ALLEGATO A

FIGURE PROFESSIONALI CSIRT

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

INDICE

Finanziato dall'Unione europea NextGenerationEU

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

1 Scopo del documento

Il presente documento si pone come Allegato al documento “Linee Guida per la Realizzazion di CSIRT”, al fine di fornire una panoramica sulle figure professionali, che compongono il modello organizzativo di un CSIRT, a supporto dell’erogazione dei servizi richiesti per il raggiungimento degli obiettivi prefissati all’interno del mandato del CSIRT stesso.

Per ogni figura professionale, che può essere impegnata in una singola *area di operatività* o trasversalmente su più *aree*, viene fornito un dettaglio aggiuntivo in merito alle competenze richieste. Le competenze illustrate, rappresentano soltanto un estratto della totalità delle competenze che devono essere soddisfatte dal ruolo in esame.

2 Figure professionali

Come definito all’interno del paragrafo “*3.3 Modello organizzativo e figure professionali*” del documento di Linee Guida, un CSIRT 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:

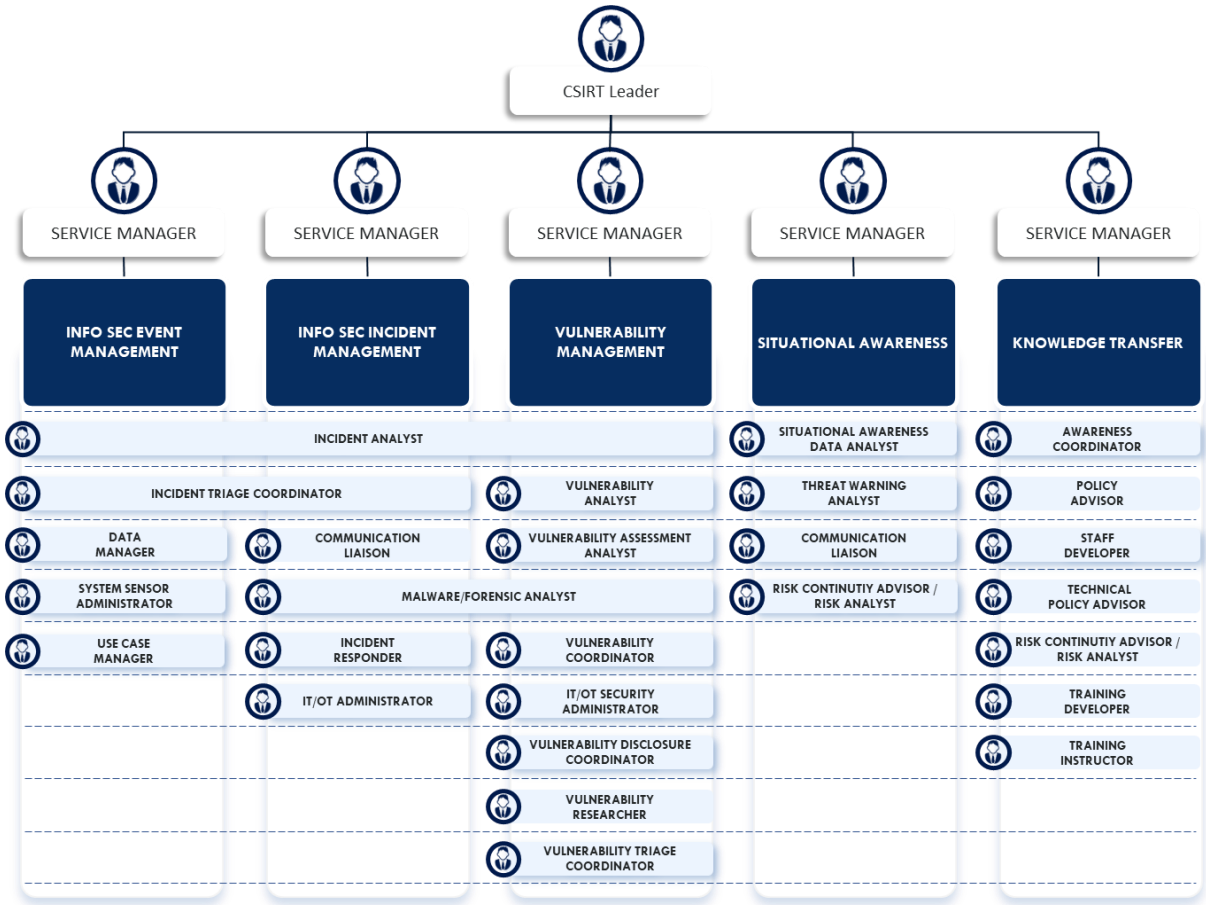

Figura 1 - Descrizione di alto livello del modello organizzativo di un CSIRT

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Il personale, preposto 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.

2.1 Incident Analyst

L'**Incident Analyst** è la figura professionale che si occupa di monitorare e accertare 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.

È una figura impiegata trasversalmente sulle *aree* Information Security Event Management, Information Security Incident Management e Vulnerability Management e le competenze richieste sono riassunte nell'immagine seguente:

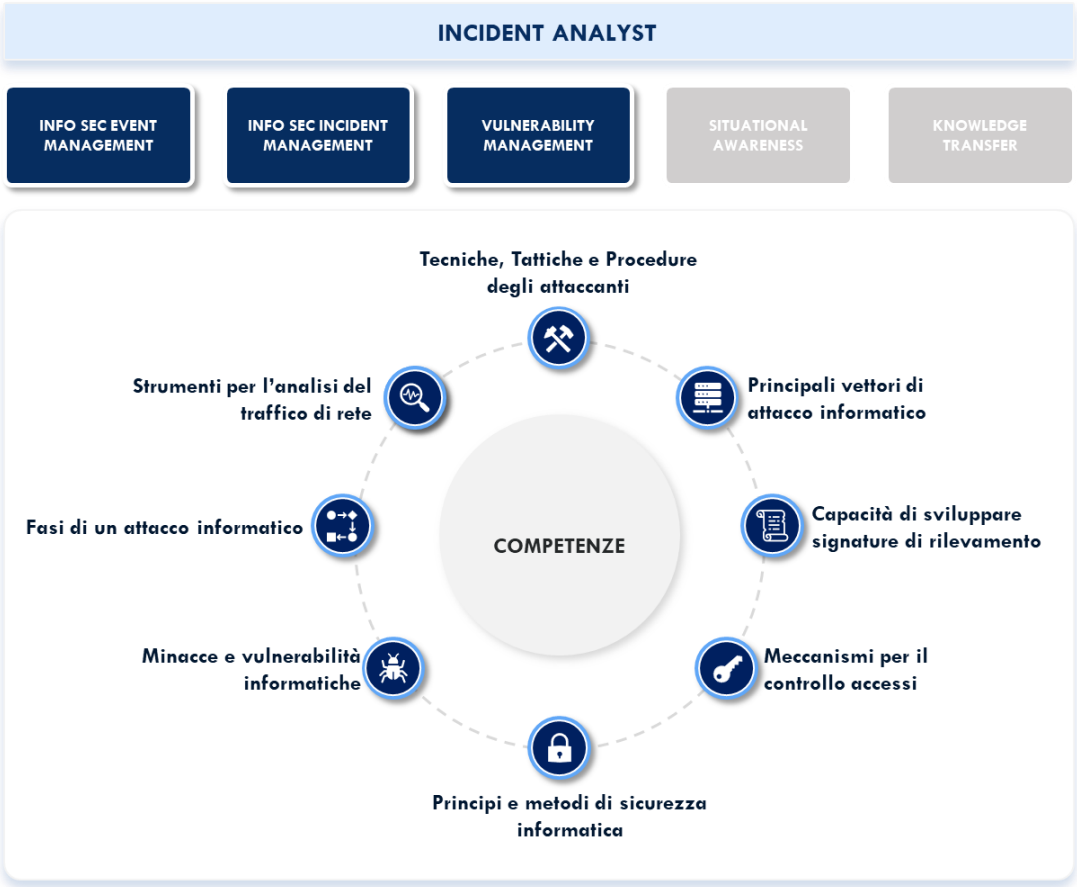

Figura 2: Principali competenze per la figura Incident Analyst

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.2 Incident Traige Coordinator

L'**Incident Triage Coordinator** è la figura professionale che analizza e prioritizza, sulla base di criteri formalizzati e condivisi, gli eventi/incidenti di sicurezza per poi inoltrarli al processo di gestione incidenti.

È una figura impiegata trasversalmente sulle *aree* Information Security Event Management e Information Security Incident Management e le competenze richieste sono riassunte nell'immagine seguente:

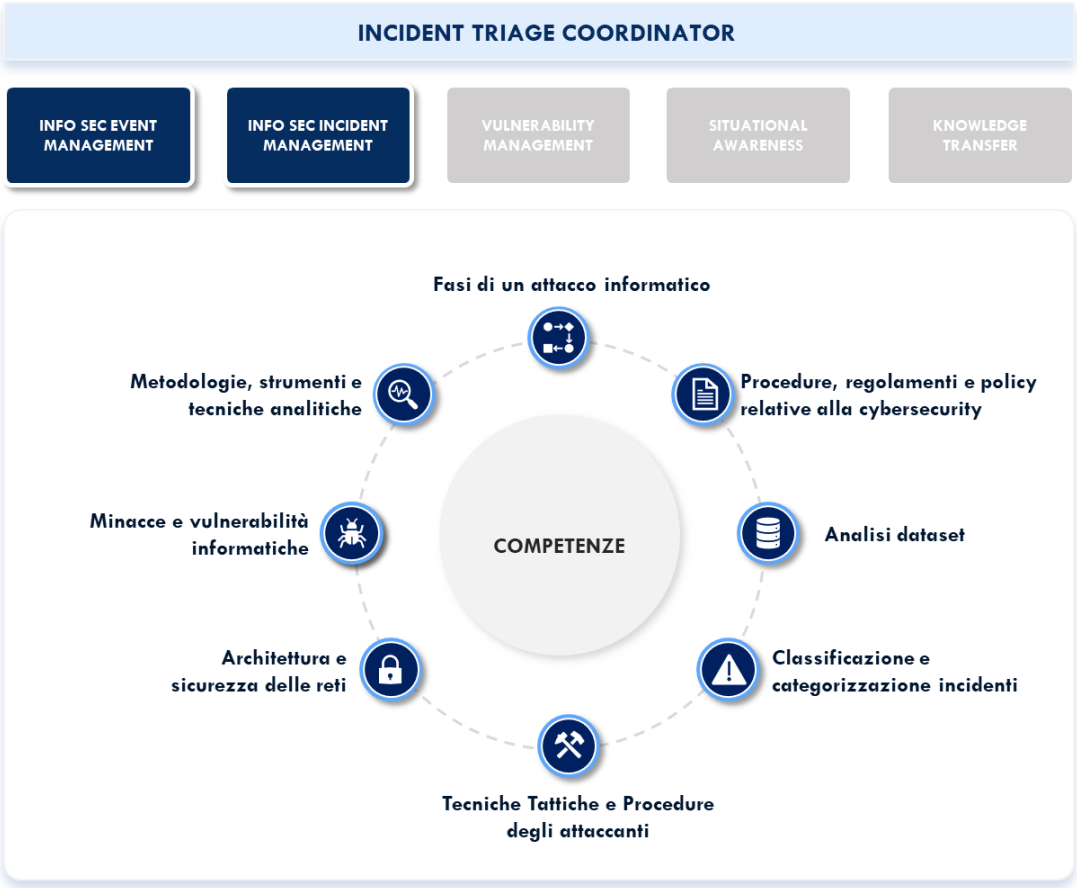

Figura 3: Principali competenze per la figura Incident Triage Coordinator

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.3 Data Manager

Il **Data Manager** è la figura professionale 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.

