SERVICE SCHEDULE

PULSANT CLOUD PROTECT DEFEND

This is a Service Schedule as defined in the Conditions. Where the Services set out in this Service Schedule form part of the Services to be supplied under a Contract (as defined in the Conditions), this Service Schedule forms part of the Contract.

In this Service Schedule, references to Clauses are to Clauses of the Conditions, and references to paragraphs are to the paragraphs of (i) this Service Schedule or (ii) whichever other document is specifically referred to.

1 Additional Definitions

In this Service Schedule the following words and expressions shall have the following meanings:

1.1 **"Alert Logic"** – A third-party company which the Supplier partners with. The Cloud Protect Defend service is powered by Alert Logic tools and technology.

1.2 **"Agent"** – An application that runs on an asset within the Customer's infrastructure, collecting log and event data from that asset.

1.3 **"Appliance"** – A stand-alone dedicated physical virtual server hosted within the Customer's infrastructure, collecting and consolidating data from Agents to be securely transmitted to the Alert Logic Cloud for analysis.

1.4 **"Critical Severity Security Incident", "High Severity Security Incident"** — a security incident which, at the Supplier's sole discretion, poses a risk to the Customer that requires a heightened level of response. Security incident severity levels are illustrated in the "Pulsant Service Description – Cloud Protect Defend" document.

1.5 **"Managed Server Service"** — a service by which the Supplier provides management of servers belonging to the Customer; such a service is extra to the scope of this Cloud Protect Defend Service and will be defined under a separate service schedule.

2 Pulsant Cloud Protect Defend – Service Scope and Description

2.1 Pulsant Cloud Protect Defend Service is a full-stack security and compliance solution that provides vulnerability and configuration assessment, log management, network intrusion detection and out-of-band web application protection with 24x7x365 threat monitoring.

2.2 The Customer confirms that it has considered and accepts full responsibility for all scenarios relating to any failure conditions and functionality of each related or dependent service where those services are not provided by the Supplier.

2.3 Pulsant Cloud Protect Defend Services are provided to the Customer for so long as the Contract remains in force in accordance with the terms of the Contract and the Supplier's acceptable use, security and access policies and procedures.

2.4 Pulsant Cloud Protect Defend Service is subject to payment by the Customer of the Supplier's Charges for installation and support services, as set out in the Order Form or as subsequently agreed between the parties from time to time.

2.5 The Service is governed by a fair usage policy that provides each purchased node with 100MB of storage for daily logs. This usage is aggregated across all purchased nodes to allow an adequate amount of logs to support a standard deployment.

2.6 In the event the Customer utilises the Service in excess of the fair usage policy and does not bring usage within the entitlement tier or amount identified on the Order Form within thirty (30) days and remain within its entitlement, the Customer will be billed for such excess usage commencing from the first day of the first month of excess usage. If the Order Form does not specify the rates for excess usage, the per-unit rate for the excess usage of the Services will be equal to 1.25 times the then-current list price for the appropriate tier for such Services.

2.7 The Supplier will perform the following activities during the set up of the Service:

2.7.1 Install and configure the Service to protect servers within the Customer's infrastructure, where that infrastructure is managed by the Supplier.

2.7.2 Install and configure Agents on all servers identified on the Order Form, where the Supplier is responsible for those servers under a Managed Server Service.

2.7.3 Install and configure an Appliance server in the Customer's infrastructure.

2.7.3.1 Any physical or virtual infrastructure required to install the Appliance server on are outside the scope of this Service and may be charged separately.

2.7.4 Perform an initial security assessment of the pre-existing infrastructure that is to be covered by the Service and advise the Customer on remedial actions to address any vulnerabilities we identify.

2.7.5 Configure firewall rules on devices managed by the Supplier, enabling Agent-Appliance communication and secure forwarding of logs and data to the Alert Logic cloud.

2.7.6 Where the Customer's network environment is managed by the Supplier, configure the environment to enable Agent communication and secure forwarding of data required by the Service.

2.7.7 Ensure that log collection for targeted data sources is properly installed, apply whitelisting requested by the Customer, and validate that target source log data is being sent for storage and analysis.

2.7.8 Set up IDS scanning schedules and policies in consultation with the Customer.

2.7.9 Provide the Customer with access to a Service management portal.

2.7.10 Set up and manage user accounts and configuration on the Service management portal.

2.8 The Supplier will perform the following on-going activities for so long as the Contract remains in force:

2.8.1 Monitor the Appliance server to ensure that it continues to function correctly, including applying any required upgrades or patches to the server.

2.8.2 Monitor installed Agents to ensure they continue to function correctly, including applying any required upgrades or patches to the Agent, on servers which the Supplier is responsible for managing under a Managed Server Service.

2.8.3 Tune the log collection service element to whitelist traffic in response to a Change request from the customer, noting that this may be a chargeable activity.

2.8.4 Perform on-going Service optimisation activities such as adjusting log data sources, modifying assignment policies, and performing network changes.

2.8.5 Run scheduled external PCI scans and additional PCI scans to verify that vulnerabilities have been addressed.

2.8.6 Provide the Customer with summarised data collected by the Service, via the Service management portal.

2.8.7 Provide the Customer with three standard reports monthly – Vulnerability Summary, Incident Analysis, and Vulnerability Variance. Other standard reports may be requested in life through a change request. Bespoke reports and platform audits are not in the scope of the managed service. These may be provided by the Supplier, at the Customer's request and the Supplier's discretion, as chargeable work.

2.8.8 Apply critical security patches to servers managed by the Supplier, in accordance with the patching process and schedule agreed under any applicable Managed Server Service provided by the Supplier.

2.8.9 Apply other patches as requested by the Customer in accordance with the agreed Change process under any applicable Managed Server Service provided by the Supplier.

2.8.10 Initiate patching of identified vulnerabilities in response to Critical Severity Security Incidents and High Severity Security Incidents, where such activities are within the scope of patching activities agreed with the Customer as part of a Managed Server Service provided by the Supplier. Remediation measures outside the scope of a Managed Server Service provided by the Supplier may, at Customer's request and Supplier's discretion, be performed by the Supplier as chargeable work.

2.8.11 Respond to any security incident identified by the Service by:

2.8.11.1 Classifying the incident according to severity.

2.8.11.2 Alerting the Customer of any High Severity Security Incident or Critical Severity Security Incident.

2.8.11.3 Initiating appropriate remedial activity in response to any High Severity Security Incident or Critical Severity Security Incident, on receiving authorisation from the Customer; such activity is limited to infrastructure within the scope of a Managed Server Service provided by the Supplier.

2.8.11.4 Listing in the Customer Service management portal all security incidents classified lower than a High Severity Security Incident; no alert will be issued to the Customer for these incidents.

2.8.12 Manage all security incident responses, liaising between the Customer and Alert Logic at all times.

2.8.13 Manage any changes to user accounts and configuration on the Alert Logic portal.

2.9 If the Order Form includes the additional Service Management option, the Supplier will:

2.9.1 Provide a monthly security posture report.

2.9.2 Provide a critical watch report.

2.9.3 Provide a service management report with additional security insights.

2.10 The Supplier will not:

2.10.1 Install, configure, or support Agents on infrastructure not managed by the Supplier.

2.10.2 Perform any remediation on infrastructure that is not managed by the Supplier, unless explicitly agreed.

2.10.3 Perform any patching on infrastructure that is not managed by the Supplier, unless explicitly agreed.

2.10.4 Guarantee that all attacks against the server will be detected and/or blocked by the Service, or accept liability for damage caused by any attacks that are not blocked by the Service.

2.11 The Supplier will not be liable for any damage or disruption to Customer infrastructure or data caused by external factors such as attempted data breaches.

2.12 The Supplier will not manage or configure any of the Customer's devices that are not explicitly included under a management contract with the Supplier. This includes, but is not limited to:

2.12.1 Security devices such as firewalls.

2.12.2 Network devices such as switches and routers.

2.13 The Supplier will not perform any remediation activities on Customer infrastructure that is not managed by the Supplier.

2.14 The Customer is expected to follow the Supplier's recommendations for the remediation of security vulnerabilities; the Supplier shall not be held responsible for any negative impact caused by security incidents where such recommendations are not followed.

