TLP:CLEAR

Metrics for the Computer Security Incident Response Team (CSIRT) Services Framework

Version 1.0 – January 2026

Notice: This document describes what the Forum of Incident Response and Security Teams, Inc. (FIRST.Org) believes are best practices. These descriptions are for informational purposes only. FIRST.Org is not liable for any damages of any nature incurred as a result of or in connection with the use of this information.

Table of Contents

CSIRT Services Framework with Metrics

1 Introduction

The **CSIRT Services Framework Metrics** document is designed to complement the *FIRST CSIRT Services Framework v2.1*, a widely adopted reference model that defines the services, functions, and activities commonly performed by Computer Security Incident Response Teams (CSIRTs). The FIRST Framework provides a structured and technology-agnostic description of CSIRT service capabilities, but it does not prescribe how to measure the performance, effectiveness, or operational quality of those services.

This metrics document, created by the FIRST Metrics SIG, fills that gap. Its purpose is to define a practical, structured set of quantitative and qualitative metrics that organisations can use to assess, track, and improve the services described in the FIRST Framework. The metrics do not alter or reinterpret the underlying framework; instead, they build upon it by adding measurable indicators that align directly with each service function. In each case, we have aimed to list metrics that are meaningful, practical, and straightforward to understand.

Because organisations vary widely in mission, maturity, tooling, and resourcing, the metrics in this document are intended to be adaptable rather than prescriptive. Each metric includes a description, type, required data, and suggested measures, but individual organisations may tailor the metrics, adjust thresholds, or select alternative statistical methods as appropriate for their environment.

Used together, the two documents offer a comprehensive approach to understanding, managing, and improving CSIRT operations. The Framework describes *what* a CSIRT does; the Metrics document supports measuring *how effectively* those services are being delivered.

Note:

The scope of this release intentionally covers Service Areas through Section 7 of the CSIRT Services Framework; metrics for the remaining Service Areas, Sections 8 and 9, will be completed in a subsequent version of this document.

This initial version of the Metrics for the CSIRT Services Framework reflects current practitioner experience and the varying maturity of CSIRT operations, which may result in differences in depth or presentation across service areas. Future revisions are expected to further normalize structure, terminology, and level of detail based on community feedback and practical use.

We welcome comments and feedback.
Please direct your email to *framework-metrics[@]first.org*.

2 Structure

To maintain clarity and interoperability, this document follows the same hierarchical structure as the FIRST Framework. Each metric is labelled using the corresponding section numbering (for example, 5.1.1.1 indicates the first metric for function 5.1.1). This cross-referencing makes it possible to use both documents together: the Framework provides the conceptual model, while this metrics document provides the means to evaluate how well that model is being executed in practice. In some cases, we have used x.0.0.x for metrics at the *service area*, not *functional*, level.

Note that the high-level section numbering omits Sections 3 and 4. This is by design, to ensure correlation with the CSIRT Services Framework, where Service Area numbering starts at Section 5.

2.1 Key Elements in the CSIRT Services Framework

The framework for CSIRT services is based on the relationships of these key elements:

SERVICE AREAS – SERVICES – FUNCTIONS

These elements are defined as:

SERVICE AREAS

Service areas group services related to a common aspect. They help to organize the services along a top-level categorization to facilitate understanding and communication.

SERVICES

A service is a set of recognizable, coherent functions oriented towards a specific result. Such results may be expected or required by constituents or on behalf of or for the stakeholder of an entity.

FUNCTIONS

A function is an activity or set of activities aimed at fulfilling the purpose of a particular service.

2.2 Additional Element in this Metrics Document

This document includes an additional element – Metrics – resulting in:

SERVICE AREAS – SERVICES – FUNCTIONS – METRICS

Each defined metric relates specifically to its function in the CSIRT Service Framework.

2.3 Conventions

The following conventions apply throughout this document to promote clarity and consistency across all service areas and metrics:

- **Metric titles** use sentence case, with only the first word capitalized.
- **Metric identifiers** follow the numbering of the CSIRT Services Framework (for example, *5.1.1.2*) and are used consistently for cross-reference. Additionally, we have defined some Service Area, and Service level metrics, in which cases the number schemes are x.0.0.x and x.0.x.x
- **Data requirements** within each metric are listed as N1, N2, N3, and so on, and this numbering resets for every metric.
- **Data completeness**: All data elements required for understanding or calculating a metric are included within that metric's own data requirements section.
- **Notes section**: Each metric may include optional notes to clarify use cases, interpretation considerations, or implementation boundaries.
- **Metric types**: Each metric identifies a type (for example, *Efficiency*, *Effectiveness*, *Quality*, or *Coverage*). These types are descriptive and not intended to impose analytical constraints.
- **Neutral framing**: Metrics are written to be technology-agnostic and organisationally neutral so that teams can adapt them to their own tooling, workflows, and maturity levels.

2.4 Metrics Table Template

The template below is used as a standard definition for each metric.

Metric Attribute	Details
Name	*This is the exact name of the metric. It should match the name that is in the section heading.*
Description	*Provide a detailed description of the metric. How does it relate to the function? What is the intent? Anything that will clarify how this metric is to be used.*
Type	*See Section 2.5 for detailed descriptions of the metrics types.*

Metric Attribute	Details
Data Required	*Note the specific data points that will be required to calculate this metric. Each individual data point should be a discrete number from which a clear calculation can be made.*
Calculation	*The formula to be used with the above data points to create the metric. The result should be numeric.*
Measure	*This should be one of {Percentage, Mean, Median, Number, Ratio}*
Notes	*Any additional notes that may provide further clarification on this metric. Often this may include comments on the level of effort required for creating this metric. It may include additional insights into why this metric was included, or how to use it. In some cases, we have included sample target ranges.*

2.5 Types of Metrics

We use four types of metrics, directly based on the NIST Measurement Guide for Information Security. These types help ensure the correct focus for each measurement.

Following is the definition of each:

Implementation measures demonstrate the progress of specific controls. Monitoring implementation may include assessment results, such as a tally of known systems or a binary "yes/no" about which systems have up-to-date patches. Implementation measures look at quantitative outputs and are usually demonstrated in percentages.

Effectiveness measures evaluate how well implementation processes and controls are working and whether they are meeting the desired outcome. An effectiveness assessment can either concentrate on the evidence and results of a quantitative analysis of measures or be applied in a qualitative "yes/no" paradigm.

Efficiency measures examine the timeliness of controls by determining the speed at which they give useful feedback, and how quickly those issues are addressed.

Impact measures articulate the impact of information security on an organisation's unique mission, goals, and objectives including change quantification on areas such as business value, cost savings, trust scores, etc.

2.6 Notes on Statistical Analysis Methods

Unless otherwise specified, the metrics in this document do not prescribe the use of a particular statistical method. In cases where no method is indicated, organisations may analyse the resulting values using common approaches such as mean, median, percentile distributions, or other summary statistics that best reflect their operational environment.

Where a specific statistical method is recommended, it should not be viewed as restrictive. Raw values may still be trended over time, and alternative statistical techniques may be applied when they provide clearer insight or greater analytical value.

Note: Top level numbering now skips to Section 5 to maintain correlation with the CSIRT Services Framework

5 Service Area: Information Security Event Management

5.1 Service: Monitoring and detection

5.1.1 Function: Log and sensor management

Metrics: The following metrics are defined for this function:

- Sensor / source availability
- Sensor / source criticality definition

5.1.1.1 Metric: Sensor / source availability

Metric Attribute	Details
Name	Sensor / source availability
Description	This metric is designed to help ensure that sensors are appropriately available for generating and reporting security events. Without monitoring availability, it is difficult or impossible to assure that your SIEM has a complete data set, which is critical for monitoring and investigations.
Type	Effectiveness
Data Required	(N1) Binary indicators of individual sensors' availability, measured over discrete time intervals, e.g. every 5 minutes This number can be gathered in a variety of manners; try to pick a method that most likely guarantees data is being transmitted appropriately. (N2) Number of reporting intervals (may be user selected)
Calculation	(N1) / (N2) * 100
Measure	Percentage
Notes	Possible availability targets: ● Fully available (e.g., 24x7) ● Expected Available (e.g., 8x5 or as planned) Exclude planned outages per log source type, per criticality.

	Organisations might have different sensor availability requirements for different periods (like operations peaks, non-working hours). Then a few sensors' availability metrics can be measured for the same sensor.

5.1.1.2 Metric: Sensor / source criticality definition

Metric Attribute	Details
Name	Sensor / source criticality definition
Description	To manage sensor availability and outage response time, a criticality definition should be defined for each sensor. The criticality levels can be defined in any manner to suit your business (e.g., P1, P2, P3 vs. high, medium, low.) The important idea here is that the criticality labels are applied across the full distribution environment.
Type	Implementation
Data Required	(N1) Number of sensors (N2) Number of sensors with criticality level defined
Calculation	N2 / N1 * 100
Measure	Percentage
Notes	

5.1.2 Function: Detection use case management

Metrics: The following metrics are defined for this function:

- Detection coverage against threat TTPs
- Instruction coverage against number of detection use cases
- False positives ratio per detection use case

5.1.2.1 Metric: Detection coverage against threat TTPs

Metric Attribute	Details
Name	Detection coverage against threat TTPs
Description	By measuring detection use case coverage against TTPs of threats you have determined to be relevant in a risk-oriented way, it is possible to measure how well your use cases are performing against those TTPs derived from your threat assessment.
Type	Effectiveness
Data Required	(N1) Count of TTPs relevant for your organisation (N2) Count of your detection use cases mapped to corresponding TTPs
Calculations	N2 / N1 * 100
Measure(s)	Percentage
Notes	We recommend using the MITRE ATT&CK framework for your threat assessment. We recommend adding and taking into consideration a criticality definition on the TTP matrix to help analyse where to apply resources.

5.1.2.2 Metric: Instruction coverage against number of detection use cases

Metric Attribute	Details
Name	Instruction coverage against number of detection use cases
Description	This is a simple metric to help indicate how well your detection coverage is organized, by counting how many of your detection use cases have instructions for analysts defined.
Type	Implementation
Data Required	(N1) Number of detection use cases (N2) Number of detection use cases with instructions
Calculation	N2 / N1 * 100

Metric Attribute	Details
Measure	Percentage
Notes	Having identifiers for your detection use cases corresponding with identifiers for your instructions will help.

5.1.2.3 Metric: False positive ratios per detection use case

Metric Attribute	Details
Name	False positive ratios per detection use case
Description	The ratios of false positives within detection use cases can help identify those use cases that may benefit from tuning. This metric provides two ratios – one against all verdicts, and one against only true positive verdicts
Type	Effectiveness
Data Required	For each detection use case: (N0) total number of events (N1) total number of events with True Positive verdict (N2) total number of events with False Positive verdict
Calculations	N2 / N0 * 100 This is the percentage of false positives for all detections N2 / N1 * 100 This is the ratio of false positive to true positives
Measure	Percentage Ratio
Notes	

5.1.3 Function: Contextual data management

Metrics: The following metric is defined for this function:

- Quality of contextual data

5.1.3.1 Metric: Quality of contextual data

Metric Attribute	Details
Name	Quality of contextual data
Description	Quality defined by percentage of incorrect information received from the external sources providing contextual information. We measure this by counting the number of errors received for the queries launched. These errors can be due to different causes, for example, source unavailability, allowed query limit exceeded, or detected mistakes.
Type	Effectiveness
Data Required	(N1) Number of queries for context (N2) Number of errors
Calculation	N2 / N1 * 100
Measure	Percentage
Notes	Determining incorrectness (number of errors) can be difficult and likely to occur downstream from contextual data use.

5.2 Service: Event analysis

5.2.1 Function: Correlation

Metrics: The following metric is defined for this function:

- Mean manual alert correlation

5.2.1.1 Metric: Mean manual alert correlation

Metric Attribute	Details
Name	Mean manual alert correlation
Description	The goal of this metric is to evaluate the efficiency of our alert correlation capabilities, to support efficient event analysis. To measure this, we examine how many alerts require manual correlation for each incident. This indicates the number of correlations that are missed pre-triage.
Type	Efficiency
Data Required	(N1) Number of alerts manually correlated with each incident (manual duplicates)
Calculation	Calculate manual alert correlation level (CL) for each incident as 1 / N1 (pct) Calculate the mean of the CL (mCL).
Measure	Mean
Notes	Higher mCL is better

5.2.2 Function: Qualification

Metrics: The following metrics are defined for this function:

- Completeness of qualification documentation for alerts triage
- Time to acknowledge alerts and incident reports
- Ratio of true-positives to false-positives
- Time to detect incident

5.2.2.1 Metric: Completeness of qualification documentation for alerts triage

Metric Attribute	Details
Name	Completeness of qualification documentation for alert triage
Description	Each qualification should have documentation explaining the verdict choice.
Type	Implementation
Data Required	(N1) Number of alerts triaged (N2) Number of alerts with qualification documentation
Calculation	N2 / N1 * 100
Measure	Percentage
Notes	Will likely need to gather the data required via sampling.

5.2.2.2 Metric: Time to acknowledge alerts and incident reports

Metric Attribute	Details
Name	Time to acknowledge alerts and incident reports
Description	Consistent reaction times to alerts within risk appetite is an indicator to investigate how well the analysts doing the job are equipped and staffed to handle the job expected of them by the organisation. Also, alerts urgency can be a significant factor in the success of your mission.
Type	Implementation
Data Required	(T1) Time at which the alert report is raised (T2) Time at which the report is acknowledged and analysis is started, either by human or machine
Calculation	T2 - T1 (time to acknowledge)
Measure	Number
Notes	It is highly recommended to have timings of alert creation and acknowledgement recording by machine or system.

Metric Attribute	Details
	You will want to analyse the collection of Time to Acknowledge values across a time slice. You may want to analyse per alert type, analyst, or another attribute.

5.2.2.3 Metric: Ratio of true-positives to false-positives

Metric Attribute	Details
Name	Ratio of true-positives to false-positives
Description	Measured at the closure of the alerts, True-positives versus False-positives ratio
Type	Effectiveness
Data Required	(N1) Count of true-positive alerts (N2) Count of false-positive alert
Calculation	N1 / N2
Measure	Ratio
Notes	The higher ratio is the more effective ("producing a result that is wanted") detection rules are inspired by reading Threat detection metrics: exploring the true-positive spectrum | by Alex Teixeira. One noted difficulty is ensuring that we have a clear definition and timely marking of what is false-positive and true-positive.

5.2.2.4 Metric: Time to detect

Metric Attribute	Details
Name	Time to detect
Description	Indicates how fast incident detection toolset generates alert or incident from processed log sources
Type	Efficiency

Metric Attribute	Details
Data Required	(N1) The time at which the event itself first occurred (N2) The time at which the event was detected
Calculation	N2 - N1
Measure	Number
Notes	Evaluate this metric to generate statistical analyses over time and type. Note that not all log sources are consolidated instantly, but rather a pulling method is used, focusing on such a metric requires understanding the impact of more frequent polling. Refer to Security Incident Timing Metrics on the FIRST Portal.

6 Service Area: Information Security Incident Management

6.1 Service: Information security incident report acceptance

6.1.1 Function: Information security incident report receipt

Metrics: The following metrics are defined for this function:

- Time to acknowledge incident reports
- Percentage of acknowledged reports

6.1.1.1 Metric: Time to acknowledge incident report receipt

Metric Attribute	Details
Name	Time to acknowledge incident report receipt
Description	Measuring reaction times to incident reports can be used to investigate how well the analysts doing the job are equipped and staffed to handle the job expected of them by the organisation. Also, for some alerts urgency can be a significant factor in the success of your mission.
Type	Efficiency
Data Required	(N1) Time at which the initial incident report received (N2) Time at which acknowledgement of that receipt was sent
Calculation	N2 - N1
Measure	Number
Notes	Evaluate this metric to generate statistical analyses such as median over time and type of incident.

6.1.1.2 Metric: Percentage of reports that are acknowledged

Metric Attribute	Details
Name	Percentage of Reports that are Acknowledged
Description	This is an easy metric to track report acknowledgement, ensuring processes can be evaluated to avoid having reports fall through the cracks.
Type	Effectiveness
Data Required	(N1) Number of reports (N2) Number of reports acknowledged
Calculation	N2 / N1 * 100
Measure	Percentage
Notes	

6.1.2 Function: Information security incident triage and processing

Metrics: The following metrics are defined for this function:

- Percentage of quality issues in triage instances
- Time from incident receipt to triage completion

6.1.2.1 Metric: Time from incident receipt to triage completion

Metric Attribute	Details
Name	Time from incident receipt to triage completion
Description	This metric can be used to track the amount of time involved in triage activities. By tracking triage durations you can spot trends, compare entities, and analyse your data for efficiency improvements. We caution against setting targets for triage completion due to the risk of negative impact on quality.
Type	Effectiveness
Data Required	(N1) The point in time when the security event is available for triage (N2) The point in time when the triage is completed

Metric Attribute	Details
Calculation	N2 - N1
Measure	Number
Notes	This metric will be most useful when analysed across a variety of attributes such as event report source or analyst team. You can also use receipt acknowledgement as the starting point for this metric if it is more appropriate for your organisation. Refer to Security Incident Timing Metrics on the FIRST Portal

6.1.2.2 Metric: Percentage of quality issues in triage instances 🔗

Metric Attribute	Details
Name	Percentage of quality issues in triage instances
Description	Like section 5.2.2, this function includes triaging activity during which verdict, categorization, and prioritization may be assigned. Use this metric to evaluate the quality of this function's output, with the intent of improving functional processes as needed.
Type	Implementation
Data Required	(N1) Number of potential security incidents evaluated (N2) Number of errors in triage processing
Calculation	(N2 / N1) * 100
Measure	Percentage
Notes	Shows quality - if the rate is above the set target threshold determine improvement needed, e.g. additional triage training or improved automation. For simplicity this metrics groups multiple attributes into quality issues. Group or ungroup attributes according to your preference. "Errors" and "Reported Deficiencies" are alternate terms for quality issues.

6.2 Service: Information security incident analysis

6.2.1 Function: Information security incident triage (prioritization and categorization)

Metrics: The following metrics are defined for this function:

- Error rate of incident triage
- Incidents with altered priority

Note: Section 6.2.1 implies that an initial assessment of an information security incident might already be included in a previous step. The information may have been provided to the CSIRT via one of the following channels:

- CSIRT communication channels, in which case may or may not have qualification completed. [refer to Section 6.1.1- Information Security Incident Report receipt]
- Internal detection and monitoring capability [refer to Section 5.2.2 - Event Analysis: Qualification]

In the above case, qualification has already been accomplished and metrics from those sections may have already been applied.

If the initial assessment has not been completed, then perform the qualification and apply the metrics 5.2.2.1-4 and 6.2.1.1-2 (where it makes sense).

We have added metrics 6.2.1.1-2 as specific to this section.

6.2.1.1 Metric: Error rate of incident triage

Metric Attribute	Details
Name	Error rate of incident triage
Description	Ensure that incidents have been triaged according to the Security Incident Response Policy to improve the quality of the incident triage.
Type	Effectiveness
Data Required	(N1) The number of information security incidents where triage has been performed.

Metric Attribute	Details
	(N2) The number of information security incidents for which a subject matter expert review revealed triage was not done correctly according to policy.
Calculation	(N2) / (N1) * 100
Measure	Percentage (lower is better)
Notes	This metric expects that there is a process in which a subject matter expert reviews security incidents to validate the effectiveness of incident triage regarding categorization. This may not always be the case. Risk and compliance environments vary in organisations. You should define what areas of the triage attributes that matters most to you, make it part of your SME review process and consider collecting data for each one to have a more granular understanding of what parts of your triage function are more prone to errors. Example: An expert review process collecting data on categorisation and initial prioritization could reveal that triage fails half the time and it is always the initial prioritization and never the categorization that fails, pinpointing where you should put your effort.

6.2.1.2 Metric: Incidents with altered priority

Metric Attribute	Details
Name	Incidents with altered priority
Description	Number of Security Incidents that have their prioritization changed in their lifecycle
Type	Efficiency
Data Required	(N1) Number of security incidents with altered priority
Calculation	N1

Metric Attribute	Details
Measure	Number
Notes	It may be difficult to have an accurate history of how many times the priority for an incident may have changed. Although changes to an incident's priority during its lifecycle are a valid activity, by analysing the incidents whose priority changed, a team can dig deeper into why this is happening. For example, additional data during triage may help analysts set the priority correctly.

6.2.2 Function: Information collection

Metrics: The following metrics are defined for this function:

- Accuracy of information data sources
- Chain of custody compliance
- Completeness of contextual data

6.2.2.1 Metric: Accuracy of information data sources

Metric Attribute	Details
Name	Accuracy of information data sources
Description	Assess the reliability and accuracy of information sources providing data and details regarding the security incident.
Type	Effectiveness
Data Required	(N1) Number of data sources and stores used in your incident (N2) Number of data sources and stores where data accuracy has been validated
Calculation	N2 / N1 * 100 (percentage)
Measure	Percentage
Notes	It may be difficult to reliably validate data accuracy.

Metric Attribute	Details
Name	Accuracy of information data sources
Description	Assess the reliability and accuracy of information sources providing data and details regarding the security incident.
Type	Effectiveness
Data Required	(N1) Number of data sources and stores used in your incident (N2) Number of data sources and stores where data accuracy has been validated
Calculation	N2 / N1 * 100 (percentage)
Measure	Percentage
	Accuracy of information data sources will need to be measured through validation processes or other feedback mechanisms. You may need to use sampling for measurements.

6.2.2.2 Metric: Chain of custody compliance

Metric Attribute	Details
Name	Chain of custody compliance
Description	Track the completeness of authenticity and integrity controls for data sources used in your security operation, as they adhere to chain of custody compliance restrictions
Type	Effectiveness
Data Required	(N1) Number of the data sources and stores used in your incident (N2) Number of data sources and stores where sufficient controls are in place to protect the compliance integrity of the data.
Calculation	N2 / N1 * 100 (percentage)
Measure	Percentage
Notes	You will need to define a baseline for what integrity controls are required for your operation and assess your data sources against integrity control baseline.

Metric Attribute	Details
Name	Chain of custody compliance
Description	Track the completeness of authenticity and integrity controls for data sources used in your security operation, as they adhere to chain of custody compliance restrictions
Type	Effectiveness
Data Required	(N1) Number of the data sources and stores used in your incident (N2) Number of data sources and stores where sufficient controls are in place to protect the compliance integrity of the data.
Calculation	N2 / N1 * 100 (percentage)
Measure	Percentage
	You can increase maturity by checking with your local authorities if your integrity controls would be sufficient for the data to be used in evidence in court. Reference for more details on chain of custody: https://www.cisa.gov/sites/default/files/publications/cisa-insights_chain-of-custody-and-ci-systems_508.pdf

6.2.2.3 Metric: Completeness of contextual data

Metric Attribute	Details
Name	Completeness of contextual data
Description	This metric will help you have an overview of the amount of incident data your team collected and attached to incidents.
Type	Effectiveness
Data Required	(N1) Total number of incidents (N2) Total number of incidents with contextual data attached
Calculation	N2 / N1 * 100
Measure	Percentage

Metric Attribute	Details
Notes	This metric does not necessarily address the quality of your contextual data, but rather its presence. If observables are referenced in the incident, they should be included with the case.

