## SCHEDULE A: SERVICE DEFINITION FOR DDoS MITIGATION SERVICE

### 1. DDoS Mitigation Service Description

The Distributed Denial of Service ("DDoS") Mitigation Service is designed to mitigate DDoS attacks targeted at an internet facing resource on the Exponential-e network. This Service is available per Smart Wires service, one DDoS Service is required for each Smart Wires service. It comes in 3 options: Bronze, Silver and Gold, with the Bronze and Silver being priced per Service, and the Gold being priced based on Circuit Bandwidth, in steps of 1Gbps as stated on the Order Form. Traffic on circuits not supplied by Exponential-e and connected to the Exponential-e network will not be covered by the DDoS service.

**Detection**

Traffic is monitored for the selected Smart Wires Service and classified based on the Cloud-Based Data Feed. Traffic matching known bad criteria from the variety of feeds is classified as DDoS. Alerts are generated when the amount of DDoS traffic goes above a configured level set by Exponential-e and adjusted from time to time to align with industry best practice and trends. The following are examples of the types of traffic that when detected would be classified as DDoS: DNS Amplification, IP Fragment, ICMP, IP Protocol 0, MS SQL Amplification, NTP Amplification, SNMP Amplification, SSDP Amplification, TCP Null, TCP RST, TCP SYN. The triggers monitor both the total amount of DDoS traffic going to a single IP address on the selected Smart Wires Service, and the total amount of DDoS traffic going to a Smart Wires Service on any IP address.

**Mitigation**

Once an alert is triggered, mitigation is automatically launched, regardless of which mitigation package is purchased. When the Exponential-e DDoS mitigation platform recognises attack traffic, traffic destined for the targeted IP address, estate or asset will be either blocked at the edge of the Exponential-e network or re-directed to Exponential-e's DDoS mitigation platform for inspection, depending on the mitigation package purchased. Diverted traffic will be subject to multiple layers of Traffic Cleaning. While Traffic Cleaning is in progress, an increase in latency may be experienced.

The DDoS Mitigation Service is designed to automatically detect and mitigate an attack for its whole duration. Certain situations (such as where an attack is so large that it affects other Partners/End Users) might require a manual mitigation by Exponential-e and in this case the total mitigation period will be time-limited to 72 consecutive hours at no additional charge. Should the Partner request mitigation be continued past this point, additional charges will apply at Exponential-e's then standard engineering Professional Service rates.

Exponential-e will use all reasonable endeavours to ensure that non-attack traffic is received as normally as possible during a DDoS attack. Under the Silver and Gold packages, Blackholing of traffic will only be used by Exponential-e if Exponential-e determines that all other measures have failed or are likely to fail.

Exponential-e does not warrant or guarantee that the DDoS Mitigation Service will prevent or mitigate all DDoS attacks.

The following options apply:

**Bronze Package**

The Bronze Package provides proactive alerts when an attack has been detected and destination IP Blackholing as mitigation action. The Bronze Package includes reporting via a portal, also providing information on traffic types and trends for up to 30 days.

**Silver Package**

The Silver Package includes all reporting elements from the Bronze Package, with additional dynamic Layer 4 access-control list (ACL) filtering. The Silver Package protects assets against typical volumetric attacks such as reflection or amplification. To mitigate a high number of anomalous requests, the system utilises Smart blocking which creates a set of dynamic rules to intelligently block the majority of attack traffic at network edge.

**Gold Package**

The Gold Package includes all elements from the Silver Package, with additional Network Scrubbing and Layer 7 Application layer mitigation. A network scrubbing platform delivers clean traffic to the hosts/assets under attack. Large attacks are neutralised with the volumetric protection in the network, and the remaining traffic is sent to the scrubber for forensic scanning and filtering. Live traffic is analysed, with malicious traffic removed and clean traffic passed on for delivery. Scrubbing offers protection against sophisticated attacks on application and network layers.

**Emergency Option**

Available to Partners/End Users that (a) are experiencing a DDoS attack and need immediate protection, or (b) require to expedite the start of the service, this option can be contracted via the Order Form attached at Appendix A to this Service Definition in the case of (a). Following implementation, a period of fine-tuning and close liaison with the Partner/End User will be undertaken to mitigate the attack. There is a risk for non-attack Partner/End User data in transit to be lost whilst this fine-tuning is undertaken and the Partner/End User accepts this risk.

