Profilo

|  |  |
| --- | --- |
| Titolo del profilo  | JUNIOR INFORMATION SECURITY CONSULTANT  |
| Descrizione sintetica  | Figura professionale di riferimento per insiemi definiti di attività e progetti collegate alla gestione della sicurezza delle informazioni.  |
|    Missione  | Contribuisce nell’attuazione della strategia definita all’interno del suo ambito di responsabilità (sia questo un progetto, un processo, una location) partecipando al ruolo di raccordo tra la struttura di governance della Cyber security e il resto del personale operativo. Controlla il rispetto alle regole definite e del cogente in materia di sicurezza delle informazioni.  |
|   | Attua misure di sicurezza organizzazione.  | per proteggere  | le reti e i  | sistemi informatici di una  |
|          Principali Task  | * Partecipazione al controllo delle reti dell’organizzazione per rilevare violazioni della sicurezza e indagare quando si verifica.
* Utilizzo del software, quali firewalls, web application firewalls e programmi di data encryption per proteggere informazioni sensibili.
* Collaborazione nella stesura documentazione e reportistica relativa a violazioni di sicurezza e la valutazione del danno da questa causato.
* Partecipazione alla effettuazione dei test di penetrazione, ovvero quando gli analisti simulano gli attacchi per cercare le vulnerabilità nei loro sistemi prima che possano essere sfruttate.
* Aiuto nella pianificazione e realizzare un modello con cui un'organizzazione gestisce la sicurezza informatica.
* Partecipazione nell’adozione di standard di Sicurezza e di best practices per l’organizzazione.
* Attuazione delle raccomandazioni di sicurezza al management o al personale IT
* Supporto agli utenti quando devono installare o conoscere nuovi prodotti e procedure di sicurezza.
 |
|   | B.2.  | Integrazione dei componenti  | Livello 3  |
| B.3.  | Testing  | Livello 3  |
| C.4.  | Gestione del problema  | Livello 3  |
| D.1.  | Sviluppo  della informatica  | strategia  | per  | la  | Sicurezza  | Livello 2  |
| E.8.  | Gestione della sicurezza dell’informazione  | Livello 3  |
| E.9.  | Governance dei sistemi informativi  | Livello 2  |
|            Conoscenze  | * Conoscenza delle metodologie di vulnerability assessment, penetration test, compliance management e Security Audit.
* Conoscenza delle diverse tipologie di attacco informatico, delle tecniche di penetration test, degli strumenti software utilizzati e dei più importanti tool ed exploit disponibili pubblicamente.
* Conoscenza di network security (firewall, web application firewall, IPS, Network access control, pila TCP/IP).
* Conoscenza delle metodologie e linee guida ISO in materia di Risk Assessment e Risk Treatment e degli strumenti a supporto delle fasi di gestione del rischio.
* Conoscenza acquisita dalla partecipazione a progetti di Risk Assessment.
* Conoscenza acquisita dalla partecipazione alla definizione di modelli per l’analisi del rischio.
* Conoscenza della normativa e linee Guida AgiD di settore in materia di Sicurezza Informatica.
* Conoscenza della normativa in materia di privacy.
* Conoscenza delle policy e linee guida di sicurezza a supporto dei processi organizzativi su diversi ambiti di applicazione (es. gestione del rischio, classificazione delle informazioni, gestione degli incidenti, utilizzo sicure dei servizi informatici).
 |
|        Abilità  | * Capacità di contribuire alla redazione di documentazione a supporto dei processi di compliance rispetto alle normative applicabili (es. Documento programmatico della sicurezza, Studio di fattibilità per la continuità operativa...).
* Capacità di contribuire alla redazione di documentazione tecnica e di progetto.
* Capacità di partecipare allo studio dei sistemi e delle reti di computer per la valutazione dei rischi per determinare come migliorare le politiche e i protocolli di sicurezza.
* Capacità di contribuire alla correlazione dei cambiamenti dei sistemi informatici con gli attacchi informatici possono essere difficili da rilevare.
* Capacità di supporto nell’anticipare i rischi per la sicurezza delle informazioni e nell’implementare nuovi modi per proteggere i sistemi informatici e le reti delle organizzazioni.
* Capacità di collaborare nella risposta agli avvisi di sicurezza, nella correzione dei

difetti nei sistemi e nelle reti di computer.  |
| Certificazioni  | N/A  |
| Titolo di studio  | Laurea triennale in materie scientifiche o cultura equivalente.  |
| Anzianità lavorativa  | Minimo 4 anni da computarsi successivamente al conseguimento della diploma di laurea, di cui almeno 2 nella funzione  |