Advanced Threat Hunting Service Definition

Purpose

To proactively identify and neutralize advanced threats that evade traditional detection mechanisms by leveraging hypothesis-driven hunts, behavioural analytics, and threat intelligence. This service strengthens the organization's security posture by uncovering hidden adversary activities across endpoints, networks, cloud, and OT environments. It is augmented by CTEM for exposure-driven prioritization and Interpres for adversary-informed coverage mapping.

Service Overview

Advanced Threat Hunting is a proactive security service designed to:

- Detect sophisticated threats that bypass signature-based and automated detection.
- Use MITRE ATT&CK-aligned methodologies for structured hunting.
- Correlate telemetry from multiple sources (endpoint, network, cloud, OT).
- Apply behavioural analytics and anomaly detection techniques.
- Enrich hunts with global and client-specific threat intelligence.
- Integrate CTEM insights to prioritize hunts based on exposure risk.
- Utilize Interpres to validate detection coverage against adversary tactics and techniques.

Key Activities

- **Hypothesis-Driven Hunts** – Develop and execute custom hunt hypotheses based on threat scenarios.
- **Telemetry Correlation** – Aggregate and analyze data from SIEM, EDR, and other sources.
- **Threat Intelligence Integration** – Incorporate internal and external intelligence feeds.
- **Behavioral Analytics** – Identify anomalies and patterns indicative of malicious activity.
- **CTEM Integration** – Align hunt priorities with exposure management insights.
- **Interpres Augmentation** – Map hunt coverage to adversary behaviors for continuous improvement.
- **Hunt Execution & Reporting** – Perform hunts and deliver detailed reports with findings and remediation steps.
- **Continuous Improvement** – Update detection rules and hunting playbooks based on hunt outcomes.
- **Strategic Advisory** – Provide roadmap for hunt maturity and capability enhancement.

Value Delivered

- **Reduced Dwell Time** – Accelerates detection of stealthy threats before they cause damage.
- **Enhanced SOC Efficiency** – Minimizes false positives and alert fatigue.
- **Improved Visibility** – Covers hybrid environments including endpoints, cloud, and OT.
- **Risk-Based Prioritization** – Focus hunts on high-risk exposures using CTEM insights.
- **Adversary-Informed Coverage** – Strengthen detection logic through Interpres mapping.

- **Continuous Detection Logic Improvement** – Strengthens defences against evolving attack techniques.
- **Strategic Alignment** – Aligns threat hunting with business risk priorities.

Service Levels

- **Proactive Hunts:** Conducted monthly or as per agreed cadence.
- **Reporting:** Detailed hunt reports delivered within defined timelines post-hunt.
- **Advisory Sessions:** Scheduled quarterly to review hunt outcomes and roadmap.

Roles & Responsibilities

- **Threat Hunting Lead** – Oversees hunt strategy and execution.
- **Threat Intelligence Analyst** – Provides enrichment and context for hunts.
- **CTEM Specialist** – Identifies exposure-driven priorities for hunts.
- **Interpres Analyst** – Maps hunt coverage to adversary tactics and techniques.
- **Client Security Team** – Reviews findings and implements recommendations.

Dependencies

- Access to SIEM, EDR, and telemetry sources.
- Integration with CTEM and Interpres platforms.
- Client engagement for hypothesis validation and remediation actions.