LINEE GUIDA PER LA REALIZZAZIONE DI CSIRT

Agosto 2023

Finanziato dall'Unione europea
NextGenerationEU

DIPARTIMENTO
PER LA TRASFORMAZIONE
DIGITALE

Finanziato dall'Unione europea
NextGenerationEU

DIPARTIMENTO
PER LA TRASFORMAZIONE
DIGITALE

AGENZIA PER LA CYBERSICUREZZA NAZIONALE

L'adozione del D.L. 14 giugno 2021, n. 82 ha ridefinito l'architettura nazionale cyber e istituito l'Agenzia per la Cybersicurezza Nazionale (ACN) a tutela degli interessi nazionali nel campo della cybersicurezza.

L'ACN è Autorità nazionale per la cybersicurezza e assicura il coordinamento tra i soggetti pubblici e la realizzazione di azioni pubblico-private volte a garantire la sicurezza e la resilienza cibernetica per lo sviluppo digitale del Paese. Persegue, inoltre, il conseguimento dell'autonomia strategica nazionale ed europea nel settore del digitale, in sinergia con il sistema produttivo nazionale, nonché attraverso il coinvolgimento del mondo dell'università e della ricerca.

Favorisce specifici percorsi formativi per lo sviluppo della forza lavoro nel settore e sostiene campagne di sensibilizzazione oltre che una diffusa cultura della cybersicurezza. Promuove la cooperazione e lo sviluppo di azioni e progetti internazionali volti alla realizzazione di un cyberspazio globale sicuro.

Contatti: info@acn.gov.it

Seguici sui nostri canali social:

Agenzia per la Cybersicurezza Nazionale

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

ESCLUSIONE DI RESPONSABILITÀ

Le presenti Linee Guida sono state redatte sulla base di modelli, framework e best practice condivisi a livello nazionale ed internazionale al fine di fornire alle Organizzazioni uno strumento di supporto per lo studio della normativa di settore e la definizione di un proprio modello di servizio per l'attivazione e/o il potenziamento di CSIRT.

Il presente documento fornisce, a titolo meramente esemplificativo e non esaustivo, indicazioni sulle possibili azioni da realizzare e competenze da potenziare per innalzare il livello di resilienza cyber di un'organizzazione.

Il rispetto delle indicazioni ivi contenute non esclude in alcun modo l'occorrere di eventuali eventi ed incidenti di natura informatica, intendendosi l'Agenzia per la Cybersicurezza Nazionale esonerata da qualsiasi responsabilità che possa derivare dall'applicazione delle stesse. Resta fermo, pertanto, l'onere per ciascuna Organizzazione di porre in essere tutte le azioni ritenute necessarie per la prevenzione e mitigazione del rischio nonché la risoluzione degli impatti derivanti dalla realizzazione di eventi e incidenti informatici.

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

INDICE

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

EXECUTIVE SUMMARY

Il presente documento è strutturato nel seguente modo:

1. **Introduzione**: fornisce il contesto di riferimento di CSIRT identificandone ruolo e obiettivi.
2. **Approccio metodologico**: descrive l'approccio metodologico utilizzato per la stesura delle linee guida volte alla realizzazione di CSIRT. In particolare, viene fornita una disamina dello stato dell'arte, in relaziona anche alle normative nazionali ed europee di riferimento
3. **Modello di riferimento per l'attivazione di CSIRT**: illustra i servizi che il CSIRT può erogare mediante un opportuno modello organizzativi, comprensivo di requisiti sul personale e loro competenze, tecnologie e processi.
4. **Approccio per l'implementazione di CSIRT**: descrive l'approccio per l'attivazione ed il miglioramento continuo di un CSIRT.
5. **Glossario**: riporta i principali termini e acronimi utilizzati nel documento al fine di facilitarne la lettura.

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

1 Introduzione

Lo sviluppo tecnologico al quale si è assistito negli ultimi anni ha determinato la comparsa e l'evoluzione di rischi e minacce informatiche a danno dell'ecosistema cyber nazionale, così come esso è stato definito da documenti di policy di ACN. A fronte di questo panorama, la Strategia Nazionale di Cybersicurezza 2022-2026 di ACN persegue a livello strategico tre obiettivi brevemente descritti di seguito:

- **protezione** degli asset strategici nazionali attraverso un approccio sistemico orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli che possono abilitare una transizione digitale resiliente del Paese;
- **risposta** alle minacce, agli incidenti e alle crisi cyber nazionali attraverso l'impiego di elevate capacità nazionali di monitoraggio, rilevamento, analisi e risposta e l'attivazione di processi che coinvolgano tutti gli attori facenti parte dell'ecosistema di cybersicurezza nazionale;
- **sviluppo** consapevole e sicuro delle tecnologie digitali, della ricerca e della competitività industriale, in grado di rispondere alle esigenze del mercato.

In linea con questi obiettivi, ACN si propone di condividere informazioni, conoscenze e analisi su rischi, minacce e incidenti informatici in maniera bidirezionale con il settore pubblico e privato, sviluppandone le competenze e supportando la Pubblica Amministrazione e i settori produttivi nazionali nell'adattarsi a un panorama cyber in costante evoluzione.

Tale proposito trova espressione nella redazione e diffusione di **Linee Guida e Best Practice**, ovvero pubblicazioni di ACN che mirano ad **accrescere le competenze e conoscenze** degli attori interessati nell'ambito della cybersicurezza, contribuendo a comporre le differenze e i divari tra gli stessi nel grado di resilienza e consapevolezza, favorendo la **mitigazione dei rischi, la prevenzione e la risposta alle minacce cibernetiche**.

Si illustrano brevemente nel seguito le differenze principali tra le due tipologie di documento:

- le **Linee Guida** forniscono un indirizzo su come procedere in una determinata situazione. In generale, le linee guida forniscono una panoramica su come agire in situazioni in cui non esista una prassi o uno standard riconosciuto dal consenso come il metodo o la tecnica "migliore";
- le **Best Practice** rappresentano l'insieme delle attività, esperienze o azioni che hanno dimostrato di produrre risultati positivi rispetto ad altre e vengono prese come riferimento o utilizzate per ottenere le migliori performance. Illustrano indicazioni validate e riconosciute dalla comunità di esperti del settore che hanno come scopo quello di esplicitare i requisiti e i controlli utili a un corretto processo di gestione della sicurezza informatica e delle informazioni.

In sintesi, le Linee Guida e le Best Practice costituiscono un insieme di pratiche condivise all'interno del sistema Paese per quanto riguarda il settore della cybersecurity.

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

1.1 Scopo del documento

Questo documento di linee guida si **rivolge a quelle organizzazioni che vogliono istituire o potenziare un Cyber Security Incident Response Team (CSIRT)** seguendo le migliori prassi e standard internazionali.

Un **CSIRT**[1] [1], *"è un team organizzato di esperti di cybersicurezza il cui obiettivo principale è la gestione degli incidenti informatici. Un CSIRT offre quindi tutti quei servizi volti a prevenire, mitigare e risolvere gli impatti di incidenti informatici."*

Un CSIRT è quindi uno delle principali strutture organizzative necessarie per innalzare il livello di cyber resilienza di un'organizzazione, contribuendo alla definizione di un percorso virtuoso di monitoraggio e miglioramento continuo nella gestione del rischio cyber. Difatti, nel corso degli anni, il ruolo del CSIRT di un'organizzazione si è evoluto dalla fornitura di servizi di monitoraggio e gestione degli incidenti, al coordinamento e alla comunicazione, sia con soggetti interni che interlocutori della Pubblica Amministrazione e partner internazionali.

In linea con gli standard internazionali e le prassi, due elementi identificativi e costitutivi di un CSIRT sono:

1. Il Mandato [1]: *descrive gli obiettivi di base di un CSIRT, in termini di servizi forniti verso la propria Constituency.*

2. La Constituency [1]: l'insieme di soggetti ed entità che potranno accedere ai servizi offerti dal CSIRT, eseguire attività di scambio informativo e con i quali il CSIRT dovrà definire le relative modalità di ingaggio, di cooperazione e di affiliazione.

La realizzazione di un CSIRT e la sua continua evoluzione permette ad un'organizzazione, quindi alla constituency di riferimento, di traguardare i seguenti obiettivi:

- identificazione di un centro di competenza specializzato a supporto della gestione del rischio cyber nella Constituency;
- messa a terra di processi e procedure di preparazione, prevenzione e gestione degli incidenti informatici;
- analisi specialistiche sulle vulnerabilità e su artefatti raccolti nel corso delle attività di gestione degli incidenti informatici;
- realizzazione di attività di miglioramento continuo in ambiti di prevenzione e formazione in ambito cyber;
- identificazione di un unico punto di contatto per la constituency con gli interlocutori esterni di rilevanza.

L'integrazione delle reti e dei sistemi digitali sta sempre più portando a incidenti informatici i cui impatti sono distribuiti tra più organizzazioni. La gestione e risoluzione di questi incidenti necessità quindi di una rete di collaborazione tra i CSIRT. A tal riguardo, a seguito del DPCM

[1] Anche noto come CIRT (Computer Incident Response Teams), CERT (Computer Emergency Response Teams), SIRT (Security Incident Response Teams) e altri ancora.

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

n. 65 dell'8 agosto 2019 (Direttiva NIS), l'Italia si è dotata di un CSIRT nazionale, adesso attivato presso l'ACN e denominato **CSIRT Italia.** In linea con la Strategia Nazionale di Cybersicurezza, il CSIRT Italia ha, tra gli altri, il compito di favorire e coordinare la realizzazione della rete nazionale dei CSIRT e quindi della risposta coordinata agli incidenti informatici.

Un CSIRT, realizzato sulla base delle linee guida del presente documento, potrà quindi giovarsi di un modello già messo in atto dallo stesso CSIRT Italia, facilitando eventuali collaborazioni con l'ACN per la preparazione e il supporto alla gestione e risposta a incidenti informatici.

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2 Approccio metodologico

Modelli, framework e prassi internazionali per la realizzazione, nonché accreditamento, di CSIRT sono stati sviluppati e validati dalla comunità tecnica da molti anni. Al fine di definire una linea guida completa, ma al tempo stesso conciliabile con differenti livelli di maturità di un'organizzazione, è stata fatta una sintesi e armonizzazione delle migliori pratiche internazionali. Nello specifico, sono state analizzate e quindi armonizzate le seguenti:

- **CSIRT AND SOC GUIDELINE** [2]: linee guida emesse dall'**Agenzia dell'Unione Europea per la Cybersicurezza** (**ENISA**) che hanno l'obiettivo di definire lo scopo e l'ambito di un CSIRT, quali servizi è in grado di offrire e qual è l'iter di avvio e gestione.
- **CSIRT SERVICE FRAMEWORK** [3, 4]: framework istituito dal **FIRST** (leader riconosciuto a livello mondiale per la risposta agli incidenti), che descrive in modo strutturato una raccolta di servizi di cybersecurity e di funzioni associate che i CSIRT possono fornire alle proprie Constituency. Questo framework ha l'obiettivo di facilitare la creazione e il miglioramento delle operazioni, in particolare nel supportare attività di miglioramento e potenziamento del portafoglio dei servizi offerti.
- **SIM3 MODEL** [5]: framework ideato dalla Open CSIRT Foundation che introduce una serie di requisiti atti alla valutazione del livello di maturità dei servizi offerti da un CSIRT. Questo strumento viene utilizzato sia come metodo di accreditamento dal Trusted Introducer (TI), che durante il processo di adesione per il FIRST oltre che dall'ENISA.

