Tailored Threat Intelligence Service Definition

Purpose

To deliver customized, actionable threat intelligence aligned with the client's industry, technology stack, and risk profile. This service enhances situational awareness and enables proactive defence against emerging threats targeting the organization's environment. It is augmented by CTEM for exposure-driven prioritization and Interpres for adversary-informed intelligence mapping that strengthens MDR and detection strategies.

Service Overview

Tailored Threat Intelligence provides:

- Continuous monitoring of global threat landscapes and adversary tactics.
- Intelligence enrichment specific to client assets, geographies, and business operations.
- Integration of threat intelligence into detection and response workflows.
- Augmentation through CTEM to prioritize intelligence based on exposure risk.
- Utilization of Interpres to map intelligence to adversary behaviours and improve detection coverage.
- Strategic advisory for threat-informed risk management and security posture improvement.

Key Activities

- **Threat Landscape Monitoring** – Track global and sector-specific threat trends.
- **Adversary Profiling** – Identify threat actors targeting client's industry and region.
- **Customized Intelligence Feeds** – Deliver curated intelligence relevant to client's environment.
- **CTEM Integration** – Align intelligence priorities with exposure insights and attack surface analysis.
- **Interpres Augmentation** – Validate intelligence coverage against adversary tactics and techniques.
- **Integration with SOC Operations** – Embed intelligence into SIEM, EDR, and SOAR workflows.
- **Threat Reports & Alerts** – Provide timely intelligence reports and actionable alerts.
- **Campaign Tracking** – Monitor ongoing threat campaigns and emerging attack vectors.
- **Strategic Advisory** – Recommend mitigation strategies based on intelligence insights.

Value Delivered

- **Proactive Defense** – Anticipate and mitigate threats before they materialize.
- **Enhanced Detection** – Improve SOC efficiency with enriched context for alerts.
- **Risk-Based Prioritization** – Focus on high-impact threats using CTEM insights.
- **Adversary-Informed Coverage** – Strengthen detection logic through Interpres mapping.
- **Strategic Decision Support** – Inform security investments and risk management strategies.
- **Continuous Improvement** – Adapt defences to evolving threat actor tactics.

Service Levels

- **Intelligence Delivery:** Daily or weekly feeds based on client requirements.
- **Reporting:** Monthly strategic threat landscape reports.
- **Advisory Sessions:** Quarterly reviews to align intelligence with business priorities.

Roles & Responsibilities

- **Threat Intelligence Lead** – Oversees intelligence collection and dissemination.
- **Analyst Team** – Curates and validates intelligence for relevance and accuracy.
- **CTEM Specialist** – Provides exposure-driven prioritization for intelligence application.
- **Interpres Analyst** – Maps intelligence to adversary behaviours for improved detection.
- **Client Security Team** – Consumes intelligence and implements recommended actions.

Dependencies

- Access to client asset inventory and risk profile.
- Integration with SIEM/SOAR platforms for automated intelligence application.
- Collaboration with SOC and incident response teams for operationalization.