Managed Endpoint Detection and Response Service Description

PDI's Managed Endpoint Detection and Response (mEDR) Service provides 24x7x365 security monitoring and management for Customer-deployed and operational EDR solutions. PDI provides support for multiple vendor platforms such as Carbon Black, CrowdStrike, and SentinelOne.

Managed EDR Service includes a) monitoring the EDR vendor's platform for security alerts, b) investigating the validity of the alert, c) responding to identified security events, d) notifying the Customer's designated contacts of alert status and severity level and e) providing subsequent status updates on alert status. PDI maintains the vendor's EDR platform on the Customer's behalf, manages its universal blocked/allowed list(s), and stores EDR alert data for 400 days.

Service Components

Endpoint Management System Integrations with PDI

For Customers with installed and operational endpoint agents, the PDI Implementation Team collaborates with the Customer and the endpoint software vendor to integrate the Customer's EDR management system with PDI's platform for log and alert collection**.**

PDI-Provided Endpoint Agents

For Customers that use endpoint agents provided by PDI, the endpoint agents and the endpoint vendor's management systems are installed, tested, and integrated by the PDI Implementation Team. In addition, periodic endpoint agent updates (provided by the endpoint software vendor) are deployed by the PDI Service Implementation Team at no additional cost.

Dedicated Log Collection Appliances

For endpoint vendor platforms that require a dedicated log collection appliance (physical or virtual), PDI can provide both on-premise and cloud-based solutions. The type of collector PDI provides is based on several factors and requires assistance from PDI's Implementation Team to determine the type and size of collector best fitted to the Customer's network.

Threat Monitoring and Analysis

PDI's Security Operations Center (SOC) provides Customers with 24x7x365 monitoring, triage, and response for alerts generated by the Customer's EDR platform. In addition to the endpoint vendor system, the PDI SOC team utilizes additional cybersecurity tools and systems to investigate Customer logs for Indicators of Compromise (IOCs).

Remediation Guidance for Detected Threats

PDI's Security Analysts review security alerts generated by the vendor's management platform and act based on the guidance outlined in the Customer's customized Runbook. Custom Customer Runbooks allow PDI to minimize the impact on a Customer as the compromised systems are restored to operational status.

Policy Management

The PDI Security Operations Center works with the endpoint vendors to minimize false positives and false negatives. PDI also collaborates with the Customer to modify policies for improving the accuracy of their vendor's EDR platform.

Security Review

As part of the Service, PDI provides a Security Review (via myNuspire) that includes real-time service health/performance, log analytics, reporting, and recommendations. For an additional charge and at the Customer's request, PDI-guided Security Reviews include an analyst-guided review of open recommendations, service health/performance, industry-specific threat intel, and log analytics.

Case Management

As a part of the service, the Customer can open and manage cases in the myNuspire Customer Portal as well as via email and our toll-free service telephone number. For cases to be resolved, the Customer must respond to issues

raised in new cases and updates to current cases.

Letter of Agency

If PDI is providing third-party management for a Customer-licensed endpoint solution, PDI may need legal authority to (i) transition the Customer's existing EDR vendor management platform and EDR management services to PDI's Managed EDR Services and (ii) manage the Customer's EDR Services and act on behalf of the Customer when interacting with the EDR vendor. The Customer agrees to request and assist PDI in obtaining an API key from their EDR vendor to integrate the Customer's vendor management platform with PDI's vendor management platform. In many cases, a signed "Letter of Agency (LOA)" between the Customer and PDI is sufficient to procure access by PDI to the vendor management system to act on behalf of the Customer and is the responsibility of the Customer.

EDR Service Management Transition

The Customer's acceptance of this Master Service Agreement authorizes PDI to (i) Transition the Customer's existing EDR vendor management platform and EDR management services to PDI's Managed EDR Services and (ii) Manage the Customer's EDR Services and act on behalf of the Customer when interacting with the EDR vendor. The Customer agrees to request and assist PDI in obtaining an API key from their EDR vendor to integrate the Customer's vendor management platform with PDI's vendor management platform.