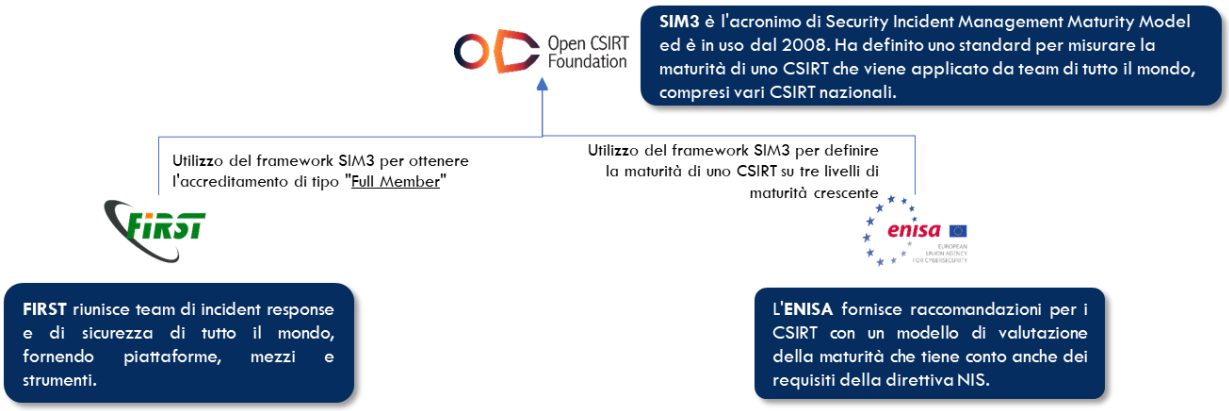

Figura 1 - Framework e standard internazionali a supporto della realizzazione di un CSIRT

A partire dai framework di riferimento sopra citati, è stato definito un **modello di riferimento** per la realizzazione o il potenziamento di un CSIRT che si compone delle dimensioni di seguito riportate:

1. **modello di servizio**: descrive il catalogo dei servizi offerti da un CSIRT per la realizzazione del proprio mandato a favore della Constituency;
2. **processi**: identifica sequenze di azioni assegnate a specifiche figure professionali per la realizzazione di attività con il supporto degli opportuni strumenti tecnologici;
3. **modello organizzativo e figure professionali**: descrive la struttura organizzativa di un CSIRT, in termini di organigramma, con il dettaglio delle figure professionali necessarie

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

per l'erogazione dei servizi offerti e dei relativi ruoli e responsabilità, nonché delle modalità di interazione tra le diverse figure;

4. **strumenti**: descrive gli strumenti utilizzati dal personale del CSIRT per raggiungere gli obiettivi previsti all'interno del mandato.

Figura 2 - Modello di riferimento per l'attivazione di un CSIRT

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

3 Modello di riferimento per l'attivazione di un CSIRT

3.1 Modello di Servizio

I servizi erogati da un CSIRT identificano le specifiche operative offerte che compongono il modello di servizio, il quale si può declinare secondo tre livelli gerarchici: Aree, Servizi e Funzioni, così dettagliati:

1. *Aree,* c.d. Service Area*,* definiscono le aree di operatività per un CSIRT e sono così identificate:
   - Information Security Event Management.
   - Information Security Incident Management.
   - Vulnerability Management.
   - Situational Awareness.
   - Knowledge Transfer.
2. *Servizi,* c.d. Service, rappresentano un insieme di funzioni riconoscibili, coerenti e orientate per ottenere uno specifico risultato.
3. *Funzioni,* c.d. Function, rappresentano un insieme di attività volte a realizzare un particolare servizio o comunque utilizzare nel contesto di differenti servizi.

Tale struttura gerarchica consente ad un CSIRT di organizzare le proprie *Funzioni* in *Servizi,* i quali risultano aggregati all'interno di specifiche *Aree*, aventi come principale obiettivo il raggiungimento di quanto previsto dal proprio mandato.

A tal proposito, in linea con il mandato e la Constituency, il modello di servizio può essere opportunamente declinato e implementato. Le definizioni delle aree, servizi e funzioni che seguono sono volte a fornire un quadro comune e armonizzato per la realizzazione o potenziamento di un CSIRT.

Nell'immagine seguente, si riporta graficamente la struttura gerarchica del modello di servizio proposto, a seguire, il modello viene descritto seguendo la struttura gerarchi di Aree *X* (indicate con X.), relativi Servizi *y* (indicate con X.y) e quindi delle costituenti Funzioni *z* (indicate con X.y.z).

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

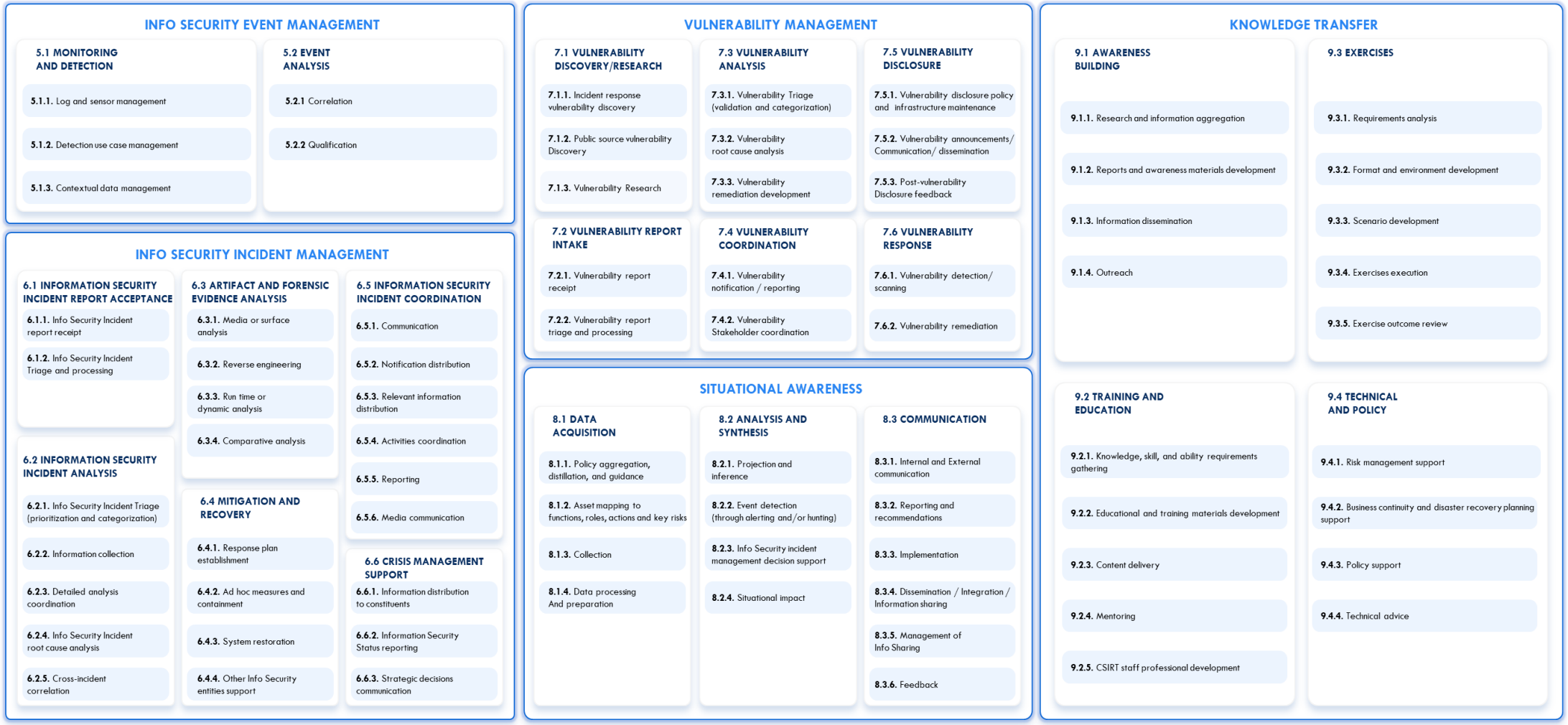

Figura 3 - Mappa completa delle aree, dei servizi e delle funzioni erogabili da un CSIRT.

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

5 - Information Security Event Management

Nella presente area sono inclusi tutti quei servizi atti abilitare la raccolta, il monitoraggio e l'analisi di eventi di sicurezza, con il fine di identificare, ed eventualmente qualificare, potenziali incidenti di sicurezza. Si riportano di seguito, i principali obiettivi perseguiti da questa area:

- adeguata gestione delle fonti, degli use case e dei dati di contesto dell'organizzazione;
- efficace monitoraggio e gestione ed analisi degli eventi di sicurezza;
- eseguire attività di correlazione degli eventi al fine di collegare più eventi pervenuti all'interno dell'infrastruttura di monitoraggio e poter identificare in modo efficace potenziali incidenti e/o ridurre, per quanto possibile, i falsi positivi.

I servizi e funzioni associati a questa area sono i seguenti:

- ***5.1 Monitoring and detection***: servizio volto all'abilitazione dell'elaborazione automatizzata e continua degli eventi di sicurezza – inclusivo della gestione delle fonti, degli use case e dei dati contestuali – al fine di rilevare eventuali anomalie che possono successivamente essere qualificate come incidenti di sicurezza. Tale servizio si declina nelle seguenti funzioni:
  - **5.1.1 Log and sensor management**: efficace gestione delle diverse sorgenti di log e dati al fine di ottenere un flusso costante di eventi di sicurezza da poter analizzare sfruttando gli *use case* configurati all'interno dell'infrastruttura di monitoraggio.
  - **5.1.2 Detection use case management**: definizione, verifica, miglioramento, aggiornamento e configurazione degli *use case* di monitoraggio di supporto agli analisti per l'identificazione di eventi di sicurezza.
  - **5.1.3. Contextual data management**: gestione dei vari dati contestuali (esempio, dati provenienti da un Configuration Management Database, da sistemi di Threat intelligence oppure da Sistemi di Identity and Access Management) utilizzati poi successivamente per il monitoraggio e la correlazione degli eventi di sicurezza.
- ***5.2 Event Analysis***: esecuzione di attività di triage per l'esecuzione di una prima analisi dell'evento identificato, nonché l'esecuzione della qualifica degli stessi al fine di identificare eventuali falsi positivi e/o incidenti confermati. Tale servizio si declina nelle seguenti funzioni:
  - **5.2.1 Correlation**: correlazione degli eventi di sicurezza provenienti da diverse fonti e che impattano uguali risorse (esempio, sistemi, servizi, clienti) e/o le stesse identità (esempio, utenti), o comunque che possono essere evidenza di un potenziale incidente in corso. Tali attività fornisce all'analista una vista più ampia delle informazioni su cui eseguire le analisi, e quindi ridurre ulteriormente la capacità di identificazione di potenziali incidenti.
  - **5.2.2 Qualification**: validazione di un potenziale incidente di sicurezza come un reale incidente (vero positivo), o come un falso positivo. Nel contesto di tale attività si procederà inoltre con l'esecuzione di attività di arricchimento, di assegnazione di punteggi di rischio e di identificare potenziali eventi addizionali correlati.

