS

13.1 The Customer will not create, amend, download, receive, store, send, publish, transmit, upload or otherwise distribute any material, including information, pictures, music, video or data, that is considered to be:

13.1.1 harmful, immoral, improper, indecent, defamatory, offensive, abusive, discriminatory, threatening, harassing or menacing;

13.1.2 promoting or encouraging of illegal, socially unacceptable or irresponsible behavior, or that may be otherwise harmful to any person or animal;

13.1.3 in breach of the intellectual property rights of BT or any other company or person, for example by using, distributing or copying protected or 'pirated' material without the express permission of the owner;

13.1.4 in breach of the privacy or data protection rights of BT or any other person or company; or

13.1.5 in contravention of any license, code of practice, instructions or guidelines issued by a regulatory authority.

13.2 The Customer will ensure that all material that is derived from the machines or networks that it uses in connection with the Service is not in breach of this AUP.

14. SYSTEMS AND SECURITY

14.1 The Customer will not:

14.1.1 take any action that could:

(a) damage, interfere with, weaken, destroy, disrupt, harm, violate, disable, overburden, overtake, compromise, hack into or otherwise adversely affect any computer system, network or the internet access of the BT Network or network of any other person or company; or

(b) adversely affect or tamper with BT's security, the BT Network or any system or security network that belongs to any other person or company.

14.1.2 access any computer system or network belonging to any person or company for any purpose without permission, including to probe, scan or test the security of a computer system or network or to monitor data traffic;

14.1.3 connect the BT Network to machines, equipment or services that do not have adequate security protection or that are able to be used by others to carry out conduct that is not allowed by this AUP; or

14.1.4 collect, take or harvest any information or data from any BT services, BT's system or network or attempt to undermine any of BT's servers or systems that run BT services.

Section C Compliance and Regulation

15. EXPORT OF CONTENT USING CLOUD SERVICES

15.1 The Service comprises of a cloud service that utilises software and technology that may be subject to export control laws of various countries. The Customer is solely responsible for any compliance related to the way the Customer uses the Service and the location the Service is used including access by Users to the Service and for the Customer's Content transferred or processed using the Service, including any publication of such Content.

Section D Charges, Subscription Term and Termination

16. CHARGES

16.1 The Customer will pay the Charges for the Service and any optional features (including upgrades and re-configuration) as specified in the Order; including but not limited to:

16.1.1 Charges per element re-configured after the Operational Service Date must be agreed and documented in a new Order;

16.1.2 Charges for Service Requests that are outside of the Customer's quarterly allowance;

16.1.3 Charges for professional services;

16.1.1 Charges if work cannot be undertaken remotely and requires BT to attend the Site(s);

16.1.1 Charges for additional Custom Rules that are not covered by the existing BT Standard Default Rule Set; and

16.1.2 Charges if the Controlled Deployment Period is extended for any reason beyond 90 days after receiving Notice from BT in accordance with Part B.

16.2 In addition to the Charges set out in the Order, the Customer may be liable for the following additional Charges:

16.2.1 Charges for (de-)commissioning the Service outside of Business Hours;

16.2.2 Charges for expediting provision of the Service at Customer's request after BT has informed Customer of the delivery date;

16.2.3 Charges for investigating Customer reported Incidents where BT finds no Incident or that the Incident is outside the Service Management Boundary;

16.2.4 Charges for restoring Service if the Service has been suspended by BT in accordance with the terms of the Governing Agreement.

16.3 For any period where the Service is provided for less than one month, the full monthly charge will be applied.

16.4 Usage Volume Reasonable Use Policy

16.4.1 Where the Customer's use of the Service exceeds the agreed GB/day volumes set out in the Order, BT may increase the Subscription Charges to reflect the increase in usage volumes (as determined by the average usage volume in GB/day measured over a consecutive three-month period) by placing the Customer in the next Monthly Usage Volume Band increment, in accordance with Paragraph 9.2.

16.4.2 BT will notify the Customer at least one month in advance before any changes to the Charges are applied in relation to Paragraph 16.4.1. Any such changes will be documented in a Supplemental Order.

