SCHEDULE F: SERVICE DEFINITION FOR ADVANCED FIREWALL MONITORING

1. Service Description for Advanced Firewall Monitoring

Exponential-e's Advanced Firewall Monitoring Service provides the Customer with the following elements:

- 24 x 7 x 365 firewall monitoring
- ProVision Web Customer Portal
- Reporting
- Alerting
- Notification & Escalation
- 24x7x365 Analysis.

Exponential-e's Advanced Firewall Monitoring Services is delivered through Global Security Operations Centres (SOCs) which operate 24 hours per day, 7 days per week, 365/6 days per year. All aspects and communications are provided in the English language only.

The Syslog stream from the firewalls which are subject to this Service (as identified and documented during on-boarding) will be monitored and analysed. The Syslog feeds for monitored devices, will be sent to a VisionLink collector.

The Sys*log* streams collected by VisionLink are parsed, normalised, and sent to the ProVision threat engine for additional analysis. The rules in the threat engine (as agreed in consultation between Exponential-e and the Customer during the on-boarding process) raise any suspicious logs or patterns of behaviour to "an Event". Events that will be brought to the attention of the Customer's designated POC(s) by the creation of a Ticket within ProVision. Events are classified in to 4 severities as follows:

- *Emergency* – Existence of conditions which indicate a potential security incident has occurred
- *Critical* – Existence of conditions which indicate the presence of a potential security threat requiring attention
- *Warning* – Potential Incidents that may have been averted but warrant investigation and confirmation
- *Informational* – System and vendor information to bring additional context to higher priority Events

All progress of Events will be tracked within the ProVision Ticket. The SOC 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.

ProVision security stream data consisting of processed log information (Alerts) will be stored for a period of 90 days, unless otherwise agreed in writing with the Customer.

Component Elements

ProVision Portal

Exponential-e provides the ProVision Portal for access to the Service. The Portal is the interaction between the SOC Analysts and the Customer. Through the ProVision Portal, the Customer can:

- View Dashboards for summary of Service
- Manage Devices/Assets and system inventory
- View and search Alert logs and Events
- View and update profile information
- View and update Customer information
- Access Reports
- Search, update and manage all types of Tickets
- Access appropriate Knowledge Base articles

Reporting

The Service provides preconfigured reports available in the ProVision Portal.

Reporting includes but is not limited to:

- Monthly Management Report (Overview of Service for the monthly period)
- Estate (Users, Managed Assets/Devices)
- Tickets (Management Report, Support Tickets, Security Tickets)

- Authentication (Management Report, Summary Report, By User, By Device, By Disabled Accounts)
- Security Analysis (Management Report, Events, Log Messages, Anti-Virus, Policy Changes)
- Traffic (Management Report, Dropped Traffic, By Source, By Destination, By Destination Port)

Additional Reports can be requested during On Boarding and can be adapted throughout the life-time of the Service (subject to availability of data). Exponential-e reserves the right to add/remove/change the reporting in the ProVision Portal.

VisionLink

VisionLink works as the Syslog collector. VisionLink is typically located in the Exponential-e virtual data centre or on the Customer Site and receives the Syslog stream of the firewalls covered by the Service. VisionLink is supplied as Software / Agent that is installed on to a VM either by Exponential-e (where the VisionLink is located in the Exponential-e virtual data centre) or the Customer (where the VisionLink is located at the Customer Site). Exponential-e will provide the image for the VisionLink for installation on either an Exponential-e or the Customer VM instance. Specifications for the VM will depend on the number of Devices/Assets covered by the Service and will be advised during On Boarding. The VisionLink agent is installed on Ubuntu 14.04 LTS (or later approved system). It is Exponential-e or the Customer's responsibility (as applicable) to ensure that the VM is available for the installation of the VisionLink by it.

On Boarding

Exponential-e will work with the Customer to bring all firewalls in to live Service during the On Boarding process. This is typically 30-60 days from order acceptance but will depend on the number of firewalls to be covered by the Service and availability of Customer personnel.

The On Boarding consists of 2 parallel streams:

- *Technical* – to set up the infrastructure required for the service. This includes; Installation of VisionLink, collection of Syslogs, creation of Events & Tickets, Portal training;
- *Information Gathering* – to provide as much context as possible to enrich the analysis. This involves either completing a document or online tool to gather all the required information to set up the Service. Areas covered are contact details, facilities, network design, topology, platforms, apps and users.

Customer Responsibilities

1 Firewall – the Customer must confirm the internet-facing firewall to be covered by the Service

2 Software License/Subscriptions – the Customer must ensure that each firewall covered by the Service has the appropriate full manufacturer's product license and subscriptions for the duration of the Service. Firewalls or Software that are considered end of life by the manufacturer will not be covered by the Service

3 Hardware Support – the Customer must ensure that all firewalls have full manufacturer's support for the duration of the Service

4 Security Operation – the Customer must ensure that all firewalls covered by the Service contain a valid Rulebase or configuration to protect the security of the Service

5 Connectivity – the Customer must ensure appropriate connectivity. Exponential-e 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.

6 Syslog Stream - the Customer must ensure the log stream is directed at VisionLink for Service operation.

7 Customer Point of Contact (POC) – the Customer must provide in writing a primary point of contact (POC). The POC will provide access to knowledgeable technical staff, and/or third party resources, to assist Exponential-e with any hands-on support or working with third-party vendors.