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.

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.

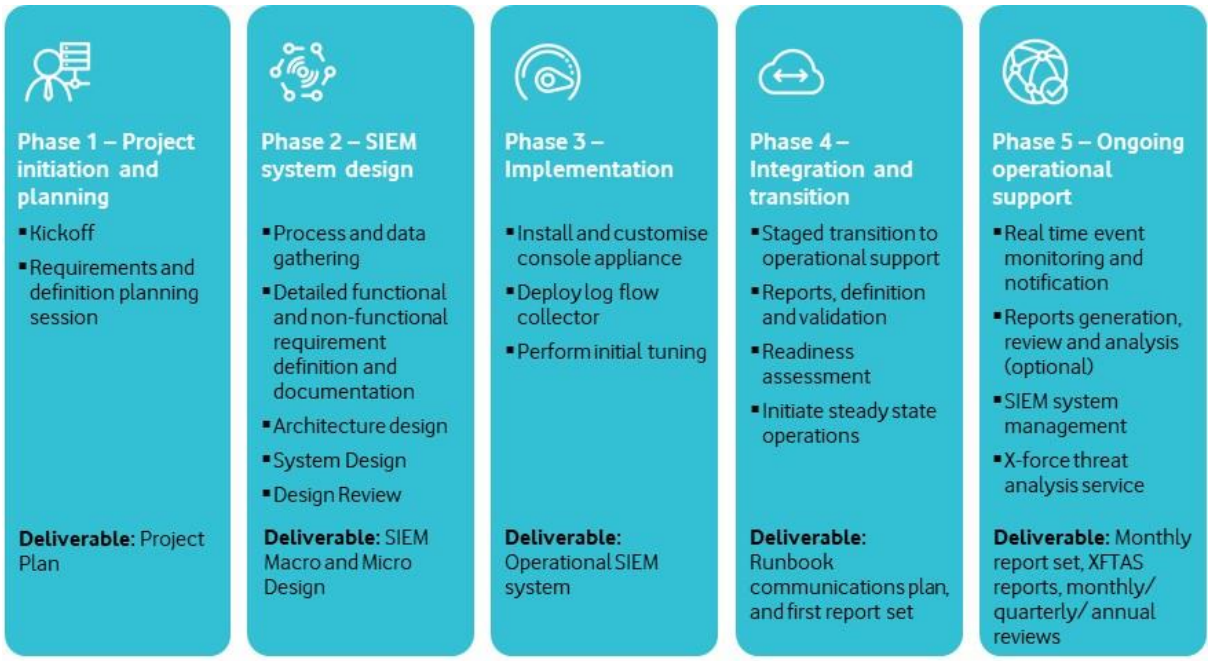
2. Service Elements

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) Iimplementation 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

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.