17. TERM, TERMINATION AND RENEWAL

17.1 The Order sets out any Subscription Term (also called "**Minimum Period of Service**") applicable to the Service, as well as any associated volume commitments, invoicing terms and the termination Charges that are specific to the Service.

17.2 Unless otherwise agreed to the contrary, following the expiration of the Subscription Term, the Service shall continue unless and until terminated in accordance with the terms of the Governing Agreement referenced in the Order.

18. END OF SERVICE

18.1 On termination of the Service, the Customer will:

18.1.1 retrieve all Customer data from the Service;

18.1.2 provide BT with all assistance necessary to remotely decommission all applications supporting the Service; and

18.1.3 remove all Software associated with the Service for Customer's Devices used in connection with the Service.

18.2 on termination of the Service, BT will:

18.2.1 terminate Customer's access to the Portal/s, the Service and cease to provide all other elements of the Service; and

18.2.2 where permitted under applicable mandatory law, delete any other Content, including any configuration data relating to BT's management of the Service. This will be done fifteen working days after termination of the Service.

Section E Service Levels and Service Credits

There are no Service levels with Service credits available for this Service. BT will provide Service targets as set out in Part B.

Section F Data Protection

This section supplements the data provisions that may be set out in the Governing Agreement:

19. DURATION OF THE PROCESSING OF PERSONAL DATA

19.1 BT or its Sub-Processor will Process the Customer Personal Data for the Service for as long as BT provides the Service and for as long as BT may be required to Process the Customer Personal Data in accordance with Applicable Laws.

20. THE NATURE AND PURPOSE OF THE PROCESSING OF PERSONAL DATA

20.1 The nature and purpose of the Processing of Customer Personal Data by BT includes:

20.1.1 BT monitors Customer Log data generated by the Customer's network, security or IT systems that is then forwarded to the BT SOAR platform for processing and analysis. Data is then deposited into a secure data centre which is fully hosted within the UK and used to create Customer reports.

20.1.2 The Customer is responsible for any data sent in the Customer Logs to the Splunk SIEM Platform.

21. TYPES OF PERSONAL DATA AND CATEGORIES OF DATA SUBJECTS

21.1 The types of Customer Personal Data Processed by BT or its Sub-Processors or the Customer may include:

21.1.1 Name;

21.1.2 Email address;

21.1.3 Employee ID;

21.1.4 Company name;

21.1.5 IP Address;

21.1.6 Network or device location; and

21.1.7 System logs.

This list is not exhaustive as the Customer will specify what Customer Personal Data is Processed.

21.2 The Customer Personal Data will concern the following categories of Data Subjects:

21.2.1 Customer's end users; and

21.2.2 Customer's employees and other third parties of the Customer; and

21.2.3 Any Data Subject as controlled by the Customer.

This list is not exhaustive as the Customer as Controller will specify any other categories of Data Subjects.

Section G Defined Terms and Abbreviations

For the purposes of this Schedule defined terms and abbreviations shall have the meaning ascribed to them within the body of the Schedule or below:

"**Acceptable Use Policy**" means the policy as set out at Part A, Section C.

"**Acceptance Tests**" means those objective tests conducted by the Customer that when passed confirm that the Customer has accepted the Service and that the Service is ready for use save for any minor non-conformities that will be resolved as an Incident.

"**Administrator**" means the person(s) authorised by the Customer who is responsible for managing the Service using the Portal/s.

"**Alerting Incident**" means a Security Incident created by the Service as a result of a Standard Default Rule or Custom Rule meeting its alerting threshold.

"Applicable Laws" means the laws as set out in the Governing Agreement as may be amended from time to time.

"**BT Network**" means the communications network of BT.

"**Business Day**" means generally accepted working days at the locality of the Site, excluding any national or bank holidays.

"**Business Hours**" means between the hours of 0900 and 1700 in a Business Day at the locality of the specific Site.

"**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 Service.

"**Charges**" means the fees and charges payable by the Customer in relation to a Service as set out in the Order.

"**Complex Service Request**" or "**CSR**" is a chargeable Service Request which does not fall within the Simple Service Request category.

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

"**Controlled Deployment**" means the controlled deployment phase of the Service.

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

"**Controller**" shall have the meaning given to it in the GDPR.

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

"**Customer Contact**" means any individuals authorised to act on the Customer's behalf for Service management matters.

"**Custom Rule**" means bespoke Correlation Rules, specific to the Customer's requirements and individual deployment, that are created in the Service.

"**Custom Rule Allowance**" means the Customer's standard allowance of Custom Rules set out in Part B.

"Customer Commited Date" means the date provided by BT on which delivery of the Service is due to start.

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

"**Customer Personal Data**" means any Personal Data Processed as a Processor by BT in the context of providing the Services under this Governing Agreement.

"**Customer Logs**" means, the log sources (parsed) being sent to the Splunk SIEM Platform by the Customer for use of the Service.

"**CySOC"** means BT's cyber security operations center, where BT's team of security analysts and specialists use various security technologies to monitor Security Incidents as part of the Service provided to the Customer.

"**Data Subjects**" shall have the meaning given to it in the GDPR.

"**Device**" means any equipment, including but not limited to log forwarding devices, laptops and servers, used by the Customer or the Customer's employees to provide or gain an access to Customer's applications, systems and platforms.

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

"**Enabling Services**" means the services as defined in Part B – Service Description.

"**Event**" means an event that is generated by the Customer's network, security or IT systems that is then forwarded to BT SOAR for processing and analysis.

"GDPR" means the General Data Protection Regulation (EU) 2016/679 ("EU GDPR") and any amendment or replacement to it, (including any corresponding or equivalent national law or regulation that implements the GDPR as applicable to the Processing).

"**Governing Agreement**" means the general terms and conditions which govern this Schedule.

"**Indicators of Compromise**" or "**IOCs**" are pieces of forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network.

"**Incident**" means either a Technical or a Security Incident.

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

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

"**Remediation Advice**" means a recommended mitigating action which should be taken by the Customer to address the impact of IOCs identified by BT.

"**Operational Service Date**" means the date upon which the Service is made operationally available to the Customer and may be called the "Service Start Date" in some Governing Agreements.

"**Order**" means means an Order that accompanies a Service Schedule for a new Service and contains the Parties agreement on Charges and any other relevant commercial information related to the Service referred to in the Order.

"**Personal Data**" shall have the meaning given to it in the GDPR.

"**Planned Maintenance**" means scheduled maintenance that is planned 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.

"**Processing**" and "**Processor**" shall have the meaning given to it in the GDPR.

"**Portal**" means the online user interfaces used by the BT and/or the Customer to manage the Service in-life, as set out in Part B.

"**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.

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

"**Service Request**" means a request from the Customer to make a change to the Service, including but not limited to a Simple Service Request or Complex Service Request.

"**Simple Service Request**" or "**SSR**" is a non-chargeable Service Request within the Customer's quarterly allowance as set out in Part B.

"**SOAR**" means Security Orchestration Automation and Remediation.

"**Splunk SIEM Platform**" means the Customer's security information and event management platform.

"**Standard Default Rule**" or "**Standard Default Rule Set**" means a set of rules which BT can apply to the Customer's Service to assist with monitoring by BT and indentification of Alerting Incidents, as set out in Part B - Service Description.

"**Sub-Processor**" means a BT Affiliate or BT's supplier or subcontractor that BT engages to Process Customer Personal Data for the purposes of this Governing Agreement.

"**Subscription Term**" means the term contracted for this Service as set out in the Order. In some Governing Agreements this may also be called "Minimum Period of Service".

"**Supplier**" means Splunk Inc., who are responsible for providing the Customer's Splunk SIEM Platform.

"**Technical Incident**" means either any unplanned interruption to, or a reduction in the quality of, the Service or a Service component.

"Threat Analytics Manager" or **"TAM"** means the the BT person which provides support to the Customer for any in-life service management aspects as set out in Part B.

"**Ticket**" means the unique reference number provided by BT for a Technical Incident raised by the Customer.

"**Urgent Custom Rule(s)**" means in respect of Custom Rules 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.

"**User**" means any person who is permitted by the Customer to use or access a Service.

"**Usage Volume**" means the agreed Events Per Second usage volume as set out in the Order and calculated on the Customer's average monthly usage.

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