TLP:CLEAR

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

Version 0.7.1 Review

Team Types
within the Context
# of CSIRT Services Framework (v2.1)

1.Purpose

As of October 2023, specific Forum of Incident Response and Security Teams (FIRST) Services Frameworks have been developed up to now for two team types: Computer Security Incident Response Teams (CSIRTs) and Product Security Incident Response Teams (PSIRTs). While there are established definitions of CSIRT and PSIRT, in practice, even those definitions have slightly different meanings within some communities or contexts. Rather than simply building on these established definitions, volunteers from the global community, the CSIRT Framework Development Special Interest Group (CSIRT SIG), are working diligently to develop an informal shared understanding of relevant terms.

Other team types (e.g., Security Operations Centers [SOCs] and Information Sharing and Analysis Centers [ISACs]) are becoming increasingly vital for addressing urgent Cyber Insecurity. Therefore, it is necessary to establish standard definitions for at least some of these team types.

In 2022, experts in the global community discussed this need, which resulted in a project with in the CSIRT SIG to define the following team types that provide information security incident management capabilities:

- Computer Security Incident Response Teams (CSIRTs)
- Information Sharing and Analysis Centers (ISACs)
- Product Security Incident Response Teams (PSIRTs)
- Security Operations Centers (SOCs)

We discuss these four terms in greater detail in Section 3.

When discussing these terms, the CSIRT SIG did not address national or sectorial variants, but they will tackle them in the future. The *CSIRT Services Framework* explains current and well-established terms, such as *coordinating CSIRT* and *enterprise CSIRT*; there is nothing wrong with using those terms. However, until the four basic team type definitions are widely accepted, providing further detail might not be beneficial and might even hinder discussion. Future versions of this document will include definitions for *team sub-types* based on a wider discussion and the adoption of the above four basic terms (i.e., team types). This version of the *Team Types* document is the first one being considered by the global community through the CSIRT SIG.

2.Background

Over the years, 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 certain topics and activities are missing from these lists and frameworks.

FIRST is interested in enabling the global development and maturation of CSIRTs and other security incident management entities. A community-driven approach to developing an improved *CSIRT Services Framework* as part of the CSIRT SIG was launched, and an initial version was published in 2017. The current Version 2.1 has five distinct service areas and 21 associated services.

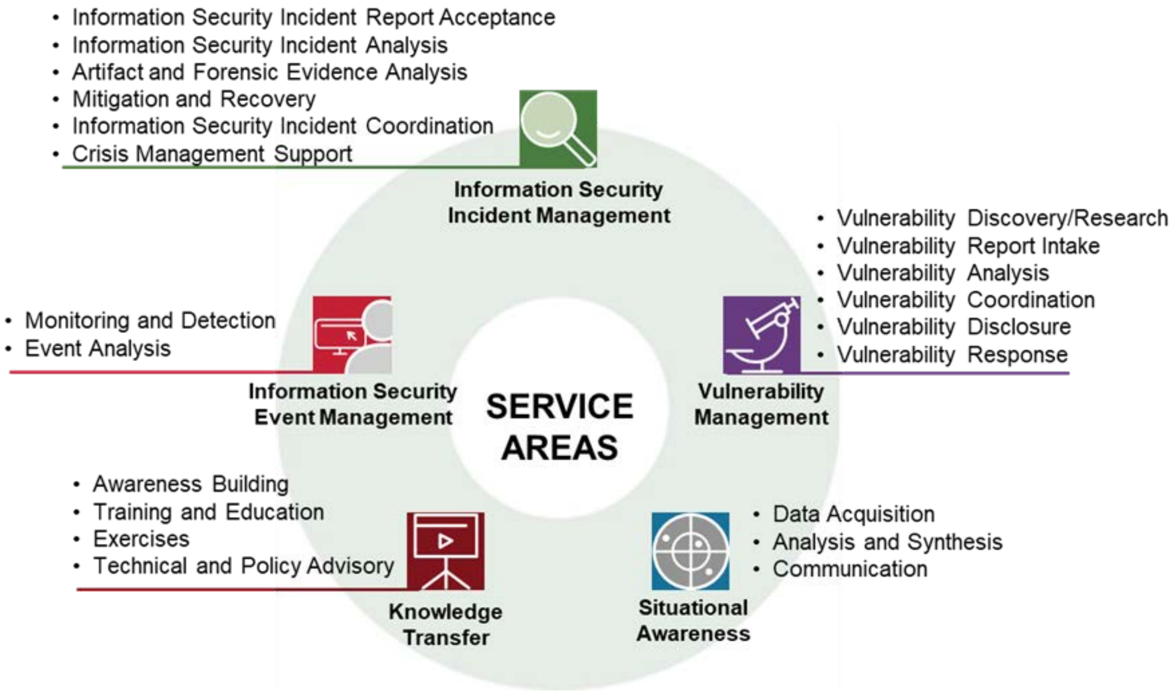

• Information Security Incident Report Acceptance
• Information Security Incident Analysis
• Artifact and Forensic Evidence Analysis
• Mitigation and Recovery
• Information Security Incident Coordination
• Crisis Management Support
Information Security Incident Management
• Vulnerability Discovery/Research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

*Figure 1: The Five Service Areas and Their Associated Services of the **CSIRT Services Framework** v2.1*

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.

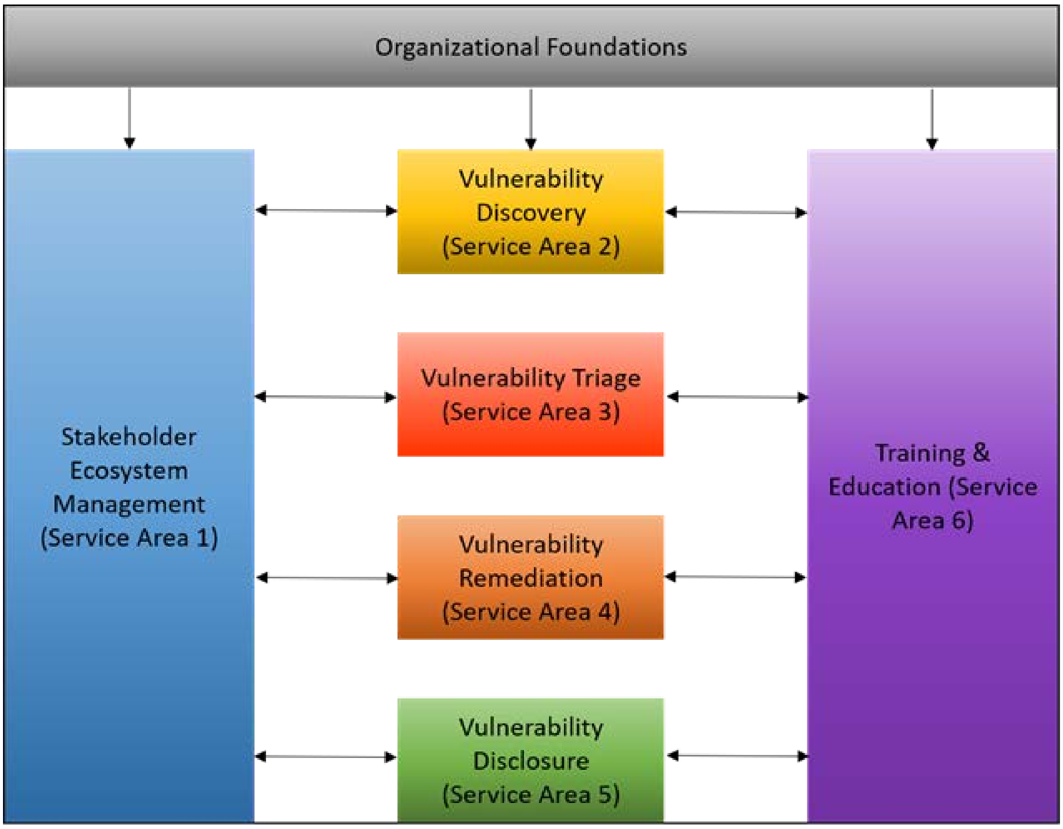

Organizational Foundations
Stakeholder Ecosystem Management (Service Area 1)
Vulnerability Discovery (Service Area 2)
Vulnerability Triage (Service Area 3)
Vulnerability Remediation (Service Area 4)
Vulnerability Disclosure (Service Area 5)
Training & Education (Service Area 6)

Figure 2: Interdependencies of Service Areas within the PSIRT Services Framework v1.1

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 *CSIRT and PSIRT Services Frameworks* is to help establish and improve team operations. These frameworks are intended to help teams identify and define their core categories of services and provide a standard set of terms and definitions to be used throughout the community. 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. Each team must choose the services 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 incident management capabilities and the entities that collaborate with them. This is the main focus of this document.