È una figura impiegata nell' *area* Information Security Event Management e le competenze richieste sono riassunte nell'immagine seguente:

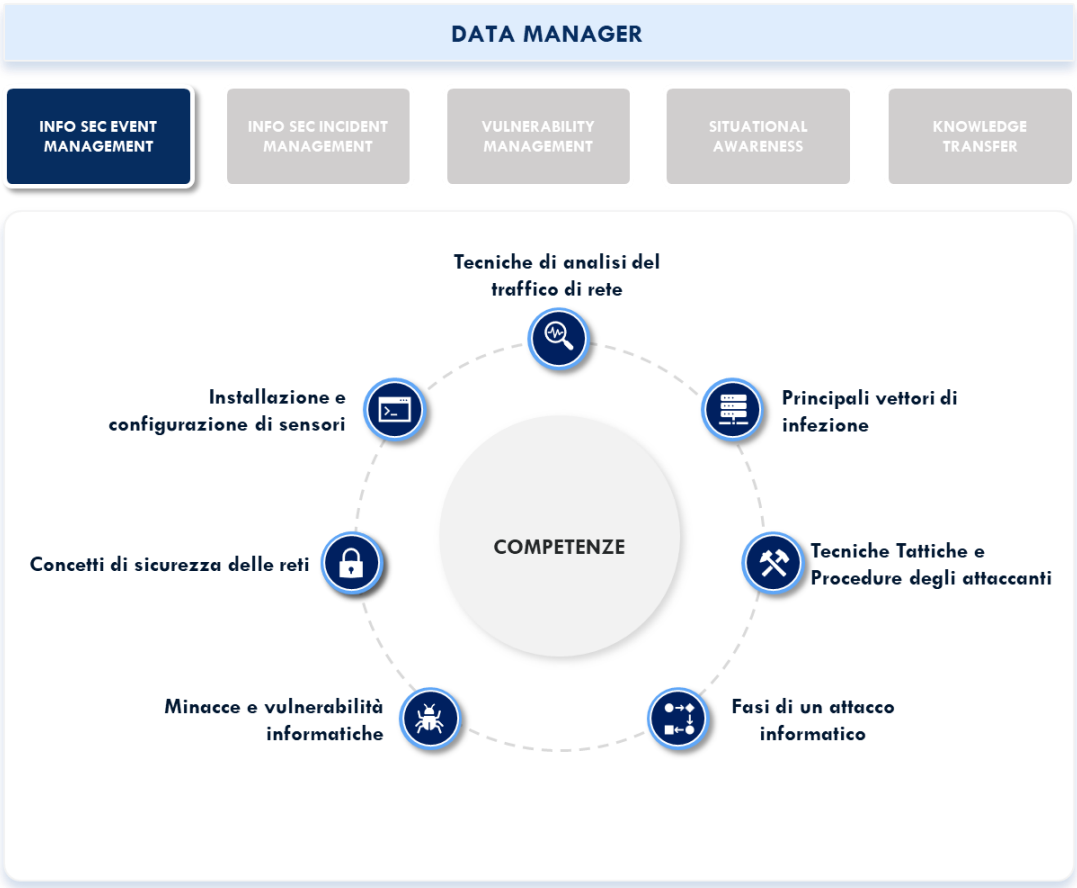

Figura 4: Principali competenze per la figura Data Magager

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.4 System and Sensor Administrator

Il **System and Sensor Administrator** è la figura professionale 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.

È una figura impiegata nell' *area* Information Security Event Management, ma in alcune circostanza può anche far parte di altre *aree*, e le competenze richieste sono riassunte nell'immagine seguente:

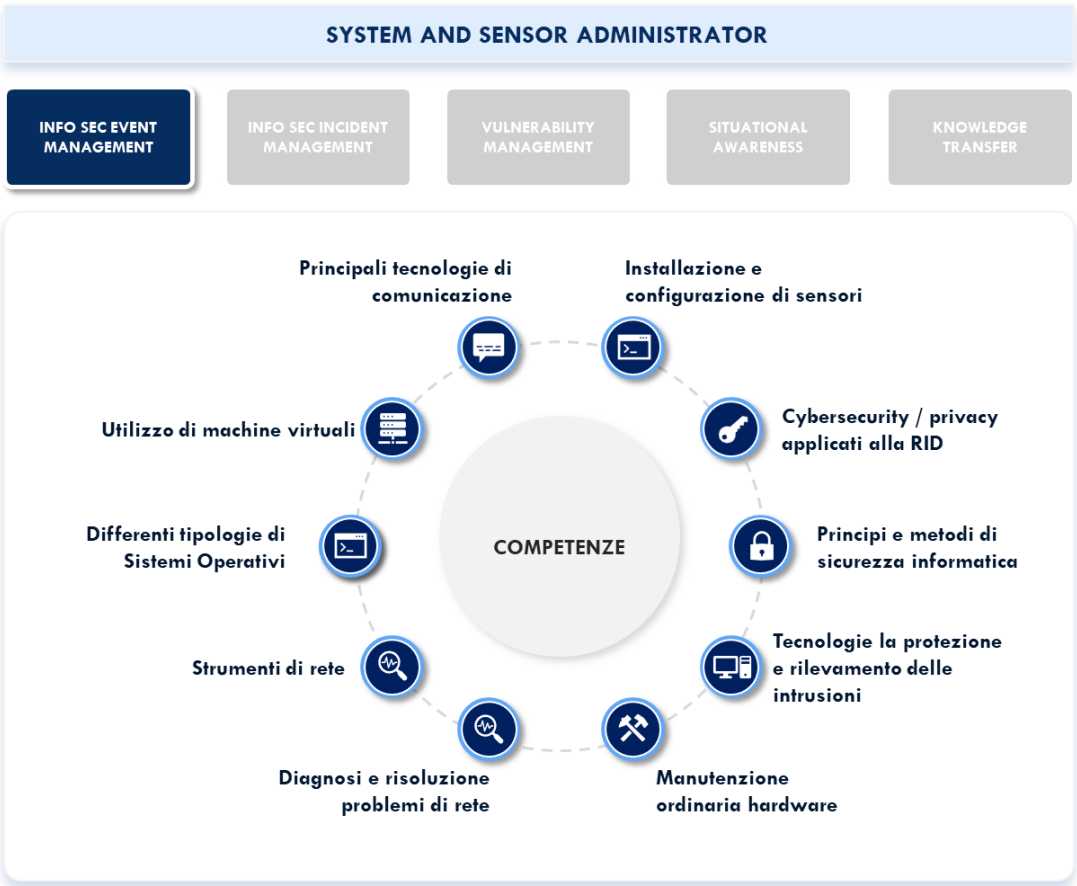

Figura 5: Principali competenze per la figura System and Sensor Administrator

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.5 Use Case Manager

Il **Use Case Manager** è la figura professionale responsabile della gestione dell'intero ciclo di vita dei casi d'uso di rilevamento vitali per l'identificazione di potenziali incidenti di sicurezza.

È una figura impiegata nell' *area* Information Security Event Management e le competenze richieste sono riassunte nell'immagine seguente:

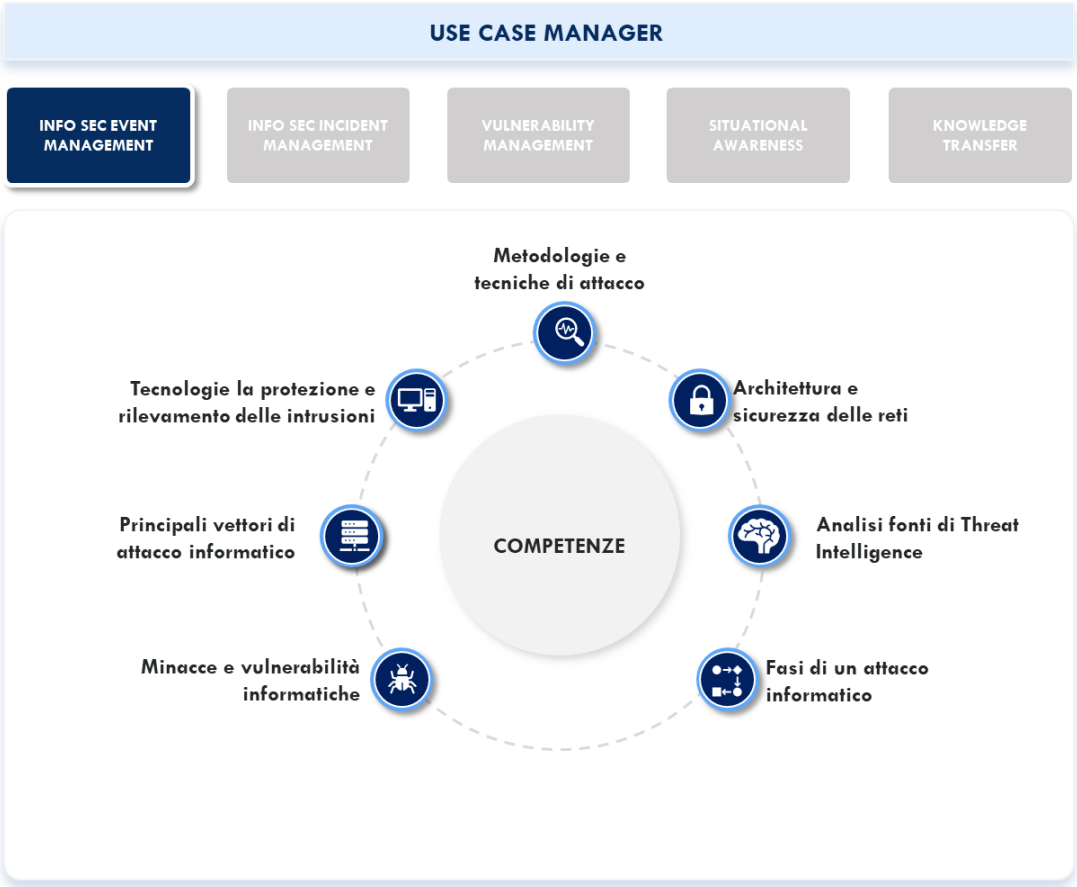

Figura 6: Principali competenze per la figura Use Case Magager

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.6 Communication Liaison

Il **Communication Liaison** è la figura professionale responsabile della comunicazione con i media e con eventuali ulteriori attori interessati, verso i quali ha la responsabilità di comunicare dettagli, tecnici e non, che riguardano l'incidente di sicurezza in corso.

È una figura impiegata trasversalmente sulle *aree* Information Security Incident Management e Situational Awareness e le competenze richieste sono riassunte nell'immagine seguente:

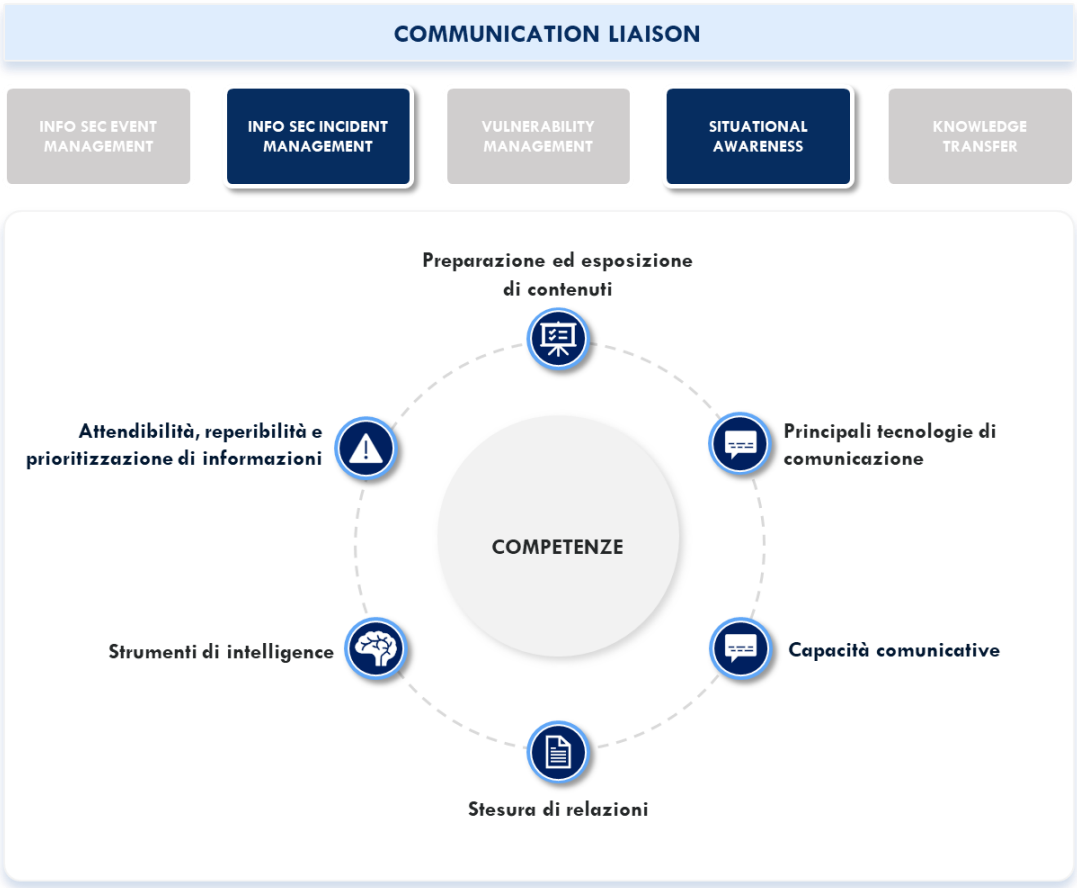

Figura 7: Principali competenze per la figura Communication Liaison

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.7 Malware/Forensic Analyst

Il **Malware/Forensic Analyst** è la figura professionale che 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.

È una figura impiegata trasversalmente sulle *aree* Information Security Incident Management e Vulnerability Management e le competenze richieste sono riassunte nell'immagine seguente:

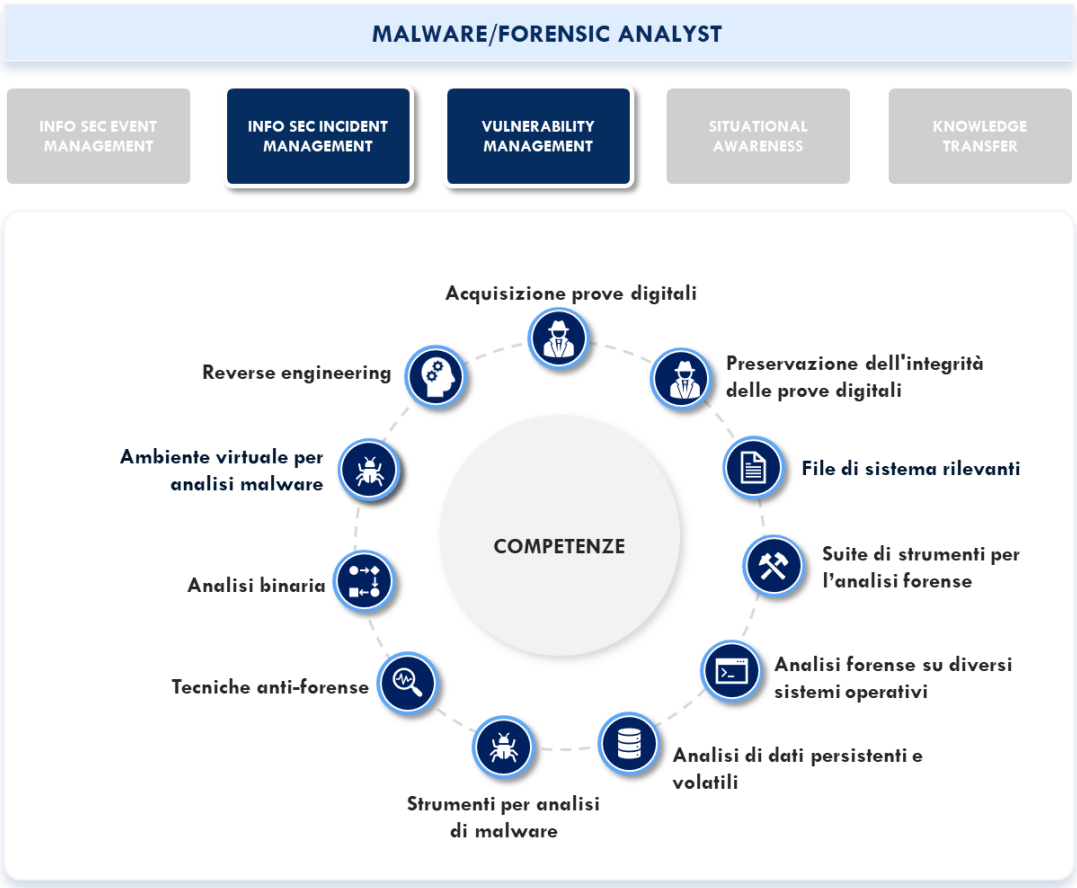

Figura 8: Principali competenze per la figura Malware/Forensic Analyst

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.8 Incident Responder

L'**Incident Responder** è la fisi occupa end-to-end delle attività di risposta all'incidente in corso, ivi incluse le attività di acquisizione/analisi delle evidenze.

È una figura impiegata nell' *area* Information Security Incident Management e le competenze richieste sono riassunte nell'immagine seguente:

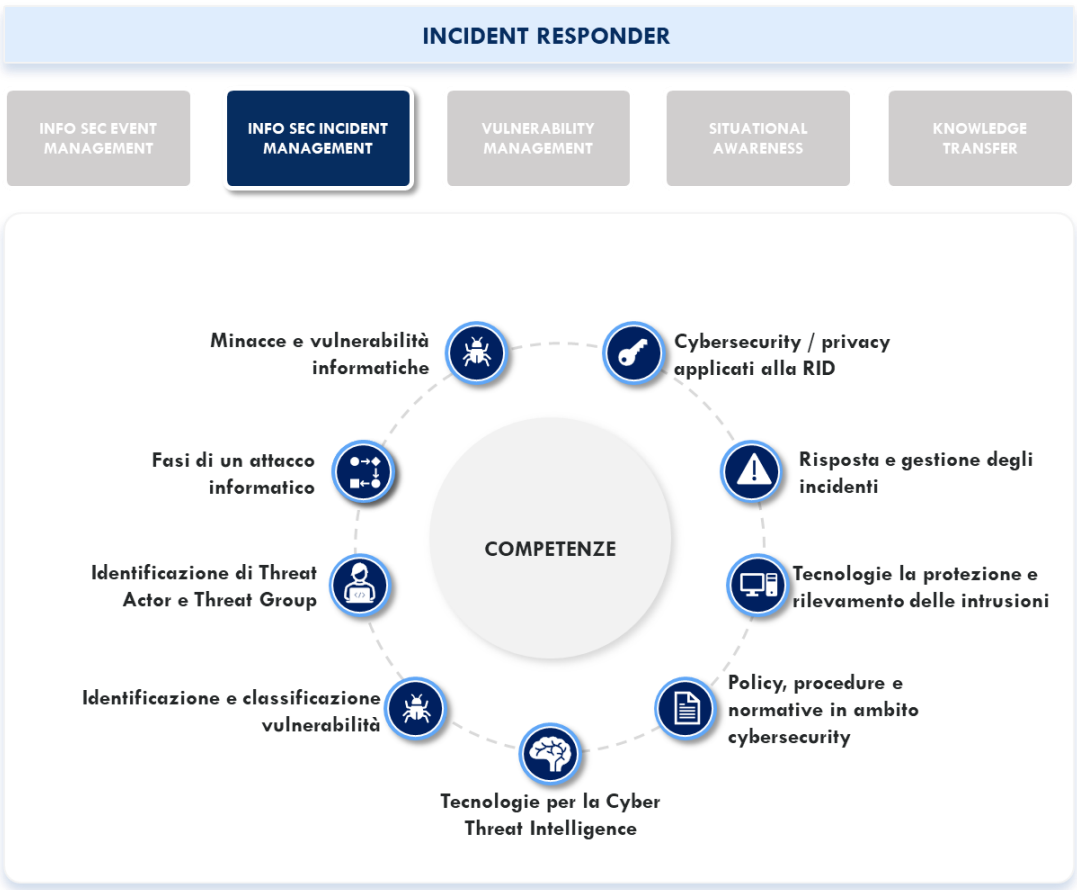

Figura 9: Principali competenze per la figura Incident Responder

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.9 IT/OT Administrator

L'**IT/OT Administrator** è la figura professionale che ha l'obiettivo di ripristinare le funzionalità degli asset (esempio, sistemi, reti, ecc.) coinvolti durante l'incidente di sicurezza.

È una figura impiegata nell' *area* Information Security Incident Management e le competenze richieste sono riassunte nell'immagine seguente:

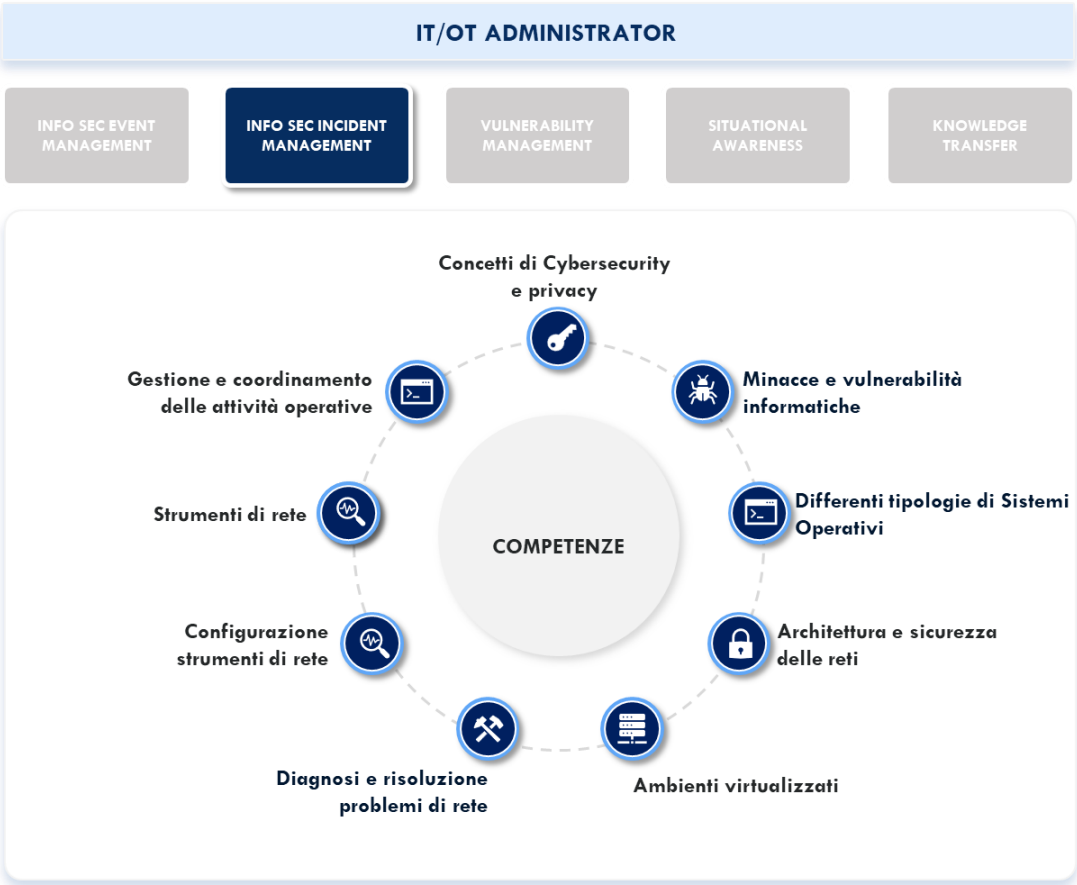

Figura 10: Principali competenze per la figura IO/OT Administrator

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.10 Vulnerability Analyst

Il **Vulnerability Analyst** è la figura professionale che 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.

È una figura impiegata nell' *area* Vulnerabilty Management e le competenze richieste sono riassunte nell'immagine seguente:

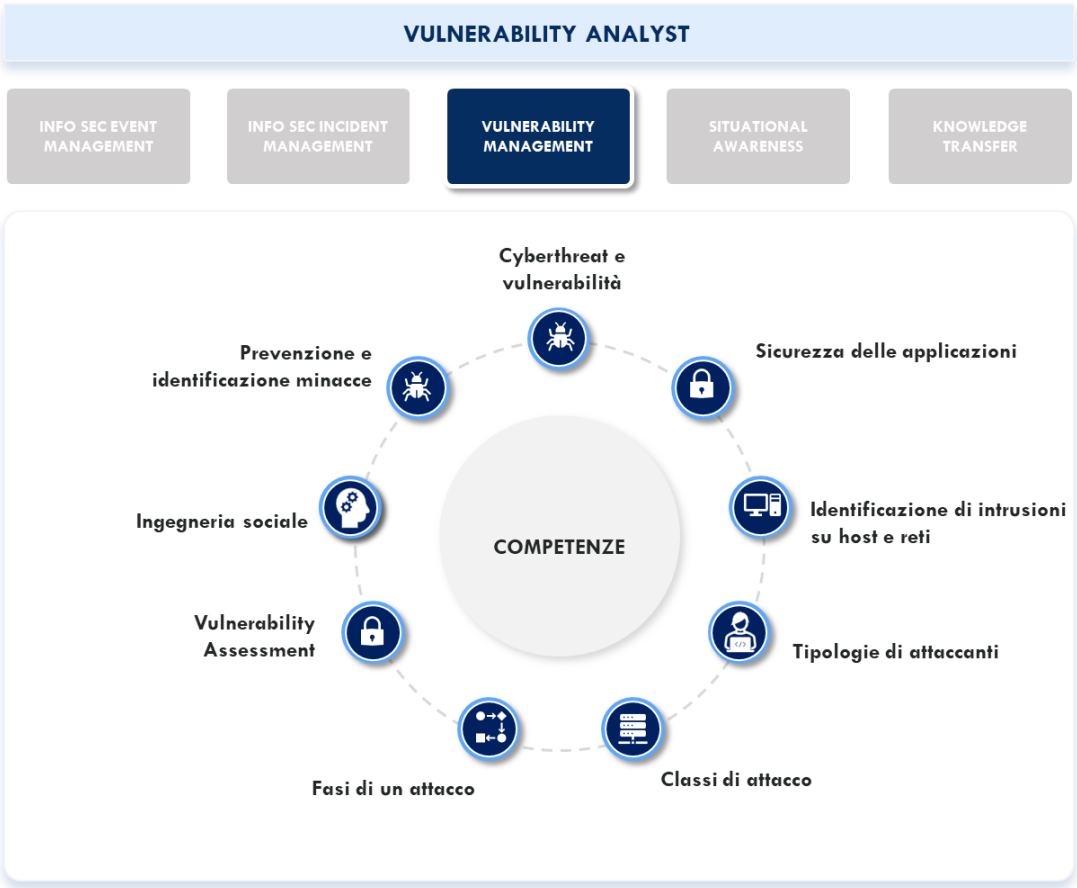

Figura 11: Principali competenze per la figura Vulnerability Analyst

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.11 Vulnerability Assessment Analyst

Il **Vulnerability Assessment Analyst** è la figura professionale che ha l'obiettivo di rilevare e di identificare attivamente le potenziali vulnerabilità note, presenti nei sistemi/applicazioni apparenenti alla Constituency.

È una figura impiegata nell' *area* Vulnerabilty Management e le competenze richieste sono riassunte nell'immagine seguente:

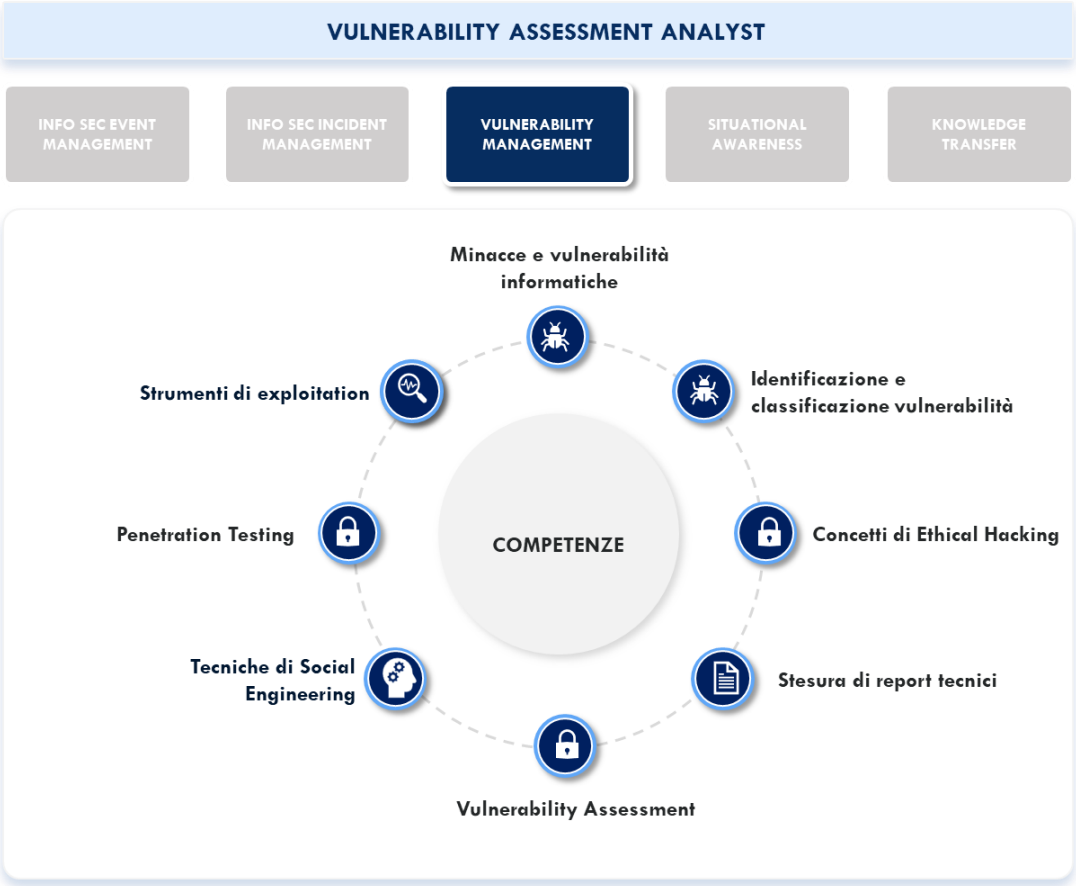

Figura 12: Principali competenze per la figura Vulnerability Assessment Analyst

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.12 Vulnerability Coordinator

Il **Vulnerability Coordinator** è la figura professionale che 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.

È una figura impiegata nell' *area* Vulnerabilty Management e le competenze richieste sono riassunte nell'immagine seguente:

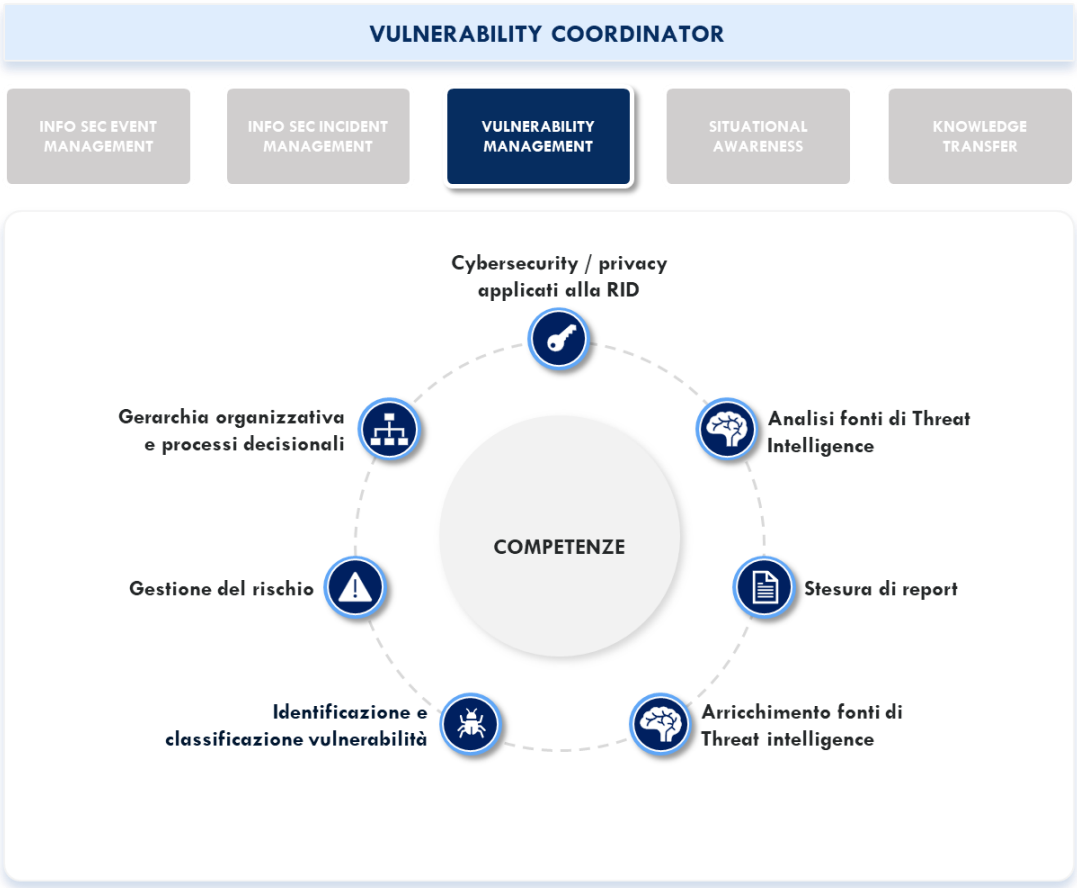

Figura 13: Principali competenze per la figura Vulnerability Coordinator

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.13 IT/OT Security Administrator

L'**IT/OT Security Administrator** è la figura professionale che esegue attività di mitigazione / risoluzione delle vulnerabilità attraverso l'applicazione di aggiornamenti hardware / software o di configurazioni.

È una figura impiegata nell' *area* Vulnerabilty Management e le competenze richieste sono riassunte nell'immagine seguente:

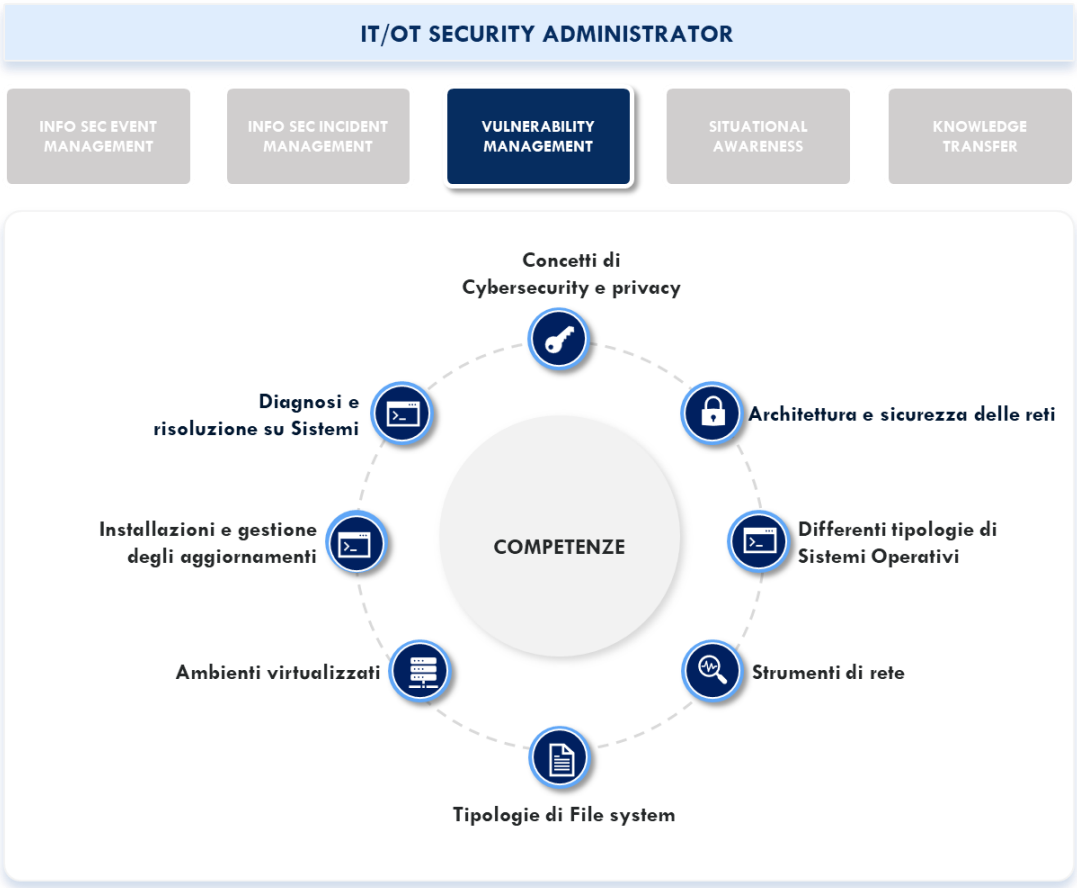

Figura 14: Principali competenze per la figura IT/OT Security Administrator

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.14 Vulnerability Disclosure Coordinator

Il **Vulnerability Disclosure Coordinator** è la figura professionale che 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.

È una figura impiegata nell' *area* Vulnerabilty Management e le competenze richieste sono riassunte nell'immagine seguente:

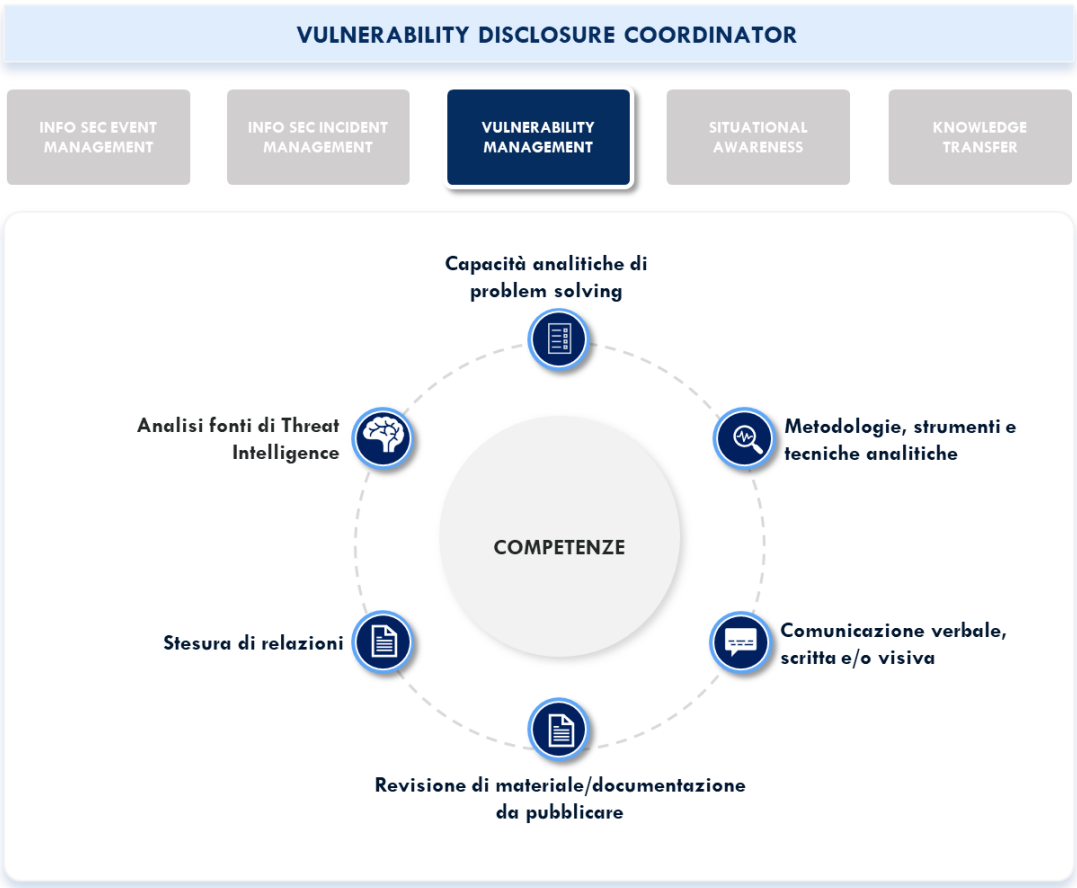

Figura 15: Principali competenze per la figura Vulnerability Discosure Coordinator

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.15 Vulnerability Researcher

Il **Vulnerability Researcher** è la figura professioanle che 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.

È una figura impiegata nell' *area* Vulnerabilty Management e le competenze richieste sono riassunte nell'immagine seguente:

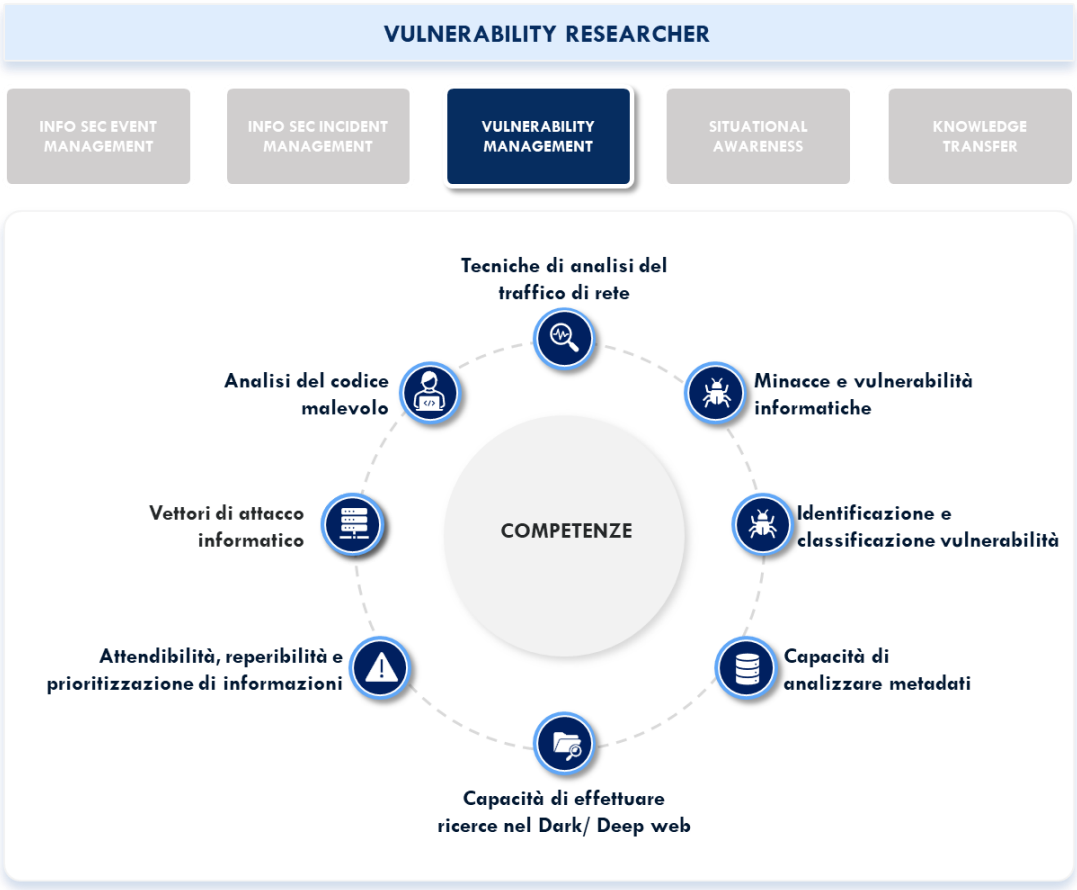

Figura 16: Principali competenze per la figura Vulnerability Researcher

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.16 Vulnerability Triage Coordinator

Il **Vulnerability Triage Coordinator** è la figura professionale che 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.

È una figura impiegata nell' *area* Vulnerabilty Management e le competenze richieste sono riassunte nell'immagine seguente:

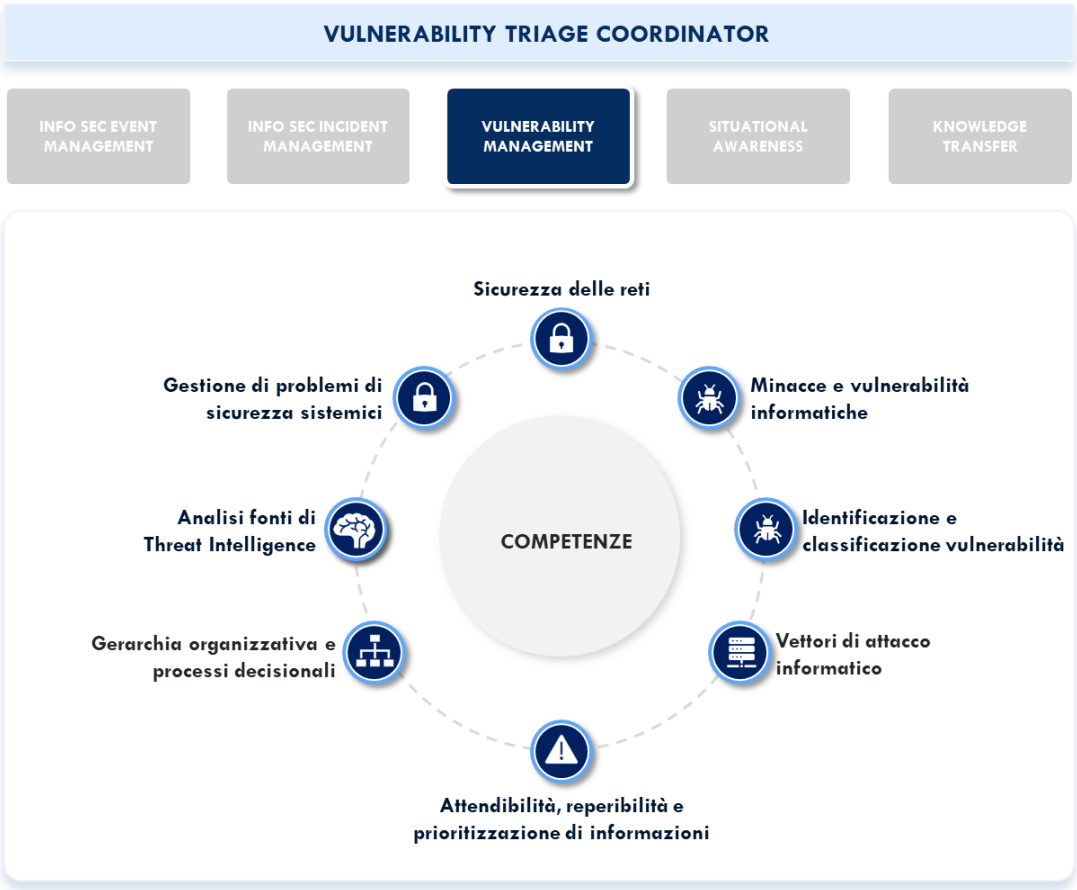

Figura 17: Principali competenze per la figura Vulnerability Triage Coordinator

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.17 Situational Awareness Data Analsyt

Il **Situational Awareness Data Analyst** è la figura professionale che si occupa di raccogliere, aggregare ed analizzare le informazioni operative e di contesto provenienti da più fonti interne dell'organizzazione al fine di deternaminare il contesto situazionale.

È una figura impiegata nell' *area* Situational Awareness e le competenze richieste sono riassunte nell'immagine seguente:

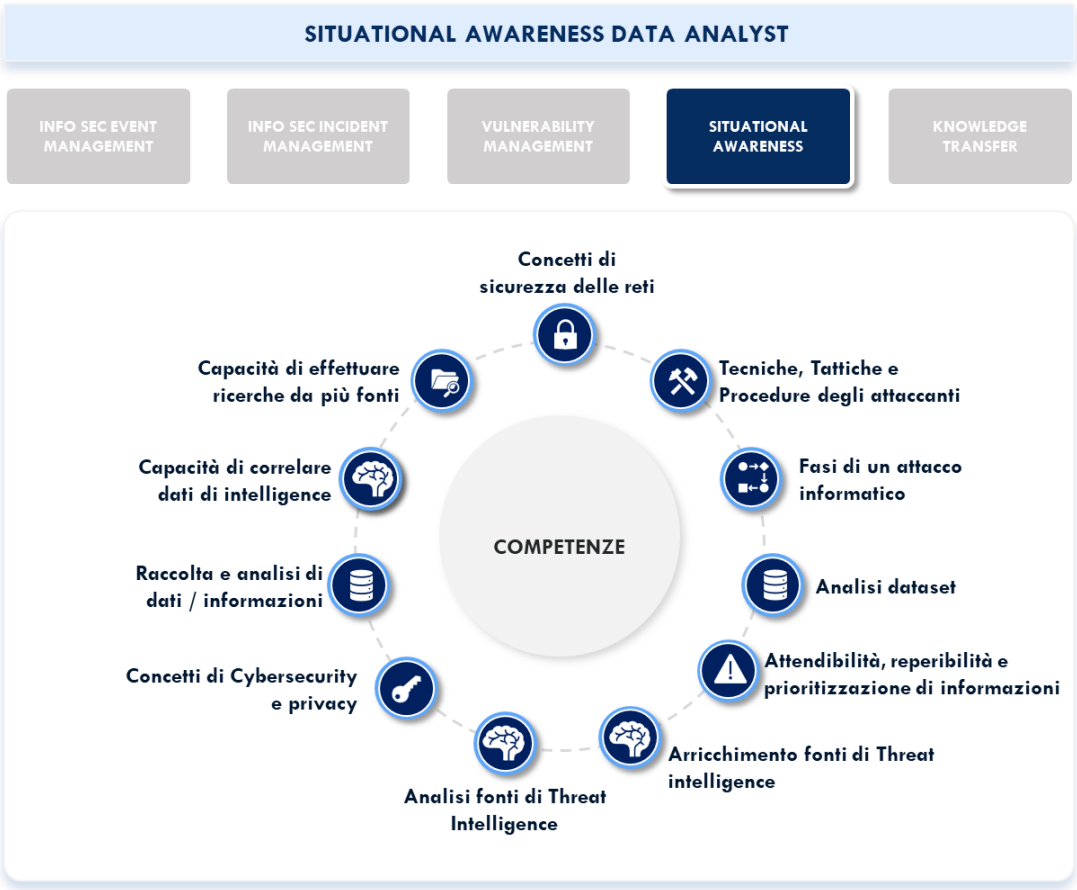

Figura 18: Principali competenze per la figura Situational Awareness Data Analyst

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.18 Threat Warning Analyst

Il **Threat Warning Analyst** è la figura professionale che ha l'obiettivo di fornire alla propria organizzazione informazioni circa le minacce attuali (esempio, eventuali campagne in corso, impatti).

È una figura impiegata nell' *area* Situational Awareness e le competenze richieste sono riassunte nell'immagine seguente:

Figura 19: Principali competenze per la figura Threat Warning Analyst

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.19 Risk & Continuity Advisor/Risk Analyst

Il **Risk & Continuity Advisor / Risk Analyst** è la figura professionale 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.

È una figura impiegata nell' *area* Situational Awareness e le competenze richieste sono riassunte nell'immagine seguente:

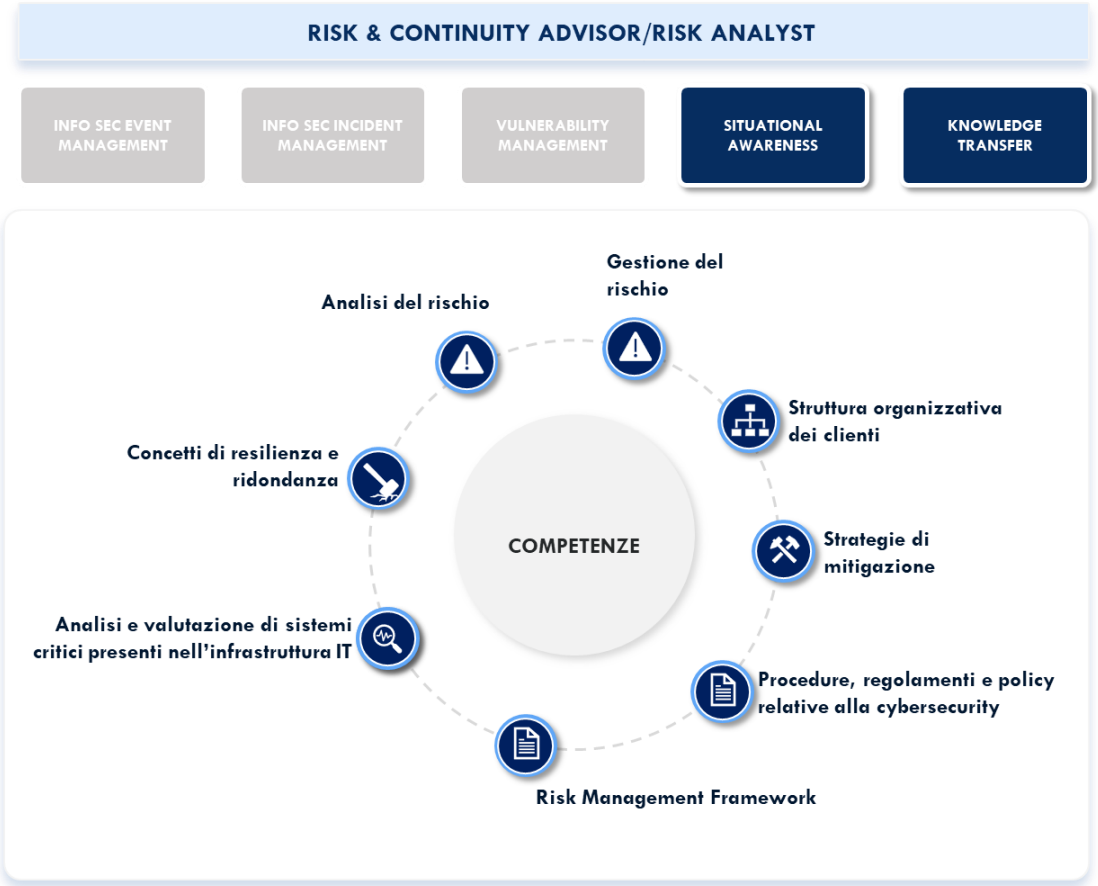

Figura 20: Principali competenze per la figura Risk & Continuity Advisor / Risk Analyst

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.20 Awareness Coordinator

Il **Awareness Coordinator** è la figura professionale che 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.

È una figura impiegata nell' *area* Knowledge Transfer e le competenze richieste sono riassunte nell'immagine seguente:

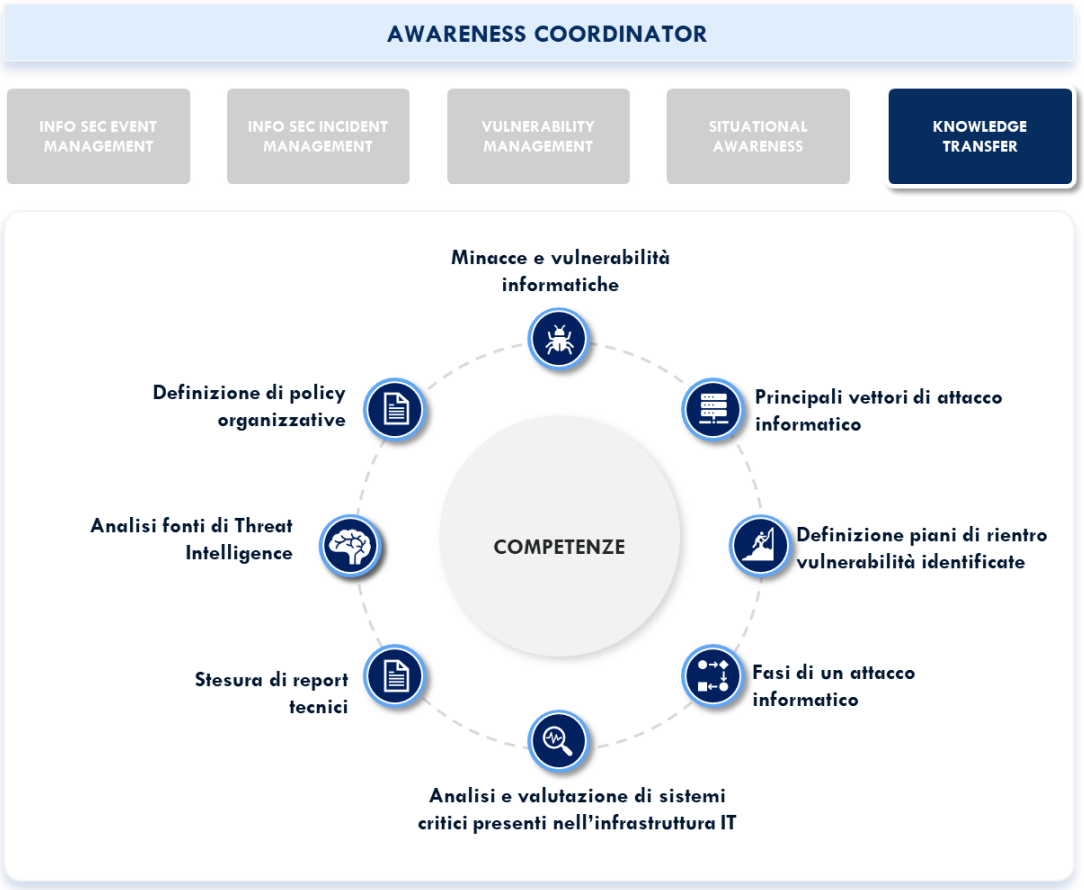

Figura 21: Principali competenze per la figura Awareness Coordinator

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.21 Policy Advisor

Il **Policy Advisor** è la figura professionale che collabora con la Constituency e con i principali attori interessati per contribuire alla creazione e all'attuazione delle politiche della stessa.

È una figura impiegata nell' *area* Knowledge Transfer e le competenze richieste sono riassunte nell'immagine seguente:

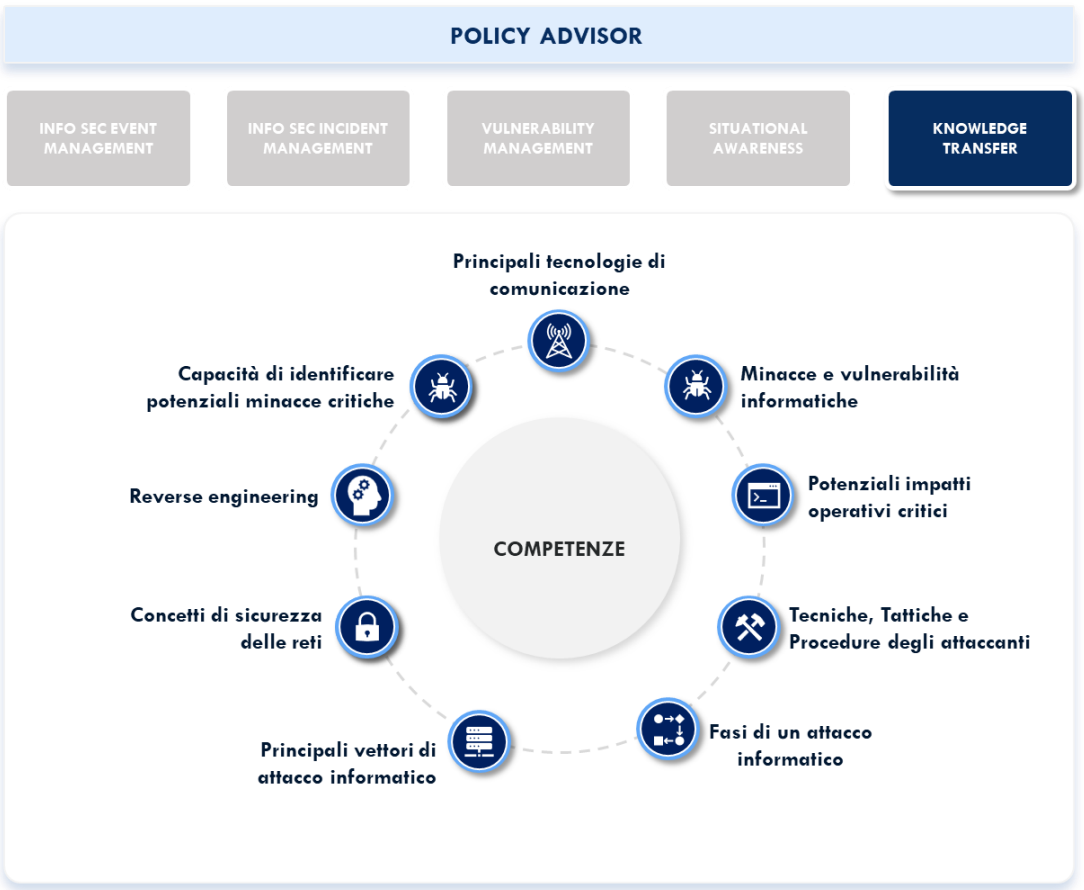

Figura 22: Principali competenze per la figura Policy Advisor

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.22 Staff Developer

Lo **Staff Developer** è la figura professionale che 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.

È una figura impiegata nell' *area* Knowledge Transfer e le competenze richieste sono riassunte nell'immagine seguente:

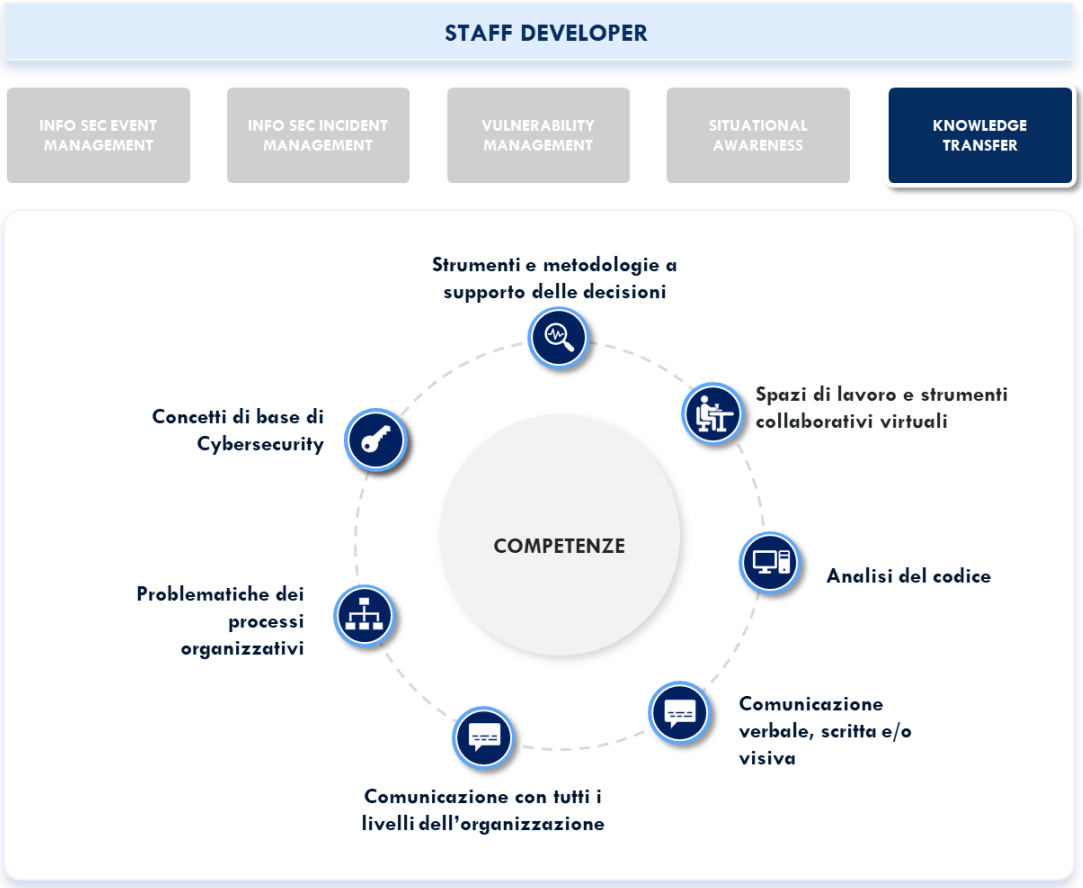

Figura 23: Principali competenze per la figura Staff Developer

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.23 Technical Policy Advisor

Il **Technical Policy Advisor** è la figura professionale che 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.

È una figura impiegata nell' *area* Knowledge Transfer e le competenze richieste sono riassunte nell'immagine seguente:

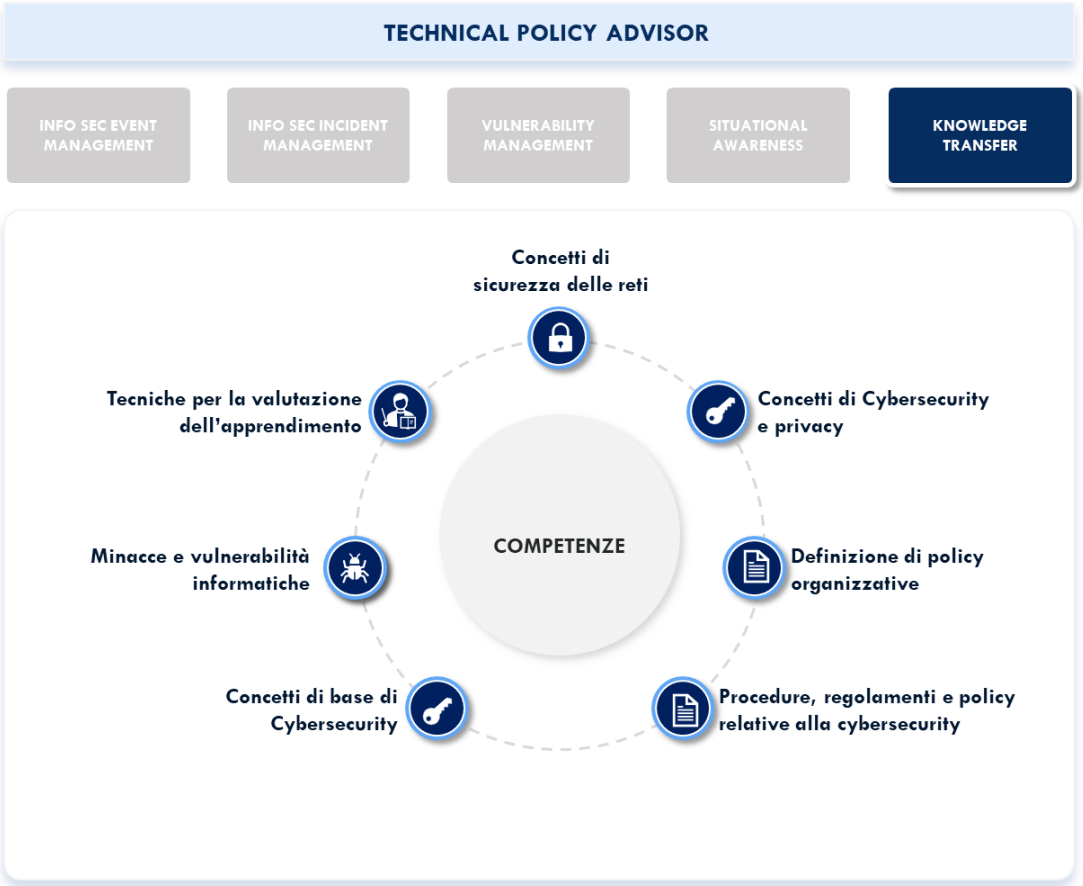

Figura 24: Principali competenze per la figura Technical Policy Advisor

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.24 Training Developer

Il **Training Developer** è la figura professionale che ha il compito di sviluppare i contenuti per le attività di formazione ed esercitazione che dovranno poi essere impiegati per l'erogazione delle attiivtà formative all'interno e/o all'esterno del CSIRT.

È una figura impiegata nell' *area* Knowledge Transfer e le competenze richieste sono riassunte nell'immagine seguente:

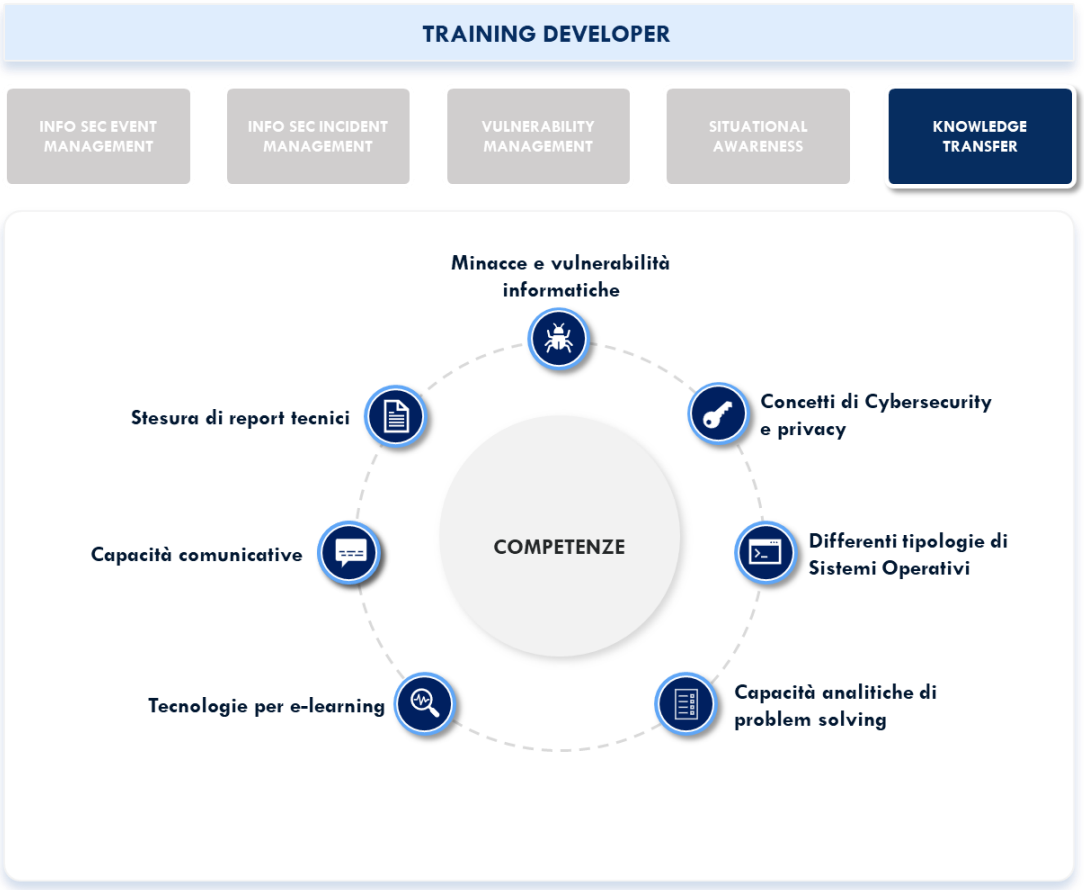

Figura 25: Principali competenze per la figura Training Developer

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

2.25 Training Instructor

Il **Training Instructor** è la figura professionale che 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.

È una figura impiegata nell' *area* Knowledge Transfer e le competenze richieste sono riassunte nell'immagine seguente:

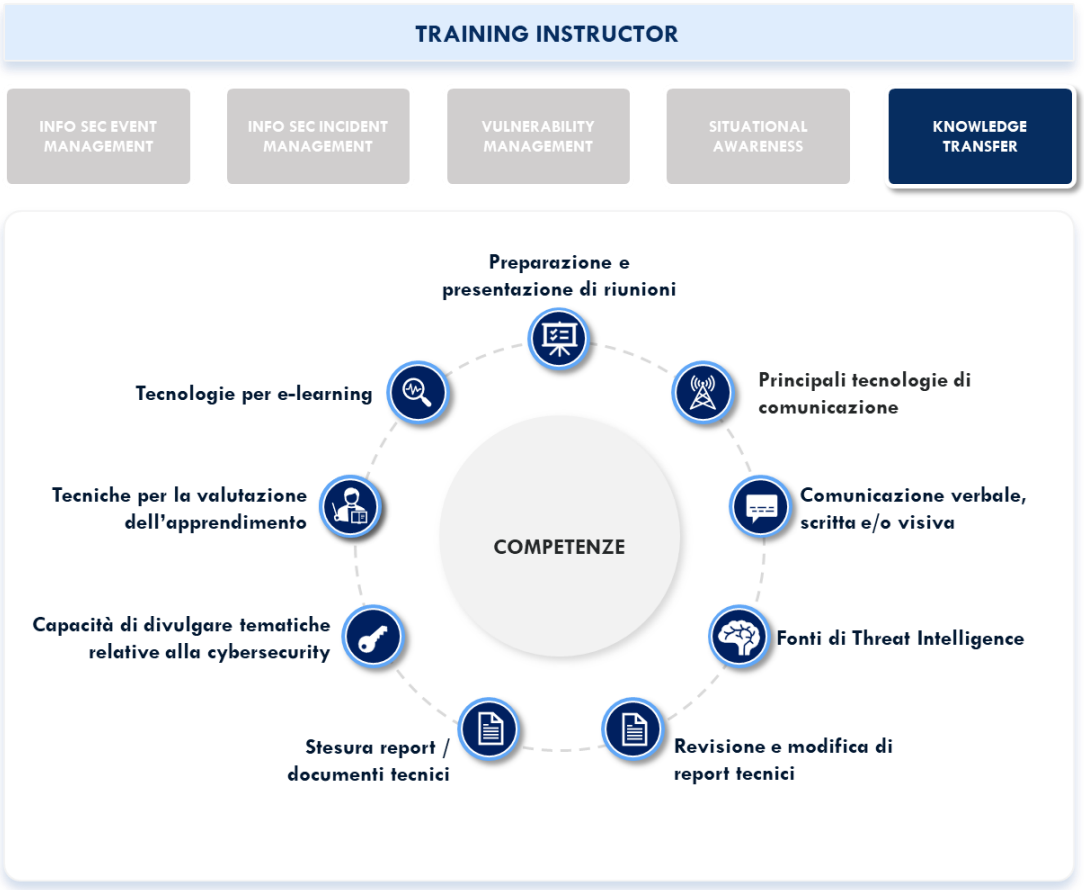

Figura 26: Principali competenze per la figura Training Instructor

Finanziato dall'Unione europea NextGenerationEU
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE