Service Specific Terms

Cloud Managed Security Services

Vodafone Business Customers

1. The Service – Overview

1.1 The Vodafone Cloud Managed Security Services service (the "**Cloud Managed Security Services**") comprises of a set of managed security services for public, private and hybrid cloud environments. The term "Service" or "Services" in these Service Specific Terms means the Cloud Managed Security Service.

2. Service Terms Structure

2.1 These Service Specific Terms include:

(a) the service specification, which sets out a description of the Service, including optional Service Elements and complementary Services (where applicable) and may be updated from time to time (the "**Service Specification**"). The specific Service Elements selected by Customer will be set out in the Commercial Terms and/or Order;

2.2 The following documents further govern Vodafone's supply of the Service and form part of the Agreement, applying in the order of precedence set out in the General Terms:

(a) the Commercial Terms;

(b) the General Terms;

(c) the Fixed Service Terms;

(d) the Extra Service Terms;

(e) the Service Specification;

(f) the Statement of Work or the Order, which confirms the Service Elements selected by/for Customer;

(g) any other documents referenced as incorporated in these Service Specific Terms; and

(h) any applicable policies and guidelines, as provided from time to time by Vodafone.

2.3 Notwithstanding any terms in any framework agreement between the Parties, if there are any conflicting terms in these Service Specific Terms, the following order of precedence applies (highest level of precedence first): (a) the Commercial Terms; (b) the Service Specific Terms; and (c) the General Terms or other framework agreement.

3. The Service

3.1 The Service shall comprise of;

(a) Core Service Elements; and

(b) Additional Optional Service Elements (where selected)

The Core Service Elements and Optional Service Elements selected by the Customer shall be set out in the Commercial Terms and/or Order. The Service Specification summarises the Core Service Elements that are included in the base Charges, and the Optional Service Elements available for an extra charge.

4. Service Specific Conditions of Use

4.1 **Mandatory Accompanying Services**: In order to receive the Service, Customer must also purchase from Vodafone under separate agreement and maintain the following "**Mandatory Accompanying Services**" (the terms and charges for the Mandatory Accompanying Services are not included in these Service Terms): Integrated Managed Infrastructure ("IMI") for Public Cloud. If Customer fails to purchase or maintain the Mandatory Accompanying Services, Vodafone may terminate the Service and charge Customer any applicable Recovery Charge.

4.2 **Third Party Providers**: Service Elements are provided by a subcontractor or other Third Party Provider. Terms and conditions relevant to those Service Elements are set out in the Extra Service Terms. Vodafone will use a subcontractor or Vodafone Group Company that has the necessary authority to provide a Service Element where

required by Applicable Law. Vodafone may novate any Customer Agreements as required in order to comply with Applicable Law.

4.3 **Third Party Agreement**: A Third Party Provider will deliver the MSS Portal including the Educational Materials. Third Party Provider terms will be set out in a separate agreement directly between Customer and the Third Party Provider (including, if relevant, shrink-wrap or click through agreements). If Customer fails to accept the Third Party Provider's terms and conditions, Customer will not be able to access MSS Portal and Vodafone is excused from liability for failure to deliver.

4.4 **Educational Materials**: Customer is granted a licence on all Educational Materials and Customer acknowledges and agrees the Educational Materials remain the exclusive property of the Third Party Provider. Third Party Provider grants a licence in accordance with the terms provided in the MSS Portal. Educational Materials are provided "as is" and without warranty or indemnity of any kind, express or implied, including without limitation, the warranties of merchantability, fitness for a particular purpose, and non-infringement of proprietary and intellectual property rights.

4.5 **MSS Portal**: Vodafone will grant Customer access to the MSS Portal. Access is limited to authorised MSS Portal Users. MSS Portal Users will be provided with a user name, password, or other access information ("**User Details**"). Customer is responsible for: (a) the security of the User Details (including not disclosing such credentials to any unauthorised individuals); (b) providing Vodafone with the identity of the MSS Portal Users and keeping that information current; (c) promptly notifying Vodafone if a compromise login credentials is suspected; and (d) MSS Portal Users' compliance with the terms of use. Vodafone accepts no liability for any unauthorised or improper use or disclosure of any User Details. Customer is liable for all acts and omissions conducted using the User Details.

4.6 **Security Reporting**: Customer will have access to reporting capabilities within the MSS Portal. Customer agrees to: (a) generate MSS related reports within the MSS Portal and (b) be responsible for scheduling reports (as requested). Assistance from a PCI qualified security assessor is not provided as part of the Service and may be ordered separately at an additional charge.

4.7 **Designated Point of Contact**: prior to the commencement of the Services, Customer will authorise Vodafone designated point of contact to act on Customer's behalf in all matters regarding the Services.

4.8 **Authorised Security Contact**: Customer can create up to three Authorised Security Contacts. Each Authorised Security Contact will be provided with (a) administrative MSS Portal permissions to Customer's MSS Agent(s) as applicable; (b) the authorisation to create Designated Services Contacts and MSS Portal Users; and (c) the authorisation to delegate responsibility to Designated Services Contacts.

4.9 **Authorised Security Contact Responsibilities**: Authorised Security Contacts will be responsible for: (i) authenticating with the SOCs using a pre-shared challenge pass phrase; (ii) maintaining notification paths and Customer's contact information, and providing such information to Vodafone; (iii) creating Designated Services Contacts and delegating responsibilities and permissions to such contacts, as appropriate; (iv) creating MSS Portal users; (v) ensuring at least one (1) Authorised Security Contact is available 24 hours/day, 7 days/week; and (vi) update Vodafone within three calendar days when Customer contact information changes.

4.10 **Designated Services Contacts**: Customer agrees (a) to provide Vodafone with contact information including roles and responsibilities for each Designated Services Contact. Such Designated Services Contacts will be responsible for authenticating with the SOCs using a pass phrase; and (b) that a Designated Services Contact may be required to be available 24 hours/day, 7 days/week based on the subset of responsibilities for which it is responsible (e.g. firewall agent(s) outage).

4.11 **Systems owned by Customer third party**: For systems (which for purposes of the provision of the Service includes but is not limited to applications, internet service providers, content-hosting firms and IP addresses) owned by a third party and that will be the subject of testing hereunder, Customer will: (a) prior to the commencement of the Service, have appropriate consents in place from all third party system owners; (b) be responsible for any risks to, or impact on, any third party systems which arise from Vodafone's performance of the Service;(c) be solely responsible for communicating any risks, exposures, and vulnerabilities identified on these systems by Vodafone's remote testing to the system owner or any other relevant third party; (d) arrange for and facilitate the exchange of information between the system owner and Vodafone as deemed necessary by Vodafone; (e) inform Vodafone as soon as possible whenever there is a change in ownership of any system that is the subject of the testing hereunder; and (f) not to disclose the Deliverables to a third party system owner unless to the extent relevant, to remediate the issues identified as part of the testing.

4.12 **Third Party Claims:** Customer agrees to reimburse Vodafone for all liabilities, costs, expenses, damages and losses incurred by Vodafone arising out of or in connection with any claim made against Vodafone or its subcontractors by a third party arising out of or in connection with Customer's failure to obtain third party licences or approvals for Third Party Provider facilities, software, hardware or resource used in connection with provision of the Service. This provision is not subject to the liability cap in the General Terms.

4.13 **Permission to Perform Testing:** Customer authorises Vodafone to perform the Service and acknowledges that the Service constitutes authorised access to Customer's computer systems. Vodafone may disclose this grant of authority to a third party if Vodafone deem necessary to perform the Service.

4.14 **Risks:** Customer agrees and accepts that the Service entails certain risks. Customer acknowledges and agrees that the following may occur as a result of the Service delivery: (a) generation of log messages may increase resulting in excessive log file disk space consumption; (b) temporary degradation of the performance and throughput of Customer's systems and associated routers and firewalls; (c) temporary changes to some data as a result of probing vulnerabilities; (d) Customer's computer systems may hang or crash, resulting in system failure or temporary system unavailability; (e) any service level agreement rights or remedies will be waived during any testing activity; (f) a scan may trigger alarms by intrusion detection systems; (g) traffic interception of the monitored network for the purpose of looking for events.

4.15 **Procedures:** Customer agrees that Vodafone may establish new procedures for Customer's use of the Services, including as Vodafone deems necessary for the optimal performance of the Services.

4.16 **Disclaimer:** Customer acknowledges and agrees:

(i) that the Service is not warranted to operate uninterrupted or error free;

(ii) that Service is not fault tolerant and is not designed or intended for use in hazardous environments requiring fail-safe operation, including without limitation aircraft navigation, air traffic control systems, weapon systems, life support systems, nuclear facilities, or any other applications in which Service failure could lead to death, personal injury, or property damage;

(iii) that it is solely within Customer's discretion to use or not use any of the information provided pursuant to the Service;

(iv) that it is Customer's sole responsibility to provide appropriate and adequate security for Customer's organisation, its assets, systems and employees;

(v) that new technology, configuration changes, software upgrades and routine maintenance, among other items, can create new and unknown security exposures. Moreover, computer "hackers" and other third parties continue to employ increasingly sophisticated techniques and tools, resulting in ever-growing challenges to individual computer system security. Vodafone's performance of the Services does not constitute any representation or warranty by Vodafone about the security of Customer's computer systems including, but not limited to, any representation that Customer's computer systems are safe from intrusions, viruses, or any other security exposures. Vodafone do not make any warranty, express or implied, or assume any legal liability or responsibility for the usefulness of any information provided as part of the Service.

5. Data Protection

5.1 Customer shall not provide any Personal Data for Vodafone to process on its behalf. In the event of a change, Customer shall immediately notify Vodafone in writing.

6. Decommission or Turn-Down of Service

6.1 If the Service is terminated, Customer may request receipt of archived data by providing Vodafone with written notice within 90 days from the date of termination or expiry of the Initial Term (or Renewal Term, if applicable), whichever occurs first.

6.2 Vodafone will charge Customer for all time and materials, and shipping charges (if applicable) utilised to restore and make the archived data available via download from a secured server. In cases where the amount of archived data is too excessive to make available via download, data will be stored on encrypted media and shipped to a location specified by Customer.

6.3 If a request is not received within the 90-day period described above, all archived data will be permanently destroyed.

7. Support and Delivery Services

7.1 **Support Service**: Vodafone will provide Customer with support service for the Service Elements ordered by Customer.

7.2 **Support Parameters**: Support service is available in English only. Support service is available as shown below:

Support Service	Service Cover Period
Incident Management for Priority 1 & 2 Incidents	24/7
MSS Portal	24/7
Incident Management for Priority 3 & 4 Incidents	Working Hours
Service Request Fulfilment	Working Hours

Incidents may be reported at any time during the Service Cover Period; however, Incident Resolution will only occur during Working Hours for Priority Level 3 and 4 Incidents.

7.3 **Contact**: Customer must appoint primary and secondary points of contact responsible for accessing the support service and communicating with Vodafone during the relevant Service Cover Period. Customer will inform Vodafone, and keep Vodafone up-to-date with the appointed individuals' identity and level of access.

7.4 **Planned and Emergency Works**: Vodafone may temporarily interrupt the Service to carry out Planned or Emergency Works. Other than during standard monthly maintenance window, Vodafone will notify Customer at least five (5) days in advance of any Planned Works. Vodafone will notify Customer at least thirty (30) minutes in advance of any Emergency Works. "**Planned Works"** means planned Vodafone-initiated changes to the Service or Equipment (for example, to carry out essential maintenance or upgrades). **"Emergency Works"** means emergency Vodafone-initiated "as needed" changes to the Service or Equipment.

7.5 **Conditions**: Customer will: (a) reimburse Vodafone for reasonable expenses associated with a Customer Site visit or for other actions taken when Customer has reported an Incident caused by an Excluded Event; and (b) permit Vodafone to interrupt the Service to resolve a Priority Level 1 or 2 Incident (or the Incident will be downgraded to a Priority Level 3 Incident).