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. This is evident not only because FIRST and other communities serve as fora of CSIRTs but because they also bring together incident management and security teams and their 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 incident management capabilities: CSIRTs, ISACs, PSIRTs, and SOCs. In this section, we define each of these team types. We also provide profiles where some team types might be integrated. These different teams can coexist. For example, a larger, broader scoped SOC might include a CSIRT as one of its divisions or departments, or a CSIRT might include a SOC. An ISAC may also 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 is the description of (1) the responsibilities and activities that each team or capability provides and (2) how to help members of the global community understand the differences, which will ultimately enable them 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. We recognize that the *PSIRT Services Framework* uses a different namespace, so we plan to map both namespaces in the future. Future documents will also describe other team types that are considered sub-types of the four team types listed above (e.g., national CSIRTs, sectorial CSIRTs).

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

3.1 Computer Security Incident Response Teams (CSIRTs)

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

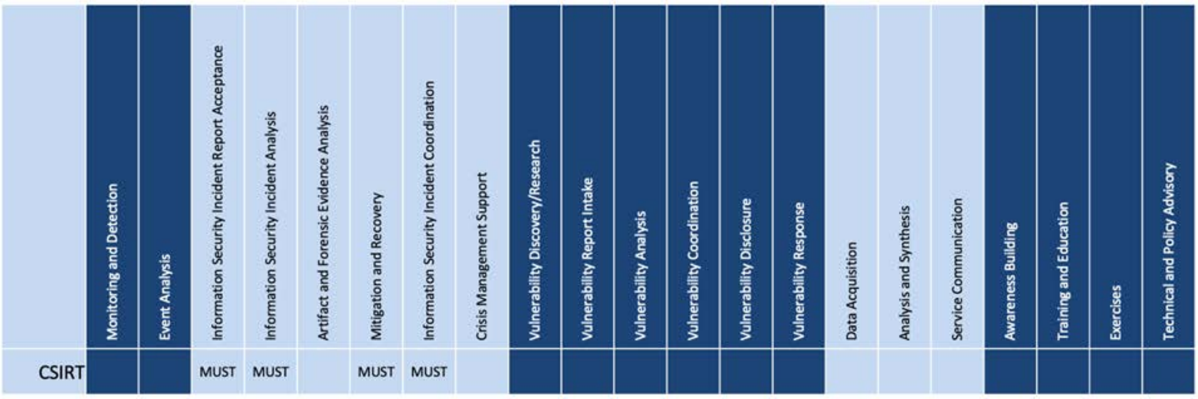
A CSIRT is often referred to as a CERT (Computer Emergency Response Team), CIRT (Computer Incident Response Team), CIRC (Computer Incident Response Center), CSIRC (Computer Security Incident Response Capability), or other name or abbreviation based on the objectives of the organization selecting its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

These types of teams specialize in information security incident management services. CSIRTs in other settings can specialize in information technology (IT), operational technology (OT) security, or specific subsets of information security. Some teams are even more focused and provide services related only to data protection incidents or malware-related incidents.

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 set-up as a single unit or even independent organization, or it might be part of a larger cyber security organization like in many National Cybersecurity Centers (NCSCs).

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

Table 1 illustrates the services that a CSIRT can and must offer. The services that CSIRTs must offer are noted as MUST. The two shades of blue are only to separate the service groupings within the service areas.



	Monitoring and Detection	Event Analysis	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 Discovery/Research	Vulnerability Report Intake	Vulnerability Analysis	Vulnerability Coordination	Vulnerability Disclosure	Vulnerability Response	Data Acquisition	Analysis and Synthesis	Service Communication	Awareness Building	Training and Education	Exercises	Technical and Policy Advisory
CSIRT			MUST	MUST		MUST	MUST														

Table 1: CSIRT Service Offerings

Artifact and Forensic Evidence Analysis 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.

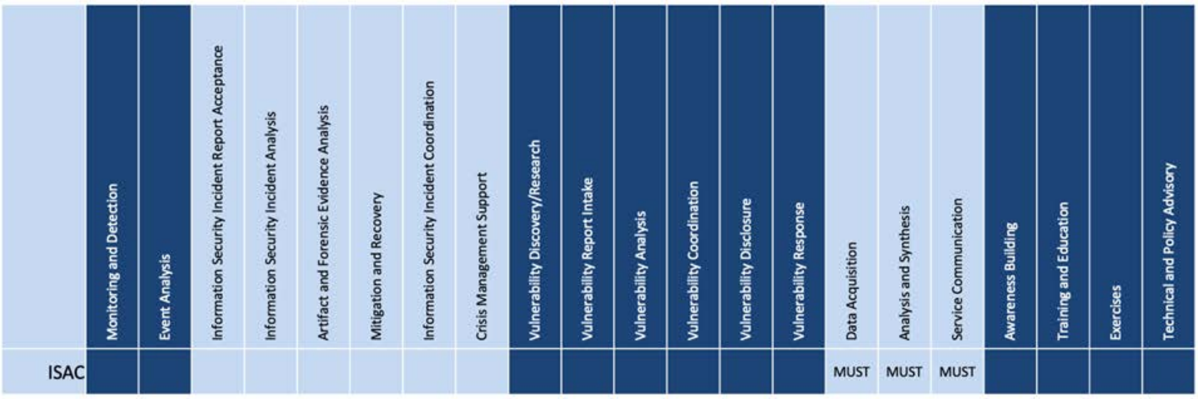
Crisis Management Support is not considered a MUST for all CSIRTs to offer. During large critical incidents, significant resources are required for coordination, communication, and overall management. If a CSIRT is not appropriately staffed, these activities may compete with other activities, such as technical investigations, incident analysis, response, and mitigation, and 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 may 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)

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.

ISACs are required in specific industry sectors in the U.S. In other regions or countries, ISAC activities are driven by industry but cover more sectors. For example, in Europe, an effort was made to collect information about various ISACs.[**2**] ISAO (Information Sharing and Analysis Organization) is an alternative name for an ISAC and is used for ISAC-type organizations.

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. The objective of synthesizing and disseminating this information is to help organizations that receive incidents to become more cyber resilient and capable of taking proactive steps when new trends are identified or when developments occur.



	Monitoring and Detection	Event Analysis	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 Discovery/Research	Vulnerability Report Intake	Vulnerability Analysis	Vulnerability Coordination	Vulnerability Disclosure	Vulnerability Response	Data Acquisition	Analysis and Synthesis	Service Communication	Awareness Building	Training and Education	Exercises	Technical and Policy Advisory
ISAC															MUST	MUST	MUST				

Table 2: ISAC Service Offerings

Table 2 illustrates the services that an ISAC can and must offer. The services that ISACs must offer are noted as MUST; The two shades of blue are only to separate the service groupings within the service areas.

ISACs focus on situational awareness services, but they might also handle some aspects of information security incident management and/or vulnerability management, usually with an emphasis on incident or vulnerability coordination and communication.

[2] https://www.isacs.eu/european-isacs

3.3 Product Security Incident Response Teams (PSIRTs)

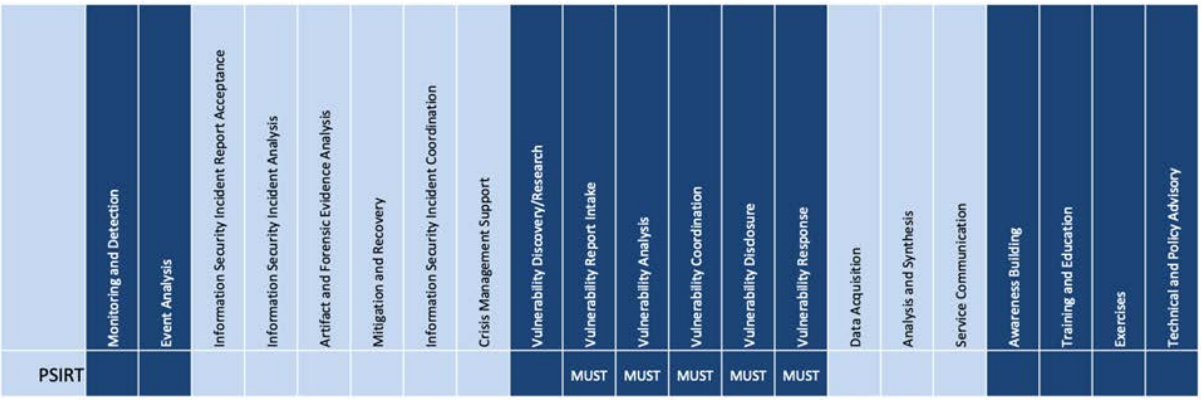
PSIRTs focus on vulnerability management in products and services. They are specialized teams or capabilities that respond within vendor organizations or service providers to handle and resolve vulnerabilities in products or services.

Many vendors or service providers, including open-source communities, have already established PSIRTs to:

1. track, mitigate, and fix vulnerabilities in their own products;
2. disseminate information about product security updates.

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.

Table 3 illustrates the services that a PSIRT can and must offer. The services that PSIRTs must offer are noted as MUST; The two shades of blue are only to separate the service groupings within the service areas.



	Monitoring and Detection	Event Analysis	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 Discovery/Research	Vulnerability Report Intake	Vulnerability Analysis	Vulnerability Coordination	Vulnerability Disclosure	Vulnerability Response	Data Acquisition	Analysis and Synthesis	Service Communication	Awareness Building	Training and Education	Exercises	Technical and Policy Advisory
PSIRT										MUST	MUST	MUST	MUST	MUST							

Table 3: PSIRT Service Offerings

Vulnerability Discovery/Research is a service that identifies new vulnerabilities. All newly identified vulnerabilities enable 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 offered by a PSIRT.

The latest version of the PSIRT Services Framework defines PSIRT as:[3]

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.

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

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 structure ensures that security assurance activities are integrated into the Secure Development Lifecycle (SDL).

Product security incident response is often associated with the maintenance phase of the SDL since most product security vulnerabilities are reported as quality escapes 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. PSIRT functions can also add value by providing guidance and oversight for handling security issues found internally.

3.4 Security Operations Centers (SOCs)

SOCs typically handle many different facets of security operations and focus on information security event management (i.e., event monitoring and detection).

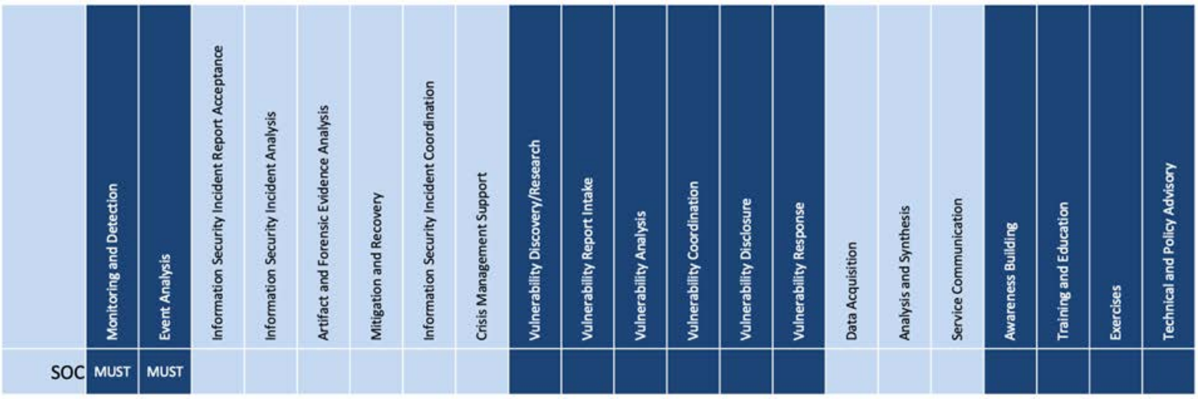
A SOC monitors the networks and systems of its parent organization or constituency for unusual, anomalous, or suspicious activity using some type of software or hardware (e.g., network taps, end-point detection, sensors, or other similar products).

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.

[3] Version 1.1: https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1.1

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

Table 4 illustrates the services that a SOC can and must offer. The services that SOCs must offer are noted as MUST; The two shades of blue are only to separate the service groupings within the service areas.



	Monitoring and Detection	Event Analysis	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 Discovery/Research	Vulnerability Report Intake	Vulnerability Analysis	Vulnerability Coordination	Vulnerability Disclosure	Vulnerability Response	Data Acquisition	Analysis and Synthesis	Service Communication	Awareness Building	Training and Education	Exercises	Technical and Policy Advisory
SOC	MUST	MUST																			

Table 4: SOC Service Offerings

4. Overview and Considerations

We studied the mandatory services that characterize each of the four basic team types that provide information security incident management capabilities:

- Computer Security Incident Response Teams (CSIRTs)
- Information Sharing and Analysis Centers (ISACs)
- Product Security Incident Response Teams (PSIRTs)
- Security Operations Centers (SOCs)

In this section, we summarize our findings and address specific questions that arose during our discussion and consideration of these team types. This section ensures a comprehensive record of the current state of affairs.

4.1 Defining Four Basic Incident Management Capabilities or Team Types

Table 5 is an aggregation of the four tables introduced in earlier sections. This table illustrates that four of the five service areas provide the foundation for the defined team types.

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 Services of the Knowledge Transfer Service Area Are Not Considered a Must for Any Team Type

All four team types (i.e., CSIRT, PSIRT, SOC, ISAC) likely perform some services of the *Knowledge Transfer* service area. This service area is clearly crucial for each type of incident management or security capability. Such 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 key to improving overall information security at organizational and community levels.

The *Training and Awareness* service area is important to all incident management capabilities and their constituencies. This service area may be more prevalent in CSIRTs and ISACs, but for defined communities of interest, PSIRTs and SOCs can also conduct these services. 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 related training materials, and delivering training is resource intensive; therefore, it is not always possible to provide *Training and Awareness services*. These services are 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). In this case, the ideal approach involves 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. This does not mean that these team types would not provide such services, but these services are not mandatory for CSIRTs, PSIRTs, SOCs, or ISACs.

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 offered, the service 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*) is omitted.

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

Global or national cyber security communities may consider investigating “false flag” operations that deliberately use marketing terms without providing the services typically associated with the team’s name used in the future.

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

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

Still in many contexts, only one team will exist today, either a SOC or a CSIRT. However, one must be careful, as a name that includes only *CSIRT or SOC* does not represent the entire set of services provided; it reflects only the focus of the team and the emphasis of the parent organization. This is especially obvious if 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 analyzing all available information security events independently. 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 who has “the lead.” 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 enforced rules on how to name an internal team.

Some organizations have, therefore, chosen to use other abbreviations, such as CDC (Cyber Defense Center) or CSC (Cyber Security Center), to convey that the combined team is more than just a CSIRT or SOC. Although CDC or CSC are recognized for their combined capabilities, the services they provide are not distinct from the four basic team types defined in this framework and are therefore not further discussed.

4.5 Common Type Name for a Combined CSIRT and PSIRT

In some organizations typically categorized as vendors, various incident management capabilities often coexist. Originally, mostly CSIRTs and PSIRTs coexisted; now, a SOC (at least) will also most likely coexist 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 give both services to the same organizational unit.

Those units find it sometimes difficult to communicate that they are both a CSIRT and PSIRT. Instead of having naming like “BRANDNAME CSIRT and PSIRT” they prefer to use a name like “BRANDNAME 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.

ANNEX 1: Acknowledgments

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

- Shin Adachi, NTT-CERT (US)
- Vilius Benetis, NRD CIRT (LT)
- Cristine Hoepers, CERT.br/NIC.br (BR)
- Baiba Kaskina, CERT.LV (LV)
- Klaus-Peter Kossakowski (Editor), Hamburg University of Applied Sciences (DE)
- Franz Lantenhammer (DE)
- Samuel Perl, CERT/CC, SEI, CMU (US)
- Robin M. Ruefle, CERT/CC, SEI, CMU (US)
- Sandy Shrum, SEI, CMU (US)
- Barbara White, SEI, CMU (US)
- Sanita Vitola, CERT.LV (LV)
- Mark Zajicek, CERT/CC, SEI, CMU (US)

ANNEX 2: Supporting Resources

- Empowering EU Information Sharing Analysis Centres (ISACs) Consortium. European ISACs. October 2023 [accessed]. https://www.isacs.eu/european-isacs/
- FIRST Computer Security Incident Response Teams (CSIRTs) Services Framework, Version 2.1. 2019. https://www.first.org/standards/frameworks/csirts/
- FIRST Product Security Incident Response Team (PSIRT) Services Framework, Version 1.0. 2018. https://www.first.org/standards/frameworks/psirts/
- 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. [page 188 and 189 in particular]