Talenti di cybersecurity e dove trovarli: train to attract, hire & retain

Presentazione del Cyber workforce Survey 2024 di SANS Institute

Alessio Pennasilico | Partner, *P4I*
Manlio Longinotti | Responsabile Italia, *SANS*
Michele Mariella | CIO Maire Tecnimont

Alessio Pennasilico

Partner, Practice Leader Information & Cyber Security Advisory Team P4I
Security Evangelist & Ethical Hacker

Membro del Comitato Scientifico Clusit

Membro del Comitato Direttivo di Informatici Professionisti AIP ITCS

Vice Presidente del Comitato di Salvaguardia per l'Imparzialità Lloyd's Register LRQA

Membro del Comitato di schema kiwa intertek

Direttore Scientifico della testata CYBERSECURITY360

Senior Advisor dell'Osservatorio Cyber Security & Data Protection del Politecnico di Milano osservatori.net digital innovation

Manlio Longinotti

SANS Institute – Responsabile Italia

Con oltre 15 anni di esperienza nell'avviamento e sviluppo di business, Manlio Longinotti dal 2022 è il responsabile SANS Institute per l'Italia.

Ha il compito di supportare le organizzazioni pubbliche e private italiane con progetti di formazione specialistica e certificazione di esperti in cyber security, con l'obiettivo di migliorarne postura di sicurezza, compliance e competitività sul mercato. In precedenza ha lavorato a progetti di sviluppo e integrazione software in Accenture e Abinsula.

Michele Mariella
CIO – Marie Tecnimont

Nato nel 1972 a Torino, è laureato in Ingegneria Elettronica. Dal 2017 è CIO del gruppo Maire, dove ha ricoperto importanti e diversi ruoli nell'ambito delle ICT e dei servizi generali.

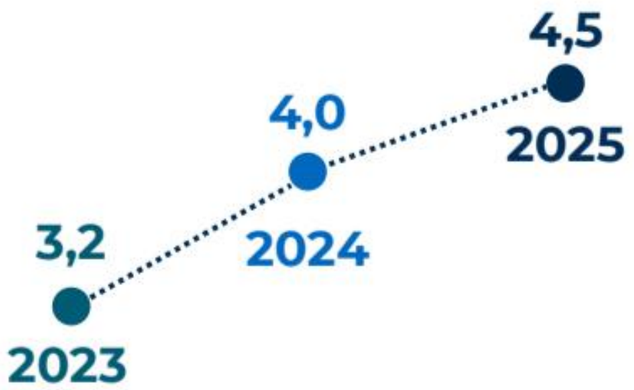
Nel 2018 ha contribuito al conseguimento del premio per il miglior progetto in ambito Smartworking istituito dal Politecnico di Milano.

Dal 2021, assume il ruolo di Coordinatore Working Group Cybersecurity in Assolombarda e dal 2024 occupa la posizione di Digital & Energy Services Vice President in Tecnimont Services SpA, societa' del Gruppo Maire.

Lo stato delle competenze cyber

La crescente complessità della cybersecurity e minacce cyber sempre più avanzate richiedono **competenze specializzate** sul tema, spesso **difficili da reperire sul mercato**

Presenza di specialisti all'interno delle grandi organizzazioni italiane (FTE)



Solo il **4%** delle grandi organizzazioni non ha introdotto specialisti di cybersecurity

Campione Survey CISO 2024: 131 Grandi Organizzazioni

Principali attività svolte dai team interni

1. **Definizione delle strategie di cybersecurity**
2. **Selezione dei fornitori**
3. **Analisi del rischio cyber**
4. **Adeguamento normativo**

Le difficoltà delle organizzazioni

Il **67%** delle organizzazioni segnala un **alto divario** di **competenze cyber**

Solo il **14%** delle organizzazioni ritiene di avere **le persone e le competenze necessarie** per raggiungere i propri obiettivi di sicurezza

