Security Platform Management Service Definition

Purpose

To ensure the continuous availability, secure configuration, and optimal performance of security analytics platforms (e.g., SIEM, data lakes) that underpin Managed Security Services. This service provides operational maintenance, configuration support, and performance monitoring for in-scope security platforms, enabling reliable threat detection and response capabilities.

Service Overview

Security Platform Management covers:

- Design, deployment, and ongoing management of SIEM and related security analytics infrastructure.
- Health and performance monitoring of platforms to maintain operational readiness.
- Secure configuration management and patching to recommended standards.
- Data source connectivity verification and log continuity assurance.
- Execution of service and change requests, including user provisioning and access control.
- Troubleshooting and re-establishing connectivity between client platforms and MSSP environment.
- Advisory on platform optimization and scalability.

Key Activities

- **Platform Health Monitoring** – Review performance, capacity, and availability.
- **Connectivity Management** – Verify and restore data source and platform connectivity.
- **Configuration & Patch Management** – Maintain secure configurations and apply updates.
- **Access Control** – Provision and manage user access and permissions.
- **Change & Service Requests** – Execute standard and complex changes (e.g., dashboard updates, integration of new data sources).
- **Log Collection Optimization** – Advise on log collection configurations for cost and performance efficiency.
- **Scheduled Maintenance** – Notify clients of planned downtime at least 48 hours in advance.

Value Delivered

- High availability and reliability of security platforms.
- Improved detection and response through optimized platform performance.
- Reduced operational risk via secure configurations and proactive maintenance.
- Cost optimization through efficient log management and data retention strategies.
- Enhanced collaboration and transparency with structured change management processes.

Service Levels

Typical SLAs include:

- **Acknowledgment of critical issues:** Within 1 hour.
- **Resolution targets:** Critical issues within 4 hours; high within 1 business day; medium within 5 business days; low within 12 business days.
- **Service Requests:** Acknowledge within 8 hours; resolve within 3 business days.
- **Change Requests:** Standard changes within 5 business days; complex changes within 10 business days.

Roles & Responsibilities

- **Platform Manager** – Oversees platform operations and SLA compliance.
- **Security Engineer** – Handles configuration, patching, and troubleshooting.
- **Access Administrator** – Manages user provisioning and permissions.
- **Client Stakeholders** – Provide approvals and participate in change governance.

Dependencies

- Access to client infrastructure and platform credentials.
- Defined change management and approval workflows.
- Integration with ITSM tools for ticketing and SLA tracking.
- Availability of platform documentation and vendor support.