Istituto Nazionale di Fisica Nucleare
NUcleo CyberSecurity

CSIRT

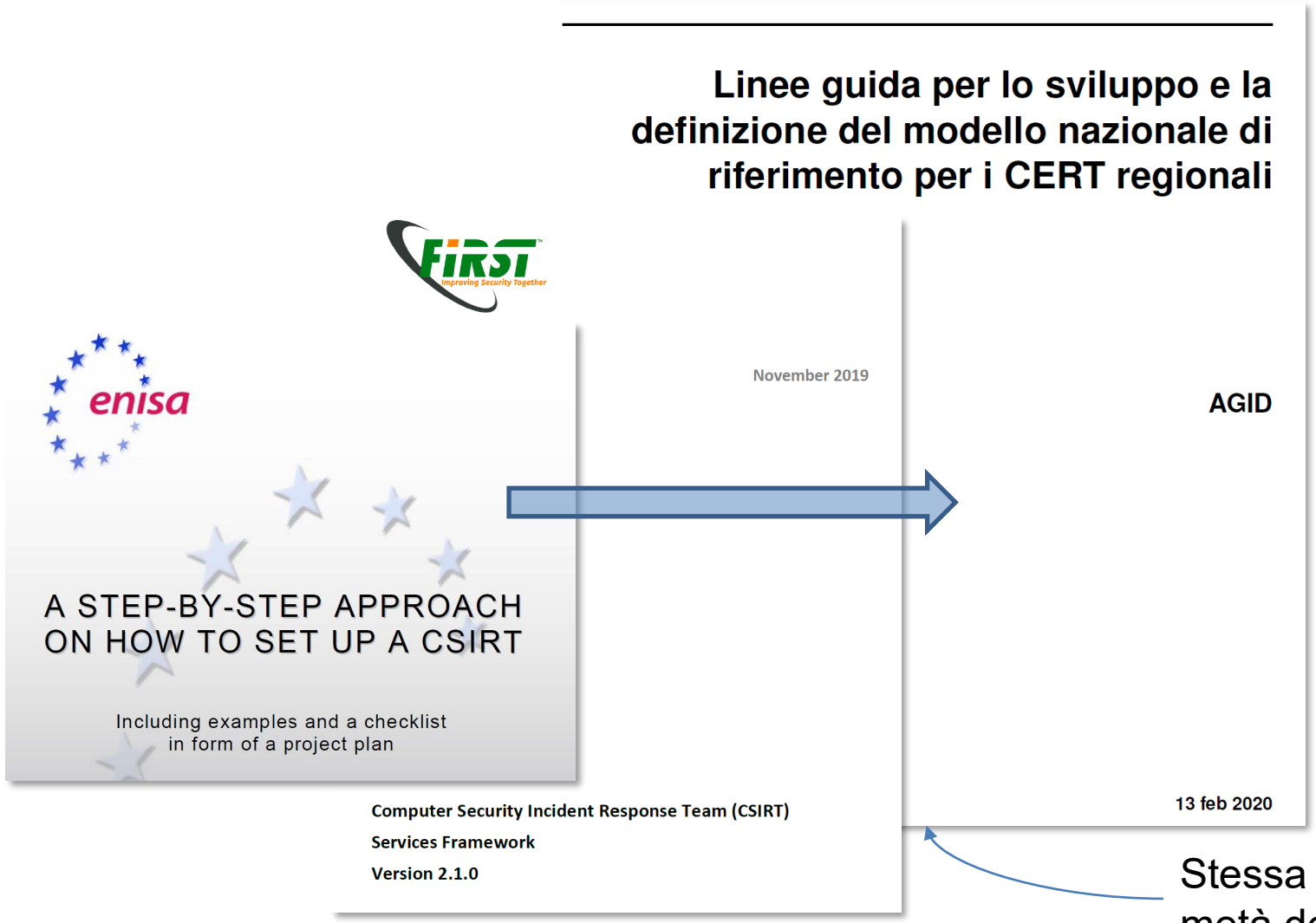
Modelli di riferimento ed evoluzione

Luca G. Carbone

Mini WS CCR sulla Sicurezza Informatica

13-15/2/2023 – Padova

Riferimenti



Stessa bibliografia,
metà delle pagine…

CSIRT

CSIRT (by ENISA, FIRST.org): a generic term for a team that provides a set of services: information and cybersecurity incident handling (code service), security monitoring, vulnerability management, situational awareness and cybersecurity knowledge management. *CSIRT is a **reactive approach** to security, responding to incidents after they have occurred.*

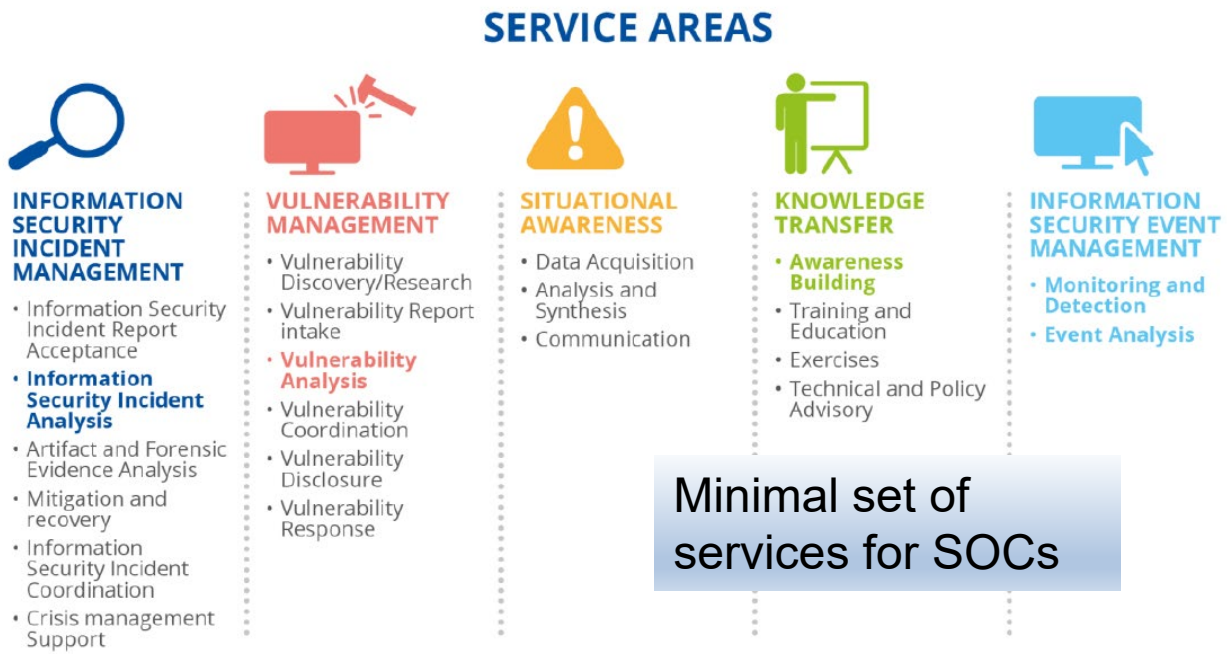
(…) CSIRT would only receive escalated alerts

Minimal set of services for CSIRTs

SOC

SOC (by SANS): A combination of **people**, **processes** and **technology** protecting the information systems of an organization through proactive design and configuration, ongoing monitoring of system state, detection of unintended actions of undesiderable state, and minimizing damage from unwanted effects. CSIRT is a reactive **approach to security, responding to incidents after they have occurred.** ***SOC is a proactive approach to security, monitoring for potential events and responding before they can*** *have an impact.*

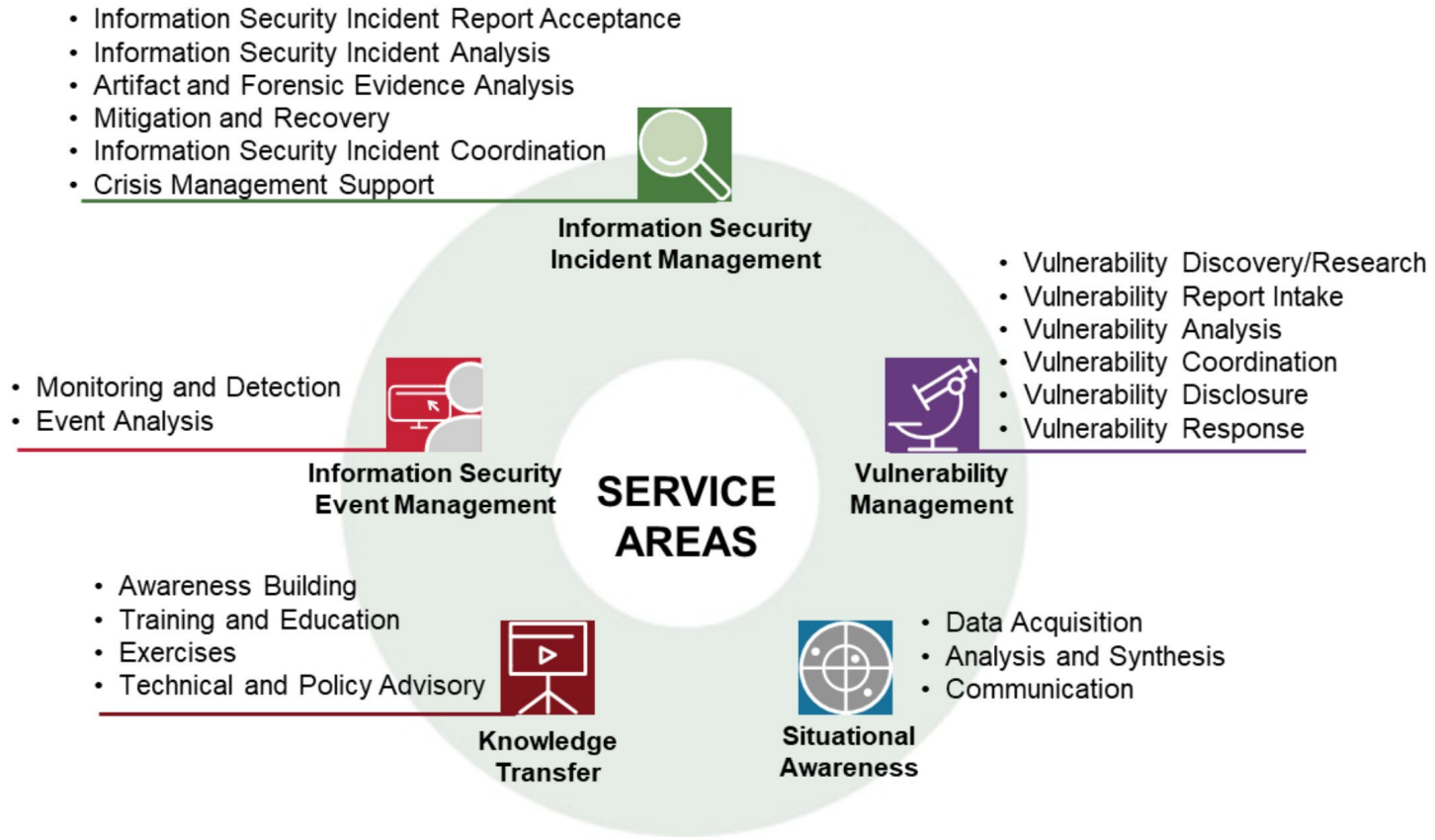
(…) SOC is the first line, they receive all alerts,



Minimal set of services for SOCs

CSIRT vs SOC

Stando alla citata *Good Practice Guide* di ENISA la distinzione tra CSIRT e SOC è in qualche misura surrettizia, poiché il modello di riferimento a cui si rifanno entrambi nel documento è il **FIRST CSIRT Services Framework:**



CSIRT services & related Functions

SERVICE AREA
Information Security Event Management

Monitoring and Detection
- Log and Sensor Management
- Detection Use Case Management
- Contextual Data Management

Event Analysis
- Correlation
- Qualification

SERVICE AREA
Information Security Incident Management

Information Security Incident Report Acceptance
- Information Security Incident Report Receipt
- Information Security Incident Triage and Processing

Information Security Incident Analysis
- Information Security Incident Triage (Prioritization and Categorization)
- Information Collection
- Detailed Analysis Coordination
- Information Security Incident Root Cause Analysis
- Cross-Incident Correlation

Artifact and Forensic Evidence Analysis
- Media or Surface Analysis
- Reverse Engineering
- Runtime or Dynamic Analysis
- Comparative Analysis

Mitigation and Recovery
- Response Plan Establishment
- Ad Hoc Measures and Containment
- System Restoration
- Other Information Security Entities Support

Information Security Incident Coordination
- Communication
- Notification Distribution
- Relevant Information Distribution
- Activities Coordination
- Reporting
- Media Communication

Crisis Management Support
- Information Distribution to Constituents
- Information Security Status Reporting
- Strategic Decisions Communication

SERVICE AREA
Vulnerability Management

Vulnerability Discovery/Research
- Incident Response Vulnerability Discovery
- Public Source Vulnerability Discovery
- Vulnerability Research

Vulnerability Report Intake
- Vulnerability Report Receipt
- Vulnerability Report Triage and Processing

Vulnerability Analysis
- Vulnerability Triage (Validation and Categorization)
- Vulnerability Root Cause Analysis
- Vulnerability Remediation Development

Vulnerability Coordination
- Vulnerability Notification/Reporting
- Vulnerability Stakeholder Coordination

Vulnerability Disclosure
- Vulnerability Disclosure Policy and Infrastructure Maintenance
- Vulnerability Announcement/ Communication/Dissemination
- Post-Vulnerability Disclosure Feedback

Vulnerability Response
- Vulnerability Detection/Scanning
- Vulnerability Remediation

SERVICE AREA
Situational Awareness

Data Acquisition
- Policy Aggregation, Distillation, and Guidance
- Asset Mapping to Functions, Roles, Actions, and Key Risks
- Collection
- Data Processing and Preparation

Analysis and Synthesize
- Projection and Inference
- Event Detection (through Alerting and/or Hunting)
- Situational Impact

Communication
- Internal and External Communication
- Reporting and Recommendations
- Implementation

SERVICE AREA
Knowledge Transfer

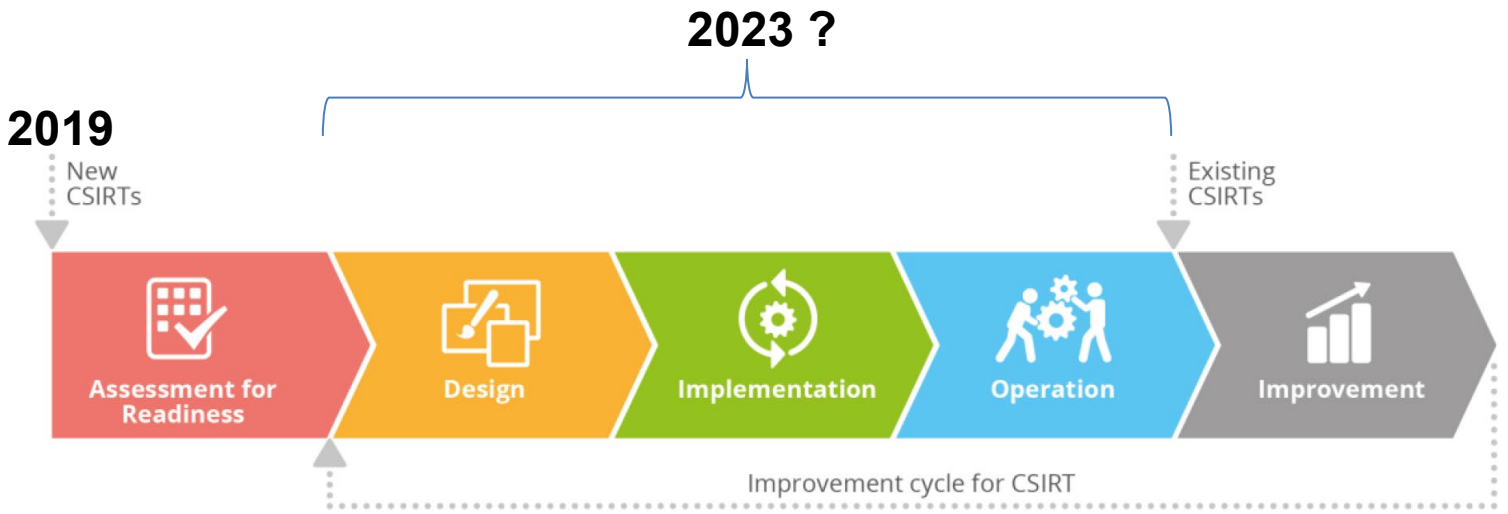
Awareness Building
- Research and Information Aggregation
- Report and Awareness Materials Development
- Information Dissemination
- Outreach

Training and Education
- Knowledge, Skill, and Ability Requirements Gathering
- Educational and Training Materials Development
- Content Delivery
- Mentoring
- CSIRT Staff Professional Development

Exercises
- Requirements Analysis
- Format and Environment Development
- Scenario Development
- Exercise Execution
- Exercise Outcome Review

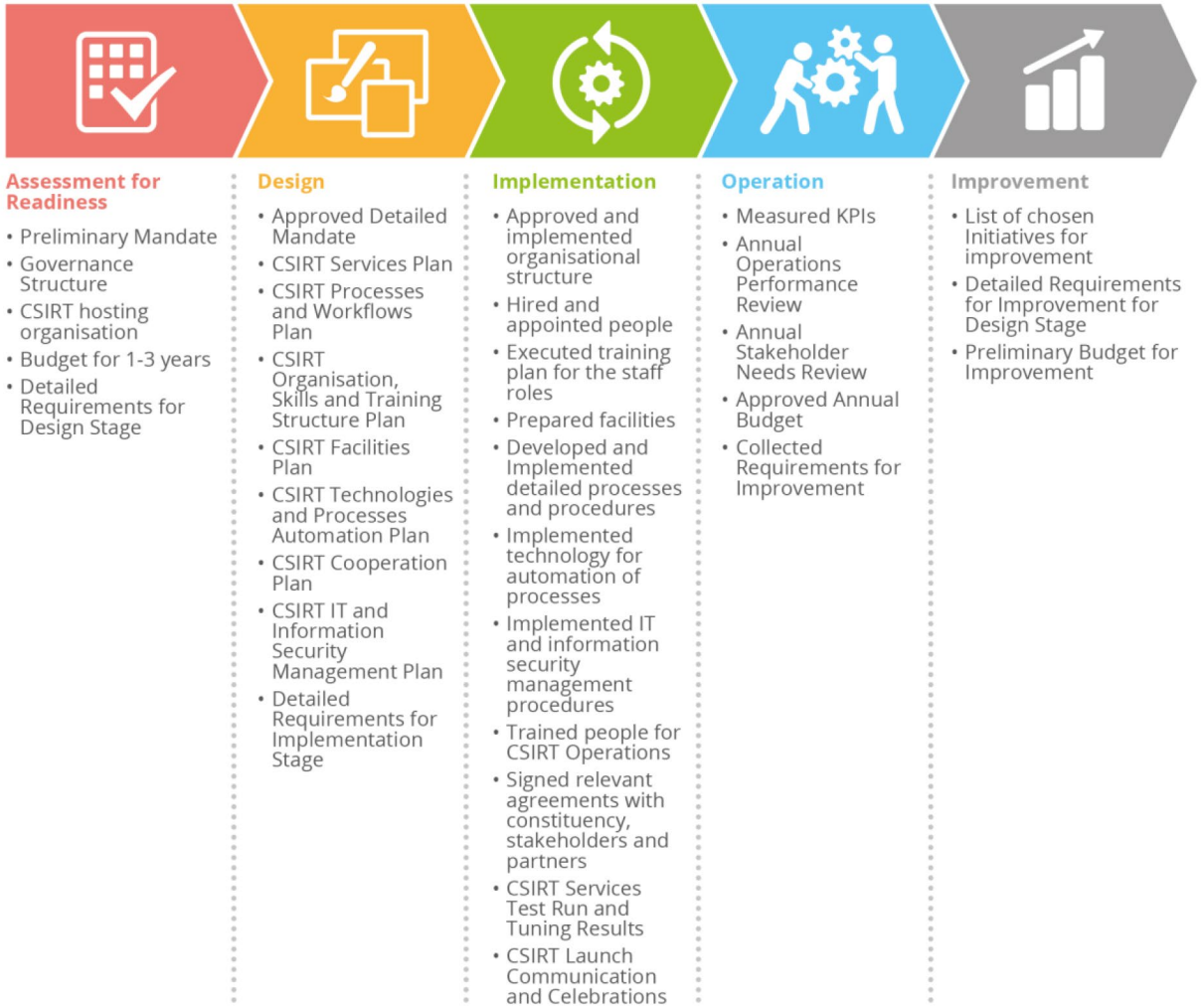
Technical and Policy Advisory
- Risk Management Support
- Business Continuity and Disaster Recovery Planning Support
- Policy Support
- Technical Advice

CSIRT lifecycle



Teoricamente siamo in piena fase **Operation**, in realtà stiamo procedendo alla unificazione di due IRT con *constituency* differenti (anche se in astratto quella di CSIRT INFN comprende quella di SIT Cloud) e processi/infrastrutture compatibili ma a loro volta difformi, per cui realisticamente parlando siamo tra le fasi di **Design** e **Implementation** (se non addirittura di **Assessment for Readiness**).

CSIRT establishment outcomes, phases and efforts



A seconda di dove poniamo il punto di partenza dovremo comprimere 6-8 mesi (nella migliore delle ipotesi – si può arrivare a 30) in 4-5 per arrivare alla fase di piena operatività in agosto.