7.6 **Agreed Delivery Date:** Vodafone will provide Customer with the delivery date of a Service Element **("Agreed Delivery Date")** and use reasonable endeavours to deliver the Service Element by the Agreed Delivery Date. If Customer requests a change before delivery of the Service Element, Vodafone will either adjust or cancel the applicable Order subject to any Recovery Charge and/or amend the Agreed Delivery Date, as applicable.

7.7 **Service Commencement Date:** Vodafone will make the Service available to Customer and notify Customer that the Service is ready for use ("**Service Commencement Date**").

7.8 **Correction:** Customer must notify Vodafone within 5 Working Days of the Service Commencement Date if the Service is not available for use and provide sufficient supporting details. Upon receipt of notification, Vodafone will take reasonable action to commence service delivery.

Service Level Terms

Cloud Managed Security Services

Vodafone Business Customers

1. Service Level Terms

1.1 **Applicability**: Service Levels apply from the Service Commencement Date for the applicable Service Element depending on the Service Level measure, unless stated otherwise.

1.2 **Excluded Events:** Vodafone is not responsible for failure to meet Service Level if the Service Level is affected by an Excluded Event.

2. Service Commencement

2.1 **Service Level:** The Service Commencement Date for a Service Element will be on or before the Agreed Delivery Date unless Customer requests a change in Services prior to the Agreed Delivery Date.

3. Service Availability

3.1 **MSS Portal Calculation:** Percentage Availability for MSS Portal is calculated as: (A – B)/A x 100. **"A"** equals the number of whole minutes in the Monthly. **"B"** equals the number of whole minutes when the Service is Unavailable in the Monthly Measurement Period.

3.2 **Service Levels:** The following Availability Service Level applies:

Service Type	Service Availability (Percentage or P)
MSS Portal	99.80
Network/Service Change Notifications: Customer is responsible for providing advance notice regarding any network or server changes or outages to the managed services environment. In the event advance notice cannot be provided, Customer is required to provide notification of changes within seven calendar days of such network or server changes. Unless otherwise specified in the Order, notification is completed by the submission or update of an inquiry ticket through the MSS Portal for changes that will be implemented by Customer. For changes that must be implemented by Vodafone, Customer must submit a policy change request ticket. If Customer fails to notify Vodafone as stated above, Vodafone will be relieved of its obligations under the MSS Portal Availability but only to the extent Vodafone is unable to meet the Service Levels as a direct result of Customer failure to notify Vodafone. **Network Traffic**: MSS Portal Availability assume network traffic has successfully reached the Agent, the Agent is healthy and not experiencing any hardware or software errors and the Agent has the ability to process the traffic against the installed policy and generate a logged event. Vodafone is not responsible for traffic that does not logically or electronically pass through an Agent, or a logged event that does not reach the SOCs, or traffic that does not generate a logged event.	

4. Priority of Incidents

4.1 The following Priority Level examples apply to the Service:

Priority Level	Priority Level examples
1	**Critical or Major**: A security Incident that results in a critical business impact, such as denial of service, loss of data or security breaches or any kind involving personal identifiable information
2	**Significant**: A security Incident that results in some business impact, such as unauthorised Access (gaining access to a resource without permission) or where data (personal identifiable or otherwise) is at risk of loss or accessibility. Additionally, a critical vulnerability identified in technologies deployed would constitute, as a minimum, Severity 2.
3	**Medium:** A security Incident that does not present an immediate threat but will require actions to be taken to remediate. Examples may include third party provider/vendor identified vulnerabilities or advisories.
4	**Low**: Inappropriate use of systems

5. Security Incident Response Times

5.1 **Security Incident Response Time Calculation**: Security Incident Response Time means the time between the Incident being reported to the SOC by creation of a ticket within the IT Security Management Tool and the time the ticket is assigned to a Security Incident Management group.

5.2 **Security Incident Response Calculation:**

5.3

Priority Level	Security Incident Response Target Time
1	2 hours
2	24 hours
3	End of next Working Day
4	End of next Working Day

6. Service Credit for Incident Response

6.1 **Service Credit:**

(a) Customer is entitled to a Service Credit where the actual Achieved Percentage does not meet or exceed the Incident Response Achieved Percentage Target in the Monthly Measurement Period as set forth below:

Type	Achieved Percentage Target
Incident Response	95%

(b) Achieved Percentage Calculation: Achieved Percentage for Security Incident Response is calculated as total number of Security Incident Responses meeting the Incident Response Target Time/total number of Security Incident investigations in the Monthly Measurement Period.

(c) Service Credit Calculation: The amount of the Service Credit is calculated as (**A x B**) where "**A**" = 12.5% of the Monthly Recurring Charges for the month in which the failure occurred and "B" = 15%.

6.2 **Service Credit Terms**

(a) Customer must claim Service Credit via its Vodafone account manager within 30 days of the end of the Monthly Measurement Period.

(b) Vodafone shall conduct an analysis to determine the cause of the failure that resulted in the Customer Service Credit claim ("**Service Failure Analysis**"). Customer shall provide all reasonable assistance to Vodafone when conducting the Service Failure Analysis. Service Credits do not apply to any Incident connected to any Excluded Event.

(c) Service Credit will be applied to Customer's invoice after Vodafone reasonably determines that Service Credit is due.

(d) Notwithstanding any other provisions of these Service Specific Terms, a Service Credit cap of 12.5% of the sum of the Charges in respect of the relevant Contract Year applies to the Service Credit payable by Vodafone in a Contract Year.

(e) If one Incident causes a failure of two or more Service Levels, only the greater Service Credit amount of the Service Levels is payable.

(f) The Service Credits as set out in these Service Specific Terms are Customer's sole and exclusive remedy against Vodafone for any failure in Service performance. Service Credits have been calculated as, and are, a genuine pre-estimate of the loss likely to be suffered by the Customer for failure in Service performance. Service Credit may only be applied to Charges for the Service and have no cash value.

