Endpoint Security Service Definition

Purpose

The Endpoint Security Service protects organizational endpoints against malware, ransomware, credential theft, exploitation, and advanced adversary techniques. It provides continuous prevention, detection, response, and hardening by leveraging EDR/XDR technology, threat intelligence, behavioural analytics, and automated containment. The service strengthens endpoint resilience across Windows, Linux, macOS, mobile, and server environments, aligned with emerging threats and business risk.

Service Overview

The Endpoint Security service is designed to:

- Prevent and detect known and unknown malware.
- Provide real-time endpoint telemetry across devices.
- Use behavioural and ML-based analytics for anomaly detection.
- Automatically isolate compromised hosts to minimize lateral movement.
- Provide visibility into endpoint vulnerabilities and misconfigurations.
- Enrich detections using global + client-specific threat intelligence.
- Integrate with CTEM for exposure-based prioritization.
- Map endpoint detection coverage against MITRE ATT&CK techniques.
- Support rapid response actions: quarantine files, kill processes, block hashes, and revoke credentials.

Key Activities

- **Endpoint Protection & Prevention -** Deploy EDR/XDR agents to enable anti-malware, anti-ransomware, exploit mitigation, and behavioural blocking.
- **Continuous Telemetry Collection -** Collect granular process, registry, network, identity, and file telemetry for advanced analysis.
- **Threat Intelligence Integration -** Enrich detection logic with internal and external intelligence sources, aligning with evolving TTPs.
- **Real-Time Detection & Response -** Detect malicious behaviour and execute automated/manual response actions including host isolation, process termination, and containment.
- **Exposure-Driven Prioritization (CTEM) -** Leverage CTEM insights to prioritize endpoint vulnerabilities, misconfigurations, and high-risk assets.
- **MITRE ATT&CK Coverage Mapping -** Validate endpoint detection coverage against adversary TTPs using Interpres-aligned methodologies.
- **Patch & Configuration Hygiene Support -** Identify missing patches, weak configurations, and insecure applications for remediation.
- **Incident Investigation & Forensics Support -** Provide endpoint-level forensics, timeline review, and root-cause analysis when incidents occur.

- **Reporting & Recommendations -** Deliver reports outlining detections, response actions, coverage gaps, and recommended improvements.
- **Continuous Improvement -** Enhance detection rules, prevention policies, and endpoint hardening based on attack trends and incident learnings.

Value Delivered

- **Reduced Risk of Compromise** – Prevents malware, ransomware, and credential theft.
- **Rapid Containment** – Automated host isolation limits adversary movement.
- **Improved Visibility** – Deep insight into endpoint activity and attack behaviours.
- **Lower SOC Load** – Reduces false positives and enriches investigations.
- **Exposure-Driven Endpoint Prioritization** – Focuses remediation on high-risk devices.
- **Adversary-Aligned Coverage** – Strengthens endpoint defences against real-world threats.
- **Continuous Hardening** – Ongoing policy tuning improves resilience.
- **Integrated Response** – Seamless collaboration between SOC, threat intel, and endpoint engineering.

Service Levels

- **Continuous Endpoint Monitoring:** 24/7 detection and response via EDR/XDR.
- **Automated Response Actions:** Host isolation, process kill, hash blocking as per policy.
- **Monthly Posture Reports:** Detection trends, vulnerabilities, misconfigurations, and improvements.
- **Quarterly Security Advisory Sessions:** Endpoint security posture and roadmap reviews.

Roles & Responsibilities

- **Endpoint Security Lead -** Owns endpoint security strategy, policy tuning, and service governance.
- **SOC Analysts (L1/L2/L3) -** Monitor, triage, investigate, and respond to endpoint security alerts.
- **Threat Intelligence Analyst -** Provides IOC, IOA, and adversary-specific insights to enhance endpoint detections.
- **CTEM Specialist -** Identifies exposure-driven endpoint weaknesses for prioritization.
- **Interpres Analyst -** Evaluates endpoint detection coverage against adversary behaviours.
- **Client Endpoint & Security Teams -** Manage patching, configuration changes, and remediation of endpoint risks.

Dependencies

- Endpoint agents deployed and operational on in-scope devices.
- Integration with SIEM, EDR/XDR platform, and telemetry pipelines.
- Access to CTEM and adversary-coverage tooling where applicable.
- Client participation for remediation activities and policy approvals.