CSIRT design phase: outcomes

- Approved detailed mandate
- CSIRT service plan
- CSIRT processes and workflows
- CSIRT organisation, skills and training structure plan
- CSIRT facilities plan
- CSIRT technologies and processes automation plan
- CSIRT cooperation plan
- …

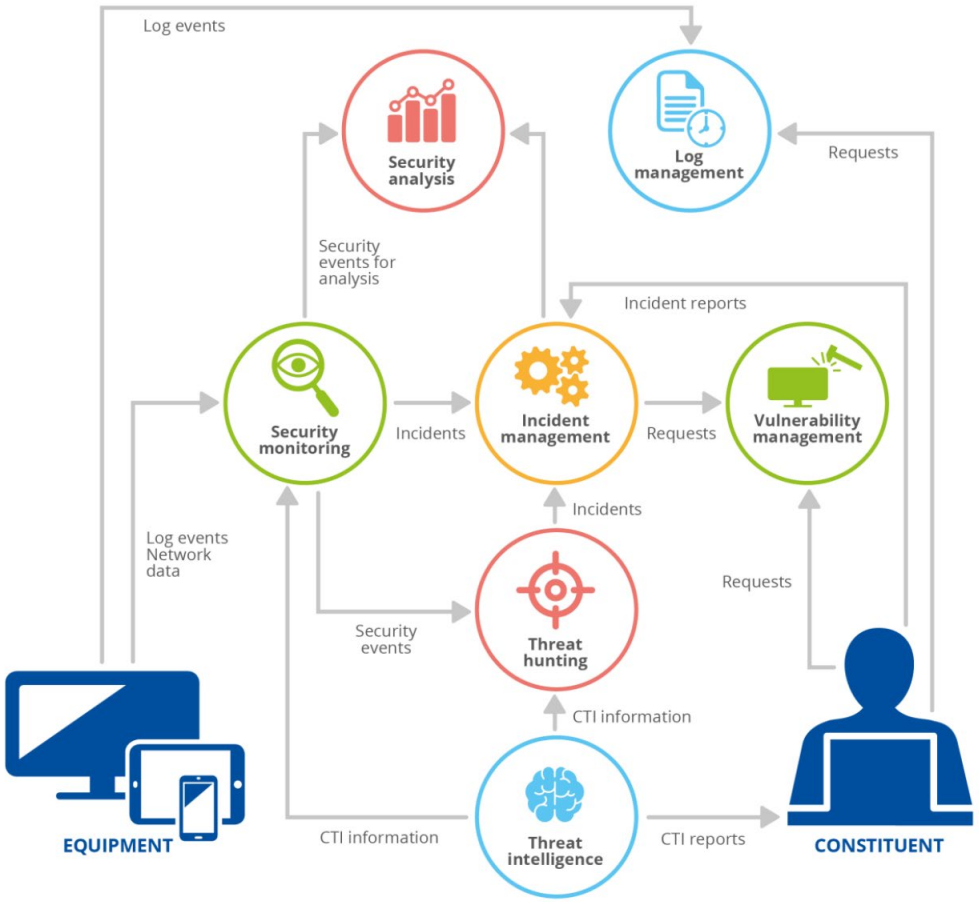
(…) in the form of either separate approved documents or one approved document.

References:

- ENISA CSIRT Maturity Framework
  - ENISA (SIM3) CSIRT Maturity self-assessment tool
- SOC-CMM: SOC Capability and Maturity Model
  - SOC-CMM self-assessment tool (per la cronaca: esiste anche il *SOC-CMM CERT self assessment tool* derivato da interazioni con FIRST.org e il *SOC-CMM to NIST CSF mapping sheet*, giusto per aumentare un po' l'entropia)

CSIRT design: examples

service/processes interrelationship



Process name	Security incident management
Description	Security incident management covers incident report registration, triage, incident resolving and incident closing
Process owner	Security incident manager
Purpose	To ensure that every incident detected is handled according to defined quality requirements and that response activities are carried out to mitigate any incidents, followed by actions to improve security measures; and to increase the maturity of the constituent's security processes so that it is more resilient to cyberthreats in the future
Service input/triggers	1. Events detected by security monitoring service activities 2. Incident reports registered by: 2.1. Phone 2.2. E-mail 2.3. Online web form 2.4. Service desk self-service interface
Service output/deliverables	1. Assistance to constituents to mitigate security incidents 2. Provision of guidelines for improving the security of the constituent's infrastructure
Service activities	1. Triage of the security incident 2. Analysis of the security incident 3. Guide the containment of the security incident 4. Guide eradication and recovery after the incident 5. Close the incident 6. Lessons learned

incident management process workflow description and diagram

CSIRT organisation & training program

SMALL (5-7 people) single-unit CSIRT

BIG (> 10 people) multi-unit CSIRT

ENISA online training material

Technical

Published under Online training material
Tagged with Training

- Building artifact handling and analysis environment
- Processing and storing artifacts
- Artefact analysis fundamentals
- Advanced artefact handling
- Introduction to advanced artefact analysis
- Dynamic analysis of artefacts
- Static analysis of artefacts
- Forensic analysis: Local incident response
- Forensic analysis: Network incident response
- Forensic analysis: Webserver analysis
- Developing Countermeasures
- Common framework for artefact analysis
- Using indicators to enhance defence capabilities
- Identification and handling of electronic evidence
- Digital forensics

CSIRT cooperation plan: trust relationship

Search for cooperation between other CSIRTs and possible national initiatives

The existence of other CSIRT initiatives and the strong need for cooperation between them has already been mentioned a couple of times in this document. It's good practice to contact other CSIRTs as early as possible to get the necessary contact with the CISRT communities. Usually other CSIRTs are very open to help newly built teams to get started.