2.15 Where the Customer does not follow the Supplier's remediation advice, the Supplier reserves the right to shut down any services running on shared infrastructure where, in the Supplier's opinion, those services have been or may be compromised to an extent that will impact the services of the Supplier's other customers.

2.16 The Customer will perform the following activities to ensure the correct set up and running of the Service:

2.16.1 Complete service activation questionnaires.

2.16.2 Participate in kick-off meetings to agree to the scope of the on-boarding process.

2.16.3 Confirm the minimum deployment configuration and timeline of activities.

2.16.4 Provide technical and security contacts to receive notifications and escalations.

2.16.5 Ensure that Customer-owned networks, systems, and applications within the scope of the Service are maintained and functioning properly.

2.16.6 Provide SSL certificates to the Supplier to allow access to sites that are to be protected.

2.16.7 Where any part of the Customer's network environment is not managed by the Supplier, it is the Customer's responsibility to ensure that the environment is correctly configured to enable Agent communication and secure forwarding of data required by the Service.

2.17 It is the Customer's responsibility to ensure that any collected application logs do not contain personally identifiable information or other sensitive information that for legal or regulatory reasons should not be shared.

3 Service Levels

3.1 The Supplier will use its reasonable endeavours to deliver the following Response Times in respect of incidents as set out in the table below.

Event Priority	Equivalent Security Incident Severity	Definition	Service Hours	Response Time
P1	Critical	• Total loss of production service; or • A significant revenue, operational, or safety impact on the entire company; or • Service degraded, affecting the entire company	24/7/365	Within 15 minutes
P2	High	• Partial loss of service affecting the company; or • Service degraded, affecting multiple departments or a single site; or • There is the potential of significant revenue, operational, or safety impact to the company if not resolved quickly	24/7/365	Within 30 minutes
P3		• Service degraded, affecting non-production services; or • Loss of service affecting a single user	Business Hours	Within 1 Hour
P4	Medium	• Degraded service affecting a single user	Business Hours	Within 2 Hours
P5	Low	• Request for information	Business Hours	Within 4 Hours

3.2 The Supplier will use its reasonable endeavours to deliver the following Service Levels in respect of the Services as set out in the table below.

Measure	Description	Value	Fee Credits
Service Hours	The hours during which the service and SLA is provided	24/7/365	
Availability: cloud based infrastructure	% of the service hours during which service availability is guaranteed (excluding planned maintenance)	100%	Pro rata proportion of the Monthly Charges for any Non-Availability Period
Availability: Customer-side components	% of the service hours during which service availability is guaranteed (excluding planned maintenance)	99.84%	Pro rata proportion of the Monthly Charges for any Non-Availability Period

4 Fee Credits

4.1 Any Fee Credits which fall due to paragraph 3.2 above are payable subject to and in accordance with the terms contained in the Conditions.

4.1.1 A pro rata proportion shall be calculated according to the number of complete minutes in the relevant calendar month and the number of complete minutes of Non-Availability in that calendar month.

4.1.2 “Monthly Charge” means the recurring Charges for the relevant Services for the relevant calendar month, net of VAT.

4.1.3 “Non-Availability” means a period of time during which the relevant Service is unavailable in breach of the Availability Service Levels set out in paragraph 3.2 above.

4.1.4 "Availability" means the percentage of the Service hours during which Service availability is guaranteed, not including Planned Maintenance.

4.1.5 “Availability” in this paragraph 4 and in paragraph 3.2 above refers to Availability of the Cloud Protect Defend Service infrastructure only; loss of Service due to network communication failure or failure of any part of the Customer’s infrastructure on which the Agent or Appliance is installed is specifically excluded.

4.1.6 The Supplier will not be liable for failure to meet Service Levels when the cause of failure is determined to be pre-existing vulnerabilities in place when the Supplier took on management of the Customer’s infrastructure.

4.1.7 The Supplier will not be liable for failure to meet Service Levels when the cause of failure is determined to be The Customer’s refusal, for any reason, to follow the Supplier’s advice in remediating vulnerabilities.