Where the Partner orders this Emergency option in scenario (a) above, the Partner acknowledges that they will also be contracting to take the Gold Package on the terms set out in Appendix A.

**Multi-Factor Authentication**

The Partner/End User will be provided with multi-factor authentication-based access to the reporting portal for the number of users specified on the Order Form.

**2. Target Service Commencement Date – Bronze/Silver/Gold Package Options**

DDoS Mitigation Service 10 Working Days*

** From order acceptance if provisioned in respect of an existing Smart Wires Service / from date of provision of any new Smart Wires Service required.*

**3. Target Service Commencement Date – Emergency Option**

DDoS Mitigation Service 4 Hours *

** From receipt of signed DDoS Mitigation Service – Emergency Option Order Form*

**4. Target Service Levels**

Target Detection Success Rate[1]: 99% per month

Target Mitigation Success Rate[2]: 99% per month

Target Time to Detect: within 1 minute of the attack starting

Target Time to Divert/Blackhole (as applicable): within 1 minute of the attack being detected

Should the Partner/End User feel they are being attacked and the DDoS system does not detect the attack, the Partner can immediately notify the Exponential-e Service Desk and this will be treated as a P1 incident.

[1] *the sum of detected attacks compared to the sum of detected attacks plus any missed ones reported by the Partner that are subsequently validated by Exponential-e as a DDoS attack*

[2] *the relevant measures set out in the applicable package commenced and continued until such time that the attack stopped or any applicable time limit on mitigation was reached.*

No Service Credits are payable.

**5. Additional Terms applicable to DDoS Mitigation Service**

The following terms apply to the provision of the DDoS Mitigation Service by Exponential-e in addition to Exponential-e's General Terms.

**5.1 Additional Partner Responsibilities**

5.1.1 The Partner shall:

5.1.1.1 notify the Exponential-e Service Desk in advance of any impending activity that can reasonably be expected to result in or encourage additional traffic to its site that may or may not be malicious in nature, including but not limited to marketing campaigns, moral hacktivist attacks and other traffic outside of the normal traffic profile for the Smart Wires Service; and

5.1.1.2 immediately inform Exponential-e if any threats are made, whether publicly, privately, intimated, inferred or directly, of any intention to initiate a DDoS or DoS attack at any time.

6. Definitions

6.1 In this Service Definition, the following terms below shall have the meaning given below.

| | |
|---|---|
| "Blackholing" | discarding all data destined for a particular IP address; |
| "DDoS" | Distributed Denial of Service; an electronic attack involving multiple computers sending repeated requests to a web-site generating false traffic with the aim of rendering it inaccessible; |

| | |
|---|---|
| “Traffic Cleaning” | Statistical analysis, active verification, anomaly recognition and the discarding of packets that do not conform to the Partner’s/End Users “normal” traffic profile. |
| “Cloud-Based Data Feed” | a data feed produced by system that continuously probes and tracks billions of IPv4 and IPv6 addresses on the internet, maps them and combines them with network-related data sets for real-time detection of distributed denial of service (DDoS) attacks. |
| “Circuit Bandwidth” | The total amount of bandwidth the Partner/End User has as part of their Smart Wires service. |

**Appendix A**

DDoS Mitigation Service – Emergency Option with Gold Package

Order Form

Partner Name:

Partner Registration Number:

Partner Contact Name:

Partner Contact Telephone:

Partner Contact Email:

Services:

**1 x DDoS Mitigation Service – Emergency Option**

Non-Recurring Charge: £975 ex VAT

**1 x DDoS Mitigation Service – Gold Package 1Gbps**

Initial Term: 12 months from the Service Commencement Date

Annual Charge: £7,000 ex VAT (including up to 5 licences for multi-factor authentication).

Any additional bandwidth (in steps of 1Gbps) to be contracted separately.

Annual Charge payable annually in advance.

**Terms and Conditions**

Exponential-e's General Terms (available at www.exponential-e.com/reseller-terms) apply to this Order.

**Service Document**

Exponential-e's Service Document for Security Services current at time of order (available at www.exponential-e.com/reseller-terms) applies to this Order.

A legally binding Contract is formed when this Order Form is signed by the Partner and Exponential-e Limited.

| **Exponential-e Signature** | **Partner Signature** |
|---|---|
| Signature…… | Signature…… |
| Name…… | Name…… |
| Position…… | Position……Director…… |
| Date…… | Date…… |