ENISAs *Inventory of CERT activities in Europe*[14] is a very good starting point for the search for other CSIRTs in the country or for national CSIRT cooperation activities.

2. Regional and national (if any) CSIRT initiatives for improving cooperation should be considered. The Trusted Introducer listed status ([43]) ([44]) is relatively easy to achieve for a CSIRT that is already operational and that has the support of other CSIRTs and participates in CSIRT-related events and conferences. CSIRTs should subsequently focus on attaining accredited status ([45]) or even certified status ([46]), The Trusted Introducer scheme is the only certification scheme currently available for CSIRTs and Trusted Introducer services are more focused to CSIRTs operating in Europe.
3. It is strongly advised that CSIRTs join the FIRST.org association as this is the major global association for CSIRTs.

TF-CSIRT Trusted introducer

TF-CSIRT Trusted Introducer

https://www.trusted-introducer.org/index.html

Home | Processes | Services | Directory | Events | Contact TI | Member View

Available languages:

Services for Security and Incident Response Teams

Security and Incident Response teams manage the handling of information security incidents within their organisation or network - their tasks broadly range from prevention and awareness raising, via incident detection to the actual tracking and resolving of incidents and drawing lessons from that. The Trusted Introducer Service - a.k.a. TI - was established by the European CERT community in 2000 to address common needs and build a service infrastructure providing vital support for all security and incident response teams.

The Trusted Introducer Service forms the trusted backbone of infrastructure services and serves as clearinghouse for all security and incident response teams. It lists well known teams and accredits as well as certify teams according to their demonstrated and checked level of maturity. Vital member's only services enabling security and incident response teams to interact more efficiently and effectively with each other are available to all accredited and certified teams.

TI Self-Service
For Team Reps & Associates

SIM3 Check
For everyone

News

Public TI Update, September 2022

Events

Joint TF-CSIRT/TI Meeting & FIRST Regional Symposium January 2023
Bilbao, Spain 31 Jan. - 02 Feb. 2023

TI categories

The TI service differentiate between four categories:

- teams are
  - listed, which provides basic information about the team itself as well as shows endorsement of the team by the TI community;
  - accredited, which ensures a defined level of best practices and acceptance of the established TI policies for such teams;
  - certified, if they have been accredited before and prove a confirmed level of maturity as defined by the TI SIM framework.
- security experts can participate as TI Associates.

The TI Accreditation and Certification requires regular efforts to maintain the team's status. Such efforts are also expected from TI listed teams. To ensure a high level of trust within the TI community, TI listed teams that have not become accredited within three years are required to demonstrate the continuous support of the listing by the TI community. This is called "re-listing". Therefore the directory of the TI service can be trusted to reflect the actual and accurate snapshot of all teams listed regardless of their status.

TI Certification is meant for those accredited teams who have internal and/or external reasons to have their maturity level gauged in an independent way. When the certification succeeds, the team can show this to their constituents, to their funding bodies, to other parties they want to cooperate with. The certified teams are and stay part of the community of accredited teams - the certification can be seen as extra branding providing it's own benefits for such teams. Again to keep this expectation over time, a re-certification is required every three years.

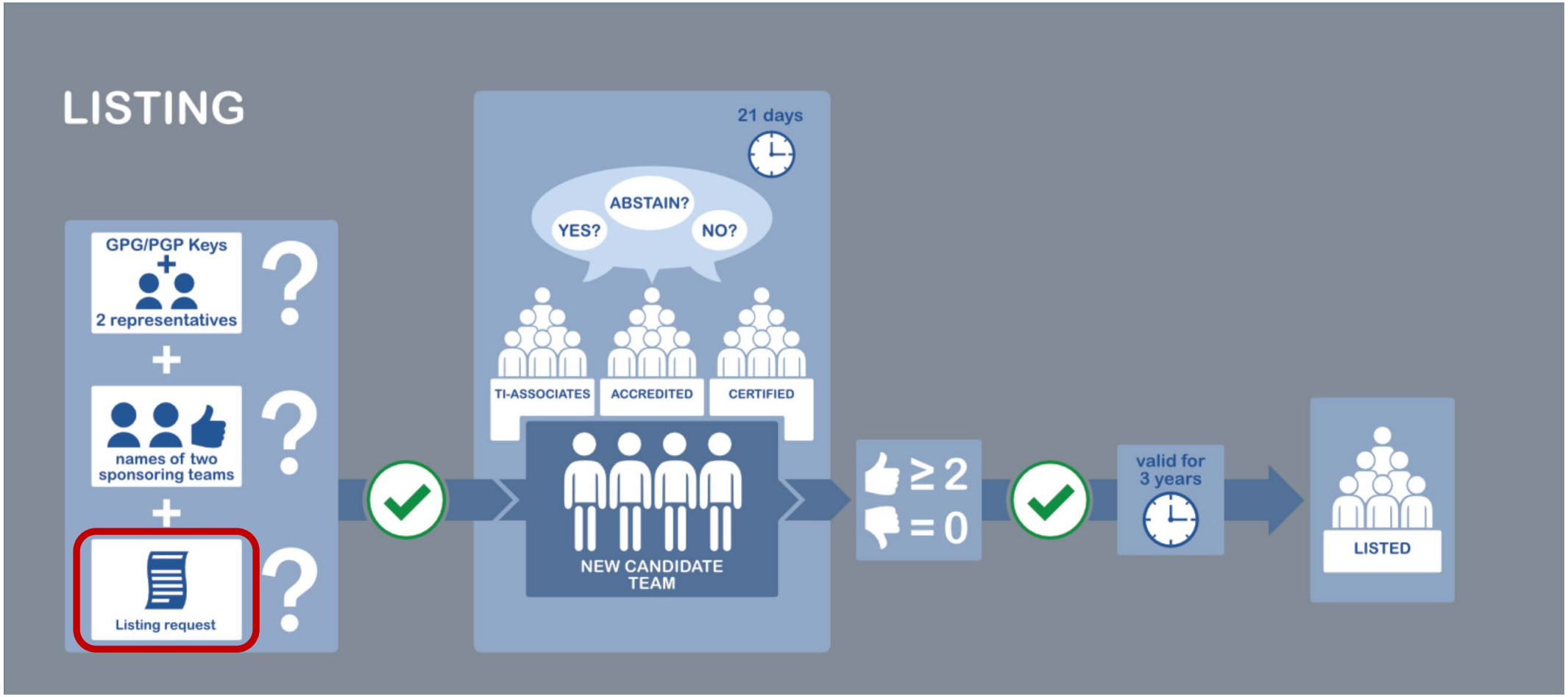
Nella UE gli CSIRT (o i CERT) della comunità NREN che possono vantare un riconoscimento TI (listed, accredited o certified) sono 78, tra cui:

- EGI CSIRT (certified)
- Funet CERT (certified *)
- GARR CERT (accredited)
- Nikhef CSIRT (listed)
- CERN CERT (listed)
- ETHZ-NSG (certified *)
- SWITCH-CERT (certified)
- GEANT CERT (certified *)

Alcuni di questi (EGI, FUNET, ETHZ, SWITCH, GEANT) sono anche membri First.

(*) in attesa di ri-certificazione

LISTING process



LISTING request

Sostanzialmente è costituita da un questionario informativo su organizzazione del team, policy, servizi offerti, … e una lista di requisiti da rispettare (*MUST/ & SHOULD criteria*):

6.2 List of all MUST Criteria

- Teams MUST be described by qualitative and a minimum number of quantitative values as per Appendix B and ensure that these descriptions continue to match reality.
- Teams MUST cooperate with the publication of all delivered data on the TI members-only website. Access is restricted to TI "accredited" and TI "certified" teams (including all certified teams), TI Associates, the TI team and the TF-CSIRT SC.
- Teams MUST cooperate with the publication of the essentials of their contact information – meaning all items marked PUBLIC in Appendix B – on the TI public website (https://www.trusted-introducer.org/).
- Teams MUST register two team representatives.
- Teams MUST actively support the TI requirement to keep the information

6.3 List of all SHOULD Criteria

- Teams SHOULD present at least their external services, if any, to the outside world as per RFC 2350,[5] including a specification of quantitative values and ensure that these descriptions continue to match reality, including indicated service levels if applicable. (Especially in the beginning starting teams may not have already answers or procedures to fill it out completely, in such case it is important to update it frequently while your team progresses.)
- Teams SHOULD regularly attend TF-CSIRT meetings.
- Teams SHOULD comply with the "CSIRT Code of Practice"[6] as ratified by the TI Accredited Teams.
- Teams SHOULD use the "SIM3 Maturity Model"[7] as a starting point for self-assessments or audits of their services. (Especially for a starting team SIM3 might not be the most interesting self-check to run, but it will also provide for a useful list of issues to consider adding to the roadmap of your team's development.)
- Teams SHOULD respond to TI reaction tests to demonstrate that they can be reached via their official contacts.

Policies SECURE

- Specify how information is handled, especially with regards to restricting access and protecting its confidentiality once received by your team? Are there legal considerations to take into account with regards to the information handling?

RFC 2350 PUBLIC

- URL of the published RFC 2350
- Date of last update and version number (if applicable)
- Distribution mechanisms for notifications about updates

SIM3 SECURE

- URL of the actual SIM3 self-check (on sim3-check.opencsirt.org)
- Date of last update

Membership of Professional Team / Security Organisations PUBLIC

- Is your team a member of FIRST and if yes, since what year?
- Is your team member of a national CERT cooperation or community and if yes, since what year?
- Specify other CERT or security communities in which your team (or your host organisation) is a member of and if yes, since what year?

Services provided to the Constituency SECURE

If you provide services not listed below – or if you believe, that the terms chosen do not fit clearly to your services – please describe those services in free text format!

These services are not yet aligned with the CSIRT Services Framework currently developed by experts within the FIRST context. We will start supporting this framework v 2.1 version later in 2020!

- Specify available reactive services, using the following list (or adding to it):
  - alerts and warnings
  - artifact analysis
  - artifact response
  - artifact response coordination

ENISA CSIRT maturity framework

The ENISA CSIRT Maturity Framework is intended to contribute to the enhancement of the global capacity to manage cyber incidents, with a focus on CSIRTs. Cyber incidents and developments are inherently transnational and effective responses depend on transnational collaboration.

(…)

The ENISA CSIRT Maturity Framework is built on three pillars:

1. ***the well-established OCF SIM3 standard***;
2. the ENISA three-tier maturity approach: a series of three pre-defined steps (**Basic**, **Intermediate**, **Advanced**) that can be used as a guideline for the steps to be taken to increase maturity, complete with practical guidance on how to work with the Maturity Framework at different phases – from pre-establishment to advanced levels of maturity;
3. the ENISA assessment methodology: self-assessment and peer-reviews applied in the CSIRTs Network.

SIM3 Security Incident Management Maturity Model

Parameter number	Parameter description	Parameter number	Parameter Description
O-1	Mandate	T-6	Resilient Messaging
O-2	Constituency	T-7	Resilient Internet Access
O-3	Authority	T-8	Incident Prevention Toolset
O-4	Responsibility	T-9	Incident Detection Toolset
O-5	Service Description	T-10	Incident Resolution Toolset
O-6	Public Media Policy	P-1	Escalation to Governance Level
O-7	Service Level Description	P-2	Escalation to Press Function
O-8	Incident Classification	P-3	Escalation to Legal Function
O-9	Participation in CSIRT Systems	P-4	Incident Prevention Process
O-10	Organisational Framework	P-5	Incident Detection Process
O-11	Security Policy	P-6	Incident Resolution Process
H-1	Code of Conduct/Practice/Ethics	P-7	Specific Incident Processes
H-2	Staff Resilience	P-8	Audit & Feedback Process
H-3	Skillset Description	P-9	Emergency Reachability Process
H-4	Staff Development	P-10	Best Practice Internet Presence
H-5	Technical Training	P-11	Secure Information Handling Process
H-6	Soft Skills Training	P-12	Information Sources Process
H-7	External Networking	P-13	Outreach Process
T-1	IT Assets & Configuration	P-14	Governance Reporting Process
T-2	Information Sources List	P-15	Constituency Reporting Process
T-3	Consolidated Messaging System(s)	P-16	Meeting Process
T-4	Incident Tracking System	P-17	Peer Collaboration Process
T-5	Resilient Voice Calls		

45 parametri suddivisi in 4 categorie:

- **Organisational**
- **Human**
- **Tools**
- **Processes**

a ognuno dei quali assegnare un punteggio da 0 a 4:

Level	Status	Indicators
0	Not available / undefined / unaware	-
1	Implicit	Known or considered but not written down, 'between the ears,' 'tribal knowledge'
2	Explicit, internal	Written down but not formally adopted or reviewed
3	Explicit, formalised on authority of CSIRT head	Approved or published
4	Explicit, actively assessed on authority of governance levels above the CSIRT management on a regular basis	Subject to a control process and/or review

Self-assessment tool

Open CSIRT Foundation SIM3 Self Assessment Tool

Organisation | Human | Tools | Processes

With **Organisation** we refer to the ensemble of humans, resources, tools and infrastructures that work together in a planned manner. The objectives or aims of an organisation are directed by a set of specific strategic goals. As SIM3 focuses on the maturity of the management of security incidents, we need to distinguish between on the one hand strategic goals of the whole organisation, and on the other hand the (service) specific strategic goals related to that part of the organisation, that manages security incidents - commonly referred to as 'CSIRT'! The following 'O' parameters are about the mandate, setup and services of that CSIRT, and the framework connecting all organisational aspects.

Expand all / Collapse all

O-1: Mandate

Your CSIRT needs to derive the justification for its existence, its assignment from some higher level of governance. This is called the CSIRT mandate. Ideally, the mandate comes from the highest governance levels in your specific environment. Sometimes it initially comes from a lower level, like the company's head of IT, or the leadership of a ministry. But preferably it comes from the highest levels, like the board of directors, or state government - and in the latter case it can also be anchored in legislation. Does your CSIRT have such a mandate?

0	We never really discussed this and we don't formally know our mandate or assignment. We just do our work.
1	We have a pretty good idea that we are doing is what we were assigned to do, but it was never written down.

Your SIM3 Assessment URL

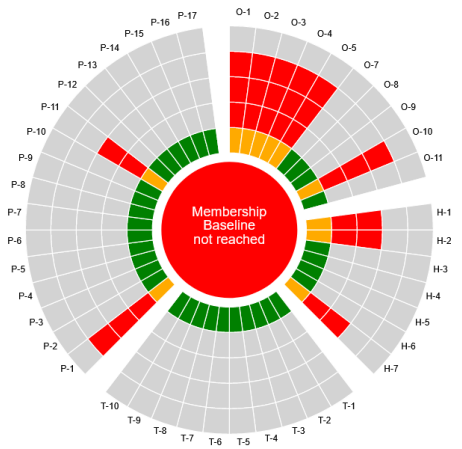
(not set yet, please answer some questions)

Choose your desired SIM3 Profile:

FIRST Membership Baseline	ENISA/GCMF Basic	ENISA/GCMF Intermediate	ENISA/GCMF Advanced	TI Certification

Spider-Chart/Show questions | Table of Results | Open Actions [29]

If you click on a specific tile you will be directed to the associated parameter on the left side.



powered by OpenCSIRT SIM3-check

Conclusioni

Serve tutto questo? Nì. La nostra peculiare situazione (CSIRT interno ma distribuito e con personale – per il momento – solo parzialmente dedicato) probabilmente ci impedirebbe di ambire alla qualifica di *TI Certified CSIRT*, ma l'adozione di alcune buone pratiche (una su tutte: documentare sempre – anche sinteticamente - organizzazione, assegnazione ruoli, processi, flussi di dati e comunicazioni, …) sicuramente ci sarebbe d'aiuto nell'attività e negli eventuali processi per le certificazione di altra natura; l'ingresso nella comunità TI come *listed* (o *accredited*) *member:*

- sancirebbe l'adozione delle *best practice* e l'adesione agli *standard* adottati dalla comunità degli CSIRT;
- testimonierebbe dell'affidabilità dello CSIRT INFN (la qual cosa potrebbe essere fondamentale nella gestione di incidenti non esclusivamente locali);
- ci metterebbe in contatto più diretto con altri team di security.

Ciò premesso, l'acquisizione dello status di listed (ed eventualmente accredited) member comporterà motivazione e impegno da parte di tutto il team, per cui la decisione va presa con *diffusa e capillare* convinzione.

backup