6.2.3 Function: Detailed analysis coordination

Metrics: The following metrics are defined for this function:

- Number of unresolved tasks at incident closure
- Time to complete tasks

6.2.3.1 Metric: Unresolved tasks at incident closure

Metric Attribute	Details
Name	Unresolved tasks at incident closure
Description	Used as an indicator of potential process failure - where tasks are not being completed by the responsible party.
Type	Effectiveness
Data Required	(N1) Number of tasks attached to the incident (N2) Number of unresolved tasks at incident closure
Calculation	(N2 / N1) * 100
Measure	Percentage
Notes	As this metric does not assess the quality of the resolution on tasks, guard against tasks that are resolved simply for the sake of this metric. Consider a QC process using sampling for quality review.

6.2.3.2 Metric: Time to complete tasks

Metric Attribute	Details
Name	Time to complete tasks
Description	Resolution time is a critical component of incident response. Therefore, tasks assigned to incidents should be completed as quickly as possible to avoid negative impact from the incident. Use this metric to assess timeliness.
Type	Efficiency
Data Required	For each task (t): (N1) Task creation time (N2) Task completion time
Calculation	Median({t(N2-N1)})
Measure	Median
Notes	Timing data should be generated (automatically) from system timestamps. Mean can be used but your time series will not likely be a normal distribution resulting in outlier impact. Using median may require stakeholder training. Can be paired with percentiles for clarification. As with 6.2.3.1, this metric does not assess the quality of the resolution on tasks. Guard against tasks that are resolved simply for the sake of this metric. Consider a QC process using sampling for quality review.

6.2.4 Function: Information security incident root cause analysis

Metrics: The following metrics are defined for this function:

- Time to complete root cause analysis
- Incidents with root cause not identified
- Root cause category analysis

6.2.4.1 Metric: Time to complete root cause analysis

Metric Attribute	Details
Name	Time to complete root cause analysis
Description	This metric is used to evaluate time involved in finding the root cause for an incident. By establishing targets or high / low ranges, this metric can be used as a starting point for conducting process analysis to find potential improvements.
Type	Efficiency
Data Required	(N1) Time at which root cause analysis begins (N2) Time at which root cause analysis is successfully completed
Calculation	N2 - N1
Measure	Number
Notes	Both the start and end time may be somewhat nebulous but try not to get too caught up in getting the exact moment. The intent of this metric is to help you evaluate efficiency within the process itself. Because this metric is intended to evaluate and drive efficiency, it should not be used as a KPI. You will likely want to analyse the trend in categorised incidents over a period as single numbers will be of limited use except when they fall outside established targets. It is also possible to analyse the set using statistical methods, e.g., median. Refer to section 4.3.4

6.2.4.2 Metric: Incidents with root cause not identified

Metric Attribute	Details
Name	Incidents with root cause not identified
Description	This metric is designed to help ensure that the root cause of an incident is identified whenever required, thereby helping to reduce the likelihood of future incidents via that same threat vector.
Type	Effectiveness
Data Required	(N1) - total number of incidents

Metric Attribute	Details
	(N2) - number of incidents with root cause not identified
Calculation	(N2) / (N1) * 100
Measure	Percentage
Notes	Low percentage is better. Root cause analysis can show how much a CSIRT understands the environment tech stack and the teams responsible for, once, in some cases, will be difficult for a CSIRT to perform this function thoroughly, but will need to know who can support. This metric does not measure successful root cause resolution as that may often be out of scope for CSIRTs.

6.2.4.3 Metric: Root cause category analysis

Metric Attribute	Details
Name	Root cause category analysis
Description	Count incident root causes according to their categorization. The intent of this metric is to identify broad areas of impact for attention, e.g. prioritisation, funding, or process improvement.
Type	Impact
Data Required	(N1) - total number of incidents with root cause category assigned (regardless of value) (N2) - count of incidents per associated root cause category (repeated for each category…)
Calculation	N2 / N1 * 100 Repeated for each category

Metric Attribute	Details
Measure	Percentage
Notes	Identifying root cause in general can be a resource intensive process. We recommend automating this as much as possible starting with your detection use case management (Section 5.1.2). Examples of root cause category may include phishing, unpatched vulnerability, password hygiene, etc.

6.2.5 Function: Cross-incident correlation

Metrics: The following metrics are defined for this function:

- Incidents correlated to other incidents
- Incidents with incorrect correlation

6.2.5.1 Metric: Incidents correlated to other incidents

Metric Attribute	Details
Name	Incidents correlated to other incidents
Description	The metric can be used to evaluate successful use of cross-incident linking via correlation.
Type	Implementation
Data Required	(N1) - total number of incidents handled (N2) - number of incidents linked to other incidents via correlation
Calculation	N2 / N1 * 100
Measure	Percentage
Notes	There may be some difficulty in incident correlation but if that is set up properly this metric should be easy to implement.

Metric Attribute	Details
	A relatively large percentage may demonstrate effectiveness in correlating incidents. However, if correlation is set up properly a low value may indicate that most incidents are not related. This is not a qualitative metric, so the value in this metric will be to analyse trending over time, ensuring incident correlation activity is occurring as expected.

6.2.5.2 Metric: Incidents with incorrect correlation (correlation error rate)

Metric Attribute	Details
Name	Incidents with incorrect correlation
Description	In some cases, linkage between incidents might be caused due to error in correlation - understood when looking at the linked incidents. This metric should be used only when there is a substantial number/percentage of the linkage via correlation - to detect the quality of the correlations and if needed to initiate changes in the correlation engine.
Type	Effectiveness
Data Required	(N1) - Number of incidents correlated to other incidents (N2) - Number of incidents correlated to other incidents, with an incorrect correlation
Calculation	(N2) / (N1)*100%
Measure	Percentage
Notes	N2 can be understood only when the incident correlation is analysed manually (or by AI) so may be difficult to measure. It may need to be accomplished via sample analysis.

6.3 Service: Artefact and forensic evidence analysis

6.3.1 Function: Media or surface analysis

Metrics: The following metrics are defined for this function:

- Ratio of identified malicious artefacts to total artefacts
- Ratio of artefacts with inconclusive analysis to total artefacts
- Number of never seen artefacts
- Time to identify key artefact attributes

6.3.1.1 Metric: Ratio of identified malicious artefacts to total artefacts

Metric Attribute	Details
Name	Ratio of identified malicious artefacts to total artefacts
Description	This metric identifies the ratio of malicious artefacts to the total number of artefacts discovered after media or surface analysis by the incident response team.
Type	Implementation
Data Required	(N1) Number of total artefacts analysed (N2) Number of malicious artefacts identified
Calculation	N2 / N1
Measure	Ratio
Notes	A system for storing historical media/surface analysis data is required. This data stored can be the totals themselves or better, a list of all artefacts with associated conclusions that can be summarized. A low number for this metric may show wide collection but relatively few are malicious, impacting workload. A high number may indicate strong pre-filtering but also the risk of missing non-obvious artefacts. Time trending can provide additional insights into process changes The raw numbers of malicious artefacts (N2) can also be useful for trending analysis reflecting a potential need for capacity planning regarding people, infrastructure, or process improvements.

6.3.1.2 Metric: Ratio of artefacts with inconclusive analysis to total artefacts

Metric Attribute	Details
Name	Ratio of artefacts with inconclusive analysis to total artefacts
Description	This metric identifies the ratio of inconclusive artefacts to the total number of artefacts using the number of artefacts whose verdict is inconclusive following media or surface analysis by the incident response team.
Type	Implementation
Data Required	(N1) Number of total artefacts analysed (N2) Number of inconclusive artefacts
Calculation	N2 / N1
Measure	Ratio
Notes	A system for storing historical media/surface analysis data is required. This data stored can be the totals themselves or better, a list of all artefacts with associated conclusions that can be summarized. A low number for this metric might give indication of process inefficiencies or errors, yielding inconclusive results. A high number may indicate that the team is not gathering enough artefacts for analysis and may be missing potential threats, indicating potential training or tooling gaps. Time trending can provide additional insights into process changes The raw numbers of inconclusive artefacts (N2) can also be useful for trending analysis reflecting a potential need for additional training or process improvements.

6.3.1.3 Metric: Number of never seen artefacts

Metric Attribute	Details
Name	Number of never seen artefacts
Description	This metric tracks the number of artefacts identified by your analysis process that are not found in any known feed. This number can be an indicator of how effective your team is at finding new things, or whether your team is subject to targeted attacks. It is also useful for validating artefact integrity and provenance.
Type	Impact
Data Required	(N1) Number of artefacts not found in any known repository
Calculation	N1
Measure	Number
Notes	Use of this metric assumes your team is effective at searching known indicators, whether in public or private repository. The inverse of this metric could be listed as “Hash Verification Success Rate”. Either number will suffice - number not found, or number found.

6.3.1.4 Time to identify key artefact attributes

Metric Attribute	Details
Name	Time to Identify Key artefact Attributes
Description	Measures the time taken to identify critical artefact attributes such as file types or cryptographic hashes. This can indicate efficiency improvements or bottlenecks
Type	Efficiency
Data Required	For each analysis *a* (N1) Start time of analysis (N2) Time at which key attributes are identified and the analysis is complete

Metric Attribute	Details
Calculation	median({a(N2-N1)})
Measure	Median
Notes	Your team will benefit from analysing the median trend over a period, e.g., quarterly. As with all time metrics be careful using this as a performance metric thereby potentially sacrificing quality to reach a target.

6.3.2 Function: Reverse engineering

Metrics: The following metrics are defined for this function:

- Number of reversed engineered suspicious artefacts
- Number of IOCs identified from reverse engineering
- Time to complete reverse engineering

6.3.2.1 Metric: Number of reversed engineered suspicious artefacts

Metric Attribute	Details
Name	Number of reversed engineered suspicious artefacts
Description	Count how many suspicious artefacts were reversed engineered during a time frame, ensuring completeness and throughput of the service in an organisation.
Type	Implementation
Data Required	(N1) Number of reversed engineered suspicious artefacts
Calculation	N1
Measure	Number

Metric Attribute	Details
Notes	A platform to track and maintain historical data of reverse engineering processes is required. This metric can be captured as a raw number over a period or averaged over a period of time and/or other factors.

6.3.2.2 Metric: Number of IOCs collected during reverse engineering

Metric Attribute	Details
Name	Number of IOCs collected during reverse engineering
Description	Count how many IOCs were discovered during reverse engineering during a specific timeframe, including all techniques. (dynamic, static, decompilation, etc.)
Type	Impact
Data Required	(N1) Number of IOCs collected as result of reverse engineering
Calculation	N1
Measure	Number
Notes	A platform to track and maintain historical data of reverse engineering processes is required. To effectively track and utilize the Number of IOCs collected during reverse engineering, it is essential to establish a clear and standardized definition of an IOC. This ensures consistency and enhances the reliability of this metric. Examples of IOCs include IP addresses, domains, registry keys, hashes, Mutex names, Process names, Network artefacts, Email address and Malware behaviour patterns This metric can be captured as a raw number over a period, or averaged over a period and/or other factors

6.3.2.3 Metric: Time to complete reverse engineering analysis

Metric Attribute	Details
Name	Time to complete reverse engineering
Description	Measures the time elapsed from the start of the reverse engineering process to its completion, for an individual artefact.
Type	Efficiency
Data Required	(N1) Time at which reverse engineering process started (N2) Time at which reverse engineering process completed
Calculation	N2 - N1
Measure	Number
Notes	A platform to track and maintain historical data of reverse engineering processes is required. Evaluate this metric to generate statistical analyses over time and type, such as median. This metric does not necessarily capture effort required for the reverse engineering process.