Fonte: Global Cybersecurity Outlook 2025, World Economic Forum

POLIMI SCHOOL OF MANAGEMENT | osservatori.net digital innovation

La formazione per colmare il gap

9 aziende su **10** prevedono **azioni di formazione** per superare lo **skill gap** in ambito cyber

Azioni di formazione per sviluppare competenze dedicate

83% **Specialisti IT interni coinvolti in programmi di formazione cyber**

35% **Imprese per cui la formazione cyber è un'alta priorità di spesa**

14% **Della spesa cybersecurity dedicata alla formazione**

Campione Survey CISO 2024: 131 Grandi Organizzazioni

Le recenti normative rafforzano il concetto di prevedere ruoli e competenze verticali per proteggere le organizzazioni dalla minaccia cyber.

- **Direttiva NIS2 art. 21 (e artt. 23 e 24 D.lgs. 138/2024)**

  - Formazione per gli organi direttivi, per i primi riporti alla direzione, per il team ICT.

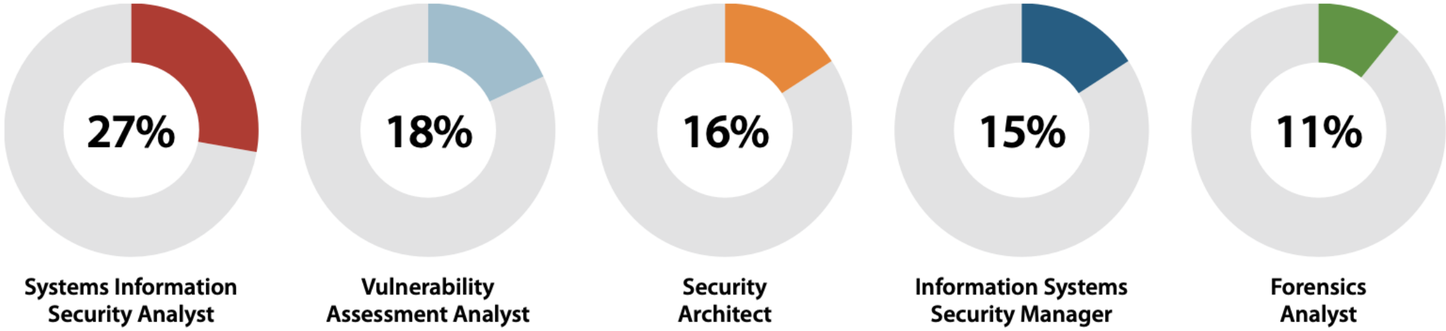
- **L. 90/2024 (cd. DDL Cyber)**
- **DORA**
- **Direttiva CER (recepita da D.lgs. 134/2024)**

  - Art. 14 c. 2 , sicurezza del personale, «adeguati requisiti di formazione e adeguate qualifiche» fra le misure tecniche da adottare per garantire la resilienza dei soggetti critici.

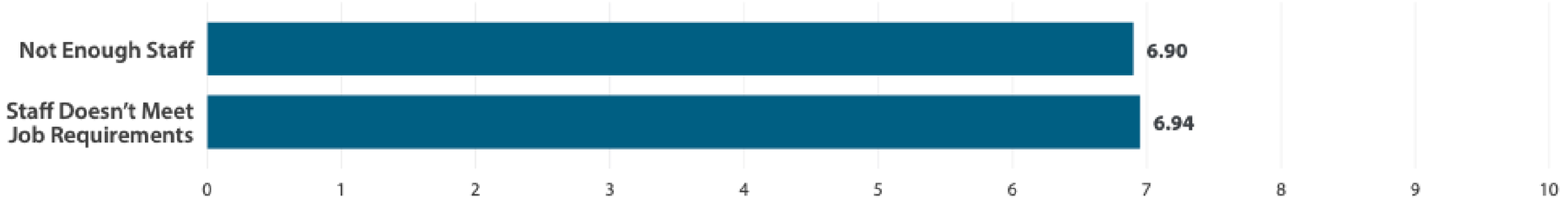
- **Cyber Resilience Act**
- **Industry specific standard: PCI DSS 4.0, ISO27001,**

I profili e le competenze più ricercate sul mercato per ruoli mid-senior.

