Forum of Incident Response and Security Teams, Inc. (FIRST.Org)

Spring 2016 | 16

Security Incident Response Team (SIRT) Services Framework

Version 1.0

114

115

SIRT Services Framework

Introduction

The following is a list of services that a Security Incident Response Team (SIRT) organization may consider implementing to address the needs of their constituency, and the mechanisms to address gaps in the ability to do so. This list is meant to capture both traditional services performed by SIRTs as well as services that have recently emerged and are being undertaken by existing teams and organizations as they evolve. This document is a listing of the services that should comprise a SIRT Services Framework.

Each service below is broken down into the primary functions and sub-functions that support a SIRT's performance of that service in support of its broader mission. Please note that while they are represented here as unique, many of the functions and sub-functions are used to effectuate the delivery of multiple services and/or functions, and can be interdependent. Although this document recognizes that those relationships exist, it does not seek to define these interrelationships at this stage.

At a future date, Services will be grouped by like Services in a Services Area. Initially, this paper will focus on three Incident Response Team Types: National CSIRT; Sector CSIRT (critical infrastructure); and, Enterprise (organizational) CSIRT. A follow-on version of the Services Framework will also add two additional types: Product Security Incident Response Teams (PSIRT); and, Regional / Multi-Party Incident Response. Future Accompanying documents will provide exemplars for each type and the Service Areas / Services / Functions that are typically seen for building a base program. An additional document outlining the Tasks and Sub-tasks as well as Actions for each Sub-Function will also be published for the development of training modules. Maturity Levels are also being coordinated with several other parties to ensure that, globally, we are working towards consensus.

Purpose

The CSIRT Services Framework defines a set of services and functions that CSIRTs implement to serve their constituency. Its purpose is to facilitate CSIRT interoperability, global capability development activities, and education and training through the use of a global community-accepted terminology and approach to what a CSIRT performs.

History

The CERT/CC CSIRT Services List has been used in many cases to serve as a consistent and comparable description of CSIRTs and their corresponding services. In recent assessments of

existing CSIRT services lists, it was determined that although it was broadly used and adapted, the CERT/CC list was outdated and missing key components that represent the mission of modern-day CSIRTs. FIRST, interested in enabling the global development and maturation of CSIRTs, recognized that this was a key piece in framing the development of a comprehensive CSIRT education program. Given the geographical and functional span of the membership of FIRST, it was determined that the community that it assembles would be an appropriate source for definitive capture and representation of the services provided by CSIRTs. It was also determined that a similar approach for PSIRT Services needs to be undertaken and will be incorporated in a future version of this Services Framework.

Definitions

As used in this document, we are defining the use of certain terms. Note that Service Areas, Services and Functions identify *what* is being done at different levels of details, while Tasks and Actions identify *how* it is being done at different levels of details. Tasks and Actions are being published in an accompanying document and can / will be updated more frequently:

- **Service Area –** group services related to a common aspect. They help to organize the services along a top-level categorization in order to facilitate understanding. (This area will be further developed in Version 2.0.)
- **Service** – the set of recognizable, coherent actions towards a specific result on behalf of or for the constituency of an incident response team. The list of functions used to implement the service.
- **Function** – a means to fulfill the purpose or task of a specified service. The list of tasks that can be performed as part of the function
- **Tasks –** The list of actions that must be performed to complete the task

- **Actions –** the list of how something is done at varying levels of detail / maturity

- **Capability** – a measurable activity that may be performed as part of an organization's roles and responsibilities. For the purposes of the SIRT services framework the capabilities can either be defined as the broader services or as the requisite functions, sub-functions, tasks or actions.

- **Capacity** – the number of simultaneous process-occurrences of a particular capability that an organization can execute before they achieve some form of resource exhaustion.

- Maturity – how effectively an organization executes a particular capability within the mission and authorities of the organization. It is a level of proficiency attained either in actions or tasks or in an aggregate of functions or services.

Types of Incident Response Teams

- National CSIRT (Computer Security Incident Response Team) – A national CSIRT refers to an entity which is constituted by a National Authority to provide national-level coordination of

cybersecurity incidents. Its constituency generally includes all government departments and agencies, law enforcement and civil society. It also, generally, is the authority to interact with the national CSIRTs of other countries, as well as with regional and international players.

- Critical Infrastructure / Sectoral CSIRT – in charge of monitoring, managing and responding to cybersecurity incidents related to a specific sector (e.g. energy, telecom, finance)

- Enterprise (Organizational) CSIRT – An Enterprise CSIRT generally refers to a team in charge of monitoring, managing and handling cybersecurity incidents impacting the internal ICT infrastructures and services of a specific organization.

- Regional / Multi-Party CSIRT – A Regional / Multi-Party CSIRT refers to team or matrixed team in charge of monitoring, managing and responding to cybersecurity incidents related to a specific region, or a number of organizations.

- Product Security Incident Response Team (PSIRT) – A Product SIRT is a team within a commercial entity (typically a vendor) that manages the receipt, investigation, and internal or public reporting of security vulnerability information related to products or services commercialized by the organization.

Service 1 Incident Management

Function 1.1 **Incident Handling:** Services related to the management of a cyber-event, to include alerting constituents and coordinating activities associated with the response, mitigation, and recovery from an incident. Incident handling is dependent upon analysis activities, which are defined in the "Analysis" section.

Sub-Function 1.1.1 **Information Collection**: Services related to the intake, cataloging, and storage of information related to events and incidents to include:

- **Incident Report Collection:** Collection of reports regarding malicious or suspicious events and incident reports from constituents and 3rd parties (such as other security teams or commercial intelligence feeds), whether manual, automated or machine readable forms.
- **Digital Data Collection:** Gathering and cataloging of digital data that may be, but are not guaranteed to be, useful in understanding incident activity (e.g., disk images, files, network logs/flows).

- **Other data types (non-digital):** Gathering and cataloging of non-digital data (physical sign-in sheets, architecture diagrams, business models, site assessment data, policies, enterprise risk frameworks, etc.).
- **Artifact Collection:** The business and technical processes used to intake, catalog, store, and track artifacts believed to be remnants of adversary activity.
- **Evidence Collection:** The business of collecting information and data for possible use in law enforcement activities, often including capturing metadata regarding the source, method of collection, and owner and custody information.

Sub-Function 1.1.2 **Response**: Services related to reducing the impact of an incident and working to restore business functions within the constituency.

- **Containment:** Stopping immediate damage and limiting the extent of malicious activity through short-term tactical actions (for example, blocking or filtering traffic); can also involve regaining control of systems.
- **Mitigation:** Preventing further damage through eradication, implementing a work-around, or implementing more in-depth and comprehensive containment strategies.
- **Repair:** Implementing changes in the affected domain, infrastructure or network necessary to fix and prevent this type of activity from reoccurring. This includes strengthening the organizational defensive posture and operational readiness by policy changes and additional training and education.
- **Recovery:** Restoring the integrity of affected systems and returning the affected data, systems and networks to a non-degraded operational state.

