Managed Detection & Response (MDR) Service Definition

Purpose

To provide 24x7 monitoring, detection, and response to advanced cyber threats across the enterprise environment. MDR combines human expertise, advanced analytics, and automation to identify and contain threats quickly, reducing dwell time and minimizing business impact. The service is enhanced by CTEM for proactive exposure management and Interpres for prioritizing detection logic based on adversary behaviours.

Service Overview

MDR delivers:

- Continuous monitoring of security telemetry from endpoints, networks, cloud, and OT environments.
- Advanced analytics and threat intelligence-driven detection.
- Rapid triage and incident response with defined SLAs.
- Integration with SIEM, EDR, and SOAR platforms for automated workflows.
- Augmentation through CTEM for exposure-based prioritization and Interpres for adversary-informed detection tuning.

Key Activities

- **Threat Detection & Analysis** – Identify malicious activity using behavioural analytics and threat intelligence.
- **Incident Response** – Contain and remediate threats based on severity SLAs.
- **Threat Intelligence Integration** – Enrich alerts with global and client-specific intelligence.
- **Detection Logic Optimization** – Continuous improvement of rules and use cases.
- **CTEM Integration** – Align detection priorities with exposure management insights.
- **Interpres Augmentation** – Map detection coverage to adversary tactics and techniques for improved efficacy.
- **Reporting & Advisory** – Deliver incident reports and strategic recommendations.

Value Delivered

- **Reduced Dwell Time** – Faster detection and containment of threats.
- **Enhanced SOC Efficiency** – Minimized false positives and alert fatigue.
- **Improved Detection Coverage** – Through CTEM-driven prioritization and Interpres mapping.
- **Proactive Risk Reduction** – Aligns detection with real-world adversary behaviours.
- **Strategic Alignment** – Supports business resilience and compliance objectives.

Service Levels

- **Critical Incidents:** Initial response within 30 minutes; notification within 30 minutes.
- **High Severity:** Response within 1 hour; notification within 2 hours.
- **Medium Severity:** Response within 4 hours; notification within 1 business day.
- **Low Severity:** Included in periodic reports.
- **Availability:** 24x7 monitoring and response.

Roles & Responsibilities

- **MDR Service Manager** – Oversees delivery and SLA compliance.
- **SOC Analysts** – Investigate alerts and execute response actions.
- **Threat Intelligence Team** – Provides enrichment and context.
- **CTEM Specialists** – Identify exposure-driven priorities.
- **Interpres Analysts** – Map detection logic to adversary tactics.
- **Client Security Team** – Implements remediation and approves changes.

Dependencies

- Integration with SIEM, EDR, and SOAR platforms.
- Access to client telemetry sources and asset inventory.
- Collaboration with client IT and security teams for remediation.