Gli HR e i Cyber Security Managers intervistati hanno indicato **i 5 profili professionali più richiesti** dalle loro organizzazioni:



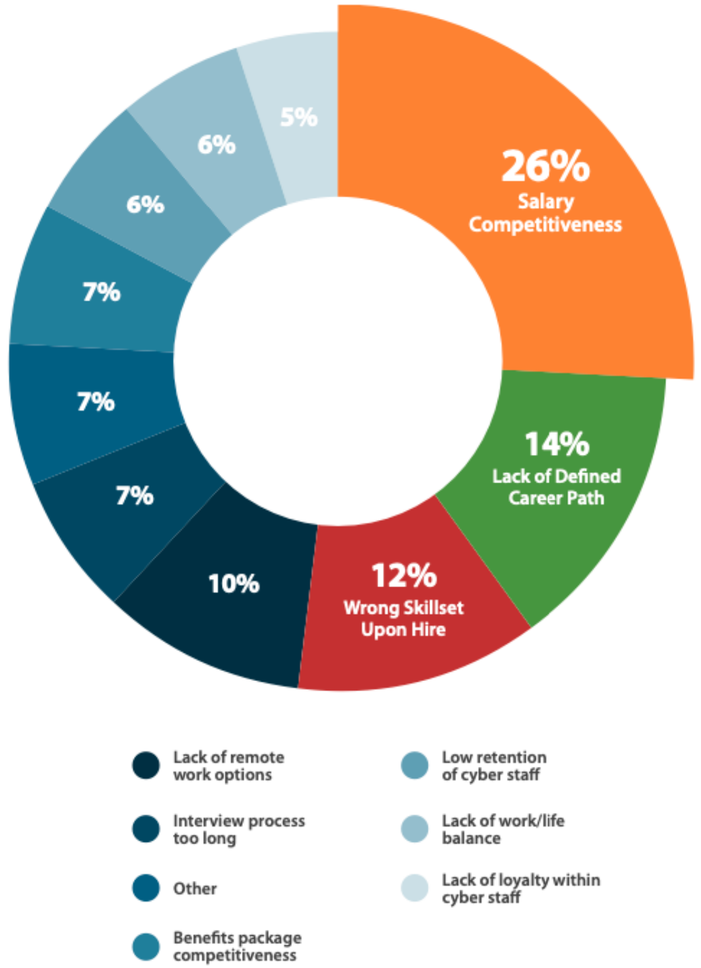
attribuendo priorità uguale alla necessità di rafforzare i team in termini di numeri (6,9) e alla presenza di giuste competenze per svolgere con successo i compiti assegnati e raggiungere gli obiettivi (6,94).



Quanto è complesso assumere specialisti in cyber security?

Alla domanda su quali fossero gli aspetti chiave da considerare per assumere con successo uno specialista in sicurezza informatica, al primo posto c'è il salario. Tuttavia, se sommiamo gli **altri fattori**, si nota che questi **possono compensare la competitività dello stipendio**.

- 14% assenza di un chiaro percorso di carriera
- 12% valutazione errata delle competenze
- 10% scarse possibilità di lavoro da remoto
- 7% processo di selezione troppo lungo