Sub-Function 1.1.3 **Coordination**: Information sharing and advisement activity both internal and external to the CSIRT. This primarily occurs when the CSIRT is reliant on expertise and resources outside of direct control of the CSIRT to effectuate the actions necessary to mitigate an incident. By offering bilateral or multilateral coordination, the CSIRT participates in the exchange of information to enable those resources with the ability to take action to do so or to assist others in the detection, protection or remediation of on-going activities from adversaries.

Sub-Function 1.1.4 **Incident Tracking**: Documenting information about actions taken to resolve an incident, including critical information collected, analysis performed, remediation and mitigation steps taken, closure and resolution.

Function 1.2 **Vulnerability, Configuration and Asset Management:** Services related to the understanding and remediation of vulnerabilities, configuration issues and inventory of assets.

Sub-Function 1.2.1 **Vulnerability Discovery Research**: The identification of new vulnerabilities through research and experimentation (i.e., fuzz testing and reverse engineering).

Sub-Function 1.2.2 **Vulnerability Reporting**: The business and technical processes used to intake, catalog, store, and track vulnerability reports.

Sub-Function 1.2.3 **Vulnerability Coordination**: Notifying appropriate organizations of a vulnerability to affect repairs and to limit the potential impacts from exploitation.

Sub-Function 1.2.4 **Vulnerability Root Cause Remediation**: Implementation of the formal corrective actions necessary to correct an identified vulnerability. Typically, done by the product vendor.

Service 2 Analysis

Function 2.1 **Incident Analysis:** Services related to identifying and characterizing information about events or incidents such as scope, affected parties, involved systems, timeframes (discovery, occurrence, reporting), status (ongoing versus completed).
[Note: More in-depth analysis of an incident occurs through other, more focused analysis tasks such as artifact, misconfiguration, vulnerability, network, or forensics information analysis.]

Sub-Function 2.1.1 **Incident Validation**: Conclusively verifying that a reported incident in fact occurred and has had some impact on the involved systems.

Purpose: To provide technical proof that an event is a security incident, network or hardware error and identify the potential security impact and damage on the Confidentiality, Availability, and/or Integrity of information assets.

***Outcome**: Determine whether a reported event is indeed an incident that needs to be handled or whether the report can be registered in the relevant systems and closed without further action. Derive particulars of the events that have lead the constituent to believe that a security incident has indeed occurred and determine whether there is malicious intent or if there is a different reason – such as misconfiguration or hardware failure.*

Sub-Function 2.1.2 **Impact Analysis**: Identifying and characterizing the impact to the business function supported by involved systems.

Purpose: To identify the size and scope of the incident to include affected parts of the infrastructure, services, data, and department or organization. A general approach to remediation can be made based on this analysis.

***Outcome**: Determine the (potential) damage that an incident has incurred or might incur. Identify not only technical aspects, but also any media coverage, loss of trust or credibility and any reputational damage.*

Sub-Function 2.1.3 **Lessons Learned**: After-action review to identify improvements to processes, policies, procedures, resources, and tools to help mitigate and prevent future compromise.

Purpose: To determine what went wrong, implement preventative measures, and share the lessons learnt to the security community through publications and presentations.

***Outcome**: Set of recommendations to be considered as potential alterations to the information systems, processes and procedures within the relevant departments in the affected organization.*

Function 2.2 **Artifact Analysis:** Services related to the understanding of the capabilities and intent of artifacts (e.g., malware, exploits, spam, and configuration files) and their delivery, detection, and neutralization.

***Purpose:** As part of the incident handling process, digital artifacts may be found on affected systems or malware distribution sites. Artifacts may be the remnants of an intruder attack, such as scripts, files, images, configuration files, tools, tool outputs, logs, etc. Artifact analysis is done to find out how the artifact may have been used by an intruder, such as to get into an organization's systems and networks, or to identify what the intruder did once in the system. Artifact analysis strives to identify how the artifact operates on its own or in conjunction with other artifacts. This can be achieved through various types of activities including: surface analysis, reverse engineering, runtime analysis, and comparative analysis. Each activity provides more information about the artifact. Analysis methods include but are not limited to identification of type and characteristics of artifact, comparison to known artifacts, observation of artifact execution in a runtime environment, and disassembling and interpreting binary artifacts. By doing an analysis of the artifact(s), an analyst tries to reconstruct and determine what the intruder did, in order to assess damage, develop solutions to mitigate against the artifact, and provide information to constituents and other researchers.*

***Outcome:** Understand the nature of a recovered digital artifact along with its relationship to other artifacts, attacks, and exploited vulnerabilities. Identify solutions to mitigate against analyzed artifact(s) by understanding the tactics, techniques, and procedures used by intruders to compromise systems and networks and carry out malicious activities.*

Sub-Function 2.2.1 **Surface Analysis**: Identifying and characterizing basic information and metadata about artifacts (e.g., file type, strings output, cryptographic hashes, file size, filename); along with reviewing any public or private source information about the artifact.

***Purpose:** As a first step in gathering basic information, surface analysis compares information gathered from the artifact with other public and private artifacts and/or signature repository. All known information (i.e., potential damage, functionality, and*

mitigation) is gathered and analyzed. Further analysis may be required depending on the objective of the analysis being conducted.

***Outcome**: Identify characteristics and/or signature of digital artifact and any information already known about the artifact including maliciousness, impact, and mitigation.[1] (Such information can be used to determine next steps.)*

Sub-Function 2.2.2 **Reverse Engineering**: In-depth static analysis of an artifact to determine its complete functionality, regardless of the environment within which it may be executed.

***Purpose:** To provide a deeper analysis on malware artifacts to include identifying hidden actions and triggering commands. Reverse engineering allows the analyst to dig past any obfuscation and compilation (for binaries) and identify the program, script, or code that makes up the malware, either by uncovering any source code or by disassembling the binary into assembly language and interpreting it. Uncovering all of the machine language exposes functions and actions the malware can perform. Reverse engineering is a deeper analysis that is done when surface and runtime analysis do not provide the full information needed.*

***Outcome**: Derive complete functionality of a digital artifact to understand how it operates, how it is triggered, related system weaknesses that can be exploited, its full impact, and potential damage, therefore, developing solutions to mitigate against the artifact and, if appropriate, create a new signature for comparison with other samples.*

Sub-Function 2.2.3 **Runtime Analysis**: Understanding of an artifact's capabilities via observation while running the sample in a real or emulated environment (e.g., sandbox, virtual environment, and hardware or software emulators).

