SCHEDULE K: SERVICE DEFINITION FOR CSOC LITE SERVICE

1. Service Description for CSOC Lite Service

Vysiion's CSOC Lite Service provides the Customer with the following elements:

- 24 x 7 x 365 asset monitoring, analysis and alerting for up to 3 'active' firewalls or 3 High-Availability pairs of firewalls configured in an active/passive configuration. The number of active and passive firewalls covered by the Service will be specified on the Order Form;
- Customer web portal;
- Reporting

Vysiion's CSOC Lite Service is delivered through its Cyber Security Operations Centre ("CSOC").

Asset Monitoring and Alerting

The log feeds for the monitored firewalls will be sent to a virtual sensor.

The log feeds collected by the virtual sensor are parsed, normalised, and sent to a Unified Security Manager (USM) system within the AWS public cloud over an encrypted channel for additional analysis. The rules in the USM system (as agreed in consultation between Vysiion and the Customer during the on-boarding process) will raise any suspicious logs or patterns of behaviour to "an Event". An Event will be brought to the attention of the Customer's designated Point of Contact ("POC") by the creation of a ticket within Vysiion's support ticketing system.

Events are classified in to 4 priority levels as follows unless agreed otherwise by the Parties in writing during onboarding:

Priority	Description
P1	Existence of conditions which indicate a potential security incident has occurred
P2	Existence of conditions which indicate the presence of a potential security threat requiring attention
P3	Potential Incidents that may have been averted but warrant investigation and confirmation
P4	System and vendor information to bring additional context to higher priority Events

Progress of all Events will be tracked within the Customer web portal. The CSOC may also call the Customer depending on the severity of the Incident. Communication preferences are confirmed during on boarding and can be adapted throughout the lifetime of the Service.

All the security stream data consisting of processed log information ("Alert(s)") will be stored for a period of fifteen (15) days.

Customer Web Portal

Vysiion provides the Customer web portal for access to the Service. The portal is the interaction between the CSOC Analysts and the Customer. Through the Customer web portal, the Customer can:

- View dashboards for summary of Service
- View and search Alert logs and Events
- View and search 15 days of raw/untampered logs

Reporting

The Customer will have access to real time information on how the devices are operating and can download reports within the Customer Web Portal.

2. On Boarding

During the on boarding stage, the Parties will identify the in-scope firewalls. All firewalls that are in-scope will be shown on the Customer web portal.

The on boarding consists of 2 parallel streams:

- *Technical* – to set up the infrastructure required for the service. This includes: Installation of virtual sensor, collection of Syslogs, creation of events & tickets.
- *Information Gathering* – to provide as much context as possible to enrich the analysis.

3. Target Service Commencement Date

Subject to the number of devices to be covered by the Service and Customer Dependencies (set out below), the Target Service Commencement Date is between thirty (30) to sixty (60) days from order acceptance.

4. Service Level Agreement

All aspects and communications are provided in the English language only.

For incidents logged to the CSOC by the Customer, the priority can be set by the Customer acting reasonably in accordance with the table below, when logging the incident, via either email or telephone.

Severity Level	Description
S1	A critical business service is non-operational impacting the Customer organisation, multiple users or multiple sites; or severe functional error or degradation of service affecting production, demanding immediate attention. Business risk is high, with immediate financial, legal or reputational impact.
S2	The Customer is experiencing failure or performance degradation that severely impairs operation of a critical business service; or the Customer or service has been affected, although a workaround may exist; or application functionality is lost; or significant number of users or major site is affected. Business risk is high.
S3	The Customer is experiencing a problem that causes moderate business impact. The impact is limited to a user or a small site; or incident has moderate, not widespread impact; or the Customer or IT service may not have been affected. Business risk is low.
S4	Standard service request (e.g. User Guidance); or updating documentation. Low or Minor localised impact.

Target Availability

Service	Target Availability
Cyber Security Operations Centre Services - Customer Portal	99.9%

Service Credits

Service Credit*		
Measure	>0.1 below Target	10%

5. Additional Terms applicable to the CSOC Lite Service

5.1 In addition to the reasons set out in section 6.2 of the main body of this document, Vysiion shall also have no liability for any failure to meet the Target Service Commencement Date and/or target service levels due to, or as a result of, any of the following reasons:

- Change management requirements affecting monitored devices
- Network or policy changes to a monitored device not performed by Vysiion
- Loss of connectivity due to Customer connectivity issues or Customer managed issues
- Requirements which the Customer must meet before the Service can be provided and during its provision as set out below ("Customer Dependencies").

5.2 Customer Dependencies

5.2.1 The Customer shall ensure that:

(c) Each device covered by the Service has the appropriate full manufacturer's product licence and subscriptions for the duration of the Service. Software and devices that are considered end of life by the manufacturer are not covered by the Service;

(d) All devices must have full manufacturer's support for the duration of the Service; and

5.2.2 The Customer accepts the following as a condition of Vysiion providing the Service:

(c) Vysiion is not responsible for resolving the Customer's Internet Service Provider (ISP) outages, or issues with the Customer's internal network or computing platform infrastructure where Vysiion is not contracted to support those elements; and

(d) It is the responsibility of the Customer to ensure the log stream is directed at Virtual Monitoring Appliance for Service operation where applicable.