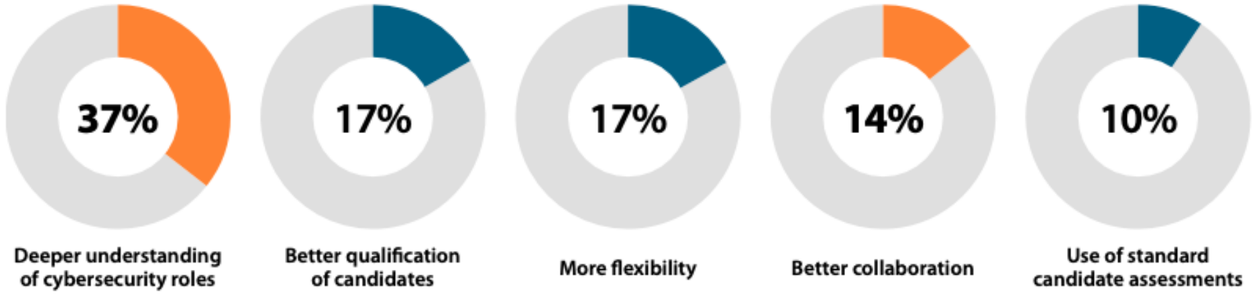


Una maggiore sinergia fra HR e Hiring manager è necessaria, soprattutto in imprese medio-piccole con budget limitati e che cercano profili junior da formare sul campo.

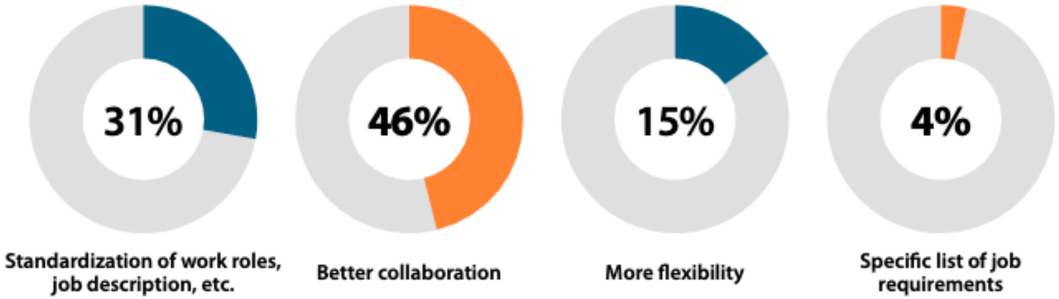
In che modo HR & Cyber Security Manager possono collaborare?

Soltanto il 14% delle organizzazioni utilizza framework come il NICE per definire ruoli e relative posizioni aperte. L'adozione di questo approccio può facilitare la ricerca di specialisti di infosec.

Il 37% degli hiring managers vorrebbe che HR avesse una comprensione migliore del ruolo che il neoassunto dovrà ricoprire...

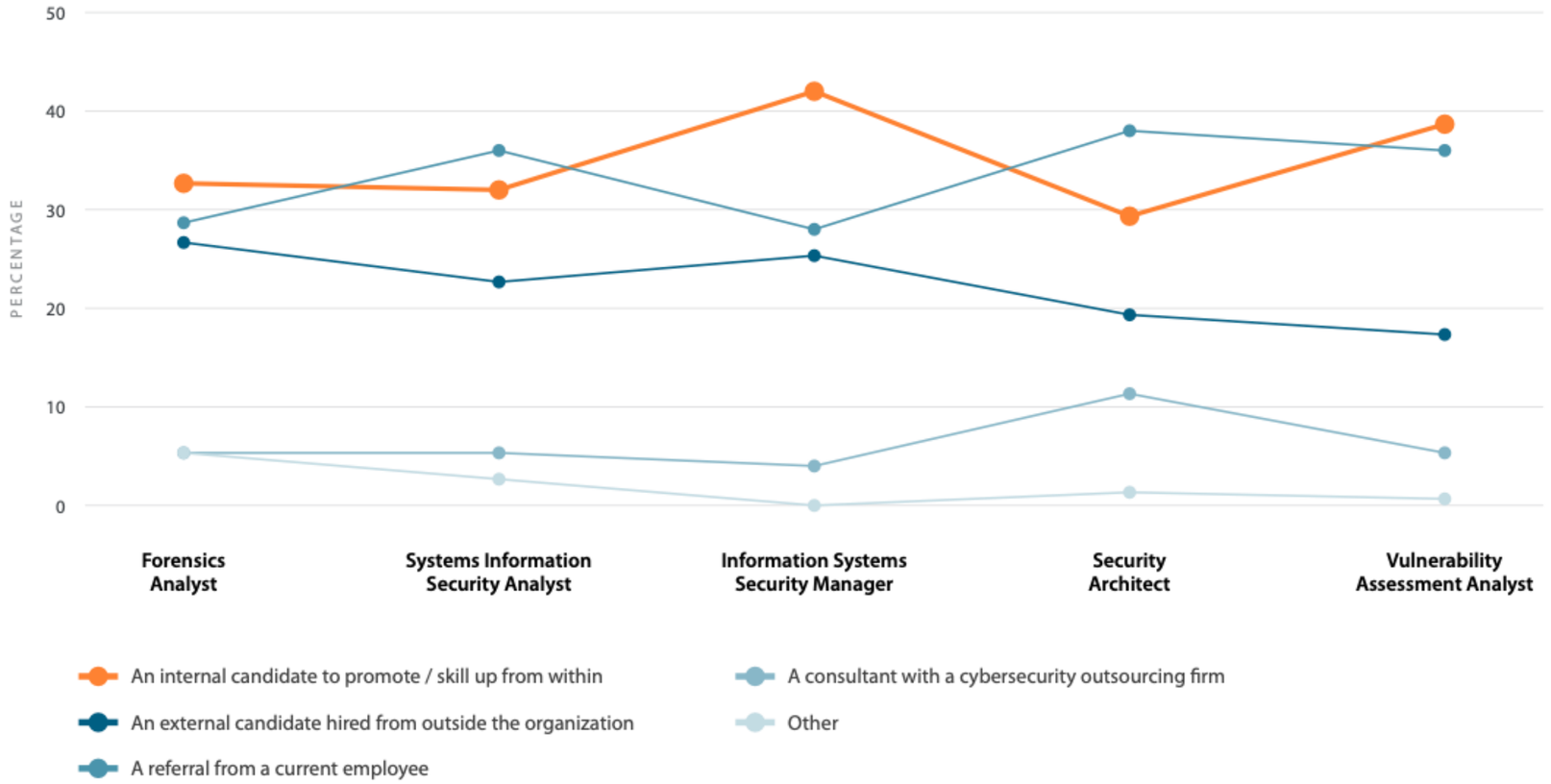


... mentre HR gradirebbe una maggiore collaborazione, insieme alla standardizzazione di job description, work roles, terminologia tecnica.



Dove si trovano (o cercano) gli specialisti della sicurezza informatica?

Il 57% delle posizioni aperte in cyber security trova risposta in candidati interni (35% upskilling, 22% referral).

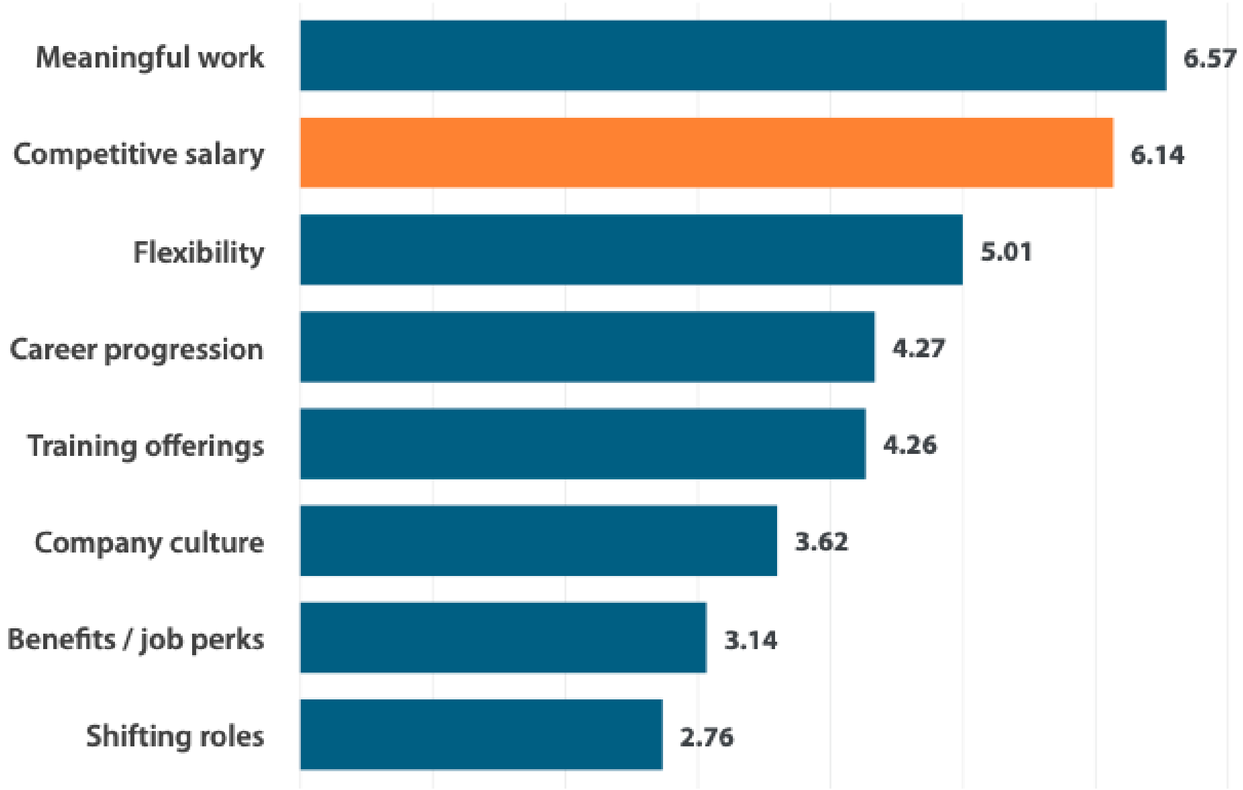


Adottare una strategia di assunzione e formazione interna all'organizzazione può ridurre il ricorso ad assunzioni dall'esterno, che abbiamo visto essere più complesse ed articolate.

Dopo l’assunzione: fidelizzare e diventare attrattivi.

L’assenza di un chiaro percorso di carriera e di formazione «pesano» più dello stipendio,

che incide nel 23% dei casi in cui un manager cerca di trattenere le persone del suo team.

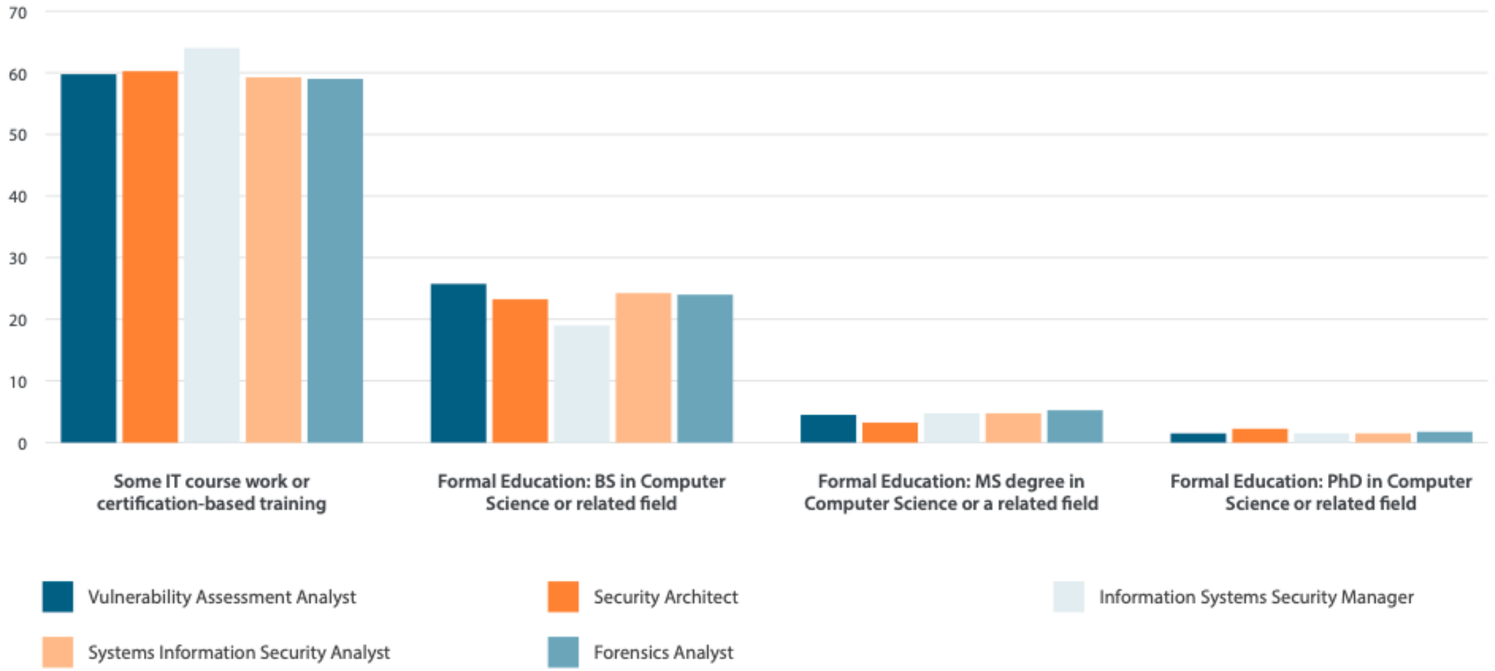


Nella scala dei fattori più incisivi per motivare e fidelizzare un esperto infosec lo stipendio è al secondo posto, il che lascia intendere come una volta **entrati a far parte di un’organizzazione i professionisti della cyber security diano più valore ad altri aspetti collaterali, spesso sottovalutati dal top management.**

Anche in questo caso, la sinergia HR – Cyber Sec. Manager può giocare un ruolo determinante.

Il valore della formazione e delle certificazioni.

Gli intervistati hanno dato importanza uguale al training tradizionale VS training on-the-job, a conferma del fatto che sono entrambi necessari per determinare il successo dei progetti e dei team.



Nel valutare il livello di preparazione dei candidati c'è una forte preferenza per chi dimostra di avere competenze tecniche, hands-on dimostrabili tramite certificazioni, oltre ad una attitudine a lavorare in un certo tipo di contesto.

Conclusioni

L’adozione di framework regolamentari (NICE, ECSF) e l’utilizzo di certificazioni professionali aiuta a standardizzare annunci di lavoro, percorsi e aspettative di carriera, terminologia tecnica, riducendo inefficienze.

La strategia più efficace per sviluppare team di cybersecurity è assumere profili di media seniority con buoni fondamentali di cybersecurity e poi fornire una formazione in linea con i requisiti specifici del ruolo.

«Non ci si dovrebbe preoccupare che le persone, una volta formate, lascino l’azienda: investire sulle persone aumenta il loro desiderio di restare». Jay Bhalodia – Managing Director, Microsoft

Per un punto di vista basato su dati EU si veda https://europa.eu/eurobarometer/surveys/detail/3176

Contatti:

Manlio Longinotti – mlonginotti@sans.org | +39 328 1358 405

Report completo al link:

https://www.sans.org/mlp/2024-attract-hire-retain-midlevel-cybersecurity-roles/

L'edizione 2025 del report verrà pubblicata sul sito SANS nel Q2.