Cloud Managed Security Services Definitions

Vodafone Business Customers

The following definitions are applicable to the Services:

Alert Condition ("AlertCon")	the global risk metric. The four levels of AlertCon are described as follows: (a) AlertCon 1: Regular vigilance. Ordinary activity compromises an unprotected network minutes to hours after first being connected to the Internet. (b) AlertCon 2: Increased vigilance. Vulnerabilities or threats to computer networks require vulnerability assessment and corrective action. (c) AlertCon 3: Focused attacks. Specific vulnerabilities and weaknesses are the target of Internet attacks and require immediate defensive action. (d) AlertCon 4: Catastrophic threat. Critical security situations within a network dictate an immediate and focused defensive action. This condition may be imminent or ongoing.
Availability	the percentage of time the Service is available for use in the Monthly Measurement Period calculated as set out the Service Availability Service Level.
Call-Off Contract	the legally binding agreement for the provision of Services made between a Customer and Vodafone including the completed Order.
Deliverables	means any deliverable, process or document to be provided by Vodafone in accordance with these Service Terms or Extra Service Terms.
Educational Materials	means but is not limited to, lab manuals, instructor notes, literature, methodologies, electronic course and case study images, policies and procedures, and all other training-related property related to the Service.
Equipment Terms	the terms regarding Equipment in the General Terms.1.0 or later, or if those General Terms are not applicable, the Equipment Terms found at http://www.vodafone.co.uk/terms
Excluded Event	any of the following: (a) an Incident with another Vodafone service purchased under a separate Customer Agreement; (b) an Incident associated with non-Vodafone-supplied power, Customer Equipment, non-maintained structured cabling or other systems or networks not operated or provided by Vodafone (including an Incident relating to consumption of services over the internet); (c) an Incident caused by the negligence, act, or omission of Customer or a third-party not within Vodafone's direct control; (d) Customer's delay or non-performance of any of Customer obligations set out in the Customer Agreement or these Service Terms; (e) an Incident or delay resulting from a request by Customer for expedited delivery of the Service; (f) Customer's request to modify or test a Service Element; (g) a Force Majeure event or Service suspension that is permitted under the Customer Agreement; (h) the inability or refusal by a Third Party Provider to provide the Mandatory Accompanying Service; (i) a configuration change during implementation; (j) an Incident caused by service failure at any other Customer Site; (k) Staged Activities; and/or (l) during an Internet Emergency.
Extra Service Terms	the additional terms that apply to certain Service Elements ordered by Customer.
Incident	an unplanned interruption to the Service, a reduction in the quality of a Service, or a failure of a Service configuration item and excludes Emergency Maintenance.

Incident Management	the end-to-end management of Incidents by Vodafone.
Internet Emergency	means when the daily AlertCon level reaches AlertCon 3.
Monthly Measurement Period	the period from the Service Commencement Date up to the end of the calendar month and then each calendar month thereafter (save for the last month that will end upon the termination date of the Service).
MSS Agent(s)	a new or existing device subscribing to the Service. MSS Agents must not be used for any other purpose
MSS Portal	the portal that provides access to an environment (and associated tools) designed to monitor and manage the security posture by merging technology and service data from multiple vendors and geographies into a common, web-based interface. The MSS Portal may also be used to deliver Educational Materials.
MSS Portal Users	users of the MSS Portal with different levels of authorisation to the MSS Portal. The MSS Portal views and permissions available to the MSS Portal Users are dictated by the Authorised Security Contact.
Service Level(s)	the service levels that apply to the provision of the Service as set out in these Service Terms.
Service Request	the document which will describe the specific dates, timeline and service term applicable to the phases of the Service and which will be based on each individual Order and Customer requirement
SOC	the Security Operations Centres. SOC will only interface with Authorised Security Contacts and Designated Services Contacts.
Staged Activities	staged simulated or actual reconnaissance activity, system or network attacks, and/or system compromises initiated by Vodafone, Customer or a contracted third party.
Unavailable or **Unavailability**	a Customer Site cannot exchange data with another Customer Site/ Customer cannot access the Vodafone IP Backbone for reasons other than an Excluded Event.

Cloud Managed Security Services

Extra Service Terms

Managed Network Security Services

Vodafone Business Customers

1. The Service – Overview

1.1 These Extra Service Terms apply when Customer orders the Managed Network Security Services ("**MNS**"). The Service provides monitoring, alerting and management of network security technologies ("**Agents**") across a variety of platforms and technologies. Agents include Firewalls, Proxy and IPS/IDS devices. Within these Extra Service Terms, the term '**Service**' means the Managed Network Security Services.

2. Service Structure

2.1 These Extra Service Terms form part of the Service Terms for Cloud Managed Security Services when Customer orders the Managed Network Security Services optional Service Element. If there is a conflict between them, these Extra Service Terms will supersede the Cloud Managed Security Services Terms, but only for the Managed Network Security Services optional Service Element.

3. Extra Service Terms

3.1 **Managed Network Security Services Summary**: The Managed Network Security Services ("MNS") provides monitoring, alerting and management of network security technologies ("Agents") across a variety of platforms and technologies. Agents include Firewalls, Proxy and IPS/IDS devices.

3.2 **Data Gathering and Project Kick-off:** Upon receiving an Order, Vodafone will send Customer the service questionnaire(s) to be completed by Customer and schedule a project kick-off call for up to one (1) hour for up to three (3) Vodafone and/or Customer assigned personnel as determined by Vodafone.

3.3 **Agent Configuration:** Upon completion of the assessment activities, Customer agrees to: (a) ensure Customer's servers and operating systems meet or exceed Vodafone's specifications, ; (b) update Agent software and/or hardware to most current Vodafone supported version; (c) configure the Agent the associated settings; and (d) assist Vodafone in remotely configuring the Agent (i.e., cabling, network access, etc.).

3.4 **Agent Policy Configuration**: Prior to the Agent Integration activities Customer agrees to: (a) provide Vodafone with the policy to be implemented via the completed service questionnaire(s); and (b) acknowledge that while Vodafone may tune the Agent policy to reduce the number of erroneous alarms during standard deployment and activation, actual policy tuning is performed over a period of time that begins after service activation.

3.5 **Agent Integration**: Upon completion of the Agent Configuration and Policy Configuration activities, Vodafone will carry out Agent integration activities.

3.6 **Testing and Verification**: Customer agrees to: (a) be responsible for development of all of Customer's specific acceptance testing plans; (b) be responsible for performing acceptance testing of Customer's applications and network connectivity; and (c) verify that logs of each Log Source are available in the MSS Portal, as applicable.

3.7 **Managed Agent Health and Availability Monitoring**: Vodafone will monitor the health status of the Managed Agents and is designed to assist in increasing availability and uptime of the Agents ("Agent Availability Alerting"). The MSS Portal will perform this activity using either Agent based monitoring or Agentless monitoring.

3.7.1 Agentless Monitoring: Customer agrees to allow Vodafone to monitor the administrative interfaces and event stream of the managed Agents when it is not technically feasible to install monitoring software on such Agents.

3.7.2 Agentless Monitoring Troubleshooting: Customer agrees to (a) participate in troubleshooting sessions with Vodafone (as required); (b) be responsible for providing all remote configuration and troubleshooting if Customer has elected not to implement an Out Of Band ("**OOB**") solution, or if the OOB solution is unavailable for any reason. Customer acknowledges and agrees that if the managed Agent is eliminated as the source of a given problem, no further troubleshooting will be performed by Vodafone.

3.7.3 Agentless Monitoring Notification: Customer will be notified if the Agent becomes unreachable through standard in-band means. Customer agrees to: (a) provide Customer's notification paths and contact

information; (b) update Vodafone within three (3) calendar days when Customer's contact information changes; and (c) ensure an Authorised Security Contact or Agent outage Designated Services Contact is available 24 hours/day, 7 days/week to receive notification of outages.

3.8 Agent Management: Agent Management will be performed by Vodafone for MNS Services. Customer agrees to: (a) work with Vodafone to perform Agent updates (as required); (b) acknowledge that all updates are transmitted and applied agreed secure media.

4. Service Specific Conditions of Use

4.1 **Internet Content Security:** Customer is responsible for providing sufficient information for each requested policy change to allow Vodafone to successfully perform such change. Customer acknowledges that: (a) Customer is solely responsible for the procurement support, licencing, maintenance, and other associated charges for the content security solution; and (b) all changes to the content security policy requested after deployment and activiation of the Agent will be counted against the current month's policy change allocation.

4.2 Project Kick-off: Customer is responsible for scheduling night and weekend work in advance and as discussed during the project kick-off call. Night and weekend work is provided at an additional cost and subject to Vodafone resource availability and blackout dates.

4.3 Troubleshooting: Customer agrees to perform all troubleshooting of availability monitoring as required by Vodafone. Vodafone will not participate in troubleshooting or problem solving activities not directly relating to the deployment and/or health of the managed Agent subscribed to the service.

4.4 Additional Acceptance Testing: Additional acceptance testing performed by Customer, or lack thereof, does not preclude Vodafone from setting the Agent or Log Source to "active" in the SOCs for ongoing support and management, as applicable.

5. Support and Service Levels

5.1 Applicability: The Cloud Managed Security Service Support Service and Service Levels apply to the Managed Network Security Services..

6. Data Protection

Customer shall not provide any Personal Data for Vodafone to process on its behalf. In the event of a change, Customer shall immediately notify Vodafone in writing.

Cloud Managed Security Services

Service Specification

Managed Network Security Services

Vodafone Business Customers

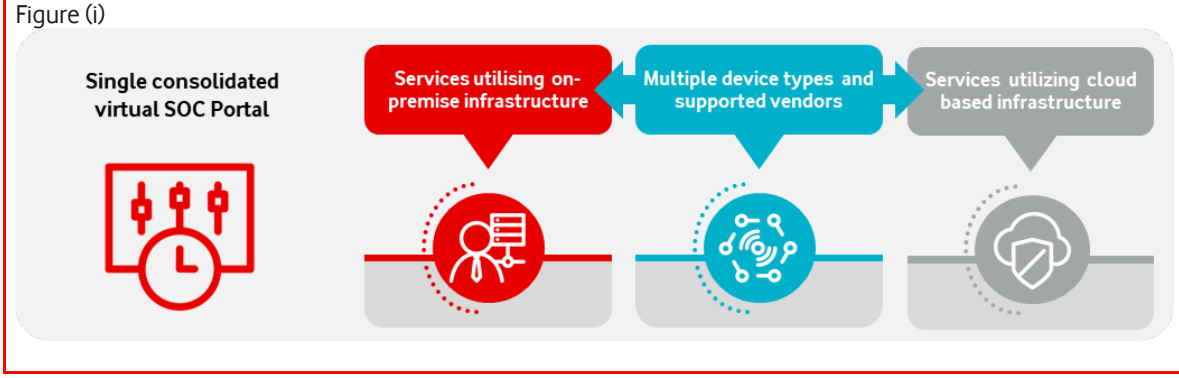
1. Introduction

1.1 The Vodafone Cloud Managed Network Security Services service (the "**MNS**") provides monitoring, alerting and management of network security technologies ("Agents") across a variety of platforms and technologies. Agents include Firewalls, Proxy and IPS/IDS devices.

2. The Service

2.1 The MNS service provides health monitoring and management of network security agents across a variety of platforms and technologies. The service enables the management of web proxy to protect cloud services, along with the management of both physical and virtual firewalls. See figure (i) below:

Figure (i)



3. Service Features

3.1 **MNS key features:**

(i) Data gathering.

(ii) Agent configuration – including configuring and hardening the OS, configuration of software and other settings based on the customers' requirements identified in the data gathering phase.

(iii) Agent policy configuration – covering guidance, suggestions and corrections to assist with functionality.

(iv) Agent integration – including activation and implementation of the security policy to the Agent.

(v) Testing and verification.

(vi) Service activation.

(vii) Availability monitoring, troubleshooting, managed Agent health, Agentless monitoring, Agentless monitoring troubleshooting, Agentless monitoring notification, Agent management, and Internet content security.

3.2 **Additional features for server workload protection**:

(i) Health monitoring to monitor health and performance of Agents.

(ii) Troubleshooting – to perform research and investigation if the Agents do not perform as expected or a potential Agent health issue is identified.

(iii) Agent management.

(iv) Security event and log delivery

(v) Correlated data through our SOC to provide advanced analytics reports which include:

1. Attack metrics, prevented attacks, vulnerability impact, and event counts/trending
2. Event correlation and analysis
3. Number of security incidents detected, priority and status
4. List and summary of security incidents

4. Service Benefits

4.1 The service delivers access to expertise, skills, techniques and methods to help manage security tooling and operations 24/7. Service benefits include:

(i) Customisable reporting available by device, group or site to help better manage threats and compliance requirements.

(ii) Firewall log monitoring, management and analytics.

(iii) Access to further information through the IBM Virtual Security Operations Centre

(iv) Access prevention of unauthorized users to help manage network availability

(v) Offers a cohesive lifecycle of security services, whether month-to-month management and monitoring or consultative services

(vi) Defence and protection from advanced threats, which allows for faster recovery from disruptions.

(vii) Increased visibility and intelligence with transparent insight into the threat landscape surrounding your business with applied risk/impact levels.

Cloud Management Security Services

Definitions

Managed Network Security Services

Vodafone Business Customers

The following definitions are applicable to these Extra Service Terms in addition to the definitions contained in the rest of the Service Terms:

Authorised Security Contact	a decision-maker on all operational issues pertaining to the MNS Services feature(s).
Designated Services Contact	a decision-maker on a subset of operational issues pertaining to each MNS Services feature, the feature's Agent(s), or a group of Agent(s).
Firewall ("FW")	a network security device that is designed to block unauthorised access and allow authorised communications based on a configuration of allow, deny, encrypt, decrypt, or proxy rules aligned with the Customer's security policy.
MSS Agent(s) or Agent(s)	is a new or existing device subscribing to MNS Services.
MSS Portal Users	the users of the MSS Portal with different levels of authorisation to the MSS Portal. MSS Portal Users can have restricted, regular, or administrative MSS Portal access to all MSS Agent(s), or just a subset of MSS Agent(s). The MSS Portal views and permissions available to the Portal Users are dictated by the Authorised Security Contact.

Cloud Management Security Services

Extra Service Terms

Managed Security Information and Event Management

Vodafone Business Customers

1. The Service – Overview

1.1 These Extra Service Terms apply when Customer orders the Managed Security Information and Event Management ("**MSIEM**") Services. The Service provides is a service that includes implementation, configuration, optimisation, management, and monitoring for a new QRadar on Cloud SIEM System. The Service is based upon the number of Events per Second that require monitoring and the number of applications in scope. Within these Extra Service Terms, the term '**Service**' means the MSIEM Services.

2. Service Structure

2.1 These Extra Service Terms form part of the Service Terms for Cloud Managed Security Services when Customer orders the MSIEM optional Service Element. If there is a conflict between them, these Extra Service Terms will supersede the Cloud Managed Security Services Terms, but only for the MSIEM Services optional Service Element.

3. Extra Service Terms

3.1 **Delivery Phases**: The Services will be performed in phases. Each phase must be fully completed before the next phase will begin. Customer must complete the prerequisites defined by Vodafone before phases three and four will begin. Vodafone is not responsible for any performance or non-performance issues with the Service caused by Customer prerequisites or Customer failing to comply with the Customer prerequisites. During each phase, the Vodafone Project Manager will assess the results of the interviews and/or workshops and either: (a) continue with the Service as set out in the Order, or (b) review the possibility of modifying the Order using the Change Control Process. The phases are set out below:

(a) Phase One – Project Initiation and Planning:: During this phase, Vodafone assists Customer with defining and compiling requirements and develops a Project Plan.

(b) Phase Two – System Design: During this phase, Vodafone creates an architectural and system design for Customer's environment. If the SIEM System is already deployed, Vodafone performs a design review.

(c) Phase Three – Implementation: During this phase, if not already deployed, Vodafone installs and configures the SIEM System components and verifies that data is being transmitted and reported.

(d) Phase Four – Integration and Transition: During this phase, Vodafone develops processes and corresponding documentation and begins transitioning management and monitoring to the operational support team.

(e) Phase Five – Ongoing Operational Support: During this phase, Vodafone provides steady state management and monitoring of the SIEM infrastructure..

4. Service Specific Conditions of Use

4.1 **Designated Project Manager:** Prior to the commencement of the Service, Customer will designate a person (the "**Customer Project Manager**") who will have the authority to act on Customer's behalf in all matters regarding the Service during Transition (Phases One to Four).

4.2 Designated Service Management Point of Contact: Prior to the initiation of the Steady State Operations, Customer will designate a Service Management Point of Contact (if different from Customer Project Manager) who will have authority to act on Customer's behalf to interface with Security Services Manager ("**SSM**") as an Authorised Security Contact (or in addition to the Authorised Security Contacts) as defined in the Communications Plan.

4.3 Technology Bundle: Customer is responsible for the procurement and provision of all hardware and software unless the Technology Bundle is included in the Service in which case Vodafone is responsible for the procurement and provision.

5. Support and Service Levels

5.1 **Applicability**: The Cloud Managed Security Service Support Service and Service Levels apply to Security Information and Event Management Service.

6. Data Protection

6.1 Customer shall not provide any Personal Data for Vodafone to process on its behalf. In the event of a change, Customer shall immediately notify Vodafone in writing.

Cloud Management Security Services

Service Specification

Managed Security Information and Event Management

Vodafone Business Customers

1. Introduction

1.1 The Vodafone Managed Security and Event Management service (the "**MSIEM**" Service) is a service that includes implementation, configuration, optimisation, management, and monitoring for a new QRadar on Cloud SIEM System. The Service is based upon the number of Events per Second that require monitoring and the number of applications in scope.

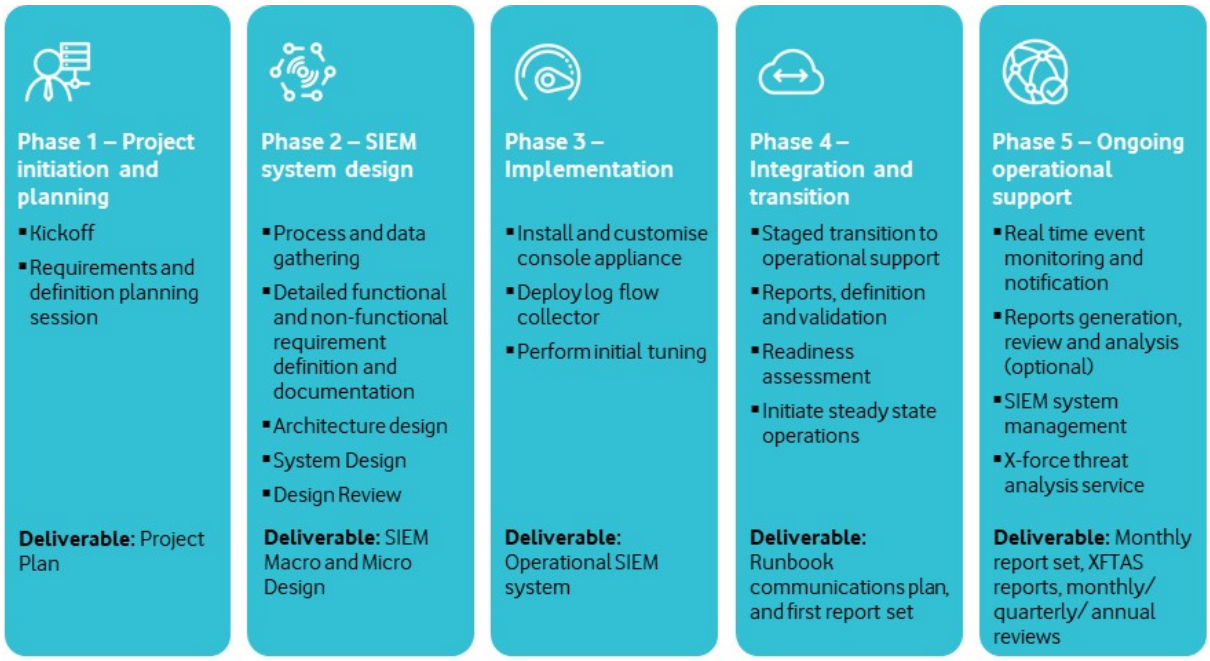
2. Service Elements

2.1 The MSIEM Service is designed to assist customers plan, implement, manage and monitor a security information and event management ("SIEM") system. It delivers a threat management system that helps identify and respond to threats, thereby helping customers improve compliance, optimise infrastructure investment and improve security posture.

2.2 The service delivers actionable data on threats by consolidating log events and network flow data from multiple devices, endpoints and applications distributed throughout the network. The service includes design, implementation, configuration, optimisation, management, and monitoring utilising IBM's QRadar on cloud ("QRoC") SIEM system.

2.3 The service is delivered in 5 phases as depicted at Figure 1. below:

Figure 1.



3. Key Features

3.1 The MSIEM solution operates across the five phases set out at Figure 1. above to provide a threat management system to help customers prepare for potential security threats. The key features of this service include;

(a) Development and delivery of a detailed, end-to-end Project Plan
(b) A comprehensive architectural and system design for the customer's environment
(c) Implementation and configuration of the SIEM System components, with validation that the data is being transmitted and reported
(d) Development of relevant operational processes and corresponding documentation, with transition management and monitoring to the operational support team
(e) Comprehensive steady state management and monitoring of the SIEM infrastructure
(f) Proactive threat mitigation
(g) Ongoing security incident identification, classification, prioritisation, escalation, workflow tracking, data analysis, and reporting
(h) Customisable and expandable service delivery and resourcing tailored to the customer's environment, strategic security goals and risk management challenges
(i) Integration with existing incident management, change management and other IT processes and operational activities
(j) Access to Security Operation Centres (SOCs) using a broad network of delivery personnel during Steady State Operations
(k) Project and Service Management to assist with successful transition.

Cloud Management Security Services

Definitions

Managed Security Information and Event Management

Vodafone Business Customers

The following definitions are applicable to these Extra Service Terms in addition to the definitions contained in the rest of the Service Terms:

Authorised Security Contact	Customer decision-maker on all operational issues pertaining to Vodafone Managed Security Services.
Communications Plan	a formal Deliverable of the Service, this is a document that comprises the information and knowledge sharing process and vehicle among workgroups, business units, and third-party entities as it pertains to the Service; includes security Incident escalation paths and contact information of Customer key stakeholders and Vodafone sales and delivery personnel.
Designated Services Contact	a network security device that is designed to block unauthorised access and allow authorised communications based on a configuration of allow, deny, encrypt, decrypt, or proxy rules aligned with the Customer's security policy.
MSS Agent(s) or Agent(s)	is a new or existing device subscribing to MNS Services.
MSS Portal Users	the users of the MSS Portal with different levels of authorisation to the MSS Portal. MSS Portal Users can have restricted, regular, or administrative MSS Portal access to all MSS Agent(s), or just a subset of MSS Agent(s). The MSS Portal views and permissions available to the Portal Users are dictated by the Authorised Security Contact.

Cloud Management Security Services

Extra Service Terms

Vulnerability Management Services

Vodafone Business Customers

1. The Service – Overview

1.1 These Extra Service Terms apply when Customer orders the Vulnerability Management Services ("**VMS**"). The Service provides the Customer with a fully managed scanning solution. Within these Extra Service Terms, the term '**Service**' means the VMS.

2. Service Structure

2.1 These Extra Service Terms form part of the Service Terms for Cloud Managed Security Services when Customer orders the VMS optional Service Element. If there is a conflict between them, these Extra Service Terms will supersede the Cloud Managed Security Services Terms, but only for the Vulnerability Management Services optional Service Element.

3. Extra Service Terms

3.1 **Service Activities**:

3.7.4 **VMS Deployment and Activation**: Vodafone will provide the Qualys scanning platform and Vodafone will work with Customer to configure the Service and provide remote assistance to deploy the required scanning agents for internal scanning. Customer agrees that additional acceptance testing performed by Customer, or lack thereof, does not preclude Vodafone from setting the internal scanner and/or the scanning agent to "active" in the SOCs for ongoing support and management.

3.7.5 **Scan Fundamentals**: Vodafone will work with Customer to create the Vodafone recommended scan profiles and schedules. Customer agrees to provide a single point of contact to work with Vodafone on issues pertaining to transition, steady state support, and all new business requirements.

3.7.6 **Managed Agent Health and Availability Monitoring**: Vodafone will monitor the health status and availability of the agent and monitor the number of agents specified in the Order. Customer will work with Vodafone to resolve internal scanner outages. Vodafone will not participate in troubleshooting or problem solving activities relating to any scanners not subscribed to the Service; nor will Vodafone provide health and availability monitoring of the scanning agents.

3.7.7 **Scanning Agent Management Services**: Vodafone will provide scanning agent application ("Agents"). Agent(s) are owned by Vodafone or its suppliers. Vodafone will select and provide Customer with Agent(s) at their discretion;. Customer has the right to use the selected Agent(s) only as directed by Vodafone and in accordance with the manufacturer's terms and conditions. Customer may not use them for any other purpose. Vodafone will manage the Agent(s). If enabling software/and or hardware, this is accompanied by a separate license agreement, the terms of such license agreement also apply.

3.7.8 **Services Vulnerability Scanning and Reporting**: When utilizing the MSS Portal, Customer will have access to the Service information and reporting. Customer agrees to: (a) access the MSS Portal to view scanned reports; and (b) provide valid IP inventory for scanning. Customer acknowledges and agrees that any custom reports created are available for download and will be kept for no longer than seven (7) days from the date of creation.

3.7.9 **Ad-hoc Additional Scan Requests**: If Customer orders this option, Vodafone will undertake out of band scanning for Customer against a requirement (e.g. rescanning or scanning for specific newly discovered vulnerabilities). Customer agrees to: (a) notify Vodafone with reasonable time that an ad-hoc scan request is required; and (b) provide information of any system required to be in scope for the custom scan.

4. Service Specific Conditions of Use

4.1 Customer acknowledges that all updates are transmitted and applied via the internet.

4.2 Any fix Vodafone makes available as part of support and maintenance is made on behalf of the security technology vendor and is licensed by security technology vendor to Customer under the terms of the applicable end user license agreement ("EULA"). Vodafone provides any such fixes as is and without warranties of any kind from Vodafone.

4.2.1 The applicable Non-Vodafone Product EULA(s) are available at: http://www.ibm.com/services/iss/wwcontracts under the Third-Party End User Licence Agreements section for the applicable country.

4.2.2 Open Source and/or Freeware Disclaimer: If the security technology Agent(s) include open source software and/or freeware, such software will be provided directly from a third-party vendor and Customer's use of this software will be subject to such vendor's end user license agreement ("EULA"), available for Customer's review and acceptance prior to downloading the software. Vodafone and Vodafone makes no representations and disclaims all express and implied warranties with respect to the software.

5. Support and Service Levels

5.1 **Applicability**: The Cloud Managed Security Service Support Service and Service Levels apply to the Vulnerability Management.

6. Data Protection

6.1 Customer shall not provide any Personal Data for Vodafone to process on its behalf. In the event of a change, Customer shall immediately notify Vodafone in writing.

Cloud Management Security Services

Service Specification

Vulnerability Management Services

Vodafone Business Customers

1. Introduction

1.1 The Vodafone Vulnerability Management Services service (the "VMS") provides Customers with a fully managed scanning solution. It utilises advanced hacking techniques to test an organisation's vulnerability to criminal attackers through hacking.

2. Service Elements

2.1 The VMS service provides Customers with access to a portal ("X-Force") providing an environment (and associated tools) designed to monitor and manage the security posture by merging technology and service data from multiple vendors and geographies into a common Web-based interface. X-Force provides:

(a) Reporting Capabilities

Customers can obtain:

(i) number, types, and summary of VMS requests/tickets;

(ii) details of scans performed in a variety of predefined and customizable formats;

(iii) tuning; and

(iv) scan scheduling and configuration;

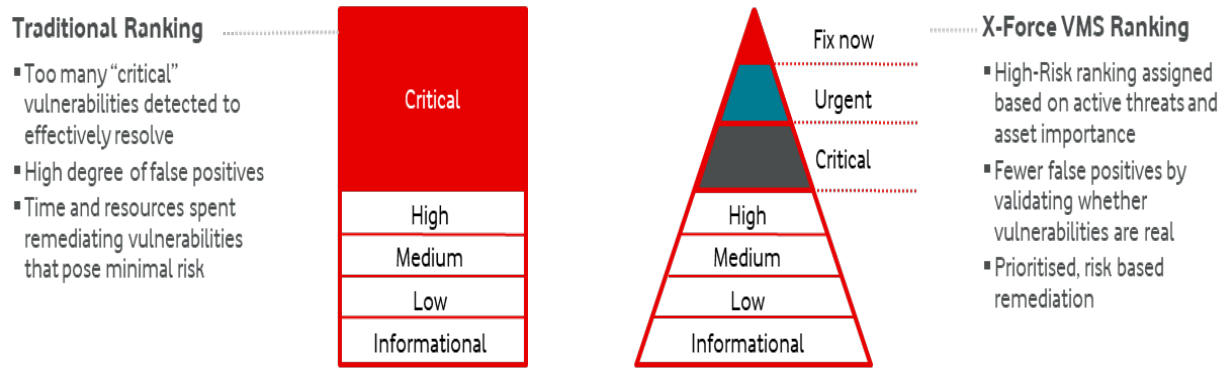
(b) Scan Results

Customers are provided with raw scan data available for thirteen months from the date of creation in the X-Force Portal which they can download as required.

(c) Ranking

VMS can quickly identify and prioritise organisations' most critical vulnerabilities. Using a proprietary algorithm, X-Force automatically ranks vulnerabilities based on asset value and threat, as summarised in figure (i) below:

Figure (i)



2.2 Deployment

(a) VMS is deployed through the X-Force portal and downloadable elements.

(b) VMS works with any scanner and level of service as summarised in figure (ii) below:

Figure (ii)