This Service Description provides details on what is included with PDI Security Solutions' Managed Detection and Response Essential Service. This serves as a guide to what you as a Client can expect from PDI Security Solutions, as well as what we will need from you as we work together.

The specific details of your order (e.g., the specific services, contract term, fees, etc.) will be specified in the accompanying Service Order.

1. Definitions

1.1. Alarm: An alarm is a high priority event that requires attention. When an Alarm takes place, the Client is notified with an email and a support ticket is opened for the PDI Security Solutions monitoring team to launch an investigation.

1.2. Event: An event is any observable occurrence in a system or network that meets predefined logic criteria defined by PDI Security Solutions. An example could be an outbound traffic request to a known malicious site, or an unusualWindows startup process added to a server. Custom rules can be created to identify specific events of interest.Please consult the PDI Security Solutions SOC team for any special requests.

1.3. Endpoint: An endpoint is a supported system or device which will receive the Managed Detection and Response Essential installation files. The list of supported systems, applications, and devices may change at any time, upon notice to the Client.

1.4. Service Levels: The standards PDI Security Solutions chooses to adhere to and by which it measures the level of service itprovides as specifically set forth below.

2. Service Overview

2.1. PDI Security Solutions' Managed Detection and Response Essential Service ("Service") provides a comprehensive servicethat leverages the PDI Security Solutions Cyphon platform to perform prevention, detection, and remote response capabilities for in-scope endpoints to facilitate the detection, prevention, and remediation of malicious threatsand activities within the Client's endpoints.

2.2. This Service leverages the PDI Security Solutions Cyphon platform. It uses advanced agent technology deployed on the Client's endpoints to monitor endpoint activities, events and behaviors for detection and prevention of malicious activities. PDI Security Solutions applies policies, filters, and correlation logic to these activities to identify potentialsecurity related events.

2.3. This Service includes management of the endpoint agents, event normalization/prioritization, correlation, and reporting as described in Section 4 below. The Service also includes 24x7x365 email notification for incidents as described in Section 4.3.

2.4. The Service does not include management or monitoring of any unsubscribed endpoint or intermediary log sources and it does not include hardware; technology training for end users or engineering resources or in-depth analysis, incident response, forensics, or countermeasures.

3. Service Activation and Configuration

Service activation is performed during the hours of 9 am and 5 pm EST, Monday through Friday, and may be performed at other times for an additional fee and with reasonable advance notice from the Client.

PDI Security Solutions will use up to the first 30 days post-activation to identify a baseline of the Client environment and tune theService. Tuning is a process of factoring out some of the expected noise of the Client's environment and optimizingthe Service to provide better visibility and anomaly detection.

4. Service Components

4.1 Advanced Endpoint Protection
4.2 Prioritization
4.3 Alarming
4.4 Reporting
4.5 Agent Monitoring

4.1. Advanced Endpoint Protection

PDI Security Solutions will provide a managed endpoint agent to provide Advanced Prevention, Detection and Response functionality. This endpoint agent will be wholly managed by the PDI Security Solutions SOC team, including policies for Prevention, Detection, Alerting, and Response capabilities. The PDI Security Solutions provided endpoint agent will providetraditional Anti-Virus/Anti-Malware, along with heuristic and behavioral detection and prevention for advancedthreats. PDI Security Solutions provides standard initial policies based on our experiences with Clients, that best fit the industry and organization types of the Client. Those policies are applied immediately in a protection mode andare monitored by the PDI Security Solutions SOC team for tuning or tweaks which may be necessary based on specifics ofthe Client systems.

4.2. Prioritization

PDI Security Solutions classifies security events based on the risk it presents to the Client. These events may require Clientnotification by PDI Security Solutions. PDI Security Solutions determines which event should be escalated to the Client through PDI Security Solutions'sprofessional judgment, tuning, and event correlation.

4.3. Alarming

When an alarm is detected, PDI Security Solutions will notify the Client within the time specified in the SLA. For notificationsthat are escalated to Client by the security operations center, PDI Security Solutions may also perform additional analysis to determine whether a security event indicates a security compromise. PDI Security Solutions provides the Client with a description of the event(s), and any contextual information identified during the investigation.

4.4. Reporting

Standard Reporting is included with the Service, providing reports on agent deployment and agent alerting activity. Reporting is reliant on appropriate data from the Customer, and if such data is not available, PDI Security Solutionswill be unable to produce the listed reports.

4.5. Agent Monitoring

PDI Security Solutions will notify the Client and make best efforts to assist with troubleshooting any missing agents which are not reporting back to the Cyphon platform. Troubleshooting may require web based conferencing or assistance to determine root causes for the connectivity issue. PDI Security Solutions will take best efforts to resolve, but connectivity is overall the responsibility of the Customer to resolve.

5. Customer Equipment & Software

Client agrees to (i) provide PDI Security Solutions with reasonable and safe access to the Client equipment necessary for PDI Security Solutions to perform the Services, including licenses and all associated information required to activate the devicewhich may include feature or activation codes, platform serial number or IP address, (ii) secure any licenses, approvals or consents required for PDI Security Solutions to access or use Client equipment necessary for PDI Security Solutions to perform the Service and (iii) procure all maintenance agreements specified by PDI Security Solutions for provision of the Service. PDI Security Solutions shall not maintain responsibility for cataloging or procuring hardware, licenses or maintenance contracts;responsibility for this hardware or software component lies solely with the Client.

Client is responsible for installing, maintaining, and supporting all of its end-point and intermediary log sources that provide raw log data.

Client agrees not to alter, modify or re-configure Client equipment unless such alteration is done at the request of PDI Security Solutions. If Client equipment becomes unavailable or unreachable, PDI Security Solutions will work with the Client to troubleshoot the issue to restore service. In the event that the device has failed and cannot be repaired, Client shall initiate an RMA process with the appropriate vendor to arrange for receipt of a replacement device. Once Client has a replacement on-site, PDI Security Solutions will provide reasonable remote support to Client to restore Service. Service levels do not apply until Client has replaced the failed equipment and PDI Security Solutions has established that it cancommunicate reliably with the new device.

6. Support

6.1. Support Hours

PDI Security Solutions' Security Operations Center ("SOC") is staffed from 24x7x365. Clients can contact the support team viaemail, telephone or web portals to initiate troubleshooting and support.

6.2. Authorized Users

Only authorized users provided by the Client will have access to support services.

6.3. Change Requests

Only authorized users can request changes to the Service such as changes in the alarming or event criteria.

7. Service Levels

7.1. Alarm Notification

PDI Security Solutions shall notify the Client via email of any alarm which is identified as a threat upon completion of investigation by the PDI Security Solutions SOC team. PDI Security Solutions SOC Analysts begin investigation of Critical and High classified threats within 15 minutes. Threats marked as Medium are investigated within 4 hours of initial alert.Threats marked as Low or Informational are investigated within 24 hours of initial alert.

7.2. Response Times

Critical Priority – Defined as alerts or indications of verified system attack or attempted breach

- Incident or Alert acknowledgement within fifteen (15) minutes
- Active investigation and remediation starting within thirty (30) minutes

High Priority – Defined as alerts or indications of suspected system attack or attempted breach

- Incident or Alert acknowledgement within one (1) hour
- Active investigation and remediation starting within two (2) hours

Medium Priority – Defined as alerts or indications of possible threats, with no defined indication of compromise or attack

- Incident or Alert acknowledgement within two (2) hours
- Active investigation and remediation starting within four (4) hours

Low Priority – Defined as alerts or indications resulting from daily reports or daily rulesets

- Incident or Alert acknowledgement within four (4) hours
- Active investigation and remediation starting within twenty-four (24) hours

7.3. The Service Levels set forth herein do not apply to any performance or availability issues:

- Due to factors outside PDI Security Solutions' reasonable control;
- Resulting from Client's or third-party hardware or software;
- Resulting from the actions or inactions of Client or third parties; or
- Attributable to the acts or omissions of Client, its employees, agents, or third parties acting on behalf of Client.

Furthermore, the obligations of PDI Security Solutions to comply with the Service Levels with respect to any incident response or help desk request are also interdependent on PDI Security Solutions' ability to connect directly to the Customerdevices on the Customer network through an authenticated server in the PDI Security Solutions Operations Center.

8. Additional Service Terms and Conditions

8.1. PDI Security Solutions reserves the right to modify the terms of this Service Description from time to time effective upon advance notice or upon posting of the revised terms online, provided that such changes do not have a materialadverse impact on the performance of the Service. Any such changes shall be effective upon the effective date provided in the applicable notice, or if no effective date is provided, then upon five (5) days following thedate of such notice or for a change to an online term five (5) days following posting of the revised

online terms.

8.2. PDI Security Solutions' Managed Detection and Response Essential Service provides security analysis and response to the Client. Deployment of PDI Security Solutions' Service in a Client network, however, cannot guarantee the unachievable goal of risk elimination, and therefore PDI Security Solutions makes no guarantee that intrusion, compromises,or any other unauthorized activity will not occur on a Client network.

8.3. PDI Security Solutions will monitor the deployed Service on a recurring basis for verification of adherence to the allotted subscription amounts. If PDI Security Solutions determines that Customer is overutilized or over-deployed beyond their contracted amounts or quantity, PDI Security Solutions will provide notification to the Customer and alter the subscribed andbilled quantity. Any disputes to overage will continue to be billed for the overage amount until the dispute is approved or settled, and credits may be issued dependent on the result of the dispute.