TF-CSIRT
Trusted Introducer

SIM3 and Services Framework

Luxembourg, 24 May 2019

HAW Hamburg
Prof. Dr. Klaus-Peter Kossakowski

Topics

- Definitions for
  - Capacity, Capability, Maturity
- TI Ratings and ENISA Levels
- Applying the CSIRT Services Framework
- SIM3 Self Check

Definitions: Capacity

[...] capacity is generally used to express the quantity of output(s) that can be delivered by a particular **capability** over a period of time, and in some cases with indication of the number of clients/requests that can be serviced concurrently, where relevant.

https://www.first.org/education/csirt_service-framework_v1.1.1#Capacity

Definitions: Capability

A measurable activity that may be performed as part of an organization's roles and responsibilities.
[...] the capabilities can either be defined as the broader Services or as the requisite Functions.

https://www.first.org/education/csirt_service-framework_v1.1.1#Capability

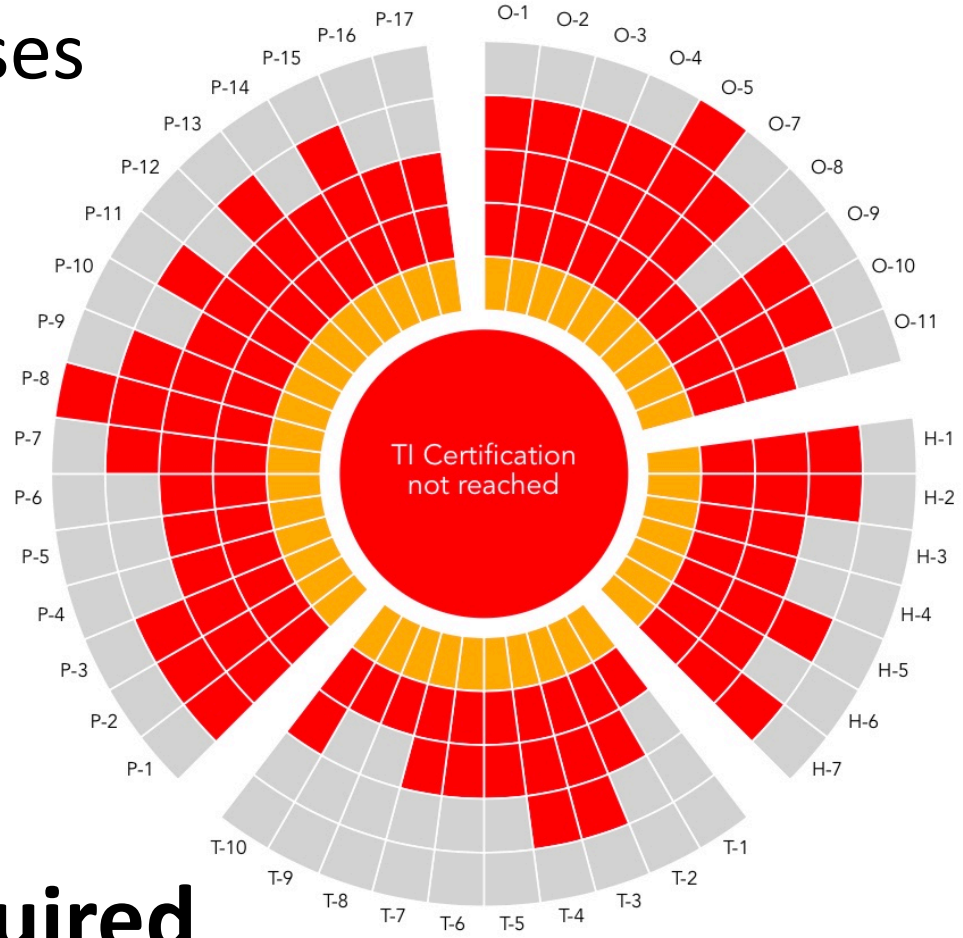
Definitions: Maturity

It is a level of proficiency attained either in executing specific functions or in an aggregate of functions or services. **The maturity of an organization will be determined by the extent, quality of established policies and documentation, and the ability to execute a set process.** The level of advancement in knowledge, skill and proficiency is measured against a defined reference model.

https://www.first.org/education/csirt_service-framework_v1.1.1#Maturity

Organisation

Processes



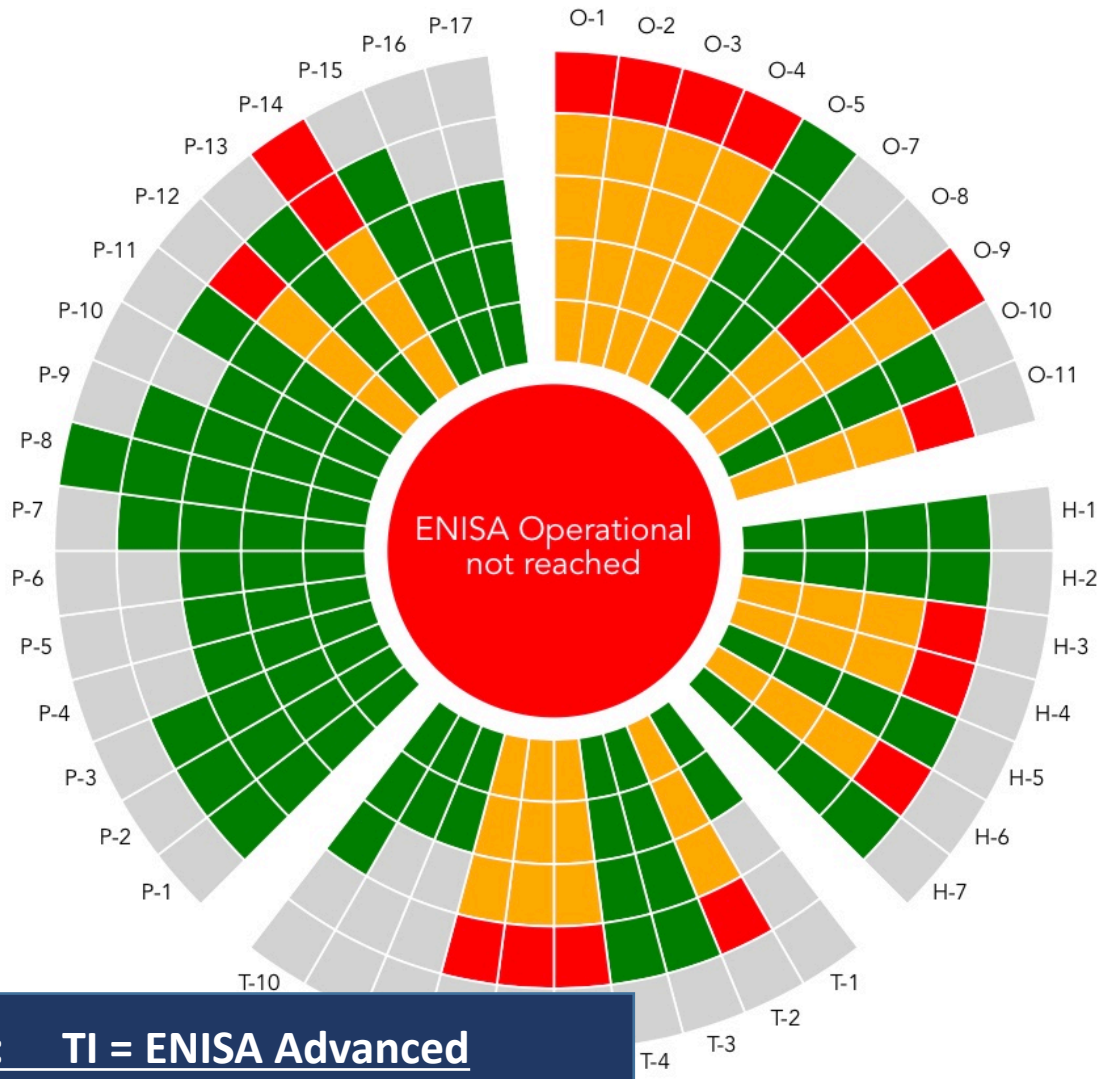
PREVIEW: New self-check coming soon!

SIM3 Areas and required Levels

Humans

Tools

ENISA OPERATIONAL



Requirements for national teams established according to the EU NIS Directive are somewhat higher!

- **Mandated by Laws**
- **Training needs**
- **Resilience**
- **Reporting**

Green: TI = ENISA Advanced
Orange: TI Levels
Red: Extra of ENISA Advanced

Applying a CSIRT Services list

(Established by CERT/CC & TI 2003)

Reactive Services

- Alerts and Warnings
- Incident Handling
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
- Vulnerability Handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination
- Artifact Handling
  - Artifact analysis
  - Artifact response
  - Artifact response coordination

Proactive Services

- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Security Quality Management Services

- ✓Risk Analysis
- ✓Business Continuity & Disaster Recovery Planning
- ✓Security Consulting
- ✓Awareness Building
- ✓Education/Training
- ✓Product Evaluation or Certification

Finaly improving: Services Framework

Service Areas:

- Information Security Event Management
- Information Security Incident Management
- Vulnerability Management
- Situational Awareness
- Knowledge Transfer

New version for review coming soon from FIRST!

TF-CSIRT
Trusted Introducer

SIM3 will use Services Framework

Services are always reviewed anyway

- Need to be described (O-5)
- Expectations need to be set (O-7)
- Processes to support the delivery (P-4/5/6/7)

Services are always compared against:

Mandate and responsibilities

Mandate & Responsibilities Services Areas & Services	provide support in IT security incident response and coordinate their prevention;	maintain recommendations on the current information technologies risks;	organize educational events, education and training in the field of information technologies security;
IS Incident Mgmt -- Triage -- Support ...			
Situational Awaren. -- Threat intelligence -- Vulnerability Adv. ...			
Knowledge Transfer -- Trainings -- Exercises ...			

Step 1:
Identify mandate and prepare table with all service areas / services

Mandate & Responsibilities Services Areas & Services	provide support in IT security incident response and coordinate their prevention;	maintain recommendations on the current information technologies risks;	organize educational events, education and training in the field of information technologies security;
IS Incident Mgmt -- Triage -- Support ...	○ ○		
Situational Awaren. -- Threat intelligence -- Vulnerability Adv. ...	○ ○	○ ○	
Knowledge Transfer -- Trainings -- Exercises			○ ○

Step 2:
Mark those services that are required to support the mandates

Mandate & Responsibilities Services Areas & Services	provide support in IT security incident response and coordinate their prevention;	maintain recommendations on the current information technologies risks;	organize educational events, education and training in the field of information technologies security;
IS Incident Mgmt -- Triage -- Support ...	✓ ✓		
Situational Awaren. -- Threat intelligence -- Vulnerability Adv. ...	○ ○	○ ○	
Knowledge Transfer -- Trainings -- Exercises			✓ ✓

Step 3:
Check marks if the services are offered and document this in table

Mandate & Responsibilities Services Areas & Services	provide support in IT security incident response and coordinate their prevention;	maintain recommendations on the current information techn	organize educational events, education and training in the field of information ;
IS Incident Mgmt -- Triage -- Support ...	✓ ✓		
Situational Awaren. -- Threat intelligence -- Vulnerability Adv. ...	○ ○	○ ○	
Knowledge Transfer -- Trainings -- Exercises			✓ ✓

Step 4:

Empty marks require more questions!

Mandate & Responsibilities Services Areas & Services	provide support in IT security incident response and coordinate their prevention;	maintain recommendations on the current information technologies risks;	organize educational events, education and training in the field of information technologies security;
IS Incident Mgmt -- Triage -- Support ...	✓ ✓		
Situational Awaren. -- Threat intelligence -- ...	○	○ ○	
Kn -- --			✓ ✓

Step 5:
Still empty columns mean mandate cannot be fulfilled!

SIM3 will use Services Framework

TI will also make use of the new terms!

No need to change the „names“ of services you use towards your constituency ;)

Services are compared against: Mandate and responsibilities

TF-CSIRT
Trusted Introducer

Thank you very much for your kind attention !

https://tiw.trusted-introducer.org

mailto:ti@trusted-introducer.org

HAW Hamburg

Prof. Dr. Klaus-Peter Kossakowski

Klaus-Peter.Kossakowski@haw-hamburg.de

TF-CSIRT
Trusted Introducer