Alta formazione in Apprendistato a.a. 2024/2025

Master in
CYBERSECURITY
www.mastercybersecuritytorino.it

Dati dell'impresa

Ragione Sociale: **_Nais srl___**

Sede Azienda: Torino

Sito web azienda: www.nais.ai ____

Breve descrizione dell'azienda: Dal 1998, Nais progetta, realizza e gestisce infrastrutture IT all'avanguardia, garantendo ai propri clienti una difesa informatica 24 ore su 24, 7 giorni su 7. Il nostro Cyber Fusion Center, specializzato in attività di Blue, Red e Purple Team, trova la sua massima espressione grazie al connubio con attività tipiche dell'AI.

Ruolo previsto in azienda per il candidato:

Gestire gli eventi identificati da sistemi automatizzati e indicatori di primo livello, lavorando alla loro bonifica utilizzando gli strumenti SOC.

Valutare vulnerabilità e rischi in collaborazione con i clienti per gestire la sicurezza delle informazioni.

Aiutare i processi e il modello operativo del SOC.

Identificazione di potenziali tentativi di intrusione, sia riusciti che sventati, attraverso la revisione e l'analisi dettagliata delle informazioni sugli eventi.

Cercare di individuare comportamenti anomali che potrebbero rappresentare minacce sconosciute, non rilevabili dalle misure di sicurezza standard.

Supportare e contribuire all'evoluzione degli strumenti SOC.

Redazione di report rilevanti da condividere con il team.

Assistere l'analista e l'architetto della sicurezza nella ricerca di soluzioni adeguate.

Collaborare con il reparto R&D in merito allo sviluppo interno di un app dedicata

all'efficientamento della gestione delle attività tipiche del SOC

smartworking in accordo con il Soc Manager, in base alle esigenze organizzative del team

Area aziendale a cui afferisce il candidato: Cyber Fusion Center

- **Profilo richiesto:** laurea in informatica, Computer engineering ed equipollenti
- lingua inglese
- capacità di lavorare in Team
- problem solving
- capacità relazionali

Soft skills: predisposizione al lavoro in team, curiosità, proattività, capacità di analisi e problem solving

Ruoli con cui il candidato dovrà interfacciarsi: Soc Manager, Red Team Leader, blue Team Leader, Soc analyst

Competenze che il candidato raggiungerà alla fine del percorso formativo:
Dimestichezza nella gestione di eventi e cybersecurity incident Discovery, network Forensics, IPS/IDS, firewall, DLP, EPP (EDR, XDR, NDR) sicurezza relativa ai database, raccolta di log e relativa analisi
Conoscenza principali SIEM/SOAR in commercio (Es: IBM QRadar, SPlunk, Microsoft Sentinel)
Conoscenza principali distribuzioni Linux, Suite Microsoft, Google G-Suite
Protocolli di rete, Networking, Active Directory, protocollo LDAP
Principali linguaggi, (Phyton, Java, C/C++, PHP, Powershell)
Penetration Test e Vulnerability Assessment
Conoscenza di linguaggi di programmazione ad oggetti come java e kotlin
Buona conoscenza della lingua inglesa scritta e parlata
Capacità relazionale e attitudine a lavorare in team