TLP:CLEAR

FIRST Services Framework: Team Types Within the Context of Services Frameworks

Version 1.2 – November 2025

Team Types

Within the Context of *FIRST Services Frameworks*

1 Purpose

Today there are many different types of operational entities that are involved in incident management. Even inside a single organization, multiple entities might exist, each with very different roles in monitoring, detecting, and handling threats, incidents, and vulnerabilities. Until the initial release of version 1.0 of this document, the cybersecurity community had no standard or common definition of these incident management capabilities or the services the capabilities offer.

The Forum of Incident Response and Security Teams (FIRST) Computer Security Incident Response Team (CSIRT) Framework Development Special Interest Group (SIG) has taken on the task of defining these incident management team types and aligning each with the services they offer based on the FIRST *CSIRT Services Framework*, which is also applicable to organizational entities or team types called Security Operation Centers.

Defining incident management team types is critical for creating structured, effective, and secure responses to cybersecurity threats. Specifying and defining types of incident management capabilities or teams will enable governments, industry, and other institutions to better align capabilities; handle threats, incidents, and vulnerabilities more effectively; and ensure that they meet diverse organizational and regulatory needs.

As of today, specific FIRST Services Frameworks have been developed for two team types: CSIRTs and Product Security Incident Response Teams (PSIRTs). While these frameworks include established definitions of CSIRTs and PSIRTs, in practice and within some communities or contexts, they have slightly different meanings. Rather than simply building on these established definitions, volunteers from the global community in the CSIRT SIG are working to develop an informal shared understanding of these and other relevant terms.

Other types of teams are becoming increasingly vital for addressing urgent cyber insecurity. Therefore, it is necessary to establish standard definitions for at least some of these teams as well. This document discusses two additional team types, Security Operations Centers (SOCs) and Information Sharing and Analysis Centers (ISACs), in greater detail in Section 3.

The terms describing the four basic team types—CSIRTs, PSIRTS, SOCs, and ISACs—are the first ones that the global community is considering. Future versions of this document will consider team sub-types such as national, sectorial, or coordination center variants; establish descriptive definitions; and identify the types of services that those teams deliver based on the *CSIRT Services Framework* service areas: Information Security Event Management, Information Security Incident Management, Vulnerability Management, Situational Awareness, and Knowledge Transfer.

2 Background

Over time, various entities (e.g., organizations, governments) in the CSIRT community have developed their own service lists and/or frameworks. However, as technology, tools, and processes have evolved, the community has realized that these lists and frameworks do not address certain topics and activities.

FIRST is interested in enabling the global development and maturation of CSIRTs and other security incident management entities. We launched a community-driven approach to developing an improved *CSIRT Services Framework* as part of the CSIRT SIG, and an initial version was published in 2017. As illustrated in Figure 1, the current version (v2.1) contains five distinct service areas and 21 associated services.

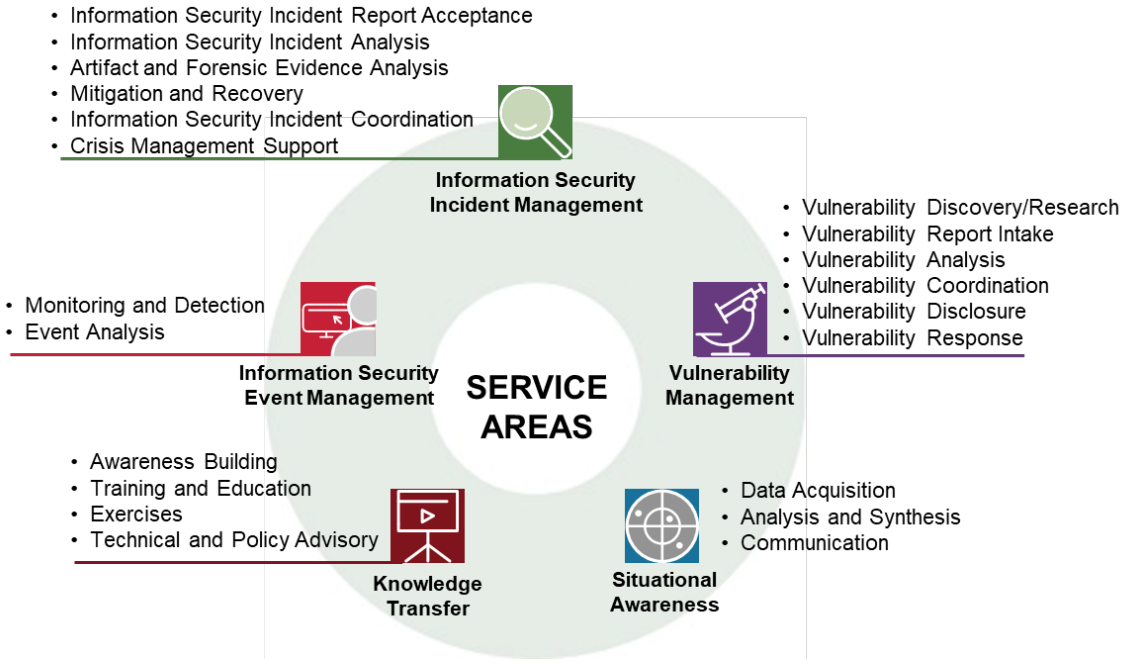

Figure 1: The CSIRT Services Framework's (v2.1) Five Service Areas and Their Associated Services

After the initial release of the *CSIRT Services Framework*, a similar approach was taken to develop a *PSIRT Services Framework* that recognizes the many operational aspects of PSIRTs that require a different set of services and corresponding activities. The first *PSIRT Services Framework* was published in 2018.

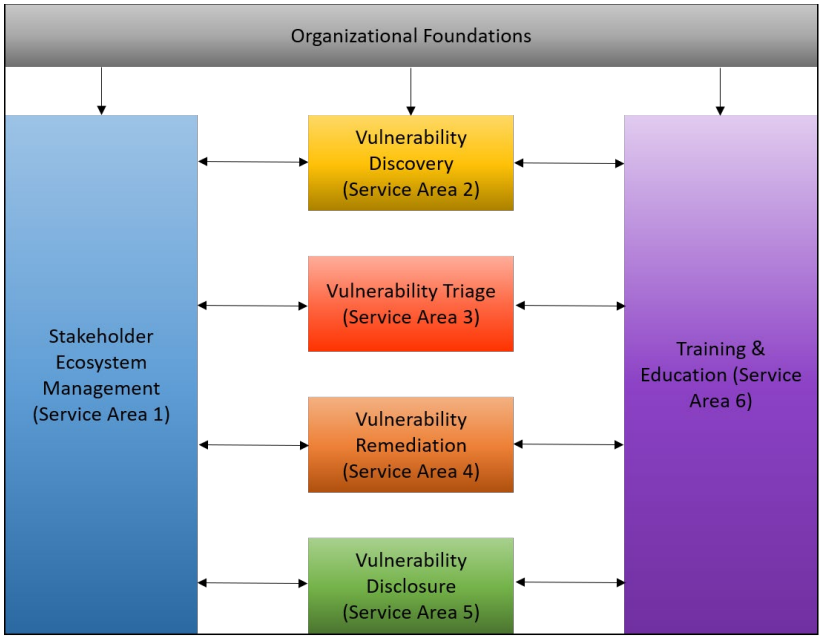

Figure 2: The PSIRT Services Framework's (v1.1) Interdependencies of Service Areas

The current versions of both the *CSIRT Services Framework* and the *PSIRT Services Framework* are available on the FIRST website:

- *CSIRT Services Framework*
  https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1
- *PSIRT Services Framework*
  https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1.1

The primary goal of these frameworks is to help establish and improve team operations. Other goals include helping teams identify and define their core categories of services and providing a standard set of terms and definitions that the community can use. The services described in these frameworks are those that a team could provide; in other words, no team is expected to provide all of the described services but can select the ones that support its mission and constituents as described by its mandate.

FIRST also recognizes that defining team types is a vital step in developing a common language for describing incident management entities and their capabilities. Therefore, in this report, we focus on team types.

3 Team Types: Capabilities that Handle Security Incidents, Threats, and Vulnerabilities

Different types of teams have various roles within the realm of information security[1] to prevent, detect, analyze, resolve, and/or mitigate information security incidents, threats, and/or vulnerabilities. These roles are evident not only because FIRST and other communities serve as forums for CSIRTs, but because these forums also bring together incident management and security teams, which have similar capabilities, to gather, discuss, and share information and develop resources.

In Section 1, we discussed the need to define four team types that provide information security and incident management capabilities: CSIRTs, ISACs, PSIRTs, and SOCs. In this section, we define each of these team types and provide profiles that show where some team types might be integrated. Each profile includes a description of the basic team type, focus area, and services offered.

The services associated with a team type are based on the *CSIRT Services Framework* v2.1. In this document, the services for each team type are provided in tables with the service areas and services listed in the first two columns. The last columns, titled "Offerings," are marked either with "MUST" or blank cells. The "MUST" designation means that this service must be provided for an organizational entity to be considered the designated team type. The term "MUST," as defined in RFC2119, "means that the definition is an absolute requirement of the specification" (see ANNEX 2). The services that are chosen as "MUST" are based on the activities usually provided by that particular team type and especially associated with the focus area that is listed in each team type description.

For example, in order for a CSIRT to be recognized as a CSIRT, the team must provide Information Security Incident Report Acceptance, Information Security Incident Analysis, Mitigation and Recovery, and Information Security Incident Coordination services within the Information Security Incident Management service area. See Table 1 for this example.

A blank cell with no "MUST" designation means that the service could be provided, is optional, or is not provided at all. For example, the Artifact and Forensic Evidence Analysis service within the Information Security Incident Management service area is not marked with "MUST" nor is the Training and Education service under Knowledge Transfer. This is because, although a CSIRT might provide these services based on its mission, constituency, or authority, this service could also be provided by another entity in another part of the parent CSIRT organization or referred to an external organization (such as law enforcement or an outside training group) for action. Oftentimes, such services may not be provided due to lack of resources, expertise, or funding.

CSIRTs, ISACs, PSIRTs, and SOCs can coexist. For example, a large, broadly scoped SOC might include a CSIRT as one of its divisions or departments; a CSIRT might include a SOC; and an ISAC

[1] *Information security* can be replaced with *cybersecurity* without affecting our discussion or definitions.

may include a SOC or a CSIRT. The hierarchy of these teams is not the most important aspect of the profiles we provide. What is most important are the following descriptions:

(1) the responsibilities and activities that each team or capability **provides**
(2) how to help members of the global community understand the **differences**

Both types of information will ultimately enable members of the global community to categorize their own team or capability in a commonly accepted manner. We based our definitions on the descriptions of services in *CSIRT Services Framework, Version 2.1* since it provides a unique and consistent namespace.[2] We recognize that the *PSIRT Services Framework* uses a different namespace, so we plan to map both namespaces in the future.

In subsequent reports, we will also describe other team types (e.g., national CSIRTs, sectorial CSIRTs) that are considered sub-types of the four team types listed above.

3.1 Computer Security Incident Response Teams (CSIRTs)

3.1.1 Description

CSIRTs provide services and support to a defined constituency. They manage information security incidents by preventing, handling (i.e., detecting, analyzing, responding), and/or coordinating information security incidents.

A CSIRT is often referred to as a CERT (Computer Emergency Response Team), CIRT (Computer Incident Response Team), CIRC (Computer Incident Response Center), CSIRC (Computer Security Incident Response Capability), or other name or abbreviation based on the objectives of the organization selecting its name. In the context of incidents, sometimes the word *computer* is used interchangeably with *cybersecurity*, *cyber*, or *information*.

A properly deployed CSIRT has a clear mandate, a governance model, a tailored services framework, technologies, and processes to provide, measure, and continuously improve defined services to raise its maturity. It might be established as a single unit, an independent organization, or a part of a larger cybersecurity organization like in many national cybersecurity centers (NCSCs).

National CSIRTs (nCSIRTs) and sectorial CSIRTs (including government CSIRTs) are special types of CSIRTs that focus on coordinating the response to information security incidents, threats, and vulnerabilities. Therefore, they provide all the services that are mandatory for any CSIRT. We will describe these and other CSIRT sub-types in future versions of this documents (release planned for mid of 2026).

2 In computing, a namespace is a set of names used to identify and refer to objects to ensure that all of a given set of objects have unique names and can be easily identified. In this report, we use namespace to refer to the names given to team types and the services they provide.

3.1.2 Focus Area

Regardless of the name used, this type of team specializes in information security incident management services or the management of incidents in other settings like information technology (IT) security, operational technology (OT) security, or specific subsets of information security. Some teams have an even narrower focus and provide services related only to incidents related to data protection or malware.

3.1.3 Services

The table here illustrates all potential services that a CSIRT can offer. The services that CSIRTs must offer are labeled MUST.

Computer Security Incident Response Teams (CSIRTs)

Service Area	Associated Services	Offering
Information Security Event Management	Monitoring and Detection	
	Event Analysis	
Information Security Incident Management	Information Security Incident Report Acceptance	MUST
	Information Security Incident Analysis	MUST
	Artifact and Forensic Evidence Analysis	
	Mitigation and Recovery	MUST
	Information Security Incident Coordination	MUST
	Crisis Management Support	
Vulnerability Management	Vulnerability Discovery/Research	
	Vulnerability Report Intake	
	Vulnerability Analysis	
	Vulnerability Coordination	
	Vulnerability Disclosure	
	Vulnerability Response	
Situational Awareness	Data Acquisition	
	Analysis and Synthesis	
	Service Communication	
Knowledge Transfer	Awareness Building	
	Training and Education	
	Exercises	
	Technical and Policy Advisory	

Table 1: CSIRT Service Offerings: Information Security Incident Management Service Area

3.1.4 Additional Considerations

Two service offerings, although important, are not mandated for all CSIRTs: *Artifacts and Forensic Evidence Analysis* and *Crisis Management Support*. Because of their unique nature, we describe them in more detail:

Artifact and Forensic Evidence Analysis

This is an important service for managing information security incidents and enabling a meaningful response. However, this service requires a significant level of expertise and relies on costly resources, which may not always be readily available or cost effective in an organizational setting, especially for small teams. While it might pose challenges, it is likely more cost effective for an internal CSIRT to outsource this service and pay only for instances that require such detailed analysis. For these reasons, we do not consider *Artifact and Forensic Evidence Analysis* a MUST for all CSIRTs to offer.

Crisis Management Support

This service is not considered a MUST for all CSIRTs to offer. During large critical incidents, significant resources are required for coordination, communication, and overall management. If a CSIRT is not appropriately staffed, these activities may compete with other activities, such as technical investigations, incident analysis, incident response, and incident mitigation. The result can be mismanaged or poorly handled information security incidents.

Crisis Management Support typically involves a broad scope of the organization and might not even be caused by an information security incident but rather a disaster or significant outage of equipment not related to malicious cyber activity. Since Crisis Management Support often requires multiple teams and departments of an organization to collaborate, a CSIRT is clearly one of the units that could be involved. However, in most cases, even in a cyber or information security incident, the CSIRT might not take the lead in managing the crisis. While a CSIRT may not be equipped to manage all types of crises, its support might be crucial, especially if a crisis affects the information infrastructure or critical information system assets.

.

3.2 Information Sharing and Analysis Centers (ISACs)

3.2.1 Description

ISACs are industry-specific organizations or capabilities that gather, analyze, share, and coordinate information about cyber threats and incidents among critical infrastructures or industry sector entities (e.g., the finance sector). ISACs can also facilitate data sharing among public and private sector groups in accordance with government policies or national laws and might even be organized as public-private partnerships.

In the United States, ISACs are required in specific industry sectors. In other regions or countries, ISAC activities are driven by the industry they belong to, but they cover more sectors. For example, in Europe, an effort was made to collect information about various ISACs.[3] An information sharing and analysis organization (ISAO) is an alternative name for an ISAC and ISAC-type organizations.

3.2.2 Focus Area

ISACs focus on analyzing information security attacks, incidents, and threats based on the insights gained through situational awareness. They focus on collecting threat information, analyzing it, and creating intelligence. Synthesizing and disseminating this information is designed to help organizations that experience incidents to become more cyber resilient and capable of taking proactive steps when new trends are identified or when developments occur.

3.2.3 Services

The table below illustrates all potential services that an ISAC can offer. The services that ISACs must offer are labeled MUST.

3 For more information about EU ISACs, see their website: https://www.isacs.eu/european-isacs.

Information Sharing and Analysis Centers (ISACs)

Service Area	Associated Services	Offering
Information Security Event Management	Monitoring and Detection	
	Event Analysis	
Information Security Incident Management	Information Security Incident Report Acceptance	
	Information Security Incident Analysis	
	Artifact and Forensic Evidence Analysis	
	Mitigation and Recovery	
	Information Security Incident Coordination	
	Crisis Management Support	
Vulnerability Management	Vulnerability Discovery/Research	
	Vulnerability Report Intake	
	Vulnerability Analysis	
	Vulnerability Coordination	
	Vulnerability Disclosure	
	Vulnerability Response	
Situational Awareness	Data Acquisition	MUST
	Analysis and Synthesis	MUST
	Service Communication	MUST
Knowledge Transfer	Awareness Building	
	Training and Education	
	Exercises	
	Technical and Policy Advisory	

Table 2: ISAC Service Offerings: Situational Awareness Service Area

3.2.4 Additional Considerations

ISACs might also handle some aspects of information security incident management and/or vulnerability management, usually with an emphasis on coordination and especially supporting dissemination and communication.

In many cases, situational awareness is also gained by CSIRTs and SOCs; however, gaining situational awareness is usually not these teams' only mission. Instead, situational awareness is acquired a result of insights drawn from the other services they provide including Information Security Incident Report Acceptance, Information Security Incident Analysis, Mitigation and Recovery, and Information Security Incident Coordination, etc. PSIRTs may also gain situational awareness as a result of their mission.

3.3 Product Security Incident Response Teams (PSIRTs)

3.3.1 Description

Many vendors or service providers, including open source communities, have already established PSIRTs. The following definition of PSIRT is from the version 1.1 (2020) of the *PSIRT Services Framework:* [4]

> *"A Product Security Incident Response Team (PSIRT) is an entity within an organization which, at its core, focuses on the identification, assessment and disposition of the risks associated with security vulnerabilities within the products, including offerings, solutions, components and/or services which an organization produces and/or sells."*

PSIRTs provide the following services:

(1) Manage the receipt of vulnerabilities and coordinate vulnerability disclosure i.e. in their own products.
(2) Track and mitigate vulnerabilities (apply provided fixes) in an upstream vendor's component that is included in their own products throughout the lifecycle of the product.
(3) Manage and coordinate vulnerability remediation with other responsible teams.

A well-deployed PSIRT is not an isolated group; it remains closely connected to the development of the organization's products and is part of the organization's broader secure engineering initiative. This organizational structure ensures that security assurance and risk reduction activities are integrated into the development lifecycle and engineering teams are involved in those processes.

Product security incident response is often associated with the maintenance phase since most product security vulnerabilities are reported as quality escapes[5] after the product's release to the market. However, PSIRTs can have a significant impact in early requirements gathering during architecture, design, planning, and risk modeling phases. PSIRTs can also add value by providing guidance and oversight for handling security issues found internally (e.g., during development).

3.3.2 Focus Area

PSIRTs focus on vulnerability management in products and services. They are specialized teams or capabilities that respond within vendor organizations or service providers to handle and resolve vulnerabilities in products or services.

3.3.3 Services

The table below illustrates all potential services that a PSIRT can offer. The services that PSIRTs must offer are labeled MUST.

[4] For more information about PSIRTs, see the *PSIRT Services Framework, Version 1.1*: https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1.1.

[5] A *quality escape* is when development and testing fail to identify/resolve a vulnerability, allowing it to reach the customer.

Product Security Incident Response Teams (PSIRTs)

Service Area	Associated Services	Offering
Information Security Event Management	Monitoring and Detection	
	Event Analysis	
Information Security Incident Management	Information Security Incident Report Acceptance	
	Information Security Incident Analysis	
	Artifact and Forensic Evidence Analysis	
	Mitigation and Recovery	
	Information Security Incident Coordination	
	Crisis Management Support	
Vulnerability Management	Vulnerability Discovery/Research	
	Vulnerability Report Intake	MUST
	Vulnerability Analysis	MUST
	Vulnerability Coordination	MUST
	Vulnerability Disclosure	MUST
	Vulnerability Response	MUST
Situational Awareness	Data Acquisition	
	Analysis and Synthesis	
	Service Communication	
Knowledge Transfer	Awareness Building	
	Training and Education	
	Exercises	
	Technical and Policy Advisory	

Table 3: PSIRT Service Offerings: Vulnerability Management Service Area

3.3.4 Additional Considerations

One service offering, although important, is not mandated for all PSIRTs: *Vulnerability Discovery / Research*. *Vulnerability Discovery / Research* is a service that identifies new vulnerabilities. Identifying vulnerabilities enables a meaningful response by the PSIRT. However, to handle known vulnerabilities, these services require significant resources, which are not always available. As other sources of knowledge about new (i.e., yet unknown) vulnerabilities become available, it is reasonable to exclude *Vulnerability Discovery/Research* from a PSIRT's portfolio. Therefore, we do not consider *Vulnerability Discovery/Research* in the mandatory services that a PSIRT offers.

PSIRTs might also provide information security incident management services and situational awareness by supporting incident response coordination, communication, and the mitigation of actively exploited vulnerabilities or the discovery of new threats within their customer base or the broader community.

While there are important differences between any CSIRT and PSIRT, it is crucial to recognize that there is also synergy between these types. The key takeaway is that CSIRTs and PSIRTs do not operate independently; they often work together. For example, many CSIRTs warn constituents about security vulnerabilities; these warnings are almost always based on information that vendor PSIRTs provide.

3.4 Security Operations Centers (SOCs)

3.4.1 Description

SOCs typically handle many different facets of security operations and focus on information security event management (i.e., event monitoring and detection). Regardless of whether it is in-house or outsourced, the analysts, experts and automatic processes monitoring the IT infrastructure need to do that continuously to facilitate faster threat detection and more (cost-) effective reactions. Very often a SOC's mission includes initiating the response process or taking proactive measures to improve the security posture of the organization, its users, its partners, or even customers.

In order to effectively monitor and address threats, the SOC usually needs maintain or gain access to an inventory of the assets that should be monitored. In addition, the SOC needs access to logs, status of assets, and security events from tools like firewalls, anti-virus, email phishing, and malware detection solutions in order to analyze and monitor the organization's current security posture.

3.4.2 Focus Area

A SOC typically focused upon monitoring the networks and systems of its organization for unusual, anomalous, or suspicious activity using multiple cybersecurity related tools. These tools can be products, software, or hardware and include network taps, endpoint detection, event sensors, and more.

Some SOCs may also perform response activities using automated or predefined use cases or playbooks; they escalate any issues that do not align with those cases/playbooks to established contacts, or they promptly alert victim organizations.

SOCs may provide information security incident management services and vulnerability management services independently or rely on other teams for support.

3.4.3 Services

The table on the following page illustrates all potential services that a SOC can offer. The services that SOCs must offer are labeled MUST.

Security Operations Centers (SOCs)

Service Area	Associated Services	Offering
Information Security Event Management	Monitoring and Detection	MUST
	Event Analysis	MUST
Information Security Incident Management	Information Security Incident Report Acceptance	
	Information Security Incident Analysis	
	Artifact and Forensic Evidence Analysis	
	Mitigation and Recovery	
	Information Security Incident Coordination	
	Crisis Management Support	
Vulnerability Management	Vulnerability Discovery/Research	
	Vulnerability Report Intake	
	Vulnerability Analysis	
	Vulnerability Coordination	
	Vulnerability Disclosure	
	Vulnerability Response	
Situational Awareness	Data Acquisition	
	Analysis and Synthesis	
	Service Communication	
Knowledge Transfer	Awareness Building	
	Training and Education	
	Exercises	
	Technical and Policy Advisory	

Table 4: SOC Service Offerings: Information Security Event Management Service Area

3.4.4 Additional Considerations

The service offerings listed for SOCs as a must are those that focus upon events monitoring and detection, and event analysis. This reflects our experience that most SOC teams are constantly sifting through logs and event on endpoints, networks, cloud services, and other infrastructure related signals to find cybersecurity relevant information. This also means the teams are performing near constant IT, OT and/or information system related event analysis. This analysis may include determining if an event is security related, determining the severity of an event, determining if the event contains any suspicious activity, determining the relationship of one event to others, and much more.

If an event (or information derived from any event) is determined to be cybersecurity related and of sufficient importance to the organization to act upon, it is often escalated by the SOC into other services including incident prevention or even incident response. These services (or portions of them) may be provided by the SOC but they do not have to be. Sometimes prevention or response services are provided by other specialized teams (or other entities/units) including proactive cyber defensive engineering teams, CSIRTs, hunt teams, and many more.

Due to their monitoring and analysis focus, SOCs may also frequently gain information that contributes to situational awareness services, vulnerability management services, or knowledge transfer.

4 Overview and further Considerations

We studied the mandatory services that characterize each of the four basic team types (i.e., CSIRTs, ISACs, PSIRTs, and SOCs) that provide information security incident management capabilities. In this section, we summarize our findings and address specific questions about these team types. This section is a comprehensive record of our work in the CSIRT SIG to develop an informal shared understanding of these team types and their capabilities.

4.1 Defining Four Basic Team Types

Table 5 is an aggregation of the four tables introduced in earlier sections. It illustrates that four of the five service areas each provide the foundation for a defined basic team type.

Service Area: Information Security Event Management	SOC	CSIRT	PSIRT	ISAC
Monitoring and Detection	MUST			
Event Analysis	MUST			
Service Area: Information Security Incident Management	**SOC**	**CSIRT**	**PSIRT**	**ISAC**
Information Security Incident Report Acceptance		MUST		
Information Security Incident Analysis		MUST		
Artifact and Forensic Evidence Analysis				
Mitigation and Recovery		MUST		
Information Security Incident Coordination		MUST		
Crisis Management Support				
Service Area: Vulnerability Management	**SOC**	**CSIRT**	**PSIRT**	**ISAC**
Vulnerability Discovery/Research				
Vulnerability Report Intake			MUST	
Vulnerability Analysis			MUST	
Vulnerability Coordination			MUST	
Vulnerability Disclosure			MUST	
Vulnerability Response			MUST	
Service Area: Situational Awareness	**SOC**	**CSIRT**	**PSIRT**	**ISAC**
Data Acquisition				MUST
Analysis and Synthesis				MUST
Communication				MUST
Service Area: Knowledge Transfer	**SOC**	**CSIRT**	**PSIRT**	**ISAC**
Awareness Building				
Training and Education				
Exercises				
Technical and Policy Advisory				

Table 5: Mapping of Service Areas to Team Types

4.2 Why *Knowledge Transfer* Is Not a Must for Any Team Type

All four team types (i.e., CSIRT, ISAC, PSIRT, SOC) likely perform some services of the *Knowledge Transfer* service area. This service area is crucial for each type of incident management or security capability because these capabilities collect relevant data; perform detailed analysis; identify threats, trends, and risks; and create best current operational practices to help organizations detect, prevent, and respond to information security incidents. Transferring this knowledge to their constituents is crucial to improving overall information security at organizational and community levels.

The Training and Awareness service is important to all incident management capabilities and their constituencies. It may be more prevalent in CSIRTs and ISACs, but for defined communities of interest, PSIRTs and SOCs can also conduct this service. Training exercises are suitable for all four team types and technical or policy advisory roles.

However, it is resource intensive for any incident management capability to develop and deliver training materials; therefore, it is not always possible to provide the Training and Awareness service. It is often more effectively handled by specialized units of a team's parent organization (e.g., a training group or an external third-party contractor with expertise in knowledge transfer). When specialized units provide this service, the ideal approach involves these units gathering input from the incident management team and subsequently producing content based on this input, which is then delivered in training and distributed in materials.

For these reasons, no *Knowledge Transfer* activities should be considered a MUST for any of the four team types. However, this does not mean that these team types would not provide these services, but these services are not mandatory for CSIRTs, ISACs, PSIRTs, or SOCs.

4.3 Why We Did Not Define *Managed Security Service Providers*

Managed security service providers offer a variety of security incident management related services, which would be considered a CSIRT or SOC offering in most other contexts. It is entirely acceptable to provide a range of services, especially when customers are paying for them.

Therefore, we believe that it is acceptable to offer CSIRT services to customers, but when they are offered, they should be compatible with our definition of services offered by a *CSIRT*. That means that additional services might be offered, but no service considered mandatory (i.e., labeled *MUST*) should be omitted.

For marketing reasons, service providers may call themselves whatever they want. Ultimately, it is the responsibility of the customer to confirm whether the services offered fulfill their requirements.

As the cybersecurity ecosystems grow and extend their scope, such membership organizations as FIRST or TF-CSIRT and all global or national cybersecurity communities need to consider team types as part of their onboarding and maintenance processes. Members should be encouraged to consistently use the proper team type not only for membership applications but also for

mandates, charters, frameworks, policies, and procedures as well as materials and communications related to their service offerings.

Because membership is usually understood as some kind of endorsement, it might be important to establish rules that prevent teams from using misleading acronyms and names that set incorrect expectations. If, for example, a team claims to be a CSIRT by name but is not offering the full set of services identified as "MUST," the team identification needs to be reconsidered. In such cases, the minimum an organization should do is clarify the team type to avoid any false impressions that might arise by looking at the membership directory.

Having team types recognized by membership organizations ensures that teams are meeting specific requirements for particular team types.

4.4 Why We Did Not Define a SOC as Part of a CSIRT or Vice Versa

As we described earlier, a SOC and a CSIRT can be implemented independently since they each can provide distinct services. However, if both teams exist within the same organization, it is imperative to establish suitable interfaces between them.

In many contexts, only one team exists—either a SOC or a CSIRT. However, whichever team it is must be careful about the services it offers. A name that includes only *CSIRT* or *SOC* might not represent the entire set of services it provides. The name only reflects the focus of the team and the emphasis of the parent organization. This is especially obvious when we analyze the requirements further:

- ***A SOC without a CSIRT*** must have a process for managing the identified information security incidents or analyzing further potential incidents. This process does not have to be a CSIRT's responsibility, but many organizations choose to implement a CSIRT-like capability that is sometimes organizationally integrated within a SOC.
- ***A CSIRT without a SOC*** must have a process for independently analyzing all available information security events. It must also manage the critical data sources used to identify attacks and assess their success. If large amounts of data must be analyzed, SOC-like services must be used. This analysis does not have to be a SOC's responsibility, but many organizations choose to implement a SOC-like capability since it is a functional and economic solution. As stated earlier, sometimes both CSIRT and SOC teams are organizationally integrated.

This framework does not address how two team types that collaborate to respond to information security incidents are structured inside the organization and which is the principal team that is ultimately responsible for the services provided. As part of its governance structure, the organization must define the roles and responsibilities and the authority of both team types. In practice, some organizations form these combined teams and call them a SOC; other organizations use CSIRT as part of the name. Both approaches are acceptable; there are no rules about how to name an internal team.

4.5 Why We Did Not Define a New Name for a Combined CSIRT and PSIRT

In some organizations that are typically categorized as vendors, various incident management capabilities coexist. Originally, mostly CSIRTs and PSIRTs coexisted; however, a SOC (at least) will now also likely coexist with the CSIRT and PSIRT in these settings. Since CSIRTs and PSIRTs share some common needs and are built on similar internal support services (e.g., a hotline for their constituents), some vendors decided to include both services in the same organizational unit.

Sometimes, those units find it difficult to communicate that they are both a CSIRT and PSIRT. Instead of using naming including the team type, like “NAME CSIRT and PSIRT” they prefer to use a unique name like “NAME XYZ.” To date, no naming conventions have been developed; however, most vendors seem to prefer establishing internal CSIRTs that manage their own information assets and infrastructures independently from customer-focused PSIRTs because of the very distinctive needs of the constituencies each of them serves.

4.6 Why We Did Not Define CDC or NCSC

Some organizations started as a CSIRT and added more services and personal resources, only to find that over time, they were doing much more than a typical CSIRT. Therefore, they chose to use other team names, such as CDC (Cyber Defense Center) or CSC (Cyber Security Center), to convey that the combined team is more than just a CSIRT, ISAC, or SOC.

Interestingly, both abbreviations are used in different communities. To date, *CDC* is used in companies, government or sector organizations where other security services are combined with CSIRT services but also ensure an appropriate level of information security through proactive measures. Sometimes CSC is used for these teams, but *CSC* is more often used within a national context for *National Cybersecurity Centers* (i.e., *NCSC*).

Although CDCs, CSC, or NCSCs are recognized for their combined capabilities, the specific security incident management services they provide are not distinct from those provided by the four basic team types defined in this framework and are therefore already covered.

ANNEX 1: Acknowledgments

The following volunteers from the global community contributed significantly to the initial release and the newly updated version of this report. They are listed in alphabetical order by their last name, without a title but with their affiliation and/or country:

- Shin Adachi, CSIRT Framework Development SIG Member
- Vilius Benetis, NRD CIRT (LT) , CSIRT Framework Development SIG Member
- Barbara Cosgriff, Product Security Team LLC (US), PSIRT SIG Member
- Cristine Hoepers, CERT.br/NIC.br (BR) , CSIRT Framework Development SIG Member
- Tadas Jakštas, NRD CIRT (LT) , CSIRT Framework Development SIG Member
- Baiba Kaskina, CERT.LV (LV) , CSIRT Framework Development SIG Member
- Klaus-Peter Kossakowski (Editor), Hamburg University of Applied Sciences (DE) , CSIRT Framework Development SIG Chair
- Franz Lantenhammer (DE) , CSIRT Framework Development SIG Member
- Samuel Perl, CERT/CC, SEI, CMU (US) , CSIRT Framework Development SIG Member
- Robin M. Ruefle, CERT/CC, SEI, CMU (US) , CSIRT Framework Development SIG Member
- Sandy Shrum, SEI, CMU (US)
- Sanita Vitola, CERT.LV (LV) , CSIRT Framework Development SIG Member
- Barbara White, SEI, CMU (US)
- Logan Wilkins, Cisco CSIRT (US), CSIRT Framework Development SIG Member
- Mark Zajicek, CERT/CC, SEI, CMU (US) , CSIRT Framework Development SIG Member

The CSIRT Framework Development team would like to especially thank the PSIRT SIG for their engagement and contributions to improving this document, made possible through the participation of Barbara Cosgriff.

ANNEX 2: Standard Definitions Taken from the IETF [RFC2119]

MUST
This word, or the terms “REQUIRED” or “SHALL”, mean that the definition is an absolute requirement of the specification.

SHOULD
This word, or the adjective “RECOMMENDED”, mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

ANNEX 3: Supporting Resources

Bradner, Scott. Key words for use in RFCs to Indicate Requirement Levels. IETF Website, March 1997 [accessed]. https://www.rfc-editor.org/info/rfc2119
[BCP 14, RFC 2119, DOI 10.17487/RFC2119]

Empowering EU Information Sharing Analysis Centres (ISACs) Consortium. European ISACs Website. October 2023 [accessed]. https://www.isacs.eu/european-isacs/

FIRST *Computer Security Incident Response Teams (CSIRTs) Services Framework*, Version 2.1. *FIRST.Org Website.* 2019 [accessed]. https://www.first.org/standards/frameworks/csirts/

FIRST *Product Security Incident Response Team (PSIRT) Services Framework*, Version 1.1. *FIRST.Org Website*. 2020 [accessed].
https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.1.pdf

Information Sharing and Analysis Organization Standards Organization (ISAO). *Frequently Asked Questions*. ISAO Website, October 2023 [accessed]. https://www.isao.org/faq/

Kossakowski, Klaus-Peter. *Information Technology Incident Response Capabilities*. Hamburg: Books on Demand, 2001. ISBN: 9783831100590. [pages 188 and 189 in particular]