6.3.2.4 Metric: Effort to complete reverse engineering analysis

Metric Attribute	Details
Name	Effort to complete reverse engineering analysis
Description	Measures the amount of effort required to reverse engineer an individual artefact.
Type	Implementation
Data Required	(N1) Effort required to reverse engineer an artefact
Calculation	N1
Measure	Number

Metric Attribute	Details
Notes	It may be difficult to estimate the effort needed to complete the reverse engineering activities and likewise difficult for the reverse engineering team to keep track of their effort expenditure. Keep these activities as simple as possible so as to not add unnecessary overhead. One method to consider is to use a point system that creates a rough estimate of the activities. (Agile story pointing provides a methodology for this. Reference this Asana blog post.)

6.3.3 Function: Run time or dynamic analysis

The following metrics are defined for this function:

- Number of artefacts analysed during dynamic analysis
- Number of IOCs identified during dynamic analysis
- Number of new IOCs identified during dynamic analysis
- Percentage of artefacts requiring re-analysis
- Incidents where runtime analysis informed containment or mitigation

6.3.3.1 Metric: Number of artefacts analysed during dynamic analysis

Metric Attribute	Details
Name	Number of artefacts analysed during dynamic analysis
Description	This is a simple metric to keep track of the number of artefacts that are analysed. It can be used in trending to keep track of how the team is operating, as well as in other metrics for successful analysis and new IOCs identified.
Type	Impact
Data Required	(N1) Number of artefacts were analysed during dynamic analysis
Calculation	N1
Measure	Number

Metric Attribute	Details
Notes	You will need a proper platform to keep track of the artefacts that are analysed during the dynamic analysis process

6.3.3.2 Metric: Number of IOCs identified during dynamic analysis

Metric Attribute	Details
Name	Number of IOCs identified during dynamic analysis
Description	Tracks the total number of IOCs observed through dynamic analysis, regardless of whether they are new or previously known. This provides a sense of the volume and breadth of indicators generated by this analysis function.
Type	Impact
Data Required	(N1) Number of IOCs identified during dynamic analysis
Calculation	N1
Measure	Number
Notes	You will need a method for extracting and recording IOCs from dynamic analysis sessions, such as from sandbox reports or network capture logs. This metric helps show the observable footprint of suspicious artefacts when executed. It may include URLs, IPs, domains, file hashes, mutexes, and more.

6.3.3.3 Metric: Number of new IOCs identified during dynamic analysis

Metric Attribute	Details
Name	Number of new IOCs identified during dynamic analysis
Description	Tracks the number of previously unknown IOCs discovered during dynamic analysis. This helps measure the uniqueness and added value of the analysis to the organisation's threat intelligence.
Type	Impact

Metric Attribute	Details
Data Required	(N1) Number of IOCs identified during dynamic analysis that were not already present in internal or shared threat intelligence sources.
Calculation	N1
Measure	Number
Notes	This metric requires comparison of extracted IOCs against an up-to-date IOC repository to confirm novelty. Matching may need to account for IOC type and normalization (e.g., domain variations). You will need a proper platform to keep track of the suspicious IOCs that are analysed during the dynamic analysis process

6.3.3.4 Metric: Percentage of artefacts requiring re-analysis

Metric Attribute	Details
Name	Percentage of artefacts requiring re-analysis
Description	Measures the percentage of artefacts that require re-analysis after the initial runtime analysis, indicating the thoroughness of the first analysis or the need for further investigation.
Type	Efficiency
Data Required	(N1) Total number of artefacts analysed (N2) Number of artefacts that required re-analysis
Calculation	(N2 / (N1) *100
Measure	Percentage
Notes	Identifying when a re-analysis is necessary; may require thorough record-keeping and review of analysis logs. A higher percentage of re-analysis may indicate a need for improved initial analysis processes or more effective tools.

6.3.3.5 Metric: Incidents where runtime analysis informed containment or mitigation

Metric Attribute	Details
Name	Incidents where runtime analysis informed containment or mitigation
Description	Tracks how often runtime analysis directly contributes to informing containment or mitigation strategies for incidents. This metric ties the value of dynamic analysis to actual incident response efforts.
Type	Effectiveness
Data Required	(N1) Number of incidents where runtime analysis informed containment or mitigation
Calculation	N1
Measure	Number
Notes	Requires detailed documentation linking dynamic analysis results to specific incident containment or mitigation actions. Demonstrates the real-world impact of runtime analysis in reducing threat impact through proactive response strategies.

6.3.4 Function: Comparative analysis

The following metrics are defined for this function:

- Number of artefacts correlated per threat actor
- Number of IOCs per threat actor

6.3.4.1 Metric: Number of artefacts correlated per threat actor

Metric Attribute	Details
Name	Number of artefacts correlated per threat actor
Description	How many artefacts were correlated per threat actor. This metric can show how many correlations were done by artefact correlation analysis, more is better.

Metric Attribute	Details
Type	Efficiency
Data Required	N1 = Number of artefacts
Calculation	N1
Measure	Number
Notes	You will need a repo of artefacts and tools to compare historically or "retro-hunting" against known and new threat actors.

6.3.4.2 Metric: Number of IOCs correlated per threat actor

Metric Attribute	Details
Name	Number of IOCs correlated per threat actor
Description	A count of the IOCs that are associated with a specific threat actor.
Type	Efficiency
Data Required	(N1) Number of IOC per threat actor
Calculation	N1
Measure	Number
Notes	You will need a repo of artefacts and toolings to compare historically or "retro-hunting" against known and new threat actors.

6.4 Service: Mitigation and recovery

6.4.1 Function: Response plan establishment

Metrics: The following metrics are defined for this function:

- Incidents meeting successful resolution criteria
- Revenue Loss due to Security Incidents

6.4.1.1 Metric: Incidents meeting successful resolution criteria

Metric Attribute	Details
Name	Incidents meeting successful resolution criteria
Description	This metric provides insight into the efficiency and effectiveness of the Incident Response Plan by measuring the total number of incidents that have been successfully resolved within a given period. It helps organisations evaluate their ability to handle disruptions and restore normal operations, contributing to overall service quality and customer satisfaction. The criteria for successful resolution should be defined in the response plan. (See notes)
Type	Effectiveness
Data Required	(N1) Number of Incidents Resolved (N2) Incidents Meeting All Resolution Criteria as defined by response plan
Calculation	(N2) / (N1) * 100
Measure	Percentage
Notes	Data Accuracy: Ensuring the accuracy of incident data and feedback Defining Resolution Criteria: Establishing clear and consistent criteria for what constitutes a successfully resolved incident An incident may be considered successfully resolved when it meets predefined criteria such as issue closure, customer satisfaction, compliance with service level agreements (SLAs), and confirmation from the reporters that the issue is resolved. Possible Resolution Criteria: ● Closure: The incident is marked as closed in the tracking system. ● Stakeholder Satisfaction: Positive feedback or confirmation from the affected party that the issue has been resolved. ● Compliance with SLAs: The incident resolution meets the time and quality standards defined in service level agreements.

Metric Attribute	Details
	• Verification: Final verification or acceptance by the incident reporter that the issue has been resolved to their satisfaction. An essential part of an incident response is to clearly define the resolution criteria that are applicable to the organisation.

6.4.1.2 Metric: Revenue loss due to security incidents

Metric Attribute	Details
Name	Revenue loss due to security incidents
Description	Measure the total revenue loss caused by security incidents over a specific period. This metric evaluates the financial and operational impact of security breaches, highlighting how incidents affect business continuity and profitability. The lower the revenue loss, the more effective the incident response and recovery processes.
Type	Impact
Data Required	**Downtime measure:** Identify Affected Systems/Services: Determine which systems or services were impacted by the incident. • n = the number of affected systems Track Duration of Downtime: Measure the time (in hours or minutes) that each affected system or service was unavailable or operating at reduced capacity. • $End\ Time_i$ = the time the incident was resolved for $System_i$ • $Start\ Time_i$ = the time the incident was resolved for $System_i$ **Quantify Revenue Loss:** • *(N1) Revenue per Unit of Time*: Calculate your business's revenue per hour or day, depending on the severity of the incident. • *(N2) Other Costs*: Factor in additional financial impacts such as regulatory fines, customer compensation, or potential loss of future business due to reputational damage. • *(N3) Impact Factor:* If operations were partially affected (e.g., slower sales, reduced customer engagement), adjust the calculation based on the percentage of impact. For example, if the business operated at 50% capacity, the Impact Factor would be 0.5).

Metric Attribute	Details
Calculation	**Calculate Total Downtime**: Add up the duration for all affected systems/services to get the total downtime for the incident: $$Total\ Downtime\ = \sum_{i=1}^{n} (End\ Time_i\ -\ Start\ Time_i)$$ **Estimate Lost Revenue**: Multiply the total downtime by the average revenue lost per hour or day: $$Revenue\ Loss = (N1\ Revenue\ per\ Unit\ of\ Time) \times (Total\ Downtime)\ X\ Impact\ Factor$$ $$Total\ Financial\ Impact\ =\ Revenue\ Loss\ +\ N2\ (e.g., fines, compensation)$$
Measure	Number
Notes	**Note**: This metric is significantly complicated to derive as evidenced with the data accuracy barriers listed below. We have included here as a starting point for those organisations interested in calculating financial impact. Data Accuracy: Ensuring the accuracy of incident data and feedback. It follows some barriers: ● Complex Incident Scope: If multiple systems or services are affected in different ways, accurately measuring total downtime can be difficult. Some systems may experience partial degradation rather than full outages, which complicates the measurement. ● Start and End Time Discrepancies: Determining the precise start and end time of the incident can be difficult, especially if the detection of the issue is delayed or if different systems are affected at different times. ● Variable Revenue Flows: Businesses may experience fluctuating revenue depending on the time of day, season, or other factors. Calculating an average revenue loss may not fully capture the true financial impact, especially during peak periods. ● Data Silos: In large organisations, operational and financial data may be housed in different systems or departments, making it challenging to integrate all necessary data for calculating lost revenue. ● Global Operations: Businesses operating in multiple regions with different time zones and currencies face additional complexities in calculating revenue loss consistently across regions. Account for Indirect Costs:

Metric Attribute	Details
	• Reputation Damage: Consider long-term financial impacts due to lost customers, diminished trust, or reputational harm that could result in future revenue losses. • Customer Compensation: Include any direct compensation to customers (e.g., refunds, discounts). • Operational Costs: Account for the costs of response efforts, such as additional labour, third-party services, or replacement of damaged equipment. Lost revenue example: If your business normally generates $10,000 per hour, and a security incident caused a system outage for 3 hours, with a 50% reduction in operational capacity, the revenue loss would be calculated as: Lost Revenue = $10,000/hour × 3 hours × 0.5 (impact factor) = $15,000 You may want to compare your total revenue loss over a period against an "expected loss" baseline for similar organisations.

6.4.2 Function: Ad hoc measures and containment

Metrics: The following metric is defined for this function:

- Time to contain

6.4.2.1 Metric: Time to contain

Metric Attribute	Details
Name	Time to contain
Description	Measures the efficacy of containing a detected threat or security incident
Type	Efficiency
Data Required	(N1) The time at which the event was detected (N2) The time of the incident was contained

Metric Attribute	Details
Calculation	N2 - N1
Measure	Number
Notes	Either a ticketing system adept at accurately recording such data or manual log analysis is necessary to assess the timing of the event occurrence. Some corner cases are hard to identify when a threat is contained, sometimes multiples containing phases happen inside the same incident. Refer to Security Incident Timing Metrics on the FIRST Portal This measurement usually spans minutes, hours, or days, contingent upon the complexity and severity of the incident. Gathering data for this metric involves timestamping the instant when containment measures are successfully implemented and validated. This timestamp can be extracted from incident tracking systems, security logs, or documented evidence of containment efforts. It is recommended the logs are aligned with the same time zone.

6.4.3 Function: System restoration

Metrics: The following metrics are defined for this function:

- Median time of resolution
- Effectiveness of Incident Response in Security Posture Improvement
- Percentage of actionable measures successfully implemented

6.4.3.1 Metric: Median time of resolution

Metric Attribute	Details
Name	Median time of resolution
Description	The metric measures the time between the onset of the incident and the point at which systems and services are restored to full functionality and capacity.

Metric Attribute	Details
Type	Efficiency
Data Required	For each incident a: (N1) Incident start time (N2) Time at which systems and services are restored
Calculation	median({a(N2-N1)})
Measure	Median
Notes	It may be difficult to know the exact time at which services are restored, and restored to "full" functionality and capacity, but it is an important point to capture. As with other data points that are difficult to determine, use a common-sense approach and keep the determination as simple as possible. Refer to Security Incident Timing Metrics created by the FIRST Metrics SIG for more information.

6.4.3.2 Metric: Effectiveness of incident response in security posture improvement

Metric Attribute	Details
Name	Effectiveness of incident response in security posture improvement
Description	This metric tracks the number of security incidents that resulted in actionable steps (e.g., corrective, preventive, and improvement actions) aimed at strengthening the organisation's security posture. High effectiveness indicates that more incidents are thoroughly investigated, and action plans are created to prevent future occurrences.
Type	Effectiveness
Data Required	(N1) Incident Count: Total number of incidents over a period (N2) Actionable Incidents: Incidents that resulted in a formalized action plan (e.g., process change, new controls, system patches).
Calculation	(N2 / N1) * 100
Measure	Percentage
Notes	How this metric can be Interpreted:

Metric Attribute	Details
	• High (>75%): Indicates proactive security posture, with most incidents leading to action plans. • Moderate (50%-75%): Incidents often reviewed but may lack consistent follow-up actions. • Low (<50%): Many incidents are not driving actionable improvements, suggesting potential areas for response process improvement. Example: If you had 100 incidents and 80 of them generated action plans: E = 80 / 100 * 100 E = 80% An 80% effectiveness rate suggests that the incident response process is well-aligned with security improvement goals.

6.4.3.3 Metric: Percentage of actionable measures successfully implemented

Metric Attribute	Details
Name	Percentage of actionable measures successfully implemented
Description	Recognizing that successful follow-up on recommended security measures and recommendations may be a lengthy process with much work outside the scope of the CSIRT, this metric tracks how well action plans are implemented.
Type	Impact
Data Required	(N1) Number of recommended security measures (N2) Number of recommended security measures successfully closed
Calculation	N2 / N1 * 100
Measure	Percentage
Notes	As mentioned in the description, the CSIRT will often not have control over how many measures are successfully implemented. Therefore, the metric should not be used as a performance indicator. Instead, it should

Metric Attribute	Details
	be used as an indicator of the broad impact of the security program and partnerships.

6.4.4 Function: Other information security entities support

Metrics: The following metrics are defined for this function:

- None

6.5 Service: Information security incident coordination

Metrics: The following metric is defined for this Service:

- Effectiveness of incident coordination stakeholder survey

6.5.0.1 Metric: Effectiveness of incident coordination stakeholder survey

Metric Attribute	Details
Name	Effectiveness of incident coordination stakeholder survey
Description	This metric aims to quantify timeliness, relevance and clarity of coordination communication and quality of the corresponding incident report for incidents with severity X and above. Please see the notes and detailed metric descriptions for full details.
Type	Effectiveness
Data Required	Ask relevant stakeholders to rate their response from 1 to 5 (5 being best, consider including N/A as an option) Q1 How would you rate how relevant the information shared was to you? (6.5.3) Q2 How would you rate the ability of the CSIRT to coordinate and maintain situational awareness during the incident? (6.5.4)

Metric Attribute	Details
	Q3 Was the information regarding current activities delivered in a timely fashion? (6.5.5) Q4 How would you rate the overall quality of the finished incident report? (6.5.5)
Calculation	You can use the metrics as is, or do an average, or a weighted average if some metrics are more important to you than others.
Measure	n/a
Notes	If your organisation does not have an approved survey platform, then consideration should be made to find one that suits your needs regarding confidentiality and security in general. This metric covers the functions 6.5.3, 6.5.4, 6.5.5. You can expand the survey method to other areas of your incident coordination service.

6.5.1 Function: Communication

Metrics: The following metric is defined for this function:

- Communication channel downtime

6.5.1.1 Metric: Communication channel downtime

Metric Attribute	Details
Name	Communication channel downtime
Description	This metric measures the time elapsed since the last received communication. If this duration exceeds expected or normal thresholds, it may indicate a potential issue with your communication channel. Use this metric to help decide when to test whether the channel is still functioning properly.
Type	Effectiveness
Data Required	(N1) Time of last message in communication channel

Metric Attribute	Details
	(N2) Current time
Calculation	N2 - N1
Measure	Number
Notes	This metric can be repeated for internal and external communication channels if needed.

6.5.2 Function: Notification distribution

Metrics: The following metrics are defined for this function:

- None; no metrics are defined for this function, but it is important to ensure that all required entries are identified and added to communication channels.

6.5.3 Function: Relevant information distribution

Metrics: The following metrics are defined for this function:

- Relevance of notification to recipients

6.5.3.1 Metric: Relevance of notification to recipients

Metric Attribute	Details
Name	Relevance of notification to recipients
Description	This metric aims to measure the relevance of the notification to the recipients by surveying them.
Type	Effectiveness
Data Required	(N1) The answer to survey question #1; a set of numbers between 1 and 5 from surveyed entities
Calculation	N1

Metric Attribute	Details
Measure	Number
Notes	This metric is designed to be bundled with other survey results from 6.5a.

6.5.4 Function: Activities coordination

The following metric is defined for this function:

- Effectiveness of incident coordination and situational awareness development

6.5.4.1 Metric: Effectiveness of incident coordination and situational awareness development

Metric Attribute	Details
Name	Effectiveness of incident coordination and situational awareness development
Description	This metric aims to measure the ability of the CSIRT to do incident coordination and create situational awareness, as observed by incident participants.
Type	Effectiveness
Data Required	(N1) The answer to survey question Q2; A number between 1 and 5 from surveyed entities (or N/A)
Calculation	N1
Measure	Number
Notes	This metric is designed to be bundled with other survey results from 6.5a.

6.5.5 Function: Reporting

The following metrics are defined for this function:

- Stakeholder satisfaction level for timeliness of information
- Stakeholder satisfaction level for incident report

6.5.5.1 Metric: Stakeholder satisfaction level for timeliness of information

Metric Attribute	Details
Name	Stakeholder satisfaction level for timeliness of information
Description	This metric aims to measure the ability of the CSIRT to provide timely reports on situational awareness regarding progress
Type	Effectiveness
Data Required	(N1) The answer to survey question Q3; A number between 1 and 5 from surveyed entities (or N/A)
Calculation	N1
Measure	Number
Notes	This metric is designed to be bundled with other survey results from 6.5a.

6.5.5.2 Metric: Stakeholder satisfaction level for incident report

Metric Attribute	Details
Name	Stakeholder satisfaction level for incident report
Description	This metric aims to measure the ability of the CSIRT to create incident reports that are understood by stakeholders
Type	Effectiveness
Data Required	(N1) The answer to survey question Q4; A number between 1 and 5 from surveyed entities (or N/A)
Calculation	N1
Measure	Number

Metric Attribute	Details
Notes	This metric is designed to be bundled with other survey results from 6.5a.

6.5.6 Function: Media communication

Metrics: The following metrics are defined for this function:

- None

6.6 Service: Crisis management support

6.6.1 Function: Information distribution to constituents

Metrics: The following metrics are defined for this function:

- Number of crisis communications distributed to constituents
- Time from crisis onset to first communication to constituents
- Percentage of constituent groups reached during crisis communication
- Percentage of communications acknowledged or acted upon by constituents

6.6.1.1 Metric: Number of crisis communications distributed to constituents

Metric Attribute	Details
Name	Number of crisis communications distributed to constituents
Description	Tracks the total number of crisis-related communications sent to constituents during the course of a specific crisis. This provides a quantitative measure of outreach effort and messaging activity.
Type	Implementation
Data Required	(N1) Total number of crisis-related communications sent to constituents
Calculation	N1
Measure	Number
Notes	Requires clear tagging or classification of messages as “crisis-related” in the communication platform or log.

Metric Attribute	Details
	This metric should be tracked over a period such as days or weeks, as crises can vary greatly in length. If there is a defined target for frequency of crisis communications the metric can be used to indicate level of compliance. Can be broken down further by communication type (email, SMS, portal update) or by constituent group

6.6.1.2 Metric: Time from crisis onset to first communication to constituents

Metric Attribute	Details
Name	Time from crisis onset to first communication to constituents
Description	Measures the responsiveness of the CSIRT communication process during a crisis by tracking how quickly the first message is sent following formal recognition of the crisis.
Type	Efficiency
Data Required	(N1) Timestamp of crisis onset (N2) Timestamp of first communication to any constituent
Calculation	N2 - N1
Measure	Number
Notes	Depends on clear documentation of crisis declaration time and communication logs. Particularly valuable for assessing preparedness and the agility of internal processes.

6.6.1.3 Metric: Percentage of constituent groups reached during crisis communication

Metric Attribute	Details
Name	Percentage of constituent groups reached during crisis communication
Description	Assesses the breadth of communication coverage during a crisis by calculating the percentage of defined constituent groups that received at least one message.
Type	Effectiveness
Data Required	(N1) Number of constituent groups that received at least one crisis communication (N2) Total number of defined constituent groups
Calculation	(N1 / N2) × 100
Measure	Ratio
Notes	Requires a well-maintained list of constituent groups and accurate delivery tracking per group. Can be further analysed by priority level or geography

6.6.1.4 Metric: Percentage of communications acknowledged or acted upon by constituents

Metric Attribute	Details
Name	Percentage of communications acknowledged or acted upon by constituents
Description	Measures the proportion of crisis messages that received a meaningful acknowledgment or prompted a recorded action by the recipient, helping gauge message effectiveness and trust.
Type	Impact
Data Required	(N1) Number of crisis communications acknowledged or acted upon by constituents (N2) Total number of crisis communications distributed
Calculation	(N1 / N2) × 100
Measure	Percentage

Metric Attribute	Details
Notes	Requires response tracking, either via read receipts, follow-up action logs, or ticket responses. Can be a proxy indicator for both trust in the CSIRT and the relevance/clarity of the message.

6.6.2 Function: Information security status reporting

Metrics: The following metrics are defined for this function:

- Time to deliver initial status report after crisis declaration
- Percentage of status reports delivered on time

6.6.2.1 Metric: Time to deliver initial status report after crisis declaration

Metric Attribute	Details
Name	Time to deliver initial status report after crisis declaration
Description	Measures the responsiveness of the CSIRT in providing its first situational update after a crisis has been formally declared.
Type	Efficiency
Data Required	(N1) Time of crisis declaration (N2) Time of first status report delivery
Calculation	(N2) - (N1)
Measure	Number
Notes	Depends on accurate timestamping of both the crisis declaration and report delivery. Can be benchmarked against policy-defined expectations for initial reporting. Statistical analysis can be performed across a set of times, such as mean or median.

6.6.2.2 Metric: Percentage of status reports delivered on time

Metric Attribute	Details
Name	Percentage of status reports delivered on time
Description	Evaluates how consistently the CSIRT meets pre-established deadlines for delivering crisis-related status reports.
Type	Effectiveness
Data Required	(N1) Number of status reports delivered on time (N2) Total number of status reports expected during the crisis
Calculation	(N1) / (N2) * 100
Measure	Percentage
Notes	Requires a pre-defined reporting schedule and consistent tracking of both expectations and actual delivery times. May be influenced by both internal delays and external coordination issues

6.6.3 Function: Strategic decisions communication

The following metric is defined for this function:

- Time from operational impact to external notification

6.6.3.1 Metric: Time from operational impact to external notification

Metric Attribute	Details
Name	Time from operational impact to external notification
Description	Measures the elapsed time between the time at which normal CSIRT operations are negatively impacted and when that information is communicated externally.
Type	Efficiency
Data Required	(N1) Time at which operational decision was made (N2) Time of corresponding external notification
Calculation	Mean(N2 − N1)
Measure	Mean
Notes	Capturing decision timestamps accurately may be difficult during fast-moving crises. Useful for evaluating the responsiveness of CSIRT communications.

7 Service Area: Vulnerability Management 🔗

7.0.0 Vulnerability Management - Service Area Metrics

Each functional area within the six services has associated metrics. In addition, here are four program-wide metrics for the Vulnerability Management service area, designed to provide insight into the *overall performance, risk posture, and operational maturity* of the vulnerability management service area. Each metric cuts across multiple services and functions in Section 7 and is presented in the standard metrics format.

The following program metrics are included in this Service Area

- Total number of vulnerabilities handled per reporting period
- Percentage of vulnerabilities with defined remediation or mitigation
- Average time from vulnerability intake to remediation
- Distribution of vulnerabilities by severity and asset class

7.0.0.1 Metric: Total number of vulnerabilities handled per reporting period

Metric Attribute	Details
Name	Total number of vulnerabilities handled per reporting period
Description	Measures the volume of vulnerabilities processed by the organisation across all intake, analysis, coordination, and response activities.
Type	Implementation
Data Required	(N1) Count of all unique vulnerabilities recorded and processed
Calculation	N1
Measure	Number
Notes	Requires centralized vulnerability tracking. May need deduplication of records from different services. Serves as a high-level indicator of workload or threat landscape exposure.

7.0.0.2 Metric: Percentage of vulnerabilities with defined remediation or mitigation

Metric Attribute	Details
Name	Percentage of vulnerabilities with defined remediation or mitigation
Description	Indicates how many of the vulnerabilities processed resulted in an actionable plan to remediate or mitigate.
Type	Effectiveness
Data Required	(N1) Number of vulnerabilities handled (N2) Number of vulnerabilities for which remediation or mitigation was defined
Calculation	(N2 / N1) × 100
Measure	Percentage
Notes	May require validation across multiple teams (e.g., analysis, coordination, IT). Highlights maturity in turning discovery into action.

7.0.0.3 Metric: Average time from vulnerability intake to remediation

Metric Attribute	Details
Name	Average time from vulnerability intake to remediation
Description	Captures end-to-end efficiency from receiving a report to executing a solution.
Type	Efficiency
Data Required	(N1) Time of vulnerability intake (report receipt or discovery) (N2) Time of remediation (patch or mitigation applied)
Calculation	N2 − N1 (averaged across all vulnerabilities)
Measure	Mean
Notes	Requires time correlation across functions and possibly across teams. Useful in identifying where delays occur across the full lifecycle.

7.0.0.4 Metric: Distribution of vulnerabilities by severity and asset class

Metric Attribute	Details
Name	Distribution of vulnerabilities by severity and asset class
Description	Categorizes vulnerabilities to assess risk concentration and trends.
Type	Impact
Data Required	Severity level (e.g., CVSS or High/Medium/Low, etc.) Asset class (e.g., data center, endpoint, IoT)
Calculation	No calculation. Show trending counts or aggregate statistics across severities and classes.
Measure	Number
Notes	Requires accurate classification and asset inventory mapping. Can inform targeted investments or patch prioritization policies.

7.1 Service: Vulnerability discovery / research

7.1.1 Function: Incident response vulnerability discovery

Metrics: The following metrics are defined for this function:

- Number of vulnerabilities identified during incident handling
- Time from incident detection to vulnerability identification

7.1.1.1 Metric: Number of vulnerabilities identified during incident handling

Metric Attribute	Details
Name	Number of vulnerabilities identified during incident handling
Description	Tracks the total number of vulnerabilities discovered through investigation of security incidents. Includes both known and previously unknown (zero-day) vulnerabilities.

Metric Attribute	Details
Type	Implementation
Data Required	(N1) Number of vulnerabilities identified as part of incident handling
Calculation	N1
Measure	Number
Notes	Requires integration between incident handling records and vulnerability tracking systems; consistent documentation practices are essential. Useful for understanding how much vulnerability discovery occurs organically through reactive investigation.

7.1.1.2 Metric: Time from incident detection to vulnerability identification

Metric Attribute	Details
Name	Time from incident detection to vulnerability identification
Description	Measures the elapsed time between the detection of an incident and the identification of an exploited vulnerability.
Type	Efficiency
Data Required	(N1) Timestamp of incident detection (N2) Timestamp when the vulnerability was identified
Calculation	N2 - N1
Measure	Number
Notes	Requires precise and consistent timestamping of both detection and analysis milestones. Indicates how quickly the CSIRT can recognize the root cause of an incident at the vulnerability level.

7.1.2 Function: Public source vulnerability discovery

***Metrics*:** The following metrics are defined for this function:

- Number of vulnerabilities identified from public or third-party sources
- Time from public disclosure to identification by CSIRT

7.1.2.1 Metric: Number of vulnerabilities identified from public or third-party sources

Metric Attribute	Details
Name	Number of vulnerabilities identified from public or third-party sources
Description	Tracks the total number of new vulnerabilities discovered by CSIRT staff through public sources or restricted third-party services.
Type	Implementation
Data Required	(N1) Number of vulnerabilities identified from public or third-party sources
Calculation	N1
Measure	Number
Notes	Requires systematic tracking of source-monitoring activities; some findings may be duplicated across sources or already known. Can be broken down by source type (e.g., mailing list, vendor site, paid service) and specific source for trend analysis.

7.1.2.2 Metric: Time from public disclosure to identification by CSIRT

Metric Attribute	Details
Name	Time from public disclosure to identification by CSIRT
Description	Measures the delay between the public or third-party disclosure of a vulnerability and the point at which CSIRT staff formally identify or log it.
Type	Impact
Data Required	(N1) Timestamp of public or third-party disclosure

Metric Attribute	Details
	(N2) Timestamp of CSIRT identification
Calculation	N2 - N1
Measure	Number
Notes	May require integration with source monitoring tools or manual tracking; disclosure time may be unclear or approximate. Shorter times indicate more responsive monitoring and better situational awareness.

7.1.3 Function: Vulnerability research

***Metrics*:** The following metric is defined for this function:

- Number of new vulnerabilities identified by CSIRT

7.1.3.1 Metric: Number of new vulnerabilities identified by CSIRT

Metric Attribute	Details
Name	Number of new vulnerabilities identified by CSIRT
Description	This is a simple count of how many new vulnerabilities were discovered by the CSIRT per period (year/month). It tracks the number of new vulnerabilities discovered by the CSIRT through deliberate research activities, such as fuzz testing or reverse engineering.
Type	Implementation
Data Required	(N1) Number of new vulnerabilities discovered by the CSIRT
Calculation	N1
Measure	Number
Notes	Requires consistent internal documentation and confirmation that the vulnerability is indeed new (not already catalogued by others).

Metric Attribute	Details
	Can be further categorized by discovery methods (e.g., fuzzing, reverse engineering, static analysis) for internal reporting.

7.2 Service: Vulnerability report intake

7.2.1 Function: Vulnerability report receipt

***Metrics*:** The following metrics are defined for this function:

- Number of vulnerability reports received from external sources
- Time to acknowledge vulnerability report
- Vulnerability reporting channel up time

7.2.1.1 Metric: Number of vulnerability reports received from external sources

Metric Attribute	Details
Name	Number of vulnerability reports received from external sources
Description	Tracks the total number of vulnerability reports received from constituents or third parties during a defined period.
Type	Implementation
Data Required	(N1) Number of vulnerability reports received through official channels
Calculation	N1
Measure	Number
Notes	Requires consistent tagging or classification of reports as “vulnerability reports” and central logging of all intake channels. Can be broken down by source type (e.g., constituent, researcher, PSIRT) or intake method (email, portal).

7.2.1.2 Metric: Vulnerability reporting channel up time

Metric Attribute	Details
Name	Vulnerability reporting channel up time
Description	Measures the percentage of time that the CSIRT's advertised vulnerability reporting channels (e.g., email, web form, portal) are available and functioning.
Type	Implementation
Data Required	(N1) Total operational time of reporting channels (N2) Total time in the monitoring period
Calculation	N1 / N2 * 100
Measure	Number
Notes	Requires automated monitoring tools or manual tracking of uptime across intake mechanisms. Downtime may result in lost or delayed reports; this is critical for maintaining trust and accessibility.

7.2.1.3 Metric: Time to acknowledge vulnerability report

Metric Attribute	Details
Name	Time to acknowledge vulnerability report
Description	This metric measures the amount of time it takes your team to acknowledge receipt of the vulnerability report.
Type	Efficiency
Data Required	(N1) Time at which the vulnerability report was received (N2) Time at which the vulnerability report was acknowledged
Calculation	N2 - N1
Measure	Number

Metric Attribute	Details
Notes	Requires clear logging of both report receipt time and acknowledgment time. Helps evaluate professionalism and responsiveness in early-stage communication with reporters. As with other “time to” metrics, this can be analysed statistically, e.g., median time to acknowledge.

7.2.2 Function: Vulnerability report triage and processing

***Metrics*:** The following metrics are defined for this function:

- Percentage of vulnerability reports triaged within defined time frame
- Percentage of vulnerability reports forwarded for handling

7.2.2.1 Metric: Percentage of vulnerability reports triaged within defined time frame

Metric Attribute	Details
Name	Percentage of vulnerability reports triaged within defined time frame
Description	Measures how many received reports were reviewed, categorized, and acted upon (e.g., forwarded or dismissed) within a policy-defined period (e.g., 3 business days).
Type	Efficiency
Data Required	(N1) Number of reports triaged within defined time frame (N2) Total number of reports received
Calculation	(N1 / N2) × 100
Measure	Percentage
Notes	Requires accurate tracking of intake, triage timestamps, and clear definition of what constitutes triage completion. Reflects responsiveness and operational discipline in early vulnerability handling.

7.2.2.2 Metric: Percentage of vulnerability reports forwarded for handling

Metric Attribute	Details
Name	Percentage of vulnerability reports forwarded for handling
Description	Measures the proportion of received reports that were formally routed for follow-up (e.g., passed to a Vulnerability Analysis service or external party) after triage.
Type	Implementation
Data Required	(N1) Number of reports forwarded after triage (N2) Total number of triaged reports
Calculation	(N1 / N2) × 100
Measure	Percentage
Notes	Requires clear recordkeeping and defined criteria for routing decisions. Indicates how often reports are considered actionable enough for further attention, either internally or externally.

7.3 Service: Vulnerability analysis

7.3.1 Function: Vulnerability triage (validation and categorization)

***Metrics*:** The following metrics are defined for this function:

- Percentage of vulnerabilities categorized and prioritized within defined timeframe
- Distribution of vulnerabilities by category

7.3.1.1 Metric: Vulnerabilities categorized and prioritized within defined timeframe

Metric Attribute	Details
Name	Vulnerabilities categorized and prioritized within defined time frame
Description	Measures how many confirmed vulnerabilities were categorized and prioritized within a predefined time window (e.g., 3 business days) following assignment to the analysis team.
Type	Efficiency
Data Required	(N1) Number of vulnerabilities categorized and prioritized within timeframe (N2) Total number of confirmed vulnerabilities received for triage
Calculation	(N1 / N2) * 100
Measure	Percentage
Notes	Requires clear tracking of handoff and triage completion timestamps; categories and prioritization levels must be formally recorded. Reflects timeliness in preparing vulnerabilities for further analysis or coordination.

7.3.1.2 Metric: Distribution of vulnerabilities by category

Metric Attribute	Details
Name	Distribution of vulnerabilities by category
Description	Tracks the proportion of vulnerabilities assigned to each predefined category during triage, helping to identify trends in vulnerability types over time.
Type	Impact
Data Required	(N1) Number of vulnerabilities per category (e.g., N1*a* = injection, N1*b* = misconfiguration, etc.) (N2) Total number of vulnerabilities categorized
Calculation	for each category *x*: (N1*x* / N2) × 100

Metric Attribute	Details
Measure	Percentage
Notes	Requires a standardized and enforced categorization scheme; may be hard to compare across analysts or time periods without normalization. Useful for trend analysis, capacity planning, and directing training or tooling improvements.

7.3.2 Function: Vulnerability root cause analysis

***Metrics*:** The following metric is defined for this function:

- Percentage of vulnerabilities with documented root cause and exploitation conditions

7.3.2.1 Metric: Percentage of vulnerabilities with documented root cause and exploitation conditions

Metric Attribute	Details
Name	Percentage of vulnerabilities with documented root cause and exploitation conditions
Description	Measures how many vulnerabilities have a completed analysis that includes both the underlying root cause (e.g., design or implementation flaw) and the conditions under which the vulnerability could be exploited.
Type	Implementation
Data Required	(N1) Number of vulnerabilities with documented root cause and exploitation conditions (N2) Total number of vulnerabilities accepted for analysis
Calculation	(N1 / N2) * 100
Measure	Percentage
Notes	Requires clear documentation standards; some analyses may remain incomplete due to limited access to source code, limited context, or dependency on third-party vendors.

Metric Attribute	Details
	This metric reflects completion of a full root cause analysis as defined by the function outcome. In cases where only the root cause or exploitation conditions are identified, but not both, the vulnerability is not counted in (N1). Partial findings may still be valuable and can be tracked separately through internal flags or workflow statuses.

7.3.3 Function: Vulnerability remediation development

***Metrics*:** The following metric is defined for this function:

- Percentage of analysed vulnerabilities with documented remediation or mitigation plan

7.3.3.1 Metric: Percentage of analysed vulnerabilities with documented remediation or mitigation plan

Metric Attribute	Details
Name	Percentage of analysed vulnerabilities with documented remediation or mitigation plan
Description	Measures how many vulnerabilities, once analysed, resulted in a documented remediation (e.g., patch, code change) or mitigation (e.g., workaround, configuration guidance) plan.
Type	Implementation
Data Required	(N1) Number of vulnerabilities with documented remediation or mitigation plans (N2) Total number of vulnerabilities analysed
Calculation	(N1 / N2) * 100
Measure	Percentage
Notes	CSIRTs may rely on vendors or third parties for fixes, which can delay or limit visibility; mitigation strategies may be incomplete or unofficial. This metric reflects whether an actionable plan was established, regardless of who develops or applies it. Vulnerabilities documented as accepted risks (with justification) may be excluded from (N1) or tracked separately depending on organisational policy.

7.4 Service: Vulnerability coordination

7.4.1 Function: Vulnerability notification/reporting

Metrics: The following metrics are defined for this function:

- Percentage of vulnerabilities for which notification was sent to appropriate parties
- Vulnerability - time to notify

7.4.1.1 Metric: Vulnerabilities for which notification was sent to appropriate parties

Metric Attribute	Details
Name	Vulnerabilities for which notification was sent to appropriate parties
Description	Measures how many confirmed vulnerabilities were reported to at least one relevant CVD participant (e.g., vendor, PSIRT, coordinator) as part of the disclosure and coordination process.
Type	Implementation
Data Required	(N1) Number of vulnerabilities for which notification was sent to a relevant CVD participant (N2) Total number of confirmed vulnerabilities requiring notification
Calculation	(N1 / N2) * 100
Measure	Percentage
Notes	Requires clear documentation of notification attempts and recipient relevance; some parties may be hard to identify or reach. "Appropriate parties" should be defined in your coordination policy or process. This metric reflects completeness of outreach, not the quality of response.

7.4.1.2 Metric: Vulnerability - time to notify

Metric Attribute	Details
Name	Vulnerability - time to notify
Description	Captures the raw time interval between the confirmation of a vulnerability and the moment external parties are notified. This provides a baseline for statistical analysis and operational review.
Type	Efficiency
Data Required	(N1) Time of vulnerability confirmation (N2) Time of vulnerability notification
Calculation	N2 - N1
Measure	Number
Notes	Requires accurate and auditable logging of confirmation and notification events. Use statistical analysis tools (e.g., median, percentiles) separately to identify trends, outliers, or policy deviations.

7.4.2 Function: Vulnerability stakeholder coordination

***Metrics*:** No metrics are defined for this function. While the function is essential to coordinated vulnerability disclosure it is not independently measurable due to its reliance on external stakeholder actions and informal communication dynamics.

7.5 Service: Vulnerability disclosure

7.5.1 Function: Vulnerability disclosure policy and infrastructure maintenance

***Metrics*:** No metrics are defined for this function. It establishes foundational policy and infrastructure but does not yield directly measurable outcomes appropriate for routine performance metrics. If measuring if policy updates or stakeholder transparency become part of an audit or maturity initiative, consider adding metrics such as percentage of constituents with access to policy or number/frequency of updates to policy

7.5.2 Function: Vulnerability announcement/communication/dissemination

***Metrics*:** The following metric is defined for this function:

- Time to disseminate vulnerability information

7.5.2.1 Metric: Time to disseminate vulnerability information

Metric Attribute	Details
Name	Time to disseminate vulnerability information
Description	Measures the elapsed time between receipt of a vulnerability report and dissemination of constituent- or public-facing vulnerability information. Indicates how quickly the CSIRT can deliver actionable insights.
Type	Efficiency
Data Required	(N1) Time of vulnerability report receipt (N2) Time of vulnerability information dissemination
Calculation	N2 - N1
Measure	Number
Notes	Timing may be affected by dependency on vendor coordination, internal review cycles, or communication policy constraints. Use of the median is preferred to mitigate the effect of outliers. Be clear on what constitutes “dissemination” (e.g., advisory publication, direct communication, etc.).

7.5.3 Function: Post-vulnerability disclosure feedback

***Metrics*:** The following metrics are defined for this function:

- Percentage of post-disclosure inquiries responded to within defined time frame
- Number of follow-up incidents or implementation issues reported by constituents

7.5.3.1 Metric: Percentage of post-disclosure inquiries responded to within defined time frame

Metric Attribute	Details
Name	Percentage of post-disclosure inquiries responded to within defined time frame
Description	Tracks the percentage of constituent or stakeholder inquiries received after a vulnerability disclosure that are responded to within a pre-established timeframe. This reflects the responsiveness and readiness of the CSIRT to support constituents
Type	Effectiveness
Data Required	(N1) Total number of post-disclosure inquiries received (N2) Number of inquiries responded to within the defined time frame
Calculation	(N2 / N1) * 100
Measure	Percentage
Notes	May require integration between feedback channels and case management systems to track timing accurately. The defined time frame should be consistent with expectations (e.g., 48 or 72 hours). Median response time may also be tracked for internal review

7.5.3.2 Metric: Number of follow-up incidents or implementation issues reported by constituents

Metric Attribute	Details
Name	Number of follow-up incidents or implementation issues reported by constituents
Description	Measures how many constituents report either new incidents or implementation challenges related to the disclosed vulnerability. This provides insight into disclosure clarity and the downstream impact of vulnerability communication.
Type	Impact
Data Required	(N1) Number of follow-up incident reports or implementation challenges referencing a disclosed vulnerability

Metric Attribute	Details
Calculation	N1
Measure	Number
Notes	Requires tagging or associating post-disclosure reports with specific disclosures. May inform future improvements in communication format, mitigation guidance, or constituent outreach.

7.6 Service: Vulnerability response

7.6.1 Function: Vulnerability detection / scanning

***Metrics*:** The following metrics are defined for this function:

- Vulnerability scanning coverage
- Number of penetration tests conducted
- Average time from vulnerability disclosure to first scan

7.6.1.1 Metric: Vulnerability scanning coverage

Metric Attribute	Details
Name	Vulnerability scanning coverage
Description	Measures the percentage of in-scope assets that are covered by vulnerability scanning activities.
Type	Effectiveness
Data Required	(N1) Number of in-scope assets (N2) Number of in-scope assets scanned for vulnerabilities
Calculation	(N2 / N1) * 100
Measure	Percentage
Notes	Requires complete and accurate asset inventory, and integration with scanning tools.

Metric Attribute	Details
	Helps assess the breadth of detection efforts. Partial scans or intermittent asset availability can impact this metric. Depending on the types of vulnerability scans defined by your organisation and the criticality of your scanned assets, you will want to break down your numbers by these variables.

7.6.1.2 Metric: Number of penetration tests conducted

Metric Attribute	Details
Name	Number of penetration tests conducted
Description	Description: Tracks the number of formal penetration tests performed within a given period.
Type	Implementation
Data Required	(N1) Count of completed penetration tests
Calculation	N1
Measure	Number
Notes	Requires a consistent definition of what constitutes a penetration test and centralized tracking. Useful for tracking program maturity and compliance with policies or regulations that require periodic testing.

7.6.1.3 Metric: Average time from vulnerability disclosure to first scan

Metric Attribute	Details
Name	Average time from vulnerability disclosure to first scan
Description	Measures the responsiveness of the organisation in initiating detection efforts following a known vulnerability announcement.
Type	Efficiency

Metric Attribute	Details
Data Required	(N1) Time of public disclosure of the vulnerability (N2) Time of first scan or assessment for that vulnerability
Calculation	N2 −−N1 Averaged across relevant time spans
Measure	Mean
Notes	Requires timestamped records of both vulnerability disclosure events and scan activities. Coordination may be required. Helps assess how quickly detection processes are triggered after new threats emerge. Outlier events may warrant additional review.

7.6.2 Function: Vulnerability remediation

***Metrics*:** The following metrics are defined for this function:

- Mean time to remediate detected vulnerabilities
- Percentage of high-severity vulnerabilities remediated within defined time frame

7.6.2.1 Metric: Mean time to remediate detected vulnerabilities

Metric Attribute	Details
Name	Mean time to remediate detected vulnerabilities
Description	Measures the average elapsed time between the detection of a vulnerability and its remediation, reflecting how quickly known risks are addressed.
Type	Efficiency
Data Required	(N1) Time of vulnerability detection (N2) Time of vulnerability remediation
Calculation	N2 −−N1 (averaged across all relevant vulnerabilities and time spans)
Measure	Mean

Metric Attribute	Details
Notes	Requires integration of vulnerability detection and patch management records with accurate timestamps. Can help identify bottlenecks in the remediation pipeline. Outliers may require deeper investigation or policy exception tracking.

7.6.2.2 Metric: Percentage of high-severity vulnerabilities remediated within defined time frame

Metric Attribute	Details
Name	Percentage of high-severity vulnerabilities remediated within defined time frame
Description	Assesses the organisation's ability to meet remediation targets for vulnerabilities with high severity or risk ratings.
Type	Effectiveness
Data Required	(N1) Number of high-severity vulnerabilities detected (N2) Number of high-severity vulnerabilities remediated within defined timeframe
Calculation	(N2 / N1) * 100
Measure	Percentage
Notes	Requires consistent severity classification (e.g., CVSS) and policy-driven remediation timeframes. A key compliance and risk metric often aligned with internal SLAs or regulatory requirements.

ANNEX 1: Acknowledgements

- Peter Aarhus (Head of Cyber Defence Centre), CDC, Ørsted (DK)
- Vilius Benetis, NRD CIRT (LT)
- Leandro Rocha, (Security Engineer), Threat Detection, Nubank (BR)
- Rômulo Rocha (Lead Information Security Engineer), Nubank (BR)
- Sigitas Rokas, NRD CIRT (LT)
- Robin M. Ruefle (Co-Service Area Coordinator), CERT/CC, SEI, CMU (US)
- Désirée Sacher-Boldewin (Head of Operational IT Security), Finanz Informatik (DE)
- Logan Wilkins (Engineering Manager), CSIRT, Cisco (US)
- Mark Zajicek (Co-Service Area Coordinator), CERT/CC, SEI, CMU (US)

ANNEX 2: Terms and Definitions

- Alert – A notification generated by a detection mechanism indicating a potential security event or security incident.
- **Artefact** – A digital object or data item collected during incident response or analysis, such as a file, memory image, network capture, or log extract.
- **Capability** – A measurable activity that may be performed as part of an organization's roles and responsibilities. For the purposes of the FIRST services framework, the capabilities can either be defined as the broader services or as the requisite functions.
- **Capacity** – The number of simultaneous process-occurrences of a particular capability that an organization can execute before they achieve some form of resource exhaustion.
- **Chain of custody** – The documented process that ensures the integrity and authenticity of data or artefacts from collection through analysis and potential legal use.
- **Constituent** – An individual, group, or organization that is served by, or otherwise relies on, the CSIRT.
- **Containment** – Actions taken to limit the spread or impact of a security incident.
- **Coverage** – The extent to which controls, detection mechanisms, or services address identified threats, assets, or requirements.
- **Data required** – The discrete data elements necessary to calculate or understand a metric, listed within each metric definition and reset per metric.
- **Dynamic (runtime) analysis** – Analysis of an artefact by executing it in a controlled environment to observe its behaviour.
- **Efficiency metric** – A metric that examines timeliness or resource utilization, including how quickly activities are performed and issues are addressed.
- **Effectiveness metric** – A metric that evaluates how well a service, function, or control achieves its intended outcome.
- **False positive** – An alert, detection, or reported condition that is determined not to represent malicious or relevant activity.

- **Function** – An activity or set of activities aimed at fulfilling the purpose of a particular service.
- **Impact metric** – A metric that articulates the effect of information security activities on organizational mission, goals, objectives, or value.
- **Implementation metric** – A metric that demonstrates the presence, completeness, or progress of controls, processes, or capabilities.
- **Indicator of compromise (IOC)** – A piece of information associated with an incident that can be used to identify potentially malicious activity, such as IP addresses, domains, file hashes, registry keys, or process names.
- **Measure** – The form of the metric result, such as Percentage, Mean, Median, Number, or Ratio.
- **Metric** – A quantitative or qualitative measurement used to assess the performance, effectiveness, efficiency, coverage, or impact of a CSIRT service or function.
- **Metric type** – A classification describing the primary intent of a metric, used to indicate what aspect of a service or function is being measured.
- **Recovery** – Actions taken to restore systems and services to normal operation following a security incident.
- **Root cause** – The underlying reason why a security incident occurred, beyond immediate symptoms or indicators.
- **Security event** – An observable occurrence in a system or network that may indicate a security-relevant condition.
- **Security incident** – A security event or series of events that has been determined to have a negative impact on confidentiality, integrity, or availability.
- **Service** – A set of recognizable, coherent functions oriented toward a specific result that may be expected or required by constituents or stakeholders.
- **Service area** – A grouping of services related to a common aspect, used to organize services at a top level to facilitate understanding and communication.
- **Situational awareness** – An understanding of the current state of incidents, threats, and response activities sufficient to support effective decision-making.

- **Stakeholder** – An individual or organization that has an interest in the CSIRT's services, performance, or outcomes, but may not directly receive services.
- **Static analysis** – Analysis of an artefact without executing it, such as examining file structure, metadata, or code.
- **Triage** – The process of reviewing, categorizing, and prioritizing events, alerts, or incidents to determine appropriate handling.
- **True positive** – An alert, detection, or reported condition that correctly identifies malicious or relevant activity.
- **Vulnerability** – A weakness in a system, service, or configuration that could be exploited to compromise security.
- **Vulnerability disclosure** – The process of communicating information about vulnerabilities to affected parties, vendors, or the public.

ANNEX 3: Supporting Resources

Asana.org.
Story points: Estimation guide for user stories in Agile
https://asana.com/resources/story-points

2. **FIRST.org.**
   CSIRT Services Framework v2.1. Forum of Incident Response and Security Teams (FIRST), 2023.
   https://www.first.org/standards/frameworks/csirt-services

3. **FIRST.org.**
   Service Incident Timing Metrics v1. Forum of Incident Response and Security Teams (FIRST), 2023.
   https://www.first.org/global/sigs/metrics/Security-Incident-Timing-Metrics_v1.0.pdf

4. **ISO/IEC 30111:2019.**
   Information technology – Security techniques – Vulnerability handling processes, International organisation for Standardization

5. **ISO/IEC 29147:2018.**
   Information technology – Security techniques – Vulnerability disclosure. International organisation for Standardization

6. **NIST SP 800-61 Rev. 2.**
   Computer Security Incident Handling Guide. National Institute of Standards and Technology (NIST), 2012

7. **NIST SP 800-55v1.**
   Measurement Guide for Information Security - Volume 1, Identifying and Selecting Measures, National Institute of Standards and Technology (NIST), 2024

8. **NIST SP 800-115.**
   Technical Guide to Information Security Testing and Assessment. NIST, 2008

9. **NIST NVD (National Vulnerability Database).**
https://nvd.nist.gov/

10. **Common Vulnerability Scoring System (CVSS) v3.1.**
FIRST.org
https://www.first.org/cvss/

11. **CERT/CC.**
Vulnerability Disclosure Policy. Carnegie Mellon University Software Engineering Institute
https://www.kb.cert.org/vuls/html/disclosure

12. **ENISA.**
Coordinated Vulnerability Disclosure Guidelines. European Union Agency for Cybersecurity, 2018
https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-guidelines

ANNEX 4: Overview of all CSIRT Services and related Functions

SERVICE AREA
Information Security Event Management

Monitoring and Detection
- Log and Sensor Management
- Detection Use Case Management
- Contextual Data Management

Event Analysis
- Correlation
- Qualification

SERVICE AREA
Information Security Incident Management

Information Security Incident Report Acceptance
- Information Security Incident Report Receipt
- Information Security Incident Triage and Processing

Information Security Incident Analysis
- Information Security Incident Triage (Prioritization and Categorization)
- Information Collection
- Detailed Analysis Coordination
- Information Security Incident Root Cause Analysis
- Cross-Incident Correlation

Artifact and Forensic Evidence Analysis
- Media or Surface Analysis
- Reverse Engineering
- Runtime or Dynamic Analysis
- Comparative Analysis

Mitigation and Recovery
- Response Plan Establishment
- Ad Hoc Measures and Containment
- System Restoration
- Other Information Security Entities Support

Information Security Incident Coordination
- Communication
- Notification Distribution
- Relevant Information Distribution
- Activities Coordination
- Reporting
- Media Communication

Crisis Management Support
- Information Distribution to Constituents
- Information Security Status Reporting
- Strategic Decisions Communication

SERVICE AREA
Vulnerability Management

Vulnerability Discovery/Research
- Incident Response Vulnerability Discovery
- Public Source Vulnerability Discovery
- Vulnerability Research

Vulnerability Report Intake
- Vulnerability Report Receipt
- Vulnerability Report Triage and Processing

Vulnerability Analysis
- Vulnerability Triage (Validation and Categorization)
- Vulnerability Root Cause Analysis
- Vulnerability Remediation Development

Vulnerability Coordination
- Vulnerability Notification/Reporting
- Vulnerability Stakeholder Coordination

Vulnerability Disclosure
- Vulnerability Disclosure Policy and Infrastructure Maintenance
- Vulnerability Announcement/ Communication/Dissemination
- Post-Vulnerability Disclosure Feedback

Vulnerability Response
- Vulnerability Detection/Scanning
- Vulnerability Remediation

SERVICE AREA
Situational Awareness

Data Acquisition
- Policy Aggregation, Distillation, and Guidance
- Asset Mapping to Functions, Roles, Actions, and Key Risks
- Collection
- Data Processing and Preparation

Analysis and Synthesize
- Projection and Inference
- Event Detection (through Alerting and/or Hunting)
- Situational Impact

Communication
- Internal and External Communication
- Reporting and Recommendations
- Implementation

SERVICE AREA
Knowledge Transfer

Awareness Building
- Research and Information Aggregation
- Report and Awareness Materials Development
- Information Dissemination
- Outreach

Training and Education
- Knowledge, Skill, and Ability Requirements Gathering
- Educational and Training Materials Development
- Content Delivery
- Mentoring
- CSIRT Staff Professional Development

Exercises
- Requirements Analysis
- Format and Environment Development
- Scenario Development
- Exercise Execution
- Exercise Outcome Review

Technical and Policy Advisory
- Risk Management Support
- Business Continuity and Disaster Recovery Planning Support
- Policy Support
- Technical Advice

ANNEX 5: Metrics List by Function

7.2.2.1..... Metric: Percentage of vulnerability reports triaged within defined time frame

7.2.2.2 Metric: Percentage of vulnerability reports forwarded for handling

7.3.1 Function: Vulnerability triage (validation and categorization)

7.3.1.1 Metric: Vulnerabilities categorized and prioritized within defined timeframe

7.3.1.2 Metric: Distribution of vulnerabilities by category

7.3.2 Function: Vulnerability root cause analysis

7.3.2.1 Metric: Percentage of vulnerabilities with documented root cause and exploitation conditions

7.3.3 Function: Vulnerability remediation development

7.3.3.1 Metric: Percentage of analysed vulnerabilities with documented remediation or mitigation plan

7.4.1 Function: Vulnerability notification/reporting

7.4.1.1 Metric: Vulnerabilities for which notification was sent to appropriate parties

7.4.1.2 Metric: Vulnerability - time to notify

7.4.2 Function: Vulnerability stakeholder coordination

7.5.1 Function: Vulnerability disclosure policy and infrastructure maintenance

7.5.2 Function: Vulnerability announcement/communication/dissemination

7.5.2.1 Metric: Time to disseminate vulnerability information

7.5.3 Function: Post-vulnerability disclosure feedback

7.5.3.1 Metric: Percentage of post-disclosure inquiries responded to within defined time frame

7.5.3.2 Metric: Number of follow-up incidents or implementation issues reported by constituents

7.6.1 Function: Vulnerability detection / scanning

7.6.1.1 Metric: Vulnerability scanning coverage

7.6.1.2 Metric: Number of penetration tests conducted

7.6.1.3 Metric: Average time from vulnerability disclosure to first scan

7.6.2 Function: Vulnerability remediation

7.6.2.1 Metric: Mean time to remediate detected vulnerabilities

7.6.2.2 Metric: Percentage of high-severity vulnerabilities remediated within defined time frame

We welcome comments and feedback.
Please direct your email to *framework-metrics[@]first.org*.