***Purpose:** To provide insight to the artifact's operation. Use of a simulated environment captures changes to the host, network traffic, and output from execution. The basic premise is to try to see artifact in operation in as close to a real-life situation as possible.*

***Outcome**: Gain additional insight on digital artifact's operation by observing its behavior during execution to determine affected host system's changes, other system interaction, and resulting network traffic in order to better understand system damage and impact, create new artifact signature(s), and determine mitigation steps. (Note: not all functionality is apparent from runtime analysis since not all artifact code sections may be triggered. Runtime only allows the analyst to see what the malware does in the test situation not what it is fully capable of doing.)*

Sub-Function 2.2.4 **Comparative Analysis**: Analysis focused on identifying common functionality or intent, including family analysis of cataloged artifacts.

Purpose: *To explore an artifact's relationship to other artifacts. It may identify similarities in code or modus operandi, targets, intent, and authors. Such similarities can be used to derive the scope of an attack (i.e., is there a larger target, has similar code been used before, etc.). Comparative analysis techniques can include exact match comparisons or code similarity comparisons. Comparative analysis provides a broader view of how the artifact or similar versions of it were used and changed over time, helping to understand the evaluation of malware or other malicious types of artifacts.*

Outcome*: Derive any commonalities or relationships to other artifacts in order to identify trends or similarities that may provide additional insights or understanding of digital artifact's functionality, impact, and mitigation.*

Function 2.3 **Media Analysis**: Services involving the analysis of relevant data from systems, networks, digital storage, and removable media in order to better understand how to prevent, detect, and/or mitigate similar or related incidents. These services may provide information for legal, forensic, compliance reviews or other historical reviews of information.

Purpose: *To collect and analyze evidence from media such as hard drives, mobile devices, removable storage, cloud storage, or other formats including paper or video. If the findings of the analysis are to be presented in a legal or compliance setting, the information will need to be collected in a forensically sound manner, which preserves the integrity and chain of custody of the evidence. The evidence may include artifacts such as malware left behind; change of state of files, registries, and other system components; network traffic capture or other log files, information in memory. Note that media analysis is looking to find evidence of what happened and optionally attribute that activity; it is different from artifact analysis, which looks to understand one artifact and its relationships. However, artifact analysis techniques may be used as part of the media analysis techniques and methods. These services may also be invoked outside a cyber incident but as part of a human resources issue or other legal or organizational investigation.*

Outcome: *Present findings that 1) inventory information assets (i.e., intellectual property or other sensitive information found); 2) provide a time-line of events that may shows additions, alterations and deletions made to any media assets involved in the incident, along with who or what performed those activities, if possible, and how all the evidence ties together to explain the extent and impact of the incident.*

Function 2.4 **Vulnerability / Exploitation Analysis:** Services provided to enable a deeper understanding of the vulnerabilities that have been a factor in a cyber-incident.

Sub-Function 2.4.1 **Technical (Malware) Vulnerability / Exploit Analysis**: Understanding the weakness(es) leveraged to instigate an incident and the adversarial tradecraft utilized to leverage that weakness.

Purpose: To inform the constituency of any known vulnerabilities (common entry points for attackers), thus systems can be kept up-to-date and monitored for exploits, minimizing any negative impact.

***Outcome**: Have a full grasp of a vulnerability and the way malicious actors will be able to use this vulnerability to execute their infiltration / exploitation of systems.*

Sub-Function 2.4.2 **Root Cause Analysis**: The understanding of the "design" or "implementation" flaw that allowed the attack.

Purpose: To identify the root cause and point of compromise, helping eradicate an issue completely.

***Outcome**: Have a firm grasp of the circumstances that allow a vulnerability to exist and in which circumstances an attacker can consequently exploit the vulnerability.*

Sub-Function 2.4.3 **Remediation Analysis**: The understanding of the steps necessary to fix the underlying flaw that enabled the attack, and prevent this type of attack in the future.

Purpose: To identify the issue that enabled the compromise, patch the vulnerability, change a procedure or design, review remediation by a third party, and identify any new vulnerabilities introduced in the remediation steps

***Outcome**: Establish a plan to improve processes, infrastructures and designs to close the specific attack vector and to prevent this attack in the future.*

Sub-Function 2.4.4 **Mitigation Analysis**: Analysis to determine the means to mitigate (prevent) the risks created as a result of an attack or vulnerability without necessarily remediating the underlying flaw that introduced it.

Service 3 Information Assurance

Function 3.1 **Risk / Compliance Assessment:** Services related to assessing risk or compliance assessment activities. This may include conduct of the actual assessment, to providing support to evaluate the results of an assessment. Typically done in support of a compliance requirement (e.g., ISO 27XXX, COBIT).

Purpose: To improve the identification of opportunities and threats; improve controls; improve loss prevention and incident management in conjunction with information security and other relevant functions.

Outcome: **Consistent process for information risk assessment and management applied to key assets and data; input to risk assessments; selection of relevant risk treatment options to include incident management and forensics where appropriate.**

Sub-Function 3.1.1 **Critical Asset/Data Inventory**: Identification of key assets and data that are critical to completing the organization's mission. These assets and data may not necessarily be owned by the organization (e.g., cloud provider or external data set). This includes identifying their location, their owner, their information sensitivity level, their mission function, and their current status / level.

Purpose: To identify on a regular basis those assets and data where incident management may be a requirement to enable the organization to complete its mission, in conjunction with the relevant lines-of-business.

Outcome: *A regularly updated inventory, list or database of key assets and data for use by the organization in risk assessments.*

Sub-Function 3.1.2 **Identify Evaluation Standard**: Gaining Organizational Risk Policy(ies) and enumerated/identified Standards by Executives for evaluation of Security Level/Status. Suggesting criteria for assessment or benchmarking for Enterprise Risk Managers and CISO's to consider. Examples of standards may include, but are not limited to, Basel II, COBIT, ITIL, Certification and Accreditation.

Purpose: To assist in the selection of an approved information risk assessment methodology for use in the organization and provide input into wider, organizational-level risk assessment and management.

Outcome: *A selected information risk assessment methodology for use across the organization; Executive-level support and buy-in for the selection made; organizational policies mandating the use of the selected risk assessment methodology where appropriate; agreed measures, templates and outputs; agreed process and procedures for information risk assessment; agreed mechanisms to integrate information risk assessment results into organizational-level risk management and decision-making.*

Sub-Function 3.1.3 **Execute Assessment**: Assist in conducting reviews and participating in assessments to ensure risk and security requirements are met / addressed.

Purpose: To complete the information risk assessment for a selected key asset or data, using the approved methodology, in as thorough a manner as possible.

Outcome: *A completed information risk assessment for the selected key asset or data.*

Sub-Function 3.1.4 **Findings & Recommendations**: Developing and providing findings, reports and/or recommendations (e.g., report writing, using the tasks in publication of information).

Purpose: To assist in the full documentation of the findings of a completed risk assessment and enumerate actions to be taken and recommendations to be considered as a result of the assessment.

Outcome: *An authorized, signed off, report detailing the critical asset or data, the risk assessment process followed, data used in the risk assessment, results, recommendations, actions, plans and timescales for distribution.*

Sub-Function 3.1.5 **Tracking**: Assist the CISO and/or Risk Manager in tracking both status of assessments and subsequent implementation of recommendations.

Purpose: To make sure that all plans, actions and recommendations are followed up and completed within the documented timescales.

Outcome: *Regular review of plans and timescales; list of completed actions; revisions to timescales if actions are not completed on time; report of progress against plans and timescales.*

Sub-Function 3.1.6 **Testing**: Active testing for compliance with risk levels. Can include penetration testing, vulnerability scanning and assessment, application testing, auditing and verification, etc.

Purpose: To test that the risk treatment(s) selected and implemented are fit for purpose, are implemented correctly, and provide the risk mitigation expected.

Outcome: *A documented test plan with expected results; documented tests and results; comparison with expected results; actions and timescales to correct any deviations from expectations.*

Function 3.2 **Patch Management:** Services that assist constituency with the capabilities necessary to manage the identification of inventory, systems to patch, deployment and verification of patch installation.

Purpose: To assist in the identification, acquisition, installation and verification of patches for products and systems and to provide an assessment of the utility and impact of patches from an incident management perspective.

Outcome: *Organizational awareness and understanding of the patches required; understanding of patches to be applied by service providers; understanding of the impact of patches on information risk; understanding of the impact on incident management.*

Function 3.3 **Operating Policies Management**: Services that develop, maintain, institutionalize, and enforce organizational concept of operations, and other policies.

Purpose: To act as a trusted advisor on business continuity and disaster recovery to a constituent or line-of-business by providing impartial, fact-based advice, taking into account the opportunity or problem under discussion, the environment in which the advice may be used and any resource constraints that apply.

Outcome: *Business decisions that incorporate business continuity and disaster recovery; incident management seen as a trusted advisor; members of the incident management team involved in business decisions when and where appropriate.*

Function 3.4 **Risk Analysis/Business Continuity Disaster Recovery Advisement:** Services provided to constituency related to organizational resilience activities based on risks identified. This could include a range of risk management activities, from conducting the actual assessment to providing analysis support in evaluating and mitigating the results of an assessment.

Purpose: To act as a trusted advisor on information security and incident management to a constituent or line-of-business by providing impartial, fact-based advice, taking into account the opportunity or problem under discussion, the environment in which the advice may be used and any resource constraints that apply.

Outcome: *Business decisions that incorporate information security and incident management; incident management seen as a trusted advisor; members of the incident management team involved in business decisions when and where appropriate.*

Function 3.5 **Security Advisement**: Services providing advice to a constituent or line-of-business on the execution and implementation of pertinent security operations or functions.

Service 4 Situational Awareness

Purpose: Situational Awareness is a collection of activities that gives an organization an awareness of its operating environment. Situational awareness involves the identification of critical elements that may affect an organization's mission, the monitoring of those elements and using this knowledge to inform decision-making and other actions.

Outcome: *Provide the necessary awareness of events and activities in and around the organization that may affect the organization's ability to operate in a timely and secure manner.*

Function 4.1 **Sensor/Metric Operations:** Services that focus on the development, deployment, and operation of systems and analysis methodologies to identify activities for investigation.

Purpose: To create the information collection infrastructure and processes necessary to provide situational awareness to the organization.

Outcome: *An operational information collection infrastructure (i.e. sensors) that provide information for situational awareness.*

Sub-Function 4.1.1 **Requirements Development**: Understanding the needs of the constituency and securing the authorizations under which the CSIRT can operate.

Purpose: The requirements development process identifies the situational awareness needs of the organization and then maps those requirements to the types of information needed to meet those objectives.

Outcome: *From an information perspective understand the level of awareness needed by the organization and its constituency. In addition, ensure the organization has all the necessary policy and legal approvals to collect the information.*

Sub-Function 4.1.2 **Identification of Necessary Data**: Determining the data necessary to fulfill requirements.

Purpose: Sensors come in a variety of forms from automated systems to humans. These sources of information (data) are used to build the situational awareness picture for an organization. The "Identification of Necessary Data" process maps situational awareness requirements to potential information sources (i.e., sensors).

Outcome: *The identification of data needed to support the situational awareness requirements of the organization. Some of the data sources may already exist while others may need to be engineered and/or acquired.*

Sub-Function 4.1.3 **Data Acquisition Methods**: Determining the methods, tools, techniques, and technologies used to gather necessary data.

Purpose: This process identifies methods for collecting, processing and storing the information (data) that is collected.

Outcome: *Determine the specific details as to how the information will be collected, stored, processed and sanitized.*

Sub-Function 4.1.4 **Sensor Management**: Maintenance and continual improvement of sensor performance relative to defined requirements.

Purpose: To maintain and monitor sensors to ensure proper functionality and accuracy.

Outcome: *Implementation of a sensor management and life-cycle sustainment program.*

Sub-Function 4.1.5 **Results Management**: Triage and dissemination of information and metrics derived from sensors. Usually, provided via a dashboard for view by various levels within an organization.

Function 4.2 **Fusion/Correlation:** Services that conduct analysis and inclusion of multiple data sources. Take feeds of information, regardless of the source, and integrate them into an overall view of the situation (Situational Awareness).

Purpose: Identify new relationships between incidents, indicators and actors that allow improved mitigation or response to a security incident.

Outcome*: Enable a consistent process for the organization to leverage new threat information, and integrate it with existing information available within the organization's knowledge repository. The final outcome of this process will be an improved set of information that enables the CSIRT to make decisions in a more efficient and accurate manner.*

Sub-Function 4.2.1 **Determine Fusion Algorithms**: Determine the methods and techniques (algorithms) or technologies used to analyze (fuse) the information.

Purpose: As part of incident handling, it is important that the CSIRT maintains a good operational view on information received from various sources. Fusion allows information to be managed in such a way that allows the CSIRT to rapidly take into account new

information as it is received, and fully contextualize this information and make it usable during the incident handling process.

***Outcome**: Develop an internal process that allows the intake of new information, its assessment in the context of existing information, and the successful exploitation of the resulting information available to the CSIRT, in the context of an incident.*

Sub-Function 4.2.2 **Fusion Analysis**: Analysis (fusing) of the data resources using the data in the knowledge management system to identify commonalities and relationships amongst the data.

Purpose: As part of incident handling, the CSIRT will need to continuously maintain an understanding of the threat a particular incident poses to the organization. In order to do so, it will need an up-to-date awareness of the incident itself and the evolution in the tactics, techniques and procedures leveraged by the adversary. It will need to continuously gather information, and assess it against existing information. Sub-function 4.2.2 will leverage the fusion algorithms selected in sub-function 4.2.1 to perform analysis of threat information obtained from external sources.

***Outcome**: Understand the impact of new threat information gathered against existing incidents, and well prepare the organization for any changes in TTP's by an adversary, or enable it to continuously update its mitigation and response techniques to better deal with related incidents.*

Function 4.3 **Development and Curation of Security Intelligence:** Services provided to internal or external constituents in the interest of developing and curating third party sources of security intelligence. Security intelligence can be defined as security and threat information that provides either operational intelligence or threat intelligence. Services may include, but are not limited to, analysis, development, distribution, and management of security intelligence, including threat indicators, threat detection logic such as antimalware rules and signatures, and adversary tactics, techniques, and procedures. These services are dependent upon information exchange activities, which are defined in section 5.6, "Outreach/Communications".

Purpose: Information from external entities is crucial for obtaining a sufficient level of situational awareness. A CSIRT needs a large amount of high-quality information relevant to its operation, but the cost and workload required to obtain it means that the efforts have to be focused on selected set of sources.

Outcome: *Multiple, high-quality data feeds covering all relevant areas of a CSIRT's operation are ingested - primarily through entirely automated processes - by the data management system (function 4.4). Another outcome is also processes to detect anomalies and changes in trends in the information streams obtained from the external sources.*

Sub-Function 4.3.1 **Source Identification and Inventory**: Continual identification, maintenance, and integration of information sources into knowledge management and analysis processes.

Purpose: Obtain relevant, high-quality information from external sources to perform effective incident response and to proactively increase the situational awareness (and the security posture of the organization, in general). External sources complement data collected internally: incident reports (function 1.1), vulnerability reports (function 1.2) and output from sensors operated by the CSIRT (function 4.1).

Outcome: *The acquisition of high-quality, relevant security information from internal, external, open source and/or commercial sources. All collected information is stored in the data management system (function 4.4).*

Sub-Function 4.3.2 **Source Content Collection and Cataloging**: The acquisition of threat information source materials. These sources may be both internal, external, open source and/or fee for service.

Purpose: Rate the quality of collected information. Observe changes in characteristics (including quantity) of data obtained from external sources to detect anomalies and/or new trends.

Outcome: *Documentation containing quality ratings of sources. Automated or semi-automated process to major changes in the overall characteristics of the information obtained from external sources.*

Function 4.4 **Data and Knowledge Management:** Services offered to constituents in support of capturing, developing, sharing, and effectively using organizational knowledge to include data markup (e.g., STIX, TAXII, IODEF, TLP), indicator databases, and malware / vulnerability catalogs.

Purpose: Constituents require cybersecurity data and knowledge at a level of quality and timeliness appropriate for their needs. Cybersecurity data consists of information intended to be processed by systems in order to support security automation. Cybersecurity knowledge consists of information intended for human cybersecurity analysts/operators. Additionally, other CSIRT services and functions require cybersecurity data and knowledge as inputs. Such information is best managed as an overall CSIRT resource given that most information is re-used across several services and functions.

***Outcome**: Cybersecurity data and knowledge of the required quality is provided to constituents in a timely fashion. Other CSIRT services and functions can easily obtain the data and knowledge they require from a single source within the CSIRT.*

- **Data Representation Management:** Standardization of how data is represented and exchanged (e.g., STIX, TAXII, IODEF, RID, etc.)
- **Data Storage Management:** The design, implementation and maintenance of storage management systems.
- **Data Digestion:** Processes and systems used to input, validate and store information.
- **Data Extraction:** Processes, policies and technical methods for extracting the information.
- **Tool Evaluation:** Evaluation and integration of tools used for data management, analysis, and collaboration.

Function 4.5 **Organizational Metrics**: Services that focus on identification, establishment, collection, and analysis of achievement of organizational performance goals, along with measuring organizational effectiveness.

Purpose: A key struggle for computer security incident response teams (CSIRT) and incident management organizations today is determining how successfully they meet their mission of managing cybersecurity incidents. As teams become more mature in terms of operational longevity, they are asking the question "How good am I really doing?". Teams are looking for ways to evaluate their operations to not only identify strengths and weaknesses in processes, technologies, and methods, but also to benchmark themselves against other similar teams. They are looking for quantitative evidence and metrics to show if they are effective in preventing, detecting, analyzing, and responding to cyber events and incidents. This function is focused on identifying what questions (information) need answering for management, CSIRT teams, and stakeholders among others to evaluate their operations and show value; establishing mechanisms for collecting the measurements to provide needed metrics, and then collecting, analyzing, and presenting results.

Outcome: *Provide the necessary awareness and empirical evidence to demonstrate how well an incident management organization is meeting and executing their mission; while identifying gaps for improvement. Use this information to facilitate decision making and improve performance and accountability.*

Service 5 Outreach/Communications

Function 5.1 **Cybersecurity Policy Advisory:** Services that support the development and adoption of cybersecurity policy to positively shape the environment of the CSIRT, its constituency, and other stakeholders by providing subject matter expert advice to inform decision makers.

Sub-Function 5.1.1 Internal

- **Policy and Legal Consultation:** Conveying policy and legal implications input related to organizational and constituent authorities and mandates.
- **Authoring Policy**: Producing policy as it relates to or affects organizations' or constituents' operations and authorities.

Sub-Function 5.1.2 External

- **Provide Policy Input:** Providing advice on technical and security policy issues that may impact the organization and its constituency or other partners.
- **Influence Policy:** Providing authoritative information or subject matter expertise to guide revision of policies, regulations, or laws. This can include, but is not limited to, testifying before legislative, scientific, or other bodies; writing position papers, white papers or articles; blogs or social media; meeting with stakeholders, etc.
- **Standards or Best Practices Development**: Contributing to the efforts of industry, global, regional, and national standards or best practice organizations (IETF, ISO, FIRST) to enable normalization of processes / best practices to maximize compatibility, interoperability, safety, repeatability, or quality.

Function 5.2 **Relationship Management**: Services that focus on establishment and maintenance of relationships for the organization.

Sub-Function 5.2.1 **Peer Relationship Management**: Development and maintenance of relationships with organizations that may be able to enable the execution of the mission of the CSIRT. This may involve ensuring interoperability or fostering collaboration between or across organizations.

Sub-Function 5.2.2 **Constituency Relationship Management**: Development and implementation of practices, strategies and technologies used to identify, distinguish, understand, manage, track, and evaluate constituents and stakeholders.

Sub-Function 5.2.3 **Communications Management**: Management of lists used to distribute announcements, alerts, warnings, data feeds and other publications or information sharing.

Sub-Function 5.2.4 **Secure Communications Management**: Management of secure communication mechanisms used for email, web, instant messaging, or voice communications.

Sub-Function 5.2.5 **Conferences / Workshops**: Providing opportunities for the CSIRT and its constituency to spend time together discussing threats and challenges that they are facing, strengthen trust relationships, exchange contacts, and share best practices or lessons learned.

Sub-Function 5.2.6 **Stakeholder Engagement/Relations**: Includes coordination with sector / vertical organizations, and maintaining formal points of contact with both internal and external stakeholders. Engagement with executive levels within the organization to educate on the mission of the organization and ensure security awareness understanding.

Function 5.3 **Security Awareness Raising** Services that work within the constituency to raise the collective understanding of threats that they face and actions that can be taken to reduce the risk posed by these threats.

Function 5.4 **Branding/Marketing**: Services that ensure that stakeholders and constituents are aware of the CSIRT and the capabilities provided by the CSIRT, as well as how they should interact with the CSIRT to convey their needs.

Function 5.5 **Information Sharing and Publications**: Services that focus on broad communication, including notifications made by the organization to their constituency in support of operations. Examples include notations of training, events, organizational policies and procedures.

Sub-Function 5.5.1 **Public Service Announcements**: Dissemination of security related information to improve awareness and implementation of organizational, constituent, sector or public security practices.

Sub-Function 5.5.2 **Publication of Information**:

- **Requirements Gathering:** Identifying what information is required to be disseminated, to whom, and in what manner and timeframe (scoping). Note: publication may be to a limited audience or more in-depth publication for partner audiences.
- **Development**: Defining the format and purpose of information products to fulfill requirements.
- **Authoring:** Accurately capturing information so that it is readily understood by the intended audience(s) (e.g., presenting the results of forensic, incident, vulnerability, and malware management activities).
- **Review:** Reviewing publication for clarity, accuracy, grammar, spelling, sensitivity, and adherence to information disclosure rules, and attaining final approval.
- **Distribution:** Delivery of information to intended audience via necessary and appropriate channels.

Service 6 Capability Building

Purpose: The make-up of a robust incident handling and response process and approach must always address capability building. It is central to an organization's overall performance and effectiveness. Organizations need to be more deliberate in understanding which capabilities truly impact their CSIRT and overall business performance and align their training programs accordingly. In a McKinsey survey, nearly 60% of the respondents indicated that building organizational capabilities is a top-three priority for their organizations. . However, when it came time to address what was needed most, just fewer than 30% actually focused their training programs on building the capability that adds the most value and what was needed for optimal performance.

One can define a capability as anything an organization does well that drives meaningful business results. Organizations need capabilities that are most critical to their overall business and Team performance and understand the outcomes of why they focus on the capabilities they have chosen. Culture does play a part in which capabilities an organization prioritizes and delivers. While top level management are usually involved in setting the tone and vision for organization capabilities, those that are most successful have aligned capabilities at the organizational level with those needed and required at the business unit or Team level.

***Outcome**: Understand, document and execute a plan and be able to utilize and measure the results and relationships of the various capability building opportunities, both at the individual Team member and at the overall organizational level of readiness. Define and practice a systematic approach that becomes part of overall workforce planning.*

Function 6.1 **Training and Education:** Capacity infers some level of capability at some level of maturity. Thus, Capability is the core building block for CSIRT Services. Capability Building provides training and education to a CSIRT constituency (which may include organizational staff, but excluding functional items such as HR training for the team) on topics related to cybersecurity, information assurance and incident response.

Purpose: A training and education program is usually the first step towards defining and putting into motion a capability building entity. This can be done through various types of activities including training and education, documented requisite knowledge, skills and abilities required, developed educational and training materials content delivery, mentoring, professional and skill development, and delivery of exercises and labs. Each of these activities will collectively contribute to the organization's and Team's capability.

***Outcome**: Understand the landscape of the training and education program as well as its relationship in supporting the CSIRT Team's Capability building. Be in a position to understand and document the types of Team and Organization results, as well as the KPIs to be able to understand progress achieved.*

Sub-Function 6.1.1 **Knowledge, Skill, and Ability Requirements Gathering**: Collecting knowledge, skill, and ability needs and the competence of a constituency in regard to determining what training and education should be provided.

Purpose: To properly assess, identify, and document what the CSIRT Team needs are in terms of requisite KSA's, to enable ready and strong Team members.

Outcome: *Identify needed characteristics of KSA's and a process by which the CSIRT Team can meet business needs and compare against others for best in class. This will help determine what level the Team is operating at, as well as if and where it has opportunities for improvement.*

Sub-Function 6.1.2 **Development of Educational and Training Materials**: Building or acquiring content of educational and training materials such as presentations, lectures, demonstrations, simulations, etc.

Purpose: Educational and training material development is used by a CSIRT Team to help maintain user awareness, keep the Team fresh with rapidly changing landscape and threats, and facilitate communications between the CSIRT and its constituencies.

Outcome*: CSIRT training and education materials that are of adequate quality; deliver to the needs of the rapidly changing CSIRT environment and utilize varied and effective presentation techniques and platforms.*

Sub-Function 6.1.3 **Delivery of Content**: Transfer of knowledge and content to "students". This can occur via various methods, such as computer-based training/online, instructor-led, virtual, conferences, presentations, lab, etc.

Purpose: A formal process for content delivery will help the Team identify a transparent approach to how CSIRT members are best able to receive their training.

Outcome: *A content delivery framework, which utilizes all available methods, presenting, learning of technical, soft skills and processes, using all alternative approaches, including hands-on labs, remote CBT and in person training, etc.*

Sub-Function 6.1.4 **Mentoring**: Learning from experienced staff, through an established relationship, can involve on-site visits, rotation (exchange), shadowing, and discussion rationale for specific decisions and actions.

Purpose: A Mentoring program is usually the first step towards defining and putting into motion a capability building entity. It can help provide a formal as well as informal mechanism for the mentor to share with the mentee about education and skill development, insights, and life and career experiences, outside of the official reporting relationship and structure of the Team.

Outcome: *A CSIRT Team that has increased retention, loyalty, confidence and overall ability to make sound decisions.*

Sub-Function 6.1.5 **Professional Development**: Helping staff members successfully and appropriately plan and develop their careers. Can include attending conferences, advanced training, cross-training activities, etc.

Purpose: Professional development is used by a CSIRT Team to promote a continuous process of securing new knowledge, skills and abilities that relate to the security profession, unique job responsibilities, and the overall Team environment.

Outcome*: Derive characteristics of professional development so the Team not only has confidence, but also has the requisite knowledge, skills and abilities that they directly transfer to practice, and are up to date based on the job roles and needs.*

Sub-Function 6.1.6 **Skill Development**: Providing training for organization staff on tools, processes, and procedures for daily operations functions.

Purpose: After the appropriate skills have been identified, a CSIRT Team needs to commit to a series of actions that will determine their ability for readiness.

Outcome: *Developed and trained staff with the needed technical, soft skills and process understanding. CSIRT members who are ready to address the daily operational challenges, supporting both the Team and its customers.*

Sub-Function 6.1.7 **Conducting Exercises**: Performing readiness testing of constituent "students" to test their ability to apply training and perform job or task functions. Can be in the form of virtual environments, simulations, field tests, table-tops, mock scenarios, or a combination.

Purpose: By conducting drills/exercises a CSIRT Team will increase its confidence in the validity of an organization's CSIR plan and its ability for execution.

***Outcome**: A Team that is as ready as possible, ensuring the KSAs key processes and execution of all work successfully together. This will also help determine the level the Team is operating at as well as if and where it has room for improvement.*

Function 6.2 **Organizing Exercises:** Services offered by the organization to constituents that support the design, execution and evaluation of cyber exercises intended to train and/or evaluate the capabilities of individual constituents and the constituency as a whole. These types of exercises can be used to:

- **Test policies & procedures:** Team assesses whether there are sufficient policies and procedures in place to meet the event. This is, generally, a paper/tabletop exercise.
- **Test operational readiness:** Team assesses whether the right people are in place to respond to the event and whether procedures are executed correctly. This, typically, involves exercising procedures.

Purpose: Exercises are conducted to improve the effectiveness and efficiency of cybersecurity services and functions. This function and associated sub-functions address both the needs of the organization as well as the needs of its constituents. More specifically, through the simulation of cybersecurity events/incidents, exercises can be used for one or several objectives:

- Demonstrate: Illustrate cybersecurity services and functions, as well as vulnerabilities, threats, and risks, in order to raise awareness.
- Train: Instruct staff on new tools, techniques and procedures.
- Exercise: Provide an opportunity for staff to use tools, techniques and procedures for which they have already received training. Exercising is necessary for perishable skills and helps improve and maintain efficiency.
- Assess: Analyze and understand the level of effectiveness and efficiency of cybersecurity services and functions.
- Certify: Determine whether a specified level of effectiveness and/or efficiency can be achieved for cybersecurity services and functions.

***Outcome**: The effectiveness and efficiency of cybersecurity services and functions will be directly improved, and lessons for further improvements will be identified. Depending on the specific objective(s) of an exercise, cybersecurity may also be demonstrated to stakeholders, staff can be trained, and the efficiency and effectiveness of services and functions can be assessed and/or certified. Lessons for improving future exercises can also be identified.*

Sub-Function 6.2.1 **Requirements**: Understanding the intent of the exercise, specifically, the objectives of all participants, to ensure that development incorporates these desires.

Purpose: The purpose of participating in exercises is to improve the effectiveness and efficiency of cybersecurity services and functions. The form of participation can be one of the following:

- Observer: Staff observe the conduct of an exercise but are not part of the target audience and are not challenged by the exercise events nor assessed for their performance. Observing without direct participation can help improve the effectiveness and efficiency of CSIRT services and functions to some extent. It can also help organize future exercises.
- Exercise Audience: Staff participate in an exercise as the target audience and are challenged by the exercise events, and may be assessed as well.

Depending on the modalities of the exercise, staff may travel to the exercise's location or participate remotely from their regular office or another suitable location. As well, the exercise may provide a specific environment or the participants may participate from their own exercise environment or their usual work environment.

***Outcome**: An improvement in the effectiveness and efficiency of cybersecurity services and functions, as well as the identification of lessons for further improvements. Depending on the specific objective(s) of an exercise, cybersecurity may also be demonstrated to stakeholders, staff can be trained, and the efficiency and effectiveness of services and functions can be assessed and/or certified. Lessons for improving future exercises can also be identified.*

Sub-Function 6.2.2 **Scenario and Environment Development**: Development of exercise scenarios in support of constituency objectives.

Purpose: The purpose of organizing exercises is to provide an opportunity for the target audience to improve the efficiency and effectiveness of their services and functions through the handling of simulated cybersecurity events/incidents.

***Outcome**: A specific target audience has improved the efficiency and effectiveness of its services and functions and has identified lessons for its further improvements. Lessons for improving future exercises have also been identified.*

Sub-Function 6.2.3 **Participation in an exercise**: An organization can have various levels of participation in an exercise due to its maturity level.

- **Evaluation:** Evaluate the outcomes of an exercise, solicit feedback, and identify lessons based on observation of the exercise.

- **Observation:** Observe a third-party exercise.
- **Coordination:** Coordinate an exercise.
- **Participation:** Participate in a cyber-exercise. Participant gets to choose the level of participation and gains from the outcome of the exercise (e.g., have a third-party evaluate their participation).

Sub-Function 6.2.4 **Identification of Lessons Learned**: Develop an after-action report which includes lessons learned or findings / best practices from the exercise.

Function 6.3 **Systems and Tools for Constituency Support:** Services that focus on recommendation, development, provision, and acquisition of cybersecurity related tools and services for a constituency. All of these systems and tools are related to CSIRT/security and not to general Information Technology; these systems could include messaging / alerting portals.

***Outcome**: CSIRT has processes and systems in place to identify constituent requirements and capabilities and acquires, provisions, or develops platforms to support these requirements.*

Function 6.4 **Stakeholder Services Support:** Services focused on technical capabilities offered by the CSIRT to assist in building capability, capacity, and maturity of CSIRT services to stakeholders. This is a maturation of service levels.

Purpose: Within the process of building and enhancing the capabilities of CSIRT constituency, a special focus is given to provide assistance on designing, acquiring, managing, operating and maintaining their infrastructure.

***Outcome:** Develop a systematic approach for infrastructure needs assessment, requirements definition, layout design, acquisition, compliance verification, maintenance and upgrades, operational training, internal and external audits.*

Sub-Function 6.4.1 **Infrastructure Design and Engineering**: Assisting in the design and engineering of the infrastructure to support constituency requirements.

Purpose: Provides broad understanding of the design methodology, knowledge of relevant standards and norms, and highlights best practices in designing and engineering the infrastructure, based on comprehensive needs assessment and analysis of the constituency requirements.

Outcome: *Practical experience in developing and comparing infrastructure design approaches and alternatives, based on international best practices and incorporating the relevant standards and norms.*

Sub-Function 6.4.2 **Infrastructure Procurement**: Assisting in the procurement of infrastructure, whether assisting in developing risk framework maturity or minimum-security requirements and standards for contract language (e.g., requiring compliance with a particular standard such as a product certification).

Purpose: Gain insight on developing the terms of reference for infrastructure procurement, in view of institutional, technical, and operational requirements.

Outcome: *Understanding the process of infrastructure procurement, while observing relevant standards and norms, and taking into consideration various technical measures and contracting procedures that need to be followed.*

Sub-Function 6.4.3 **Infrastructure Tool Evaluation**: Evaluation of tools on behalf of the constituency.

Purpose: Provide support in assessing the functionality and compliance of various tools, including hardware equipment, software, and custom applications.

Outcome: *Analysis of the performance of tools as well as their compliance with standards, norms, and the preset terms of reference.*

Sub-Function 6.4.4 **Infrastructure Resourcing**: Assisting in acquiring needed infrastructure resources. (i.e., hardware vendors, service providers, etc.)

Purpose: Highlight the key factors for achieving successful infrastructure resourcing, and develop mechanisms for establishing sustainable and effective relationships with solution providers and vendors based on clear responsibility and accountability.

Outcome: *Derive key performance indicators (KPIs) for infrastructure resourcing, with appropriate service level agreements (SLAs) that may provide for efficient and effective infrastructure resourcing.*

Service 7 Research/Development

Function 7.1 **Development of Vulnerability Discovery/Analysis/Remediation/Root Cause Analysis Methodologies**: Services that help define, identify new capabilities and improve methodologies for performing vulnerability related services or coordinating other organizations or commercial practices that can demonstrate the same.

Purpose: Some organizations will operate by only obtaining vulnerability information from external sources, but there are organizations that will have a need/desire to have organic capabilities to discover and analyze vulnerabilities. This function is intended to outline how an organization might architect these vulnerability research functions.

Outcome: *When necessary determine the methodologies an organization may use to better understand vulnerabilities.*

Function 7.2 **Development of processes for Gathering/Fusing/Correlating Security Intelligence**: Services that define, identify new capabilities, and improve methodologies for performing information analysis and sharing related services as it relates to operational and threat intelligences.

Purpose: In order to be successful, any security intelligence function must be able to collect information, as well as share relevant information with third parties. This collection is often dependent on human relationships between the sharing parties that effectuate a level of trust sufficient to enable sharing of sensitive information. An analyst must be able to develop these relationships, identify the appropriate sets of information that need to be shared, identify the protocols most suited for automated exchange, relationship management and joint investigations, and evaluate the effectiveness of an information source.

Outcome*: The organization has processes and procedures in place to collect, analyze, synthesize and assess the relevance of information from external sources that describe threats on information security assets. The organization has the organic ability to develop new sources and sharing partners.*

Function 7.3 **Development of Tools**: Services that develop, identify new capabilities, and share approaches to new tools and to automate the execution of CSIRT related processes.

Outcome*: Tools developed by CSIRTS to aid in automation of CSIRT related tasks are scalable, reliable, produce deterministic results, and do not degrade the security posture of the CSIRT using them. Frees analyst resources for non-routine tasks.*

Supporting Resources

FIRST - https://www.first.org

CERT/CC - http://www.cert.org

STIX/TAXII - https://stix.mitre.org

TLP - https://www.us-cert.gov/tlp

IETF - https://www.ietf.org

ISO/IEC 27035 -
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44379

Glossary

Application Testing – An investigation conducted to provide stakeholders with information about the quality of the product or service under test.

Basel II – The second of the Basel Accords, which are recommendations on banking laws and regulations issued by the Basel Committee on Banking Supervision.

Capability – A measurable activity that may be performed as part of an organization's roles and responsibilities. For the purposes of the CSIRT services framework, the capabilities can either be defined as the broader services or as the requisite functions, sub-functions, or tasks.

Capacity – The number of simultaneous occurrences of a particular capability that an organization can execute before they achieve some form of resource exhaustion.

CERT/CC – Computer Emergency Response Team Coordination Center.

CISO – Chief Information Security Officer.

Cloud – A distributed computing environment that allows application software to be operated using internet-enabled devices.

COBIT – Control Objectives for Information and Related Technology.

Cryptographic Hash – A hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone.

CSIRT – Computer Security Incident Response Team.

External Data Set – A third-party collection of data.

FIRST – Forum of Incident Response and Security Teams.

Function – A means to fulfill the purpose or task of a specified service.

Fuzz Testing – A software testing technique, often automated or semi-automated, that involves providing invalid, unexpected, or random data to the inputs of a computer program.

Hardware / Software Emulator – Hardware or software that enables one computer system (called the host) to behave like another computer system (called the guest). Typically, utilized to enable the host system to run software or use peripheral devices designed for the guest system.

IEC – International Electrotechnical Commission.

IETF – Internet Engineering Task Force.

IODEF – Incident Object Description Exchange Format, which is a data representation that provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incidents.

ISO – International Organization for Standardization.

ISO/IEC 27000-Series (ISO27k) – Information security standards that provide best practice recommendations on information security management, risks and controls within the context of an overall information security management system (ISMS), similar in design to management systems for quality assurance (the ISO 9000 series) and environmental protection (the ISO 14000 series).

ITIL – Information Technology Infrastructure Library, which is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business.

Maturity – How effectively an organization executes a particular capability within the mission and authorities of the organization.

Open Source – A development model that promotes universal access via a free license to a product's design or blueprint, and universal redistribution of that design or blueprint, including subsequent improvements to it by anyone.

Penetration Testing – An attack on a computer system with the intention of finding security weaknesses, potentially gaining access to it, its functionality, and data.

Reverse Engineering – The process of extracting knowledge or design information from anything man-made and re-producing it or reproducing anything based on the extracted information.

RID – Real-time Inter-network Defense, which is an inter-network communication method to facilitate sharing incident handling data while integrating existing detection, tracing, source identification, and mitigation mechanisms for a complete incident handling solution.

Sandbox – A security mechanism for separating running programs.

Service – The action of helping or doing work on behalf of or for the constituency.

STIX – Structured Threat Information eXpression, which is a collaborative community-driven effort to define and develop a standardized language to represent structured cyber threat information.

Strings Output – A resulting sequence of characters, either as a literal constant or as some kind of variable.

TAXII – Trusted Automated Exchange of Indicator Information, which is a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries.

TLP – Traffic Light Protocol. Used to ensure that sensitive information is shared with the correct audience.

1231 **Virtual Environment** – An emulation of a particular computer system.

1232 **Vulnerability Scanning and Assessment** – A security technique used to identify security weaknesses in a
1233 computer system.

1234

Annex – Service structure

As mentioned in the previous sections, the service structure adopted in this framework encompasses the identification of a three layers (service areas, service, and functions) which define the "what" and two additional layers (tasks and actions) which identify the "how".
In simple terms, the overall structure is as follows: