Cyber Health Metrics - Metric Development

Establishing Criteria for Selecting Metrics:

Selecting the right metrics is crucial for effective cybersecurity management in SMEs. To ensure we choose metrics that are both meaningful and actionable, we've established the following criteria:

1. **Relevance:** The metrics we pick should have a clear connection to the goals and range of cybersecurity for SMEs. This implies that they tackle the problems and needs encountered by small to medium-sized enterprises in safeguarding their digital assets and operations. Through the lens of importance, we can select metrics that are aligned with our organization's objectives and key focus areas.
2. **Measurability:** Metrics need to be measurable and countable, allowing for a clear and objective assessment that can be compared over time. This is important so we can accurately follow how well our cybersecurity methods are working and find places where we need improvements. Measurable metrics offer quantifiable data that help us to track advancement, decide on how resources are distributed and manage risks.
3. **Consistency:** For measuring cybersecurity performance, consistency is important to guarantee dependability and steadiness. The metrics must give consistent outcomes when used again and again, no matter if there are alterations in circumstances or surroundings. Tracking over time: Consistency with metrics allows for the tracking of trends and patterns across different periods, making it easier to perform significant analysis and understanding of cybersecurity data. Through focusing on consistency, we ensure that our metrics are dependable in giving correct views about how well our cybersecurity actions and projects work.
4. **Actionability:** Metrics must have an action element, which implies that they offer understandings prompting certain actions or methods to improve cybersecurity position. Usable metrics give those involved the power to make knowledgeable choices and apply focused tactics for reducing dangers and improving safety.
5. **Accessibility:** The metrics must be usable and accessible by the appropriate stakeholders. They should guarantee that important people who make decisions can get access to relevant cybersecurity data on time. Accessibility involves aspects like how easy it is to collect data, reporting methods and if tools or resources needed for analysing and interpreting metric results are available.
6. **Scalability:** Scalable metrics can handle changes in the size of an organization, its complexity and technological structure. This ability to scale up is important for metrics as it means they are flexible enough to adjust with growth or other alterations without losing their effectiveness and accuracy.
7. **Cost-effectiveness:** The metrics must be inexpensive to gather, gauge, and examine. This way we can reduce the number of resources needed while increasing the value from cybersecurity investments. A metric that is cost-effective allows SMEs to distribute their limited resources in an efficient manner and put emphasis on activities which have a bigger effect on security positioning.

Template for Documenting Metrics:

Metric Name: Name of the metric for easy identification.

Description: Brief description of what the metric measures and its significance.

Measurement Method: Explanation of how the metric is calculated or assessed.

Data Source: Source of data used to derive the metric.

Frequency: Frequency of measurement or assessment (e.g., daily, weekly, monthly).

Responsibility: Individual or team responsible for collecting and monitoring the metric.

Thresholds/Targets: Benchmark values or targets for the metric to indicate desired performance levels.

Trend Analysis: Analysis of trends over time to identify patterns or changes in cybersecurity performance.

Action Plan: Plan of action in response to metric results, including remediation or improvement strategies.

Pilot Metric for Cybersecurity Domains

1. **Security Posture Assessment:**
    - Metric: Vulnerability Scan Count
    - Description: Number of vulnerability scans conducted to assess security posture.
    - Measurement Method: Counting the total number of vulnerability scans performed within a specific period.
    - Data Source: Vulnerability scanning tools or platforms.
    - Frequency: Weekly.
    - Responsibility: IT security team.
    - Thresholds/Targets: Conduct at least one vulnerability scan per week.
    - Trend Analysis: Monitor changes in vulnerability scan count to identify trends in security posture assessment.

2. **Incident Response Readiness:**
    - Metric: Mean Time to Detect (MTTD)
    - Description: Average time taken to detect security incidents.
    - Measurement Method: Calculating the average duration between the occurrence of a security incident and its detection.

- Data Source: Incident response logs or tracking systems.
- Frequency: Monthly.
- Responsibility: Incident response team.
- Thresholds/Targets: Maintain MTTD below a predefined threshold (e.g., 24 hours).
- Trend Analysis: Analyse changes in MTTD over time to assess improvements in incident response readiness.

3. **Compliance and Regulatory Adherence:**
    - Metric: Compliance Score
    - Description: Assessment of compliance with relevant cybersecurity regulations and standards.
    - Measurement Method: Scoring based on adherence to regulatory requirements and industry standards.
    - Data Source: Compliance audit reports or assessments.
    - Frequency: Quarterly.
    - Responsibility: Compliance team.
    - Thresholds/Targets: Achieve a compliance score of at least 90%.
    - Trend Analysis: Track changes in compliance score to monitor progress in regulatory adherence.

4. **Risk Management Effectiveness:**
    - Metric: Risk Exposure Score
    - Description: Assessment of the organization's exposure to cybersecurity risks.
    - Measurement Method: Calculation based on the severity and likelihood of identified risks.
    - Data Source: Risk assessment reports or risk management platforms.
    - Frequency: Biannually.
    - Responsibility: Risk management team.
    - Thresholds/Targets: Maintain risk exposure score below a predefined threshold.
    - Trend Analysis: Analyse changes in risk exposure score to identify emerging risks and assess the effectiveness of risk management strategies.

5. **Infrastructure Resilience:**
    - Metric: Mean Time to Recovery (MTTR)
    - Description: Average time taken to restore critical systems and services after a cybersecurity incident.
    - Measurement Method: Calculating the average duration between the occurrence of an incident and the full restoration of affected systems.
    - Data Source: Incident response and recovery logs.
    - Frequency: As needed (after incidents).
    - Responsibility: IT operations team.
    - Thresholds/Targets: Achieve MTTR within predefined timeframes based on criticality of systems.
    - Trend Analysis: Monitor changes in MTTR to evaluate improvements in infrastructure resilience.

6. **Threat Intelligence Integration:**
    - Metric: Threat Intelligence Feeds Integrated
    - Description: Number of threat intelligence feeds integrated into security operations.
    - Measurement Method: Counting the total number of threat intelligence feeds integrated.
    - Data Source: Threat intelligence platforms or feeds.
    - Frequency: Quarterly.
    - Responsibility: Threat intelligence team.
    - Thresholds/Targets: Integrate a minimum number of new threat intelligence feeds each quarter.
    - Trend Analysis: Track changes in the number of integrated threat intelligence feeds to assess the enhancement of threat detection and response capabilities.

The validation process confirms that the selected metrics effectively assess cybersecurity domains in alignment with the organization's mission. The Security Posture Assessment metric prompts regular vulnerability scans managed by the IT security team, ensuring consistency and scalability across organizations. Incident Response Readiness, measured by Mean Time to Detect (MTTD), maintains monthly consistency and accessibility through the incident response team, supporting scalable application. Compliance and Regulatory Adherence metrics, assessed quarterly by the compliance team, target specific compliance scores, facilitating scalability across diverse regulatory environments. Risk Management Effectiveness, measured biannually, maintains accessibility through the risk management team, ensuring consistent and scalable application across varying risk profiles. Infrastructure Resilience, quantified by Mean Time to Recovery (MTTR) as needed after incidents, managed by the IT operations team, supports scalability across different infrastructure complexities. Threat Intelligence Integration, evaluated quarterly by the threat intelligence team, ensures scalability and adaptability across organizations of varying sizes, emphasizing cost-effectiveness.

The finalization of the metrics list signifies the culmination of a thorough process to select metrics aligned with the organization's mission of democratizing cybersecurity threat intelligence. Through validation, each metric has been confirmed to be relevant, measurable, actionable, and cost-effective, ensuring their effectiveness in assessing cybersecurity posture. These finalized metrics provide a cohesive framework for organizations to enhance their cyber resilience, detect threats, and contribute to collective defence efforts.