Managed Detection and Response Service Description

PDI's Managed Detection and Response (MDR) service offers a comprehensive 24x7x365 service to detect and respond to cybersecurity threats impacting the Customer infrastructure. PDI's expert Security Analysts enable MDR in the 24x7 Security Operations Center (SOC), and our Threat Detection and Response platform collects, analyzes, and stores log data from network and security infrastructure, servers, endpoints, and applications. The service facilitates compliance with regulatory requirements and provides an effective means to identify and mitigate security incidents.

Service Components

Service Onboarding

PDI assigns a Service Implementation Team (SIT) Engineer to ensure the successful onboarding and service delivery that meets the Customer's unique requirements. To initiate setup and onboarding, the SIT Engineer conducts crucial onboarding meetings with both the Customer and PDI Team. The onboarding phase has several objectives:

- Provide key Customer stakeholders access to the myNuspire portal
- Identify security challenges and compliance requirements unique to the Customer's organization
- Introduce the PDI people, processes, and technology capabilities and how to gain the most value from the Managed Service
- Schedule live portal training options
- Highlight reports and dashboards available for users and executives
- Assist with the deployment of sensors, configuration of alerts, reports, and dashboards

The information collected and validated during this phase includes but is not limited to the following:

- Number of endpoints, including manufacturer, model, and version level
- IP ranges and network design
- Regulatory information
    - Regulations the Customer requires to remain in compliance, and how that is reflected in their asset/network information, for example.
    - Please inform PDI of your PCI assets and how your networks are configured.
- Asset and event sources
- Preferred maintenance windows
- Policy information
- Contacts/escalation information
- Log types

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.

Log Collection and Retention

PDI utilizes different methods to collect data from the Customer's security and network infrastructure, depending on the environment. This could be via a log collection appliance deployed on the Customer premise (or in the cloud) or via API integrations between relevant applications and PDI's Threat Detection and Response platform.

PDI recommends that the Customer collect data from the following device types (at a minimum) and prioritize data collection in the following order:

- Firewalls/IPS Devices
- Advanced Endpoint Technology Solutions
- Active Directory
- Servers
- Email Gateways
- Other Security Devices

For all log data collected by PDI, log data storage is included for up to 400 days. Log data is stored in compressed archives stripped with an SHA-1 checksum and therefore tamper evident.

PDI provides logging standards based on the technology that exists in your environment and what will send logs to our platform.

If you provide technology to PDI that we have not interacted with before, we perform log analysis to ensure that event data can be used for security alerts, investigations, and hunting. From there, PDI develops a logging standard for that technology to follow and configure within your platform.

At the completion of this stage, PDI works with the Customer to complete basic testing of alerts and review of log data to ensure the service is operating as designed.

Ongoing Tuning

PDI's Threat Detection and Response platform is in learning mode for the first 30 days after service onboarding is complete. Security and business rules are fine-tuned during this time to match Customer requirements. Certain alerts may need to be switched on or off after review with the Customer. PDI's expert Security Analysts continue security rules tuning to identify new Indicators of Compromise (IOCs).

Threat Detection and Alerting

PDI's Security Operations Center (SOC) is engaged 24x7x365 to monitor, triage, and respond to security incidents. The SOC utilizes PDI's Threat Detection and Response platform to perform advanced analytics and investigate Indicators of Compromise. Examples include identifying malicious entities probing the Customer infrastructure, compromised systems, and potentially unsecured user behaviors. PDI aligns its alert framework to the MITRE ATT&CK® framework. Additionally, PDI provides unlimited incident response.

PDI SOC Runbook

An online, editable Runbook is made available for each Customer. The Runbook describes the Customer customizations implemented during the setup process and modifications after that. As a written record of customizations and preferences, the Runbook improves the quality and accuracy of security operations while optimizing response capabilities.

PDI's SOC escalates and reports security incidents from a variety of categories. In addition, a templated Incident Response (IR) Playbook is available to the Customer for customization. Such playbooks are useful to guide the Customer's IT Staff on remediation procedures and implementing automated remediation.

During the onboarding process, incidents that merit escalation to the Customer's IT Staff are determined and documented as part of the PDI SOC Runbook.

Threat Intelligence

Threat Intelligence feeds are incorporated into PDI's Threat Detection and Response platform for identifying and responding to threats. PDI's dedicated team of Threat Analysts oversees the creation, aggregation, scoring, and provisioning of actionable security intelligence.

Information is gathered from the following data and security trend analysis sources.

- **Open-Source Indicators of Compromise** - This is an intelligent aggregation of shared indicators by the cybersecurity community.
- **Social Intelligence** - Information collected via news, social media, and cybersecurity forums.
- **TAXII Feeds** - Closed/Open-source feeds that provide indicators written in a global format for integration and creation of indicators.

- **Malware Analysis** – Use of static and dynamic malware analysis to research samples in real-time and extract Indicators of Compromise.
- **Log Data** - PDI receives billions of logs a day from security devices. This information is used to discover active indicators as seen by all devices. In addition, device manufacturers' detection signatures help add context to our collected indicators or produce their own IOCs.