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

6 - Information Security Incident Management

Nella presente area sono inclusi tutti quei servizi dediti all'analisi, gestione e mitigazione degli incidenti di sicurezza qualificati. Si riportano di seguito, i principali obiettivi perseguiti da questa area:

- analisi incidente e identificazione della causa alla base dell'incidente in corso di gestione;
- raccolta ed analisi degli artefatti e delle evidenze;
- supporto alla Constituency nella definizione dei piani di rientro;
- coordinamento relativo alla gestione degli incidenti con tutti gli stakeholder coinvolti;
- mitigazione ed eventuale ripristino dei sistemi impattati nell'incidente.

I servizi e funzioni associati a questa area sono i seguenti:

- ***6.1 Information security incident report acceptance***: ricezione ed elaborazione delle segnalazioni relative a potenziali incidenti di sicurezza identificati dalla Constituency, dagli stakeholder e da eventuali terze parti[2]. Le informazioni relative agli incidenti possono pervenire mediante differenti canali di comunicazione, messi a disposizione dal CSIRT alla Constituency. Tale servizio si declina nelle seguenti funzioni:
  - **6.1.1 Information security incident report receipt**: ricezione dei report di incidente attraverso meccanismi e processi ben definiti e condivisi. Le informazioni contenute all'interno della segnalazione possono essere più o meno complete - e possono riguardare, ad esempio, asset, utenti, reti nonché informazioni relative ad eventuali attività di mitigazione già intraprese dall'organizzazione.
  - **6.1.2 Information security incident triage and processing**: analisi dei report relativi agli incidenti con l'obiettivo di eseguire un triage completo identificando potenziali impatti relativi sulla riservatezza, disponibilità ed integrità. Nel contesto di tali attività si procederà inoltre nell'identificazione della causa che ha portato al concretizzarsi di un incidente.
- ***6.2 Information security incident analysis****:* analizzare e comprendere i dettagli relativi ad un incidente di sicurezza, ottenendo informazioni di dettaglio, quali impatto, cause che lo hanno determinato (esempio, eventuale sfruttamento di vulnerabilità) ed eventuali exploit utilizzati. Tale servizio si declina nelle seguenti funzioni:
  - **6.2.1 Information security incident triage**: analisi dell'incidente di sicurezza con l'obiettivo di classificare, prioritizzare e valutare l'impatto che lo stesso ha avuto sui sistemi/servizi coinvolti.
  - **6.2.2 Information collection**: identificare e raccogliere tutte le informazioni necessarie per ottenere una comprensione del contesto in cui si è verificato l'incidente. Questo permette di ottenere informazioni relative all'incidente in

[2] Rappresentano le organizzazioni o enti esterni che possono collaborare con il CSIRT. Tale insieme include, ma non esclusivamente, CSIRT ITALIA, CNAIPIC, organizzazioni private ed enti istituzionali.

modo strutturato, che, successivamente, potranno essere utilizzate in qualsiasi ulteriore necessità.

- **6.2.3 Detailed analysis coordination**: effettuare, qualora sia necessario ottenere informazioni aggiuntive, delle analisi tecniche aggiuntive su un determinato incidente di sicurezza. Tali analisi addizionali, possono essere effettuate sia all'interno del CSIRT che da entità terze.
- **6.2.4 Information security incident root cause analysis**: identificare la causa principale dell'incidente di sicurezza (conosciuta come "root cause analysis"), analizzando e identificando le circostanze che hanno determinato la presenza di una vulnerabilità, e che ne hanno consentito lo sfruttamento.
- **6.2.5 Cross-Incident correlation**: eseguire una correlazione tra informazioni legate ad incidenti di sicurezza già gestiti, con l'obiettivo di determinarne le interrelazioni, cause e/o mitigazioni applicabili per migliorare e velocizzare la risposta agli incidenti di sicurezza attualmente in analisi.

- ***6.3 Artifact and forensic evidence analysis***: acquisizione, analisi e studio di tutti gli artefatti relativi a un incidente di sicurezza. Tale servizio si declina nelle seguenti funzioni:
  - **6.3.1 Media or surface analysis**: estrazione ed analisi degli artefatti relativi all'incidente in corso di risoluzione, e confronto di quanto emerso con informazioni ottenute da analisi pregresse o presenti in fonti pubbliche.
  - **6.3.2 Reverse engineering**: esecuzione di analisi statiche su artefatti con l'obiettivo di determinare, in modo esaustivo, le sue funzionalità (esempio, metodi di attivazione, impatti, metodi di propagazione, mitigazione, ecc.) indipendentemente dall'ambiente in cui può essere eseguito.
  - **6.3.3 Run time or dynamic analysis**: esecuzione di attività di analisi dinamica di un artefatto, al fine di valutarne il comportamento in esecuzione all'interno di ambienti controllati, siano essi reali e/o emulati (esempio, sandbox, ambienti virtuali).
  - **6.3.4 Comparative analysis**: esecuzione di attività di analisi comparativa tra gli artefatti collezionati durante le attività eseguite dal CSIRT, al fine di identificare eventuali similitudini tra gli stessi, in termini di modus operandi, obiettivi, intenzioni e attori.
- ***6.4 Mitigation and recovery***: attività volte al contenimento ed al ripristino dell'operatività dei sistemi coinvolti all'interno dell'incidente di sicurezza in corso di gestione. Durante tali attività dovrà, altresì, essere prevista l'implementazione di controlli atti alla risoluzione delle criticità che hanno permesso il concretizzarsi dell'incidente (esempio, vulnerabilità, errate configurazioni) limitando così eventuali future compromissioni legate alla stessa problematica. Tale servizio si declina nelle seguenti funzioni:
  - **6.4.1 Response plan establishment**: definizione e applicazione di un piano di risposta per tutti gli incidenti identificati dallo CSRIT, con l'obiettivo di ripristinare l'integrità dei sistemi impattati e la piena operatività dei servizi interessati.

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

- **6.4.2 Ad hoc measures and containment**: contenimento di un incidente di sicurezza attraverso misure specifiche per l'incidente in esame, evitando che si diffonda ulteriormente su altri sistemi e infrastrutture dell'organizzazione. Queste attività garantiscono che gli attaccanti non abbiano più accesso ai dati, sistemi e reti precedentemente compromesse.
- **6.4.3 System restoration**: applicazione di misure atte a ripristinare l'integrità dei sistemi interessati e riportare i dati, i sistemi e le reti impattate dall'incidente a uno stato operativo non degradato, ripristinando la piena funzionalità dei servizi coinvolti.
- **6.4.4 Other information security entities support**: fornire un'assistenza diretta (anche in loco) alla Constituency, supportandola sia nella risoluzione di un incidente che nella rimozione delle vulnerabilità sfruttate dagli attaccanti.

- ***6.5 Information security incident coordination***: garantire notifiche tempestive verso la Constituency oltre che un'accurata distribuzione delle informazioni. Tali attività sono svolte mantenendo il flusso di informazioni costante, tenendo traccia dello stato delle attività stesse e assicurandosi che il piano di risposta definito sia attuato correttamente. Tale servizio si declina nelle seguenti funzioni:
  - **6.5.1 Communication**: definire ed utilizzare dei canali di comunicazione sicuri ed affidabili atti a garantire la riservatezza delle comunicazioni, con la Constituency e con eventuali terze parti coinvolte nelle attività.
  - **6.5.2 Notification distribution**: comunicare alla Constituency impattata da un incidente di sicurezza, nonché ad eventuali ulteriori soggetti che possono contribuire alla gestione di tale incidente, tutte le informazioni utili alla gestione dell'incidente stesso al fine di identificare in modo chiaro tutti i ruoli ed i risultati attesi durante la cooperazione.
  - **6.5.3 Relevant information distribution**: mantenere attivo il flusso di comunicazione sia con le entità impattate da un incidente sia con le entità identificate per supportare nella risposta stesso, fornendo informazioni sempre aggiornate con l'obiettivo di adottare le azioni più opportune per la gestione dell'incidente.
  - **6.5.4 Activities coordination**: gestione e coordinamento efficiente delle comunicazioni al fine di tracciare tutti gli scambi informativi ed ottenere informazioni utili a supportare i soggetti interessati nell'identificazione, nella protezione e/o nel completamento delle attività di risoluzione dell'incidente.
  - **6.5.5 Reporting**: collezione, organizzazione e condivisione di informazioni circa lo stato attuale di completamento delle attività, al fine di assicurare un coordinamento efficace delle attività di risposta degli incidenti.
  - **6.5.6 Media communication**: condivisione con i media di informazioni accurate e di facile comprensione circa lo stato degli eventi in corso, per evitare la diffusione di informazioni fuorvianti.
- ***6.6 Crisis management support***: supportare attivamente, mediante competenze e punti di contatto, altri esperti di sicurezza, CSIRT ed altre entità per contribuire a mitigare eventuali situazioni di crisi. Tale servizio si declina nelle seguenti funzioni:

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

- **6.6.1 Information distribution to constituents**: condivisione, mediante canali appositamente predisposti, di informazioni utili alla gestione di una situazione di crisi.
- **6.6.2 Information Security Status reporting**: raccolta e condivisione di informazioni concise sullo stato attuale della sicurezza informatica all'interno della Constituency, al fine di supportare la squadra di gestione della crisi nella definizione della più appropriata strategia di risoluzione della stessa.
- **6.6.3 Strategic decisions communication**: condivisione delle informazioni relative agli impatti causati dalla crisi, al fine di supportare la definizione di una appropriata strategia di gestione della crisi stessa.

7 - Vulnerability Management

Nella presente area sono inclusi tutti quei servizi atti a supportare la Constituency attraverso attività di identificazione, analisi e gestione di vulnerabilità, siano esse nuove o già note. Si riportano di seguito, i principali obiettivi perseguiti da questa area:

- identificare ed analizzare, attivamente o passivamente, vulnerabilità non note;
- sviluppare piani di rimedio efficaci per la risposta a nuove vulnerabilità rilevate;
- condividere, in modo responsabile, informazioni relative alle nuove vulnerabilità identificate;
- supportare la Constituency nell'identificazione e risoluzione di vulnerabilità, note e non note, presenti nella sua infrastruttura.

I servizi e funzioni associati a questa area sono i seguenti:

- ***7.1 Vulnerability discovery / research***: identificare, venire a conoscenza o ricercare attivamente nuove vulnerabilità non note. Tali vulnerabilità possono essere scoperte dal personale a supporto di questa area specifica (Vulnerability Management), o da qualsiasi altro servizio erogato dal CSIRT stesso. Tale servizio si declina nelle seguenti funzioni:
  - **7.1.1 Incident response vulnerability discovery**: identificazione di una vulnerabilità non nota, sfruttata da un attaccante, rilevata durante le attività di gestione di un incidente di sicurezza.
  - **7.1.2 Public source vulnerability discovery**: identificazione di una nuova vulnerabilità mediante l'analisi di fonti pubbliche e/o fonti terze parti.
  - **7.1.3 Vulnerability research**: esecuzione di attività di ricerca attiva con l'obiettivo di identificare vulnerabilità non note.
- ***7.2 Vulnerability report intake***: collazionamento ed elaborazione delle informazioni relative alle vulnerabilità identificate e segnalate dalla Constituency e/o da entità terze al fine di validarle e classificarle. Tale servizio si declina nelle seguenti funzioni:
  - **7.2.1 Vulnerability report receipt**: ricezione dei report sulle vulnerabilità attraverso meccanismi e processi ben definiti e condivisi. Le informazioni contenute all'interno della segnalazione possono essere più o meno complete - e possono riguardare, ad esempio, dispositivi interessati, condizioni necessarie per sfruttare le vulnerabilità

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

nonché informazioni relative ad eventuali attività di mitigazione/risoluzione identificate.

- **7.2.2 Vulnerability report triage and processing**: analisi, classificazione e prioritizzazione delle segnalazioni delle vulnerabilità eseguite dalla Constituency e/o da terze parti al fine di ottenere una comprensione iniziale della vulnerabilità stessa.

- ***7.3 Vulnerability analysis***: esecuzione di attività di analisi delle vulnerabilità non note di cui il CSIRT è venuto a conoscenza, al fine di identificarne le peculiarità e valutare un piano di rimedio/mitigazione appropriato. Tale servizio si declina nelle seguenti funzioni:
  - **7.3.1 Vulnerability triage**: esecuzione di attività di analisi delle vulnerabilità al fine di classificarle, prioritizzarle e valutarne il potenziale impatto sui sistemi della Constituency - in termini confidenzialità, integrità e disponibilità delle informazioni.
  - **7.3.2 Vulnerability root cause analysis**: identificare, analizzare e validare le cause che ne determinato la presenza della vulnerabilità, nonché identificare le condizioni di sfruttabilità della stessa.
  - **7.3.3 Vulnerability remediation development**: definire le azioni/attività necessarie alla risoluzione o alla mitigazione della vulnerabilità.
- ***7.4 Vulnerability coordination***: scambiare informazioni e coordinare le attività con tutte le entità, sia interne che esterne, coinvolte nel processo di divulgazione responsabile delle vulnerabilità.
  - **7.4.1 Vulnerability notification/reporting**: notificare la vulnerabilità identificata, o segnalata al CSIRT, e coordinare lo scambio di informazioni pertinenti con gli altri attori coinvolti (esempio, fornitori, sviluppatori, PSIRT, ricercatori e altri CSIRT) che possono collaborare per analizzare e correggere la vulnerabilità.
  - **7.4.2 Vulnerability stakeholder coordination**: eseguire attività di coordinamento circa la condivisione delle informazioni tra le varie parti interessate e coinvolte nelle attività di divulgazione responsabile delle vulnerabilità.
- ***7.5 Vulnerability disclosure***: condivisione delle informazioni relative alle vulnerabilità note verso la Constituency al fine di abilitare la prevenzione, l'identificazione e la risoluzione/mitigazione delle vulnerabilità stesse. Tale servizio si declina nelle seguenti funzioni:
  - **7.5.1 Vulnerability disclosure policy and infrastructure maintenance**: definire e condividere politiche a supporto dell'esecuzione delle attività di divulgazione delle vulnerabilità e delle modalità impiegate per la condivisione delle informazioni ad esse connesse.
  - **7.5.2 Vulnerability announcements/ communication/ dissemination**: condividere con la Constituency, e/o rendere pubbliche, informazioni relative ad una vulnerabilità non nota identificata, al fine di permettere loro di rilevare, correggere, mitigare e prevenire lo sfruttamento della stessa.
  - **7.5.3 Post-vulnerability disclosure feedback**: ricevere, rispondere e fornire riscontri a domande/segnalazioni da parte della Constituency, circa una vulnerabilità non nota precedentemente divulgata.

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

- ***7.6 Vulnerability response***: utilizzare attivamente le informazioni sulle vulnerabilità note con lo scopo di adoperarle per prevenire, rilevare e mitigare le stesse. Tale servizio si declina nelle seguenti funzioni:
  - **7.6.1 Vulnerability detection/scanning**: esecuzione di attività di scansione volte all'identificazione di eventuali vulnerabilità che affliggono i sistemi della Constituency, al fine di prevenirne lo sfruttamento.
  - **7.6.2 Vulnerability remediation**: risolvere o mitigare la vulnerabilità presente sui sistemi della Constituency, con l'obiettivo di eliminare o ridurre la probabilità di sfruttamento della stessa da parte di un attaccante.

8 - Situational Awareness

Nella presente area sono inclusi tutti quei servizi che hanno lo scopo di identificare, elaborare, comprendere e comunicare gli elementi critici che possono impattare la Constituency. Si riportano di seguito, i principali obiettivi perseguiti da questa area:

- acquisizione di dati circa attività rilevanti che potrebbero impattare il quadro situazionale della Constituency;
- esecuzione di attività di analisi sui dati acquisiti con lo scopo di identificare eventuali variazioni del quadro situazionale della Constituency;
- condivisione dei risultati derivanti dalle attività di analisi alla Constituency, di supporto alla definizione ed attuazione di una strategia specifica per la mitigazione, gestione e prevenzione di potenziali minacce e incidenti.

I servizi e funzioni associati a questa area sono i seguenti:

- ***8.1 Data acquisition***: acquisire dati con l'obiettivo di aumentare la visibilità circa eventuali attività rilevanti che potrebbero influenzare l'attuale postura di sicurezza della Constituency. Tale servizio si declina nelle seguenti funzioni:
  - **8.1.1 Policy aggregation, distillation, and guidance**: raccolta, aggregazione e distribuzione delle politiche volte alla definizione di una baseline operativa accettabile.
  - **8.1.2 Asset mapping to functions, roles, actions and key risks**: acquisizione di informazioni relative al contesto dell'organizzazione circa asset, caratteristiche e baseline attese, al fine di identificare potenziali attività anomale e definire l'elenco prioritizzato degli asset potenzialmente a rischio.
  - **8.1.3 Collection**: acquisizione, da fonti interne ed esterne, delle informazioni e dei dati che possono supportare l'operatività degli altri servizi erogati dal CSIRT (esempio, Security Event Management e Incident Management).
  - **8.1.4 Data processing and preparation**: definisce un insieme di dati affidabili, coerenti ed aggiornati in grado di supportare le attività, servizi e funzioni erogate dal CSIRT.
- ***8.2 Analysis and synthesis***: esecuzione di attività di analisi volte all'identificazione di eventuali variazioni al contesto attuale che possono in qualche modo impattare gli asset e/o la postura di sicurezza della Constitutency. Tale servizio si declina nelle seguenti funzioni:

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

- **8.2.1 Projection and inference**: analisi delle informazioni raccolte durante la "Data Acquisition" al fine di indentificare il contesto attuale e prevedere quelli futuri.
- **8.2.2 Event detection:** ricerca sistematica di attività anomale all'interno e all'esterno della Constituency, eseguita sulla base di informazioni provenienti dal contesto interno ed esterno all'organizzazione. Tale attività si pone come obiettivo principale di fornire supporto alle attività di analisi dei dati (esempio, log, eventi) generati dai sensori presenti all'interno dell'infrastruttura dell'organizzazione.
- **8.2.3 Information security incident management decision support**: esecuzione di attività di analisi eseguita sulle evidenze specifiche relative al contesto situazionale, al fine di supportare la gestione degli incidenti, mediante l'identificazione di informazioni atte alla riduzione degli impatti e alla mitigazione di potenziali rischi futuri.
- **8.2.4 Situational impact**: identificazione dell'impatto potenziale previsto a valle dell'esecuzione di una previsione rispetto alla variazione del contesto situazionale attuale.

- ***8.3 Communication***: condivisione alla Constituency dei risultati delle attività di analisi seguite, al fine di identificare eventuali azioni da intraprendere a fronte di una variazione del contesto situazionale in essere. Tale servizio si declina nelle seguenti funzioni:
  - **8.3.1 Internal and external communication**: comunicare con tutte la Constituency in merito al contesto situazionale attuale e di sue potenziali variazioni.
  - **8.3.2 Reporting and recommendations**: predisposizione di reportistica e raccomandazioni accurate, tempestive e complete alla Constituency in merito ai risultati delle attività di analisi, al fine di fornire informazioni in merito ad azioni che dovrebbero essere intraprese per mantenere una adeguata postura di sicurezza.
  - **8.3.3 Implementation**: supportare la Constituency nell'esecuzione di attività di modifica all'infrastruttura sulla base delle comunicazioni ricevute e contenenti informazioni relative al contesto situazionale e ad eventuali previsioni di variazioni dello stesso.
  - **8.3.4 Dissemination / integration / information sharing**: aggregare, normalizzare, preparare e condividere con la Constituency e con entità terze, le informazioni raccolte ed analizzate nel corso delle attività.
  - **8.3.5 Management of information sharing**: gestire il trasferimento delle informazioni con la Constituency in modo efficiente, garantendo l'usabilità delle informazioni condivise.
  - **8.3.6 Feedback**: ricevere ed inviare feedback in modo efficace da e verso la Constituency, con l'obiettivo di migliorare l'accuratezza, la qualità e l'utilità delle informazioni condivise.

-9 - Knowledge Transfer

Nella seguente area sono presenti tutti quei servizi che consentono ad un CSIRT di trasferire ai propri utenti, interni ed esterni, le proprie conoscenze e competenze, al fine di supportare

le organizzazioni nell'identificazione, nella prevenzione e nella risposta agli incidenti di sicurezza. Si riportano di seguito, i principali obiettivi perseguiti da questa area:

- costruzione della consapevolezza (awareness) circa la comprensione in maniera olistica delle varie tipologie di minacce informatiche che potrebbero impattare la Constituency;
- effettuare una formazione sia tecnica che teorica mediante lezioni, corsi ed esercitazioni anche pratiche per testare il livello di istruzione dei membri sia del CSIRT che della Constituency, al fine di poter gestire in modo opportuno i potenziali incidenti che potrebbero verificarsi;
- fornire consulenza tecnica volta a supportare il miglioramento delle infrastrutture, degli strumenti e dei servizi relativi alla sicurezza informatica della Constituency;
- fornire consulenza in merito alla predisposizione ed attuazione di politiche di sicurezza per la Constituency.

I servizi associati all'area in questione che un CSIRT deve erogare sono i seguenti:

9.1 Awareness building: supportare il miglioramento generale della postura di sicurezza della Constituency, costruendo competenze che consentano loro di gestire in modo adeguato la sicurezza informatica all'interno dell'organizzazione. Tale servizio si declina nelle seguenti funzioni:

- **9.1.1 Research and information aggregation**: aggregare, raccogliere e prioritizzare le informazioni che possono essere condivise con la Constituency per migliorare la loro postura di sicurezza e poter mitigare i relativi rischi ad essa associati.
- **9.1.2 Reports and awareness materials development**: produzione di materiale informativo in differenti formati (presentazioni, video, opuscoli, ecc.) da condividere con la Constituency mediante differenti piattaforme.
- **9.1.3 Information dissemination**: diffusione di informazioni relative alla sicurezza informatica al fine di accrescere la consapevolezza degli utenti della Constituency, e supportare la stessa nell'implementazione delle best practice di sicurezza.
- **9.1.4 Outreach**: sviluppare e mantenere relazioni con esperti nel settore e con altre organizzazioni, ivi inclusi ulteriori CSIRT, che possono supportare il raggiungimento degli obiettivi presenti nel mandato del CSIRT.

- ***9.2 Training and education***: erogazione di attività di formazione al personale della Constituency, riguardante argomenti relativi alla sicurezza informatica, la sicurezza delle informazioni e la gestione degli incidenti. Tale servizio si declina nelle seguenti funzioni:
  - **9.2.1 Knowledge, skill, and ability requirements gathering**: analizzare, identificare e documentare le necessità - in termini di conoscenze, competenze e abilità – della Constituency, al fine di poter sviluppare materiale di training appropriato ed in linea con i loro bisogni.
  - **9.2.2 Educational and training materials development**: sviluppare il materiale educativo, didattico e di formazione, analizzando i bisogni della Constituency, e condiviso mediante i canali di formazioni più appropriati all'audience ed al contenuto.

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

- **9.2.3 Content delivery**: definizione e consolidamento di un processo formale, per la condivisione del materiale didattico alla Constituency, in linea con le competenze ed alle necessità dell'audience e del contenuto del materiale stesso.
- **9.2.4 Mentoring**: sviluppo di un programma di tutoraggio che consenta al personale del CSIRT, ai membri della Constituency e/o ai partner esterni di apprendere da personale esperto, ingaggiato secondo una logica continuativa.
- **9.2.5 CSIRT staff professional development**: pianificazione e implementazione di un piano di sviluppo delle carriere per il personale a supporto delle attività del CSIRT.

9.3 Exercises: servizio che prevede l'esecuzione di attività di esercitazione, sia per il suo personale che per i team della Constituency, volte a valutare e migliorare l'efficacia dei servizi e delle funzioni erogate. Tale servizio si declina nelle seguenti funzioni:

- **9.3.1 Requirements analysis**: determinare gli obiettivi che devono essere raggiunti da parte dei partecipanti alle esercitazioni.
- **9.3.2 Format and environment development**: identificazione delle risorse necessarie affinché possano essere erogate le esercitazioni pianificate, nonché definire il formato dell'esercitazione e la piattaforma per la sua erogazione.
- **9.3.3 Scenario development**: sviluppare gli scenari delle esercitazioni finalizzate al potenziamento dell'efficienza e dell'efficacia dei servizi e delle funzioni del CSIRT, nonché delle competenze, conoscenze e abilità del personale.
- **9.3.4 Exercises execution**: attività di esercitazione finalizzate alla valutazione delle competenze del personale del CSIRT, principalmente legati alla capacità ed applicare i concetti ricevuti durante la formazione.
- **9.3.5 Exercise outcome review**: sviluppo di una specifica relazione a valle dell'esecuzione delle attività di esercitazione, al fine di analizzare i risultati della stessa e identificare potenziali aree di miglioramento, nonché eventuali azioni raccomandate per il miglioramento delle competenze.

- ***9.4 Technical and policy advisor***: supportare la Constituency, o eventuali persone chiave coinvolte, nella costituzione di specifiche politiche e procedure al fine di abilitare appropriate modalità di gestione degli incidenti, gestire adeguatamente minacce e rischi, incrementando così anche l'efficacia delle attività eseguite dal CSIRT. Tale servizio si declina nelle seguenti funzioni:
  - **9.4.1 Risk management support**: supportare attivamente la Constituency durante le attività di valutazione del rischio e/o di compliance.
  - **9.4.2 Business continuity and disaster recovery planning support**: supportare la Constituency sulle tematiche di continuità operativa e disaster recovery, fornendo consigli imparziali e basati sui fatti, e strettamente legati al contesto organizzativo.
  - **9.4.3 Policy support**: supportare la Constituency sulla predisposizione ed attuazione di politiche di sicurezza, fornendo consigli imparziali e basati sui fatti oltre che strettamente legati al contesto organizzativo.
  - **9.4.4 Technical advice**: erogazione di supporto tecnico specialistico per il miglioramento delle infrastrutture, degli strumenti e dei servizi relativi alla

sicurezza informatica della Constituency, con l'obiettivo di eseguire un miglioramento generale della postura di sicurezza, delle modalità operative e delle best practice adottate.

3.2 Processi

All'interno di un CSIRT, il raggiungimento degli obiettivi operativi, nonché il rispetto del proprio mandato, richiede la definizione, l'esecuzione e il monitoraggio di processi consolidati. Al fine di garantire una corretta gestione delle attività e degli obiettivi, è necessario che i processi siano scritti formalmente, approvati dal team management e, successivamente, monitorati per valutarne le performance e poter definire ed attuare dei piani concreti di miglioramento.

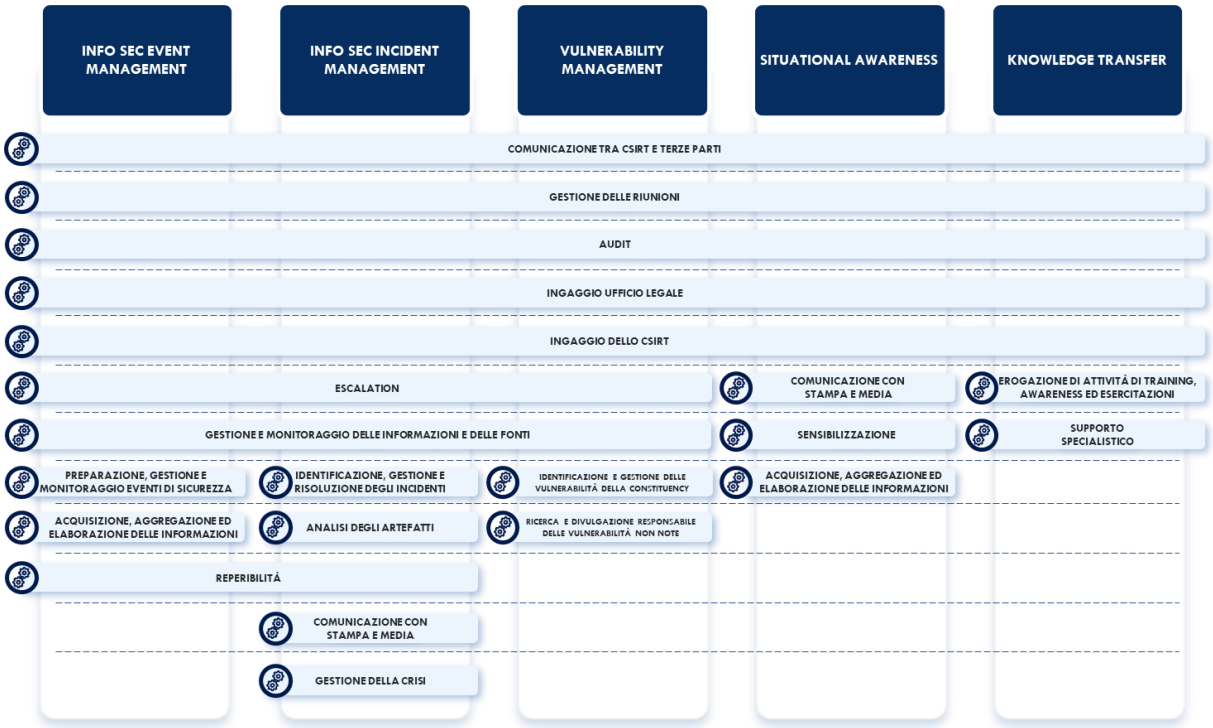

Figura 4 - Processi di un CSIRT mappati su Service Area

In continuità con il modello di servizio, si riporta di seguito una descrizione dei principali processi, ad alto livello, a supporto dell'operatività del CSIRT:

- **Comunicazione tra CSIRT e terze parti**: gestione della comunicazione con altri CSIRT e/o eventuali terze parti, circa tematiche cyber, tematiche operative (esempio, collaborazione per la risoluzione di un incidente di sicurezza) nel rispetto degli accordi tra essi stipulati.
- **Preparazione, gestione e monitoraggio degli eventi di sicurezza:** esecuzione delle attività di preparazione di quanto necessario alla ricezione ed analisi degli eventi (esempio, identificazione delle sorgenti di informazioni, gestione degli use case e raccolta delle informazioni contestuali dell'organizzazione). A valle delle attività preparatorie, nel contesto di tale processo, saranno altresì da formalizzarsi le attività a supporto del monitoraggio, dell'analisi, della correlazione e della qualifica degli eventi di sicurezza.
- **Identificazione, gestione e risoluzione degli incidenti:** esecuzione di quanto necessario alla identificazione, nonché ricezione delle segnalazioni, di incidenti di sicurezza qualificati. A valle dell'identificazione dell'incidente, il CSIRT avvierà quanto necessario ad eseguire un'appropriata gestione dello stesso, erogando attività di triage, analisi e

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

supporto nella definizione e nell'attuazione dei piani di rimedio o mitigazione. Qualora necessario, questo processo potrà essere ulteriormente declinato in procedure operative specifiche per supportare la risoluzione di incidenti specifici (esempio, gestione attacchi ransomware).

- **Analisi degli artefatti:** formalizzazione delle attività volte all'esecuzione delle analisi degli artefatti collezionati nel contesto delle varie attività operative erogate dal CSIRT. Tale processo dovrà inoltre prevedere un'adeguata comunicazione delle risultanze delle attività con i soggetti interessati.
- **Ricerca e divulgazione responsabile delle vulnerabilità non note:** identificazione, studio e analisi delle modalità di rimedio/mitigazione e divulgazione responsabile delle informazioni relative alle vulnerabilità non note. Nell'ambito di tale processo dovranno essere previste tutte le possibili modalità di identificazione delle vulnerabilità (esempio, attività di ricerca eseguite dal CSIRT, vulnerabilità segnalate dalla Constituency), nonché i ruoli, le responsabilità e le modalità relative alle attività di divulgazione.
- **Identificazione e gestione delle vulnerabilità della Constituency**: formalizzazione delle attività volte all'identificazione delle vulnerabilità presenti all'interno dell'infrastruttura della Constituency. Una volta identificate, il CSIRT dovrà eseguire attività volte a supportare la Constituency nell'identificazione e nell'esecuzione dei piani di rientro/mitigazione.
- **Acquisizione, aggregazione ed elaborazione delle informazioni:** collazionamento, aggregazione ed elaborazione delle informazioni necessarie ad un'appurata valutazione del contesto situazionale, nonché di previsione di ogni sua eventuale variazione. I risultati di tali attività dovranno essere condivisi con i soggetti interessati al fine di accrescere la loro consapevolezza relativa al contesto cibernetico circostante.
- **Supporto specialistico:** definizione delle modalità di erogazione delle attività di supporto specialistico al fine di eseguire attente valutazioni del rischio con l'obiettivo primario di supportare la Constituency nelle modalità di gestione/mitigazione del rischio. Le attività gestite nel contesto specifico di processo potranno prevedere l'erogazione di supporto nella definizione di policy e procedure ed esecuzione di consulenza tecnica per l'evoluzione del contesto tecnologico della Constituency.
- **Gestione delle riunioni**: esecuzione di una adeguata gestione delle modalità di pianificazione e di partecipazione agli incontri inerenti alle attività del CSIRT. Tali incontri potranno avere un'audience differente in relazione allo specifico argomento.
- **Audit**: esecuzione periodica di attività di audit, sia interne che esterne, volte alla valutazione di processi, politiche, procedure e prassi a supporto dell'erogazione dei servizi resi disponibili dal CSIRT.
- **Gestione e monitoraggio delle informazioni e delle fonti**: gestione del ciclo di vita delle fonti, interne ed esterne, nonché delle informazioni tramite esse recepite impiegate dal CSIRT per l'identificazione reattiva/proattiva di potenziali minacce di interesse per la Constituency.

- **Ingaggio ufficio legale**: ingaggio formale del team legale per la gestione di eventuali richieste formali pervenute nei confronti dell'organizzazione.
- **Escalation:** formalizzazione delle modalità, dei ruoli e delle responsabilità per l'esecuzione di attività di escalation al fine di eseguire in modo efficace le attività di gestione di un incidente di sicurezza.
- **Reperibilità**: gestione delle modalità di comunicazione, da e verso il CSIRT, durante le attività eseguite fuori orario base. Nel contesto di tale processo dovranno essere previste le attività relative alla gestione della turnazione, al fine di garantire una continua reperibilità (24/7) in caso di necessità, nonché le modalità di presa in carico delle segnalazioni pervenute.
- **Comunicazione con stampa e media**: gestione delle modalità e delle responsabilità relativa alle attività di comunicazione verso i media e la stampa. Tale processo dovrà essere supportato da una strategia ben definita nonché formale di comunicazione.
- **Gestione della crisi:** processo che permette al CSIRT di definire le procedure da avviare nel caso in cui sia necessario istituire un tavolo di crisi a seguito di un incidente di sicurezza, e di ingaggiare l'unità predisposta alla gestione delle crisi stessa.
- **Ingaggio del CSIRT**: processo che permette al CSIRT di essere ingaggiato da parte della Constituency attraverso canali sia interni che esterni all'organizzazione. Tale processo è di supporto a tutte le attività erogate dal CSIRT con interfaccia verso l'esterno.
- **Sensibilizzazione**: formalizzazione delle modalità di interazione tra il CSIRT e potenziali soggetti esterni allo stesso (esempio, Constituency, terze parti, partner) aventi l'obiettivo di promuovere i servizi erogati dal CSIRT, nonché ricevere riscontri relativi alla modalità di erogazione degli stessi.
- **Erogazione di attività di training, awareness ed esercitazioni:** definizione delle modalità di erogazione delle attività di training, awareness e/o di esercitazioni offerte verso la Constituency ed inclusive dei ruoli e delle responsabilità in tal senso.

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

3.3 Modello organizzativo e figure professionali

Un CSIRT, al fine di adempiere in modo opportuno al proprio mandato, dovrebbe essere composto da personale altamente qualificato le cui competenze permettano l'erogazione dei servizi previsti. In particolare, il modello organizzativo proposto per un CSIRT con il dettaglio delle figure professionali è illustrato nell'immagine seguente:

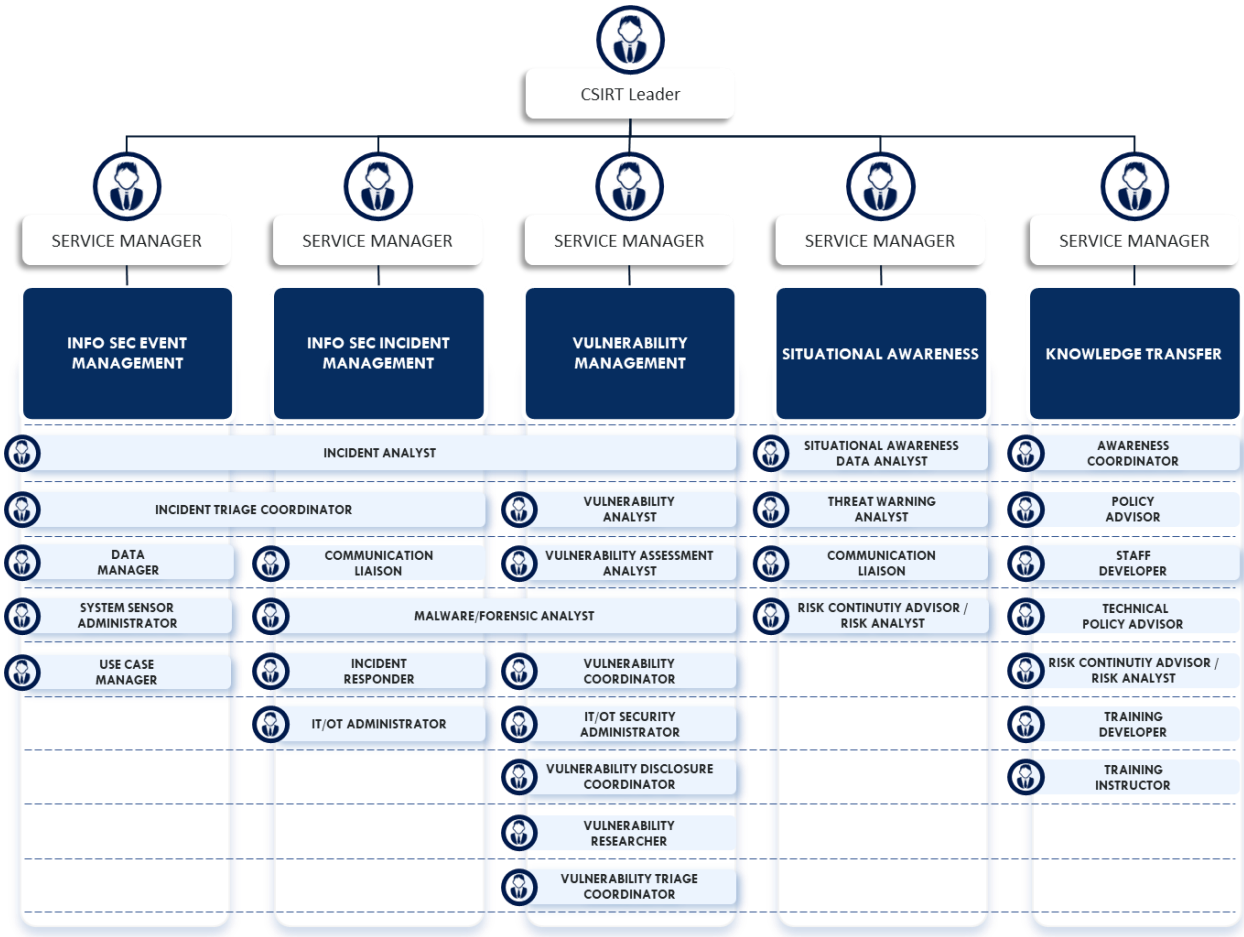

Figura 5 - Descrizione di alto livello del modello organizzativo di un CSIRT

Le figure professionali a composizione di tale modello, possono essere impiegate all'interno di più aree funzionali, e sono descritte di seguito:

- **Leader**: supervisiona i servizi erogati dal CSIRT, interagendo con gli opportuni Service Manager e relazionandosi sia con gli attori interessati sia con la Constituency.
- **Service Area Manager**: coordina l'organizzazione e l'erogazione dei servizi forniti dal CSIRT, assumendo il nome del rispettivo dominio di servizio come, per esempio, Responsabile del servizio Incident Management – Responsabile del servizio Event Management – Responsabile del servizio di Vulnerability Management – Responsabile del servizio Situational Awareness – Responsabile del servizio Knowledge Transfer.
- **Incident Analyst**: si occupa di monitorare e identificare / confermare gli incidenti di sicurezza identificati dalla piattaforma di monitoraggio e/o segnalati al CSIRT. Inoltre, ha l'obiettivo di stabilire le relazioni e dipendenze tra tutti gli eventi/incidenti di sicurezza.

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

- **Incident Triage Coordinator**: analizza e prioritizza, sulla base di criteri formalizzati e condivisi, gli eventi/incidenti di sicurezza per poi inoltrarli al processo di gestione incidenti.
- **Data Manager**: è responsabile della gestione dei dati contestuali durante il loro ciclo di vita, derivati da API, Configuration Management Database, gestione dell'identità e degli accessi o sistemi di intelligence delle minacce.
- **System and Sensor Administrator**: è responsabile della configurazione e gestione di tutte le componenti essenziali (esempio server/client, router e switch, dispositivi ICS/IoT, sensori in ambienti OT, ecc.) che forniscono log per l'identificazione di attività sospette. In alcune circostanze, tale figura può anche far parte di un'altra unità dell'organizzazione.
- **Use Case Manager**: è responsabile della gestione dell'intero ciclo di vita dei casi d'uso di rilevamento vitali per l'identificazione di potenziali incidenti di sicurezza.
- **Communication Liaison**: è responsabile della comunicazione con i media e con eventuali ulteriori attori interessati, verso i quali ha la responsabilità di comunicare dettagli, tecnici e no, che riguardano l'incidente di sicurezza in corso.
- **Malware/Forensic Analyst**: ha l'obiettivo di raccogliere, conservare, e analizzare dati ed evidenze digitali relative a incidenti di sicurezza (log di rete e di sistema, e-mail, dispositivi di archiviazione esterni), al fine di identificare eventuali dati cancellati o compromessi. Inoltre, attraverso analisi statiche e dinamiche, esegue attività di analisi dei malware identificati, al fine di analizzarne il comportamento e individuare i punti di forza e di debolezza del sistema informatico colpito.
- **Incident Responder**: si occupa end-to-end delle attività di risposta all'incidente in corso, ivi incluse le attività di acquisizione/analisi delle evidenze.
- **IT/OT Administrator**: ha l'obiettivo di ripristinare le funzionalità degli asset (esempio, sistemi, reti, ecc.) coinvolti durante l'incidente di sicurezza.
- **Vulnerability Analyst**: ha l'obiettivo di analizzare, comprendere e valutare tutti i dettagli (esempio, potenziali impatti, remediation) legati alle vulnerabilità di cui il CSIRT viene a conoscenza.
- **Vulnerability Assessment Analyst**: ha l'obiettivo di rilevare e di identificare attivamente le potenziali vulnerabilità note, presenti nei sistemi/applicazioni appartenenti alla Constituency.
- **Vulnerability Coordinator**: ha l'obiettivo di coordinare lo scambio di informazioni rilevanti con più parti (esempio, ricercatori, fornitori, sviluppatori, ecc.) coinvolte nel processo di divulgazione responsabile e coordinata delle vulnerabilità.
- **IT/OT Security Administrator**: esegue attività di mitigazione / risoluzione delle vulnerabilità attraverso l'applicazione di aggiornamenti hardware / software o di configurazioni.
- **Vulnerability Disclosure Coordinator**: ha l'obiettivo di aiutare l'organizzazione a definire la propria politica di divulgazione responsabile delle vulnerabilità e di renderla disponibile attraverso gli opportuni canali di comunicazione (esempio, web, sms, e-mail) alle parti interessate. Inoltre, aiuta l'organizzazione a definire, manutenere e aggiornare i processi e le procedure a supporto della gestione delle vulnerabilità divulgate.

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

- **Vulnerability Researcher**: ha l'obiettivo di identificare e analizzare le vulnerabilità non note attraverso attività di analisi dei sistemi/software oppure attraverso attività di reverse engineering del malware.
- **Vulnerability Triage Coordinator**: ha l'obiettivo di prendere in carico le attività di analisi delle vulnerabilità segnalate al CSIRT e di elaborarle in modo appropriato, identificandone categoria e priorità.
- **Situational Awareness Data Analyst**: si occupa di raccogliere, aggregare ed analizzare le informazioni operative e di contesto provenienti da più fonti interne dell'organizzazione al fine di determinare il contesto situazionale.
- **Threat Warning Analyst**: ha l'obiettivo di fornire alla propria organizzazione informazioni circa le minacce attuali (esempio, eventuali campagne in corso, impatti).
- **Risk & Continuity Advisor / Risk Analyst**: ha l'obiettivo di raccogliere ed elaborare le informazioni relative agli asset ed al contesto della Constituency (esempio, servizi, utenti, processi), mediante le quali predispone una mappa o un inventario degli asset, evidenziando le funzioni, i ruoli, le azioni consentite e i rischi principali legati agli asset critici.
- **Awareness coordinator**: collabora sia con la comunità che con i partner di fiducia, al fine di comprendere al meglio le minacce in corso e le azioni da intraprendere per prevenire o mitigare i rischi.
- **Policy Advisor**: collabora con la Constituency e con i principali attori interessati per contribuire alla creazione e all'attuazione delle politiche della stessa.
- **Staff Developer**: collabora con il personale esperto, al fine di identificare le lacune di conoscenza e le esigenze di formazione. Inoltre, mette in atto un programma che permette a specifiche figure (esempio, personale della Constituency, collaboratori, terze parti) di sviluppare le proprie competenze sulla sicurezza cibernetica.
- **Technical Policy Advisor**: ha il compito di verificare che le policy definite dalla Constituency includano la gestione degli incidenti, dei rischi e delle minacce. Si occupa, inoltre, di verificare che la Constituency attui in modo opportuno le best practice operative e di sicurezza suggerite.
- **Training Developer**: ha il compito di sviluppare i contenuti per le attività di formazione ed esercitazione che dovranno poi essere impiegati per l'erogazione delle attività formative all'interno e/o all'esterno del CSIRT.
- **Training Instructor**: ha il compito di fornire ai membri del CSIRT una formazione esaustiva sia tecnica, ad esempio attraverso esercitazioni pratiche, sia teorica, per esempio mediante training.

Il personale, predisposto allo svolgimento di tutte le mansioni previste dal CSIRT, richiede una formazione tecnica con una notevole formazione sul lavoro, oltre che una preparazione aggiuntiva per acquisire competenze più specifiche e di dettaglio. Vengono riportate per ogni figura professionale, all'interno dell'Allegato A, le principali competenze che dovrebbero essere possedute. Tali competenze, rappresentano soltanto un estratto della totalità delle competenze che devono essere soddisfatte dal ruolo in esame.

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

3.4 Strumenti

Un CSIRT deve disporre di una serie di strumenti che saranno di supporto al personale ed hanno l'obiettivo di permettere il corretto svolgimento delle attività preposte dal mandato del CSIRT stesso. L'insieme di tali strumenti sono, quindi, necessari per la corretta gestione operativa di un CSIRT e possono essere ad esempio la linea telefonica, la connessione internet e gli strumenti adibiti per le analisi inerenti alla gestione sia degli incidenti che vulnerabilità. Di seguito, viene riportata la figura che illustra l'insieme degli strumenti che sono previsti per un CSIRT:

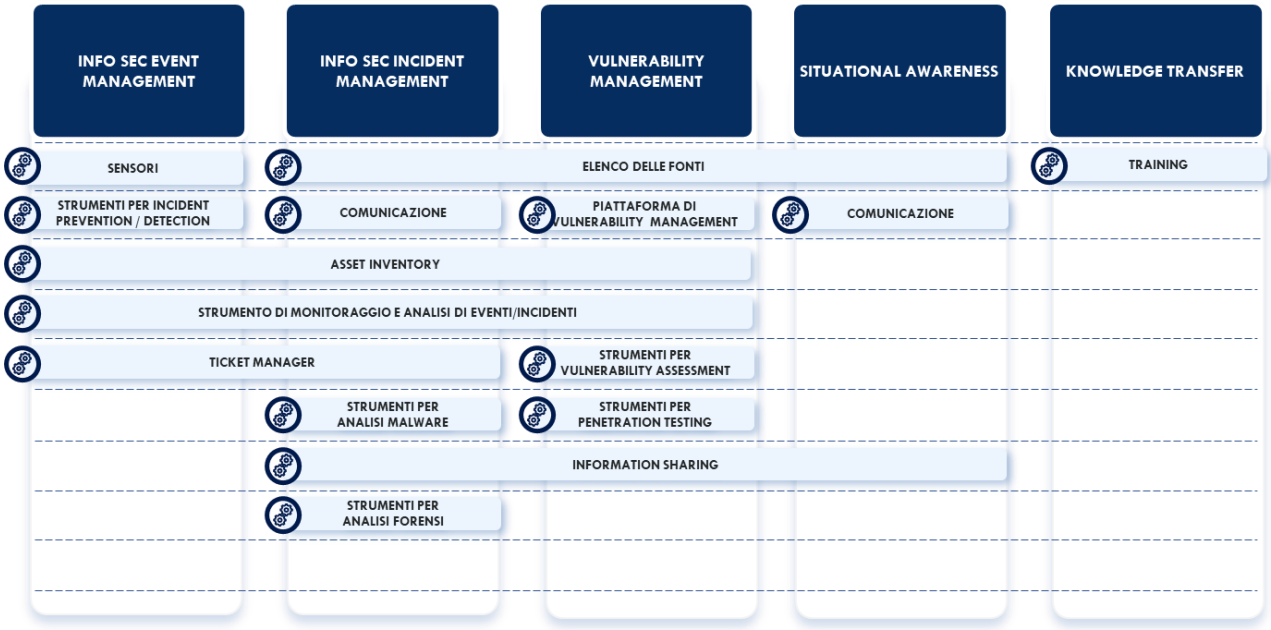

Figura 6 - Elenco degli strumenti di un CSIRT mappati per Service Area

In continuità con il modello di servizio, si riporta di seguito una descrizione dei principali strumenti a supporto delle attività:

- **Elenco delle fonti**: le fonti per un CSIRT rappresentano un insieme di informazioni utilizzabili per identificare potenziali minacce o per analizzare eventi di interesse, con lo scopo di prevenire e mitigare le minacce che potrebbero essere dannose per la propria Constituency (esempio, identificazione di account compromessi, data leak, danni reputazionali, compromissione infrastruttura IT/OT, ecc.). Tali fonti possono essere sia interne (per esempio informazioni provenienti da sensori presenti all'interno del perimetro dell'organizzazione) che esterne (esempio, servizi terze parti, canali social, web)
- **Sensori**: rappresentano degli strumenti che possono essere installati su endpoint, dispositivi mobili, rete o server. Attraverso l'uso di protocolli sicuri, hanno l'obiettivo di estrarre la telemetria e di inviarla al SIEM in modo che l'analista possa monitorare gli eventi di sicurezza;
- **Strumenti per Incident Prevention/Detection**: rappresentano parte dell'infrastruttura di monitoraggio e prevenzione a supporto della resilienza dell'organizzazione, ad esempio, Intrusion Prevention System (IPS) e Intrusion Detection System (IDS).

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

- **Asset Inventory**: rappresenta uno strumento che permette al CSIRT di predisporre di un elenco dettagliato delle risorse IT e / o OT, che fanno parte del perimetro di sua competenza. Tale elenco dovrebbe contenere informazioni sia hardware che software ben dettagliate, con lo scopo di aiutare l'analista ad indentificare/analizzare prontamente tutte quelle risorse potenzialmente coinvolte durante un incidente.
- **Strumento di Monitoraggio e Analisi di Eventi/Incidenti:** rappresentano un insieme di strumenti preposti al collazionamento, all'aggregazione, alla gestione ed alla correlazione degli eventi provenienti da differenti fonti. Tipicamente, tale ruolo è ricoperto da una soluzione di Security Information Event Management (SIEM), che permette agli analisti di individuare tempestivamente potenziali incidenti di sicurezza.
- **Ticket Manager**: rappresenta lo strumento a supporto del tracciamento delle attività realizzate per la gestione di eventi e/o incidenti identificati, supportando inoltre, quando necessario, le attività di escalation verso le strutture preposte. Le informazioni contenute nel complesso all'interno di tale strumento costituiscono parte della Knowledge base (KB).
- **Strumenti di comunicazione**: rappresentano gli strumenti di comunicazione adottati dal CSIRT durante la normale operatività e durante la gestione di eventuali eventi / incidenti. Questi ultimi, affinché il CSIRT possa assolvere alle proprie responsabilità devono essere implementate con un elevato grado di resilienza, in quanto di vitale importanza durante la gestione di un evento. Tipicamente tali strumenti sono rappresentati da telefono, e-mail, sito web e connettività Internet.
- **Piattaforma di Information sharing**: piattaforma messa a disposizione da un CSIRT con l'obiettivo di condividere le informazioni inerenti alle minacce che potrebbero impattare la Constituency. Tali piattaforme devono fornire supporto per l'aggregazione, normalizzazione ed arricchimento delle informazioni utili alla prevenzione e mitigazione delle minacce, potenzialmente dannose per l'organizzazione.
- **Strumenti per analisi forensi:** strumenti atti all'esecuzione di attività di analisi specialistica sui sistemi impattati da un incidente di sicurezza, al fine di comprendere l'origine di una compromissione ed analizzarne tutti gli aspetti. Tali strumenti devono supportare gli operatori durante, ad esempio:
    - l'acquisizione di immagini forensi (esempio, HDD, SSD, RAM, ecc.);
    - l'archiviazione sicura di immagini forensi ottenute durante le attività di acquisizione;
    - l'estrazione di artefatti dai sistemi operativi impattati.
- **Strumenti per analisi dei malware:** strumenti atti all'esecuzione di attività di analisi specialistica dei malware, con l'obiettivo di comprendere il comportamento dei malware oltre che la loro origine, attraverso attività come, ad esempio, il reverse engineering e l'estrazione degli indicatori di compromissione (IoC).
- **Piattaforma di Vulnerability Management**: piattaforma a supporto dell'identificazione, della classificazione, della prioritizzazione e del tracciamento delle vulnerabilità rilevate sui sistemi della Constituency.
- **Strumenti per Vulnerability Assessment**: insieme di strumenti atti a supportare l'identificazione delle vulnerabilità sugli asset dell'organizzazione, definire le relative priorità di rientro e di suggerire le mitigazioni appropriate al fine di ridurre o eliminare i

potenziali rischi legati alla vulnerabilità stessa. Tali strumenti possono sia integrarsi con ulteriori strumenti di Vulnerability Management oppure possono lavorare indipendentemente.

- **Strumenti per Penetration Testing**: insieme di strumenti atti a supportare l'esecuzione delle attività di Penetration Testing, in ogni sua fase (esempio, ricognizione, scansione, sfruttamento).
- **Piattaforma di Training**: piattaforma a supporto dell'erogazione di attività di formazione, tecnico e no, al personale interno al CSIRT e appartenete alla Constituency. Tali strumenti tipicamente consentono la strutturazione di corsi di formazioni con molteplici livelli di complessità, al fine di rispettare le esigenze formative della totalità del personale dell'organizzazione.

4 Approccio per l'implementazione di un CSIRT

Come descritto all'interno del paragrafo "*1.1 Scopo del documento*" un CSIRT è una struttura di governo e operativa all'interno di un'organizzazione che si prefigge, come principale obiettivo, l'innalzamento del livello di cyber resilienza di un'organizzazione. Come tale esso necessita di un adeguato ciclo di vita, che ne consenta un'adeguata implementazione e miglioramento continuo. Tale ciclo di vita – rappresentativo principalmente delle fasi di implementazione e miglioramento – può essere così definito:

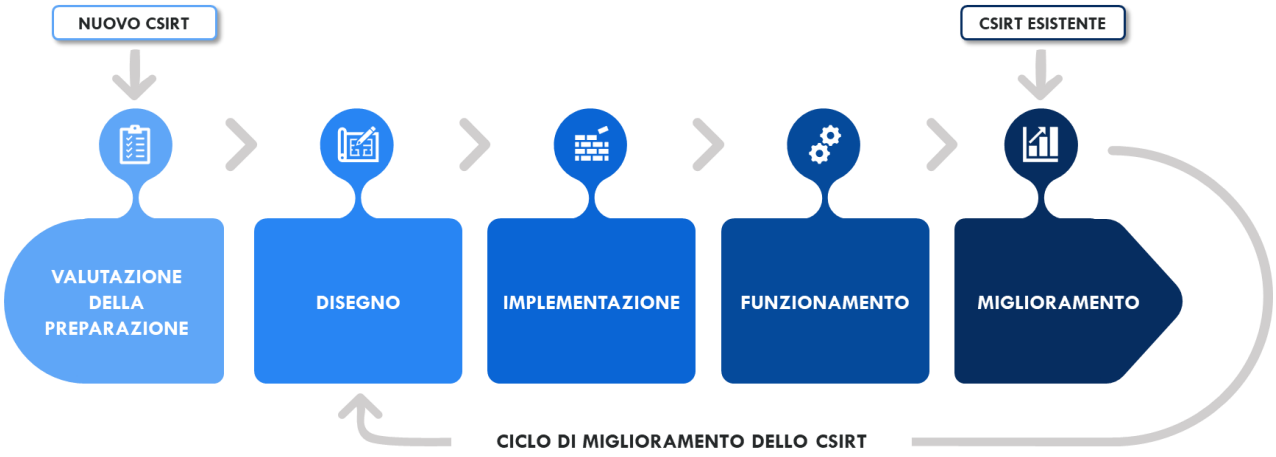

Figura 7 - Ciclo di vita di un CSIRT

Di seguito viene riportato il dettaglio per ciascuna fase riportata all'interno dell'immagine:

- **VALUTAZIONE DELLA PREPARAZIONE**: durante questa fase sono valutate le necessità e le ragioni relative all'implementazione di un CSIRT. Si dovrà procedere, ad esempio, con la definizione di un mandato preliminare, una struttura di governance, la scelta degli stakeholder con cui doversi interfacciare oltre alla Constituency e l'identificazione del budget necessario alla sua implementazione e mantenimento;
- **DISEGNO**: in questa fase si definiscono tutti gli aspetti che dovranno poi essere implementati al fine di espletare il mandato definito per il CSIRT, in termini di servizi, personale, processi e tecnologie. Quanto definito in questa specifica fase, dovrà poi essere innestato all'interno di un documento che dovrà rispettare il formato de facto riconosciuto ed utilizzato da tutti i CSIRT, cioè il RFC 2350 [6];
- **IMPLEMENTAZIONE:** in questa fase viene sviluppato e implementato tutto ciò che è stato identificato all'interno della fase di disegno, comprensivo di tutti gli aspetti organizzativi nonché servizi e tecnologie. Una volta terminata tale fase implementativa, i CSIRT sono abilitati a fornire servizi verso la propria Constituency ed avviare la fase operativa, in linea con il mandato definito nelle fasi precedenti;
- **FUNZIONAMENTO:** in questa fase il CSIRT è operativo a valle dell'implementazione di tutti gli aspetti individuati nella fase di Disegno e poi implementati nella fase di Implementazione. Questo permette al CSIRT di erogare tutti i suoi servizi, con il supporto dei processi, strumenti, persone e tecnologie predisposti nelle fasi precedenti;

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

- **MIGLIORAMENTO**: durante questa fase, un CSIRT valuta le proprie tecnologie, servizi e processi al fine di identificare i punti di debolezza e di miglioramento che il CSIRT deve prendere in considerazione affinché possano essere implementati e/o migliorati attraverso attività continua di miglioramento continuo.

Queste attività implementative e di miglioramento, in linea con il modello di riferimento presentato (*Modello di servizio*, *Processi*, *Modello organizzativo e figure professionali* e *Strumenti)* necessitano di un *profili di maturità* da traguardare al fine di pianificare opportunamente gli investimenti e le attività progettuali. A tal fine, ENISA [7] definisce i seguenti profili di maturità per un CSIRT:

- ***Base***: rappresenta il punto di partenza per un CSIRT affinché possa essere eseguita un'efficace gestione degli incidenti e collaborare in modo opportuno non solo all'interno del Paese di riferimento ma anche verso l'esterno con altri CSIRT e terze parti;
- ***Intermedio***: rappresenta un livello di maturità più elevato rispetto al livello base in termini di processi, personale e strumenti;
- ***Avanzato***: rappresenta il livello di maturità superiore rispetto ai precedenti livelli, dove il CSIRT è in grado non solo di collaborare con entità terze ma anche di gestire gli incidenti di sicurezza, compresa la condivisione delle minacce, delle vulnerabilità e dei dati di allerta preventiva.

Tali profili sono definiti sulla base del modello di riferimento del SIM3 [5], ampiamente diffuso e adottato a livello internazionale. Ogni organizzazione, in relazione alla propria complessità, deve utilizzare i livello di maturità per monitorare e permettere un miglioramento continuo delle capacità del proprio CSIRT.

In linea con il quadro regolatorio europeo e i compiti attribuiti all'ACN per la promozione di buone pratiche per la gestione degli incidenti e la risposta e il ripristino dei sistemi informativi a seguito di crisi di natura cibernetica, un CSIRT conforme con il modello di riferimento presentato nelle presenti Linee Guida, potrà auto dichiararsi come CSIRT mediante la trasmissione a CSIRT Italia del template di cui all'Allegato B.

Suddetta dichiarazione dovrà essere trasmessa tramite PEC all'indirizzo *acn@pec.acn.gov.it*, corredata da tutta la documentazione attestante il possesso dei requisiti individuati nelle presenti Linee Guide.

Attestata la conformità alle linee guida di un CSIRT, ciascuna organizzazione potrà essere chiamata a stipulare Accordi di Collaborazione con l'ACN ai fini della condivisione di informazioni, procedure e best practices con il CSIRT Italia nonché dell'accesso a servizi e strumenti offerti dall'ACN nell'ambito della prevenzione e risposta agli incidenti informatici.

Difatti, l'utilizzo di queste linee guida ha l'obiettivo di creare una rete capillare e ben strutturata tra il CSIRT Italia e i CSIRT delle principali organizzazioni nazionali, tale per cui sia facilitato lo scambio informativo, la creazione di rapporti di fiducia e il supporto, in linea con le diverse prerogative, nelle attività di gestione degli incidenti.

5 Glossario

Vengono descritti ed esplicitati gli acronimi presenti all'interno del documento.

Acronimi	Descrizione
ACN	Agenzia per la Cybersicurezza Nazionale
API	Application Programming Interface
CERT	Computer Emergency Response Teams
CERT-EU	Computer Emergency Response Team-European Union
CIRT	Computer Incident Response Teams
Constituency	Insieme di enti/divisioni che beneficiano dei servizi erogati da un CSIRT
CSIRT	Computer Security Incident Response Team
CVD	Coordinated Vulnerability Disclosure
DL	Decreto-legge
DPCM	Decreto del presidente del Consiglio dei ministri
EDR	Endpoint Detection and Response
ENISA	European Union Agency for Cybersecurity
FIRST	Forum of Incident Response and Security Teams
FW	Firewall
HDD	Hard Disk Drive
HW	Hardware
ICS	International Classification for Standards
IDS	Intrusion Detection System
IoC	Indicator of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
KB	Knowledge base
KSA	Knowledge, Skill and Ability
NCSC	National Cyber Security Center
NIS	Network and Information Security
OT	Operational Tehcnology
PGP/GPG	Pretty Good Privacy/Gnu Privacy Guard
PSIRT	Product Security Incident Response Team
RAM	Random Access Memory
RFC	Request for Comments
SDD	Solid State Drive
SIEM	Security Information and Event Management
SIM3	Security Incident Management Maturity Model
SIRT	Security Incident Response Teams
SOC	Security Operations Center
SW	Software

TLP	Trafic Light Protocol
TLS	Transport Layer Security
TTP	Tactics, Techniques and Procedures
VoIP	Voice Over Internet Protocol
WAF	Web Application Firewall

Tabella 1 - Glossario

6 Referenze

ID	Link
1	Guida alla configurazione di un CSIRT
2	How to set up CSIRT and SOC
3	FIRST CSIRT Services Framework
4	Ruoli e competenze suggerite per un CSIRT
5	Sim3 Model
6	RFC 2350
7	Livelli di maturità ENISA

Tabella 2 - Referenze

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

7 Allegati

ID Allegato	Nome	Descrizione allegato
A	Allegato A - Figure Professionali CSIRT	Descrizione delle figure professionali, e delle relative competenze, richieste per l'erogazione dei servizi da parte di un CSIRT.
B	Allegato B - Documentazione Realizzazione CSIRT	Documentazione dei documenti e allegati atti a descrivere la conformità con i requisiti della presente linea guida per la realizzazione di un CSIRT.

Tabella 3 - Allegati del documento di linee guida