Security Use Case Management Service Definition

Purpose

To design, implement, and continuously optimize detection use cases that align with business risks, threat landscapes, and compliance requirements. This service ensures that detection logic remains relevant, effective, and prioritized based on real-world adversary tactics and organizational exposure.

Service Overview

Security Use Case Management provides:

- Development of detection use cases mapped to MITRE ATT&CK and business risk scenarios.
- Continuous tuning and validation of detection logic to reduce false positives.
- Integration with SIEM, EDR, and SOAR platforms for automated alerting and response.
- Augmentation through CTEM for exposure-driven prioritization and Interpres for adversary-informed coverage mapping.
- Governance and lifecycle management for use case documentation and performance metrics.

Key Activities

- **Use Case Design** – Create detection logic aligned with threat scenarios and compliance mandates.
- **Mapping to Frameworks** – Align use cases with MITRE ATT&CK, NIST CSF, and ISO 27001.
- **Validation & Tuning** – Optimize detection rules to minimize false positives and alert fatigue.
- **CTEM Integration** – Prioritize use cases based on exposure insights and attack surface analysis.
- **Interpres Augmentation** – Assess detection coverage against adversary tactics and techniques for continuous improvement.
- **Lifecycle Management** – Maintain version control, documentation, and performance metrics for all use cases.
- **Reporting & Advisory** – Provide dashboards and strategic recommendations for detection maturity.

Value Delivered

- **Improved Detection Accuracy** – Reduce false positives and enhance SOC efficiency.
- **Risk-Based Prioritization** – Focus on high-impact threats using CTEM insights.
- **Adversary-Informed Coverage** – Strengthen detection logic through Interpres mapping.
- **Compliance Alignment** – Ensure detection meets regulatory and industry standards.
- **Continuous Improvement** – Adapt detection capabilities to evolving threat landscapes.

Service Levels

- **New Use Case Development:** Delivered within agreed timelines (e.g., 10 business days).
- **Tuning & Optimization:** Performed monthly or as per SLA.
- **Reporting:** Monthly performance reports and quarterly strategic reviews.

Roles & Responsibilities

- **Use Case Manager** – Oversees design, implementation, and lifecycle governance.
- **Detection Engineer** – Develops and tunes detection logic.
- **CTEM Specialist** – Provides exposure-driven prioritization.
- **Interpres Analyst** – Maps detection coverage to adversary behaviours.
- **Client Security Team** – Reviews and approves use case deployment.

Dependencies

- Access to SIEM, EDR, and telemetry sources.
- Integration with CTEM and Interpres platforms.
- Collaboration with SOC and threat intelligence teams for validation.