Alta formazione in Apprendistato a.a. 2025/26

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:
Nais è un'azienda tech-oriented, Centro di Eccellenza in ambito IT e cybersecurity a livello nazionale ed europeo.
Da oltre 20 anni collaboriamo con le più grandi aziende italiane grazie a un approccio basato su Managed Services e progetti ad alto valore.
Unisciti ai nostri 100+ esperti impegnati in Competence Center per offrire soluzioni IT e Cyber all'avanguardia.

Ruolo previsto in azienda per il candidato:
Le attivitá e le responsabilitá saranno:

- Supportare nella gestione degli eventi rilevati dai sistemi automatici e dal primo livello, collaborando alle attività di remediation attraverso gli strumenti del **SOC**.
- Contribuire all'analisi di criticità e rischi, affiancando il team nella gestione della sicurezza delle informazioni.
- Partecipare ai processi operativi del SOC e supportarne il modello organizzativo.
- Collaborare alla review e all'analisi degli eventi di sicurezza per identificare potenziali tentativi di intrusione, riusciti o meno.
- Sviluppare capacità di individuazione di comportamenti anomali che possano indicare nuove minacce non ancora note.
- Dare supporto all'evoluzione e al miglioramento degli strumenti SOC.
- Redigere report e documentazione a supporto del team.
- Affiancare i Security Analyst e il Security Architect nella ricerca e valutazione di soluzioni di sicurezza
- Lavoro su turni, il notturno in smartworking.
-

Area aziendale a cui afferisce il candidato: Cyber Security Operatinos Center

Profilo richiesto: Cyber Security Analyst

- Formazione in ambito informatico.
- Conoscenze di base di sicurezza informatica e networking (protocolli di rete, firewall, IDS/IPS, endpoint protection, DLP).
- Conoscenza generale di sistemi operativi (Windows/Linux) e principali problