FIRST CSIRT Framework Development SIG:

The CSIRT Services Framework ... and defining CSIRT Roles

Prof. Dr. Klaus-Peter Kossakowski (Chair)
HAW Hamburg, Germany

CSIRT Services Framework

- First Release as SIRT Services Framework: July 2016
  - Was translated into some languages by support of ITU
- Better approach in version 1.1: May 2017
  - Bug fixes as in 1.1.1 May 2019
  - Work on PSIRT Services Framework started after release of version 1.1
- Draft Release for peer review: version 2.0: July 2019
  - Major changes in structure and content, but kept the principles
- Final Release as version 2.1: November 2019
  - Will be translated in some languages by support of ITU

→ https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

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 executing specific functions or in an aggregate of functions or services. The ability of an organization will be determined by the extent and quality of established policies and documentation and the ability to execute a set process.

Maturity, but Capacity and Capabilities first

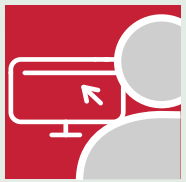
Capability - A measurable activity that may be performed as part of an organization's roles and responsibilities. For the purposes of the FIRST services framework, the capabilities can either be defined as the broader services or as the requisite functions.

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

Services Framework apply to different team types

- **No attempt to build specific team types into it:**
  Service offerings however can be described using the same service names (but different service levels or attributes)
- **No attempt to synchronize (yet) with other services frameworks:**
  If multiple frameworks describe „vulnerability management“, separate / overlapping / contradicting descriptions (based on a rather not aligned context) are possible and should be ignored (for now).

Information Security
Incident Management



Information Security
Event Management

AREAS

Vulnerability
Management

Knowledge
Transfer

Situational
Awareness

Understanding the leading principle

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

SERVICE AREAS

→ SERVICES

→ FUNCTIONS

→ SUB-FUNCTIONS

SERVICE AREA
Information Security Event Management

SERVICE AREA
Information Security Incident Management

SERVICE AREA
Vulnerability Management

SERVICE AREA
Situational Awareness

SERVICE AREA
Knowledge Transfer

SERVICE AREAS

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

Information Security Event Management

- Monitoring and Detection
- Event Analysis

Vulnerability Management

- Vulnerability Discovery/Research
- Vulnerability Report Intake
- Vulnerability Analysis
- Vulnerability Coordination
- Vulnerability Disclosure
- Vulnerability Response

Knowledge Transfer

- Awareness Building
- Training and Education
- Exercises
- Technical and Policy Advisory

Situational Awareness

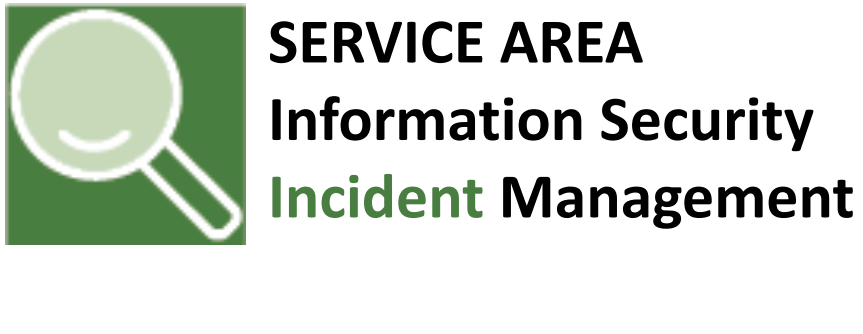
- Data Acquisition
- Analysis and Synthesis
- Communication

Defining Roles for all Functions

The new document currently written for CSIRTs (final draft expected for begin II/2022) is based on competencies for those carrying out the specific (service) functions!

- **Incident Analyst**
- **Incident Triage Coordinator**

- **Incident Responder**
- **Malware / Forensic Analyst**



SERVICE AREA
Information Security
Incident Management

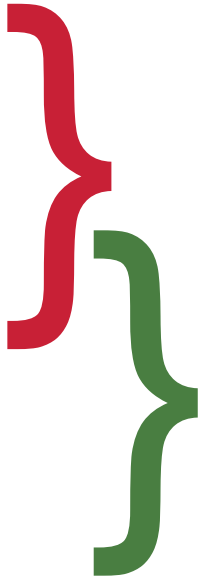
Defining Roles for all Functions

The new document currently written for CSIRTs is based on competencies for those carrying out the specific (service) functions!

- **Use Case Manager**
- **Data Manager**

- **Incident Analyst**
- **Incident Triage Coordinator**

- **Incident Responder**
- **Malware / Forensic Analyst**



SERVICE AREA
Information Security
Event Management

SERVICE AREA
Information Security
Incident Management

Each Role is defined as ...

SERVICE AREA
Information Security
Incident Management

A combination of references to mostly other documents. By referencing the content we can deliver a „lean“ document taking advantage of other resources (instead of reinventing the wheel!)

- **Description –** setting the context of the role within the service
- **General Tasks –** list general tasks to be carried out by it
- **Associated Functions** from the CSIRT Services Framework (v2.1)
- **Generic Competencies –** like „communication“ or „problem solving“
- **Role-specific Competencies –** like „threat analysis“ etc.