BT Security Threat Services – Annex to the General Service Schedule

BT Reference No. **-**** -*****

1. DEFINITIONS

The following definitions apply, in addition to those in the General Terms and Conditions and the General Services Schedule of the Agreement.

"SLM Appliance" means a combination of hardware and software owned and managed by BT that is used to deliver the SLM service.

"**STM SIEM**" means the BT event tracking, correlation, and problem ticket management system, which consists of a number of tools and technologies used by BT's security analysts.

"**CEP**" means Customer Enrolment Package, a document in which the Customer records the configuration information required for delivery of the Service.

"**LEA**" means Log Export API.

"**Log Source**" means a network connected device, operating system, database or other asset capable of generating log messages configured by the Customer to send logs to the SLM Appliance.

"**Messages**" means an alert sent from a Sensor to a Sentry, or a log message sent from a Log Source to a SLM Appliance or an accept/deny notification from a firewall.

"**OOB**" means out-of-band management and involves the use of a dedicated management channel for device maintenance. It allows a system administrator to monitor and manage a device by remote control regardless of whether the machine is powered on, or if an operating system is installed or functional.

"**Sensor**" means a device, operating system, database or other software or hardware that the Customer owns or licenses that can generate log data and is configured by the Customer to send messages to the Sentry.

"**Sentry**" means a passive data receiver owned and used by BT to provide the Services.

"**SMTP**" means Simple Mail Transfer Protocol and is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

"**SOC**" means the BT Security Operations Centre and/or STM SIEM.

"**Syslog**" means a standard for computer message logging.

"**Virtual Sentry**" means a BT proprietary virtual device to be hosted on a customer's VMware server. The Virtual Sentry performs the same functionality as the hardware sentry. The Virtual Sentry will be downloaded, installed and initially configured by the Customer.

2. SERVICE OVERVIEW

BT Security Threat Services provide the Customer with a comprehensive view of network security activity and a defence against malicious attacks. The BT Security Threat Services include the following services:

2.1 BT Security Threat Monitoring (STM)

2.1.1 STM is used to monitor security and non-security devices (Sensors). BT will provide one or more hardware or virtual Sentries at a Site(s) to monitor log data from all the Sensors listed in the Order. The Sensor must be one listed in the "BT Supported Device List", a copy of which BT will provide to the Customer upon

request. The Sentry configuration will be determined based on the Customer provided information in the CEP.

(a) For external cloud and virtual environments, BT will provide a Sentry image specific to the cloud service provider. Customer will provision a virtual instance and install the image, and configure connectivity to BT SOC. BT is responsible for all additional hardening, monitoring, and maintenance of that virtual appliance. Not all cloud providers are supported.

2.1.2 An option is available to the Customers to retain threat monitoring data within the European Union borders instead of data being collected and stored in the US SOC location. This option is referred to as "EU Data Dominion". For this option BT will evaluate the Customer requirements and if BT is able to meet the Customer requirements for the EU Data Dominion option, BT will agree in writing the scope of the Customer data that is restricted to the European Union.

2.1.3 The log data is used to monitor events such as access violations and policy violations on the devices. If the devices cannot forward log information in passive mode by using Syslog, SMTP or other passive/active modes, the Customer must load an agent-based log forwarder on to the Sensor.

2.1.4 Event rules are deployed by BT to enable real time threat detection through analysis of the log messages received. The event rules used depend on the device type(s) and product versions.

2.1.5 All messages from the Sentry are sent automatically to BT STM SIEM service which categorizes and prioritizes events, weeds out false positives, stores the data for future audit (as described below in this Annex), and presents information about critical tickets to the security analysts for review.

2.1.6 BT will provide 24x7x365 real time event response, in accordance with alert guidelines and the escalation and notification contact tree agreed by the parties, and based upon information provided by the Customer in the CEP. Customer may request changes and updates to the escalation and notification contact tree from time to time.

2.1.7 The Sentry will be capable of automatic fail-over to an alternative SOC if there is a fault in the primary SOC.

2.1.8 If the SOC detects a hardware failure in a BT-supplied Sentry, BT will order the part and coordinate its install it when it has arrived at the Site.

2.1.9 If a Virtual Sentry fails due to a problem with the Virtual Sentry image, BT will provide access to an updated image that the Customer will need to download and install on its virtual machine server. If a Virtual Sentry fails due to a hardware or OS issue, the Customer will be responsible for correcting the issue.

2.1.10 BT will give the Customer access to a portal where the Customer can access service information such as reporting and sensor information.

2.1.11 BT will retain the Customer's Messages that are transmitted to BT's SOCs as follows:

(a) 30 days of detailed information will be retained on-line in STM SIEM and the portal;

(b) Six (6) months of weekly reports will be retained on-line in the portal;

(c) One (1) year of online storage for monthly reports.

2.1.12 BT will provide Customer with both weekly event summaries and monthly CIO reports via the portal. Customer may configure automatic delivery of reports via email to designated recipients.

2.1.13 Following termination of Service, BT may continue to store the Customer's security log data in its data backup complex and BT will continue to protect such data at the same levels as existing customers. BT will use approved commercial services to destroy storage media at BT determined intervals or upon media failure.

2.2 BT Security Vulnerability Scanning (SVS)

2.2.1 The SVS service enables management of Customer IP scans which can be scheduled weekly, monthly, quarterly or on-demand. Where agreed in the Order, BT will provide the following optional service components:

(a) Security Internal Vulnerability Scanning which scans the Customer's network assets using Scanner Appliance(s) and cross-references the data compiled during a scan against a continuously up-to-date inventory of network assets. BT will provide Scanner Appliance(s) that will scan the Customer's network as scheduled. BT will ship Scanner Appliance(s) to the Customer for installation by the Customer.

(b) Security External Vulnerability Scanning which scans the Customer's IT environment from the public Internet and cross-references the data compiled during a scan against a continuously up-to-date inventory of network assets and the current state of operation.

(c) Security Vulnerability Scanning Payment Card Industry (PCI) Compliance add-on to Security Internal Vulnerability Scanning and/or Security External Vulnerability Scanning in which BT will perform, once every three (3) Months, two scans of the same target networks: an initial Pre-Compliance Scan to confirm the list of target IP addresses and identify any vulnerabilities requiring remediation, and, following a remediation period of up to seven (7) days, a PCI Compliance Scan of the target IPs identified during the preceding Discovery Scan. BT will provide the Customer with a PCI Scan Report, normally within three (3) Business Days of the scan to enable the Customer to take remedial actions to fix any identified vulnerabilities.

2.2.2 BT does not make any warranty that SVS will be error-free, free from interruption or failure, or secure from unauthorized access, or that it will detect every vulnerability in the Customer's network, or that the results generated by SVS will be error-free, accurate, or complete. SVS may become unavailable due to any number of factors including scheduled or unscheduled maintenance, technical failure of the software, telecommunications infrastructure, or the Internet.

2.2.3 Customer reporting information is stored and available via a portal. PCI scan reports and related information will be stored for a period of two (2) years from the date of scanning.

2.2.4 BT reserves the right to restrict the number of scans to no more than one per week.

2.3 BT Security Device Management (SDM)

2.3.1 BT will provide Security Device Management Services, by remotely managing the Customer's systems in the form of software or appliance(s) provided by a 3rd party equipment manufacturer or software

provider ("vendor") and owned by the Customer (or to which the Customer has license rights granted) or software or appliance(s) provided by BT and owned by BT.

2.3.2 For the other options, the Customer is responsible for providing the equipment, obtaining product/equipment support and maintenance and management of its suppliers, including event and dispatch management.

2.3.3 BT will review each managed device configuration before taking management responsibility and will provide best practice recommendations. In order to complete the review, the Customer must provide BT with remote access to the device with authority rights to retrieve the device configuration.

2.3.4 BT will provide, as necessary,

(a) maintenance updates to the Managed Device applications and underlying operating systems, and OS updates for appliance-type Devices. These include the installation and tuning of any signature updates, Managed Device application patches, and alerting configuration, within the administrative boundaries defined by the Managed Device application vendor's own management console interface. For the avoidance of doubt, this does not include comprehensive OS upgrades (such as from Windows XP to Windows 7).

(b) for administrative changes, maintenance updates and system upgrades to the Managed IPS, BT can release signatures in active mode, but recommends that all new signatures and automated event analysis blocking capability be deployed in passive mode for a period of time to test the effectiveness within the Customer's environment.

(c) additions, deletions, and modifications of rules, administrative changes, maintenance updates and system upgrades to the Managed Firewalls.

2.3.5 BT will make any changes it considers necessary to the Managed Devices to maintain the security of the Customer's environment and configuration changes to the Managed Devices to protect the Customer's network. These changes do NOT include any Customer requested changes, vendor changes, or changes needed due to business changes of the Customer. BT will inform the Customer via email or phone, and via periodic reports, of the changes it has made.

2.3.6 BT will respond to any Customer requested changes, which must be made in writing via email, as below. On validation of change requests, BT will schedule changes with the Customer, and coordinate with the Customer to implement the changes. BT will provide:

(a) Up to five (5) changes per Month per Managed Device for Pattern changes and tuning (each change can include up to ten (10) configuration changes). Tuning changes are defined as "Modifying conditions under which an existing signature will generate an outbound alert from the IDS" such as changing included or excluded source/destination networks.

(b) Up to five (5) changes per Month. In most cases, BT will schedule changes with the Customer to occur within 24 hours of request, or at a predetermined date requested by Customer. Complex changes may require more preparation time. A change is defined as "Any modification of allowable ports and/or protocols, on either ingress or egress filtering, to add, delete, or change traffic flow through the IPS between any two points on either side of the interface such

as changing a web server object to allow inbound and outbound tcp/443 traffic in addition to existing tcp/80 traffic."

(c) The Service supports devices with up to 50 discrete policy rules defined on a single IPS. Network segment changes, defined as "Adding, changing, or deleting objects connected to the IPS' network segment interface", are supported by the service, with up to five (5) such changes allowed during any Month. BT will support up to two (2) expedited changes in which BT will schedule changes with Customer to occur within four (4) hours of request, or later as defined by Customer. In no case will BT support a number of discrete policy rules per IPS or Firewall in excess of the manufacturer's recommended limit for any installation, taking into account vendor make and model, amount of traffic throughput on the device, and any other specifics which may arise as a result of existing rules or policies which are unusually complex or CPU-intensive for the device to process.

(d) BT will provide written guidance to the Customer if a requested change falls outside these parameters, with a recommendation either to upgrade the device to one more capable, or to revise the existing rules to keep under the recommended ceiling.

2.3.7 For the avoidance of doubt, any unused changes cannot be carried over from one Month to the next.

2.3.8 BT will contact the Customer if the Managed Device hardware is suspected to have failed or needs physical maintenance.

2.4 BT Security Log Management (SLM)

2.4.1 The SLM Service collects logs from all supported connected data sources, including networking, servers and applications. The SLM Service allows access to compliance reporting and to all collected enterprise log data.

2.4.2 SLM Appliances are provided, owned and managed by BT.

2.4.3 BT will provide the following information to the Customer as part of the SLM service:

(a) Log Collection. Log data will be collected from Syslog, SNMP and LEA for Checkpoint log sources.

(b) Real-Time Reporting. Log data will be normalised from a variety of log source devices. The Customer will be able to run reports and build searches on the normalised log data.

(c) Monitoring and Alerting. BT will provide health monitoring of the SLM Appliances and service.

(d) SLM Appliance Management. BT will provide, as necessary, administrative changes, maintenance updates and OS upgrades to the SLM Appliances.

2.4.4 BT shall work with the Customer to establish the baseline SLM configuration prior to implementation of the Security Log Retention service.

2.4.5 BT will contact the Customer if the SLM Appliances under management are suspected to have failed or if they need physical maintenance.

2.4.6 BT will provide 24x7x365 management of SLM Appliances.

2.4.7 Only BT shall have administrative access to the SLM Appliances.

2.4.8 BT will provide storage capacity up to the limits set out in the Order.

3. SERVICE DELIVERY

3.1 BT will remotely configure any Equipment used in the supply of Services and following installation of Equipment by BT, except for equipment associated with the SVS service, conduct a set of standard tests to ensure that the configuration at a Site is functioning correctly.

3.2 The Operational Service Date (OSD) for a Site occurs as follows:

(a) STM - when the Sentry or Virtual Sentry, as applicable, is installed and configured allowing remote connectivity by the BT SOC.

(b) SDM - when the MIDS device is installed and configured allowing remote connectivity by the BT SOC. A Sentry install is also required for monitoring. For third party IDS, IPS, or Firewall, when the BT SOC has remote connectivity and management access to the device.

(c) SLM - when the SLM Appliance is installed and configured allowing remote connectivity by the BT SOC.

(d) SVS - when the Customer is provisioned by the BT SOC in the Qualys system.

3.3 BT will provide IP address range(s) of the gateways at the BT SOC that will be supporting the Customer.

4. BT SERVICE MANAGEMENT BOUNDARY (SMB)

4.1 For Sensors not managed by BT, the Customer will be responsible for configuring the devices to transmit messages to the Sentry(s) and work with BT to reconfigure and tune the devices to reduce the generation of false positives from the Customer's infrastructure.

4.2 For Sensors monitored and managed by BT, the Customer will be responsible for enabling remote connectivity and management access to the devices by the BT SOC.

4.3 If out of band (**"OOB"**) access is required, BT will provide Secure OOB devices which will be connected to a Customer provided analogue telephone line which terminates directly from the telephone service provider to the modem. This line shall not transit the Customer's PBX, and shall not be used other than to call BT. The Customer is responsible for all call charges. OOB management is only supported with third party managed devices.

4.4 For Virtual Sentry, the Customer will be responsible for the underlying equipment, the Operating System, and the Virtual Machine environment. BTs responsibility is for the Virtual Sentry image supplied as an **OVF** package and its Sentry functionality.

5. THE CUSTOMER'S RESPONSIBILITIES

5.1 The Customer acknowledges and agrees that BT will not start its delivery processes until BT has received the completed CEP.

5.2 The Customer will promptly notify BT in writing of changes to information contained in the CEP.

5.3 The Customer shall not use the Services to monitor a third party's network or any devices or applications not expressly chosen by the Customer for its internal business purposes to be active on the Customer's network. Any exception to this must be agreed to by BT.

5.4 The Customer is responsible for ensuring that its monitored devices are sending log files to the BT Sentry device. If a period of tuning is required, the Customer acknowledges and agrees that BT will charge from the OSD as defined in section 3.

5.5 The Customer understands that it is ordering the Service for its network as currently assessed. Any Customer requested changes that require platform upgrades may result in limitations of the Service. The Customer may have the option to order upgrades to rectify this.

5.6 STM, SLM, SDM

5.6.1 The Customer is responsible for providing KVM (keyboard, video, mouse) for any on-site maintenance or support of supplied CPE. If KVM is not available at the time of the site visit, it will be treated as an aborted site visit and the Customer will be responsible for all reasonably incurred costs.

5.6.2 On termination of the Service, the Customer shall return BT owned Equipment from its Site(s) at Customer's expense.

5.6.3 The Customer is responsible for de-installation of scanners and out of band modems provided by BT and returning them to BT.

5.7 STM

5.7.1 The Customer is responsible for installing the Sentry(s) inside the Customer's network on a network segment where the Sensors being monitored can deliver Messages to the Sentry.

The Customer must provide connectivity between the appliance and BT that will enable BT to have full access to the appliance in order to perform necessary monitoring and maintenance. The connectivity is via SSL (TCP port /443. Customer will provide NAT or PAT per physical Sentry device and enable provide inbound access via SSH on request to that NAT or PAT from BT's data centre IP ranges.

5.7.2 The Customer shall provide a three (3) hour maintenance window weekly.

5.7.3 The Customer's network will have a minimum Internet connectivity of 1.5Mbps for the Sentry to use to maintain connectivity from the Customer site to a SOC.

5.7.4 For Virtual Sentry installation, the Customer must provide a suitable server and virtual machine environment for installation of the Virtual Sentry image. The Customer may use an Open Virtualization Appliance (OVA) supporting Virtual Machine vendor of its choice (e.g. VMware, Microsoft, Oracle, etc.), as the BT Virtual Sentry image is supplied as an OVA package. The Customer acknowledges that BT uses current versions of VMware VSphere when testing and will only provide install instructions for current versions of VSphere. The Customer will be provided with recommended hardware/software specifications for the server running the Virtual Sentry image.

5.7.5 The Customer must follow BT's instructions for download and installation of the Virtual Sentry image within 14 calendar days of receipt of the email from BT containing login, download, and installation instructions for the Virtual Sentry image.

5.7.6 On termination of the Service, the Customer must de-install the Virtual Sentry image within 30 calendar days.

5.8 SVS

5.8.1 The Customer is responsible for installing Scanner Appliance(s) (or virtual scanner appliance AMI) on a Customer network segment where the security devices and sensors being scanned can be accessed from the Scanner Appliance.

5.8.2 The Customer shall provide connectivity between the appliance and BT that will enable BT to have full access to the appliance in order to perform necessary monitoring and maintenance.

5.8.3 The Customer shall notify BT immediately in writing of any changes in, or increases in the number of, the IP address(es) and/or domain name(s) that are listed in its account with the BT.

5.8.4 The Customer represents and warrants that it has full right, power, and authority to consent to have the tests for vulnerabilities of the IP addresses and/or domain names which the Customer notifies BT in writing. The Customer agrees to indemnify and hold BT harmless from and against any and all liabilities, losses, damages, costs, and expenses (including reasonable legal fees) incurred by BT resulting from third party claims arising solely from the Customer's breach of this section.

5.8.5 The Customer acknowledges and agrees that the SVS service and the results of the SVS service (excluding individual factual data gathered from its network) and all Intellectual Property Rights relating thereto are exclusively owned by BT or BT's third-party supplier. The Customer also acknowledges and agrees that it will not obtain any rights or interests thereto, except as expressly granted in this Service Annex.

5.8.6 The Customer acknowledges that scanning of IP addresses and/or domain names may in some circumstances result in the disruption of other services at its Site(s).

5.8.7 The Customer agrees that it is its responsibility to perform backups of data on all devices connected to its IP addresses and/or domain names before using SVS. The Customer further assumes the risk for all damages, losses, and expenses resulting from the use of SVS.

5.8.8 The Customer agrees not to

(a) use the scanner appliance, SVS Service, Reports, API or any data or information contained in any of the foregoing, except for the limited purpose of vulnerability management with regard to the IP addresses for which the Customer has ordered the Service;

(b) rent, lease, or loan the SVS Service, or any part thereof, or permit third parties to benefit from the use of the SVS Service via timesharing, service bureau arrangements, or otherwise;

(c) open, disassemble, or tamper with scanner appliance in any fashion;

(d) transfer possession of scanner appliance to any third party; or

5.8.9 The Customer shall keep any user name and password provided for access to the SVS Service confidential and will promptly notify BT if it learns of any unauthorized use of the user name or password.

5.8.10 The Customer acknowledges and agrees that all data and information contained within the SVS Service, Scan Data and Reports (excluding individual factual data gathered from the Customer's network IP addresses), and all information concerning or materially relating to the scanner appliance(s), are

Confidential Information of BT's supplier. The Customer will not use any Confidential Information of BT's supplier for any purpose not expressly permitted by this Service Annex, and will disclose the Confidential Information of BT's supplier only to those employees who have a need to know such Confidential Information for purposes of this Service Annex, and who are under a duty of confidentiality no less restrictive than the Customer's duty hereunder. The Customer will protect BT's supplier's Confidential Information from unauthorised use, access, or disclosure in the same manner as the Customer protects its own confidential information of a similar nature, and with no less than reasonable care.

5.8.11 The Customer shall return the scanner appliance(s) to BT on termination of the SVS Service. BT reserves the right to charge the Customer the cost of replacing the devices if BT does not receive the scanner appliance(s) within forty five (45) days of termination of the Service.

5.9 SDM

5.9.1 The Customer shall obtain and keep vendor (or applicable third-party provided) support and maintenance services for the 3rd Party Managed Devices for the duration of the Services.

5.9.2 The Customer shall provide BT with exclusive administrative access to the Managed Devices and the Customer will have no administrative rights to the managed system.

5.9.3 The Customer is responsible for OS installation and licensing.

5.9.4 The Customer shall provide the following conditions for all associated management applications of Managed Devices:

(a) Management application installed on a vendor approved hardware platform, on the then current recommended OS.

(b) Server hardware for software based Managed Devices that meets the Management Application vendor's minimum requirements, matching scope of deployment.

(c) Management application must run on dedicated hardware. No other applications or services other than those used by the management application will be run on the hardware without BT's written permission.

(d) BT will have sole administrative access to the OS and application, and the device shall not be joined to a network Domain or other logical unit which possesses higher-ranking access credentials which supersede any local restrictions specific to the OS and application.

(e) BT will harden/configure the OS consistent with the management application Vendor's best practices.

5.9.5 The Customer shall respond to BT alerts regarding hardware, software and maintenance within 24 hours for SLA to remain in force.

5.9.6 The Customer, at its cost, shall perform third party hardware upgrades, including replacement of hardware that cannot support new vendor software releases or cannot meet its performance demands as reasonably directed by BT. BT will not be responsible for devices that are designated end-of-life or end-of-support by the manufacturer.

5.9.7 The Customer shall enable remote access to Managed Devices from BT SOCs via SSL and SSH or IPSEC VPN or a combination of these as required by the vendor.

5.10 SLM

5.10.1 Customer shall provide BT with complete and accurate technical and business information and a copy of Customer's security policies. Customer shall promptly notify BT in writing of changes in such information.

5.10.2 The Customer will supply a list of networks and assets using the BT provided networks which will supply logs to the SLM Appliance in the standard template. Any devices that are not listed will not be included as an asset and therefore will not be indexed. Subject to customer change request, additional assets and networks can be added/authorized by BT SOC.

5.10.3 Customer shall work with BT to establish the optimal SLM Appliance configuration before implementation of the SLM Appliance.

5.10.4 The Customer will allow BT to install any SLM Appliances inside the Customer's network on a network segment where the SLM Appliance can deliver Messages to the Sentry.

5.10.5 The Customer will work with BT's SOC to ensure that logs are collected from the Log Sources.

5.10.6 Customer shall provide a three (3) hour maintenance window weekly.

5.10.7 The Customer shall enable remote access to the agreed upon SLM Appliances from BT's SOC.

6. CHARGES AND PAYMENT TERMS

The Charges for the Service will comprise some or all of the following components, depending on the option selected on the Order:

Product	One-time Charge	Recurring Charge	Notes
STM			
STM Sensor Registration	Non-Recurring Charge		Charge is per device or sensor to be registered.
STM Service Management		Monthly Recurring Charge	Except as otherwise provided in an Order, monthly recurring Charges are based on the average number of Events Per Second (**"EPS"**) processed by the STM service during an invoicing period and a monthly Tenant fee. EPS is calculated as the total number of events logged by the platform from Customer devices monitored, divided by total seconds in the monthly invoicing period.
Sentry Configuration	Non-Recurring Charge		Charge per Sentry.

Product	One-time Charge	Recurring Charge	Notes
Sentry Appliance		Monthly Recurring Charge	Charge per single hardware or Virtual Sentry configuration or HA Sentry configuration
SLM			
SLM Site Provision	Non-Recurring Charge		Charge is per Site
SLM Service Management		Monthly Recurring Charge	Charge is based on the storage capacity set out in the Order.
SLM Appliance Install	Non-Recurring Charge		Charge per SLM Appliance.
SLM appliance		Monthly Recurring Charge	Charge per SLM Appliance.
SDM			
SDM Site Provision	Non-Recurring Charge		Charge is per Site.
SDM Service Management		Monthly Recurring Charge	Charge is based on the number and type of managed devices
SVS			
SVS Site Provision	Non-Recurring Charge		Charge is per Site
SVS Service Management		Monthly Recurring Charge	Charge is based on the number of scanned IP addresses and type of scanning (internal/external and PCI)
Scanner Appliance		Monthly Recurring Charge	Charge per Internal Scanner.

7. SERVICE LEVELS

In accordance with clause 7.2 of the General Service Schedule, unless otherwise agreed in the Order, the SLA Categories for Availability for each service are as follows:

Service	SLA Category
Security Threat Monitoring, Platform Availability	A
Security Log Management, Single SLM configuration	F
Security Device Management	F
Security Vulnerability Scanning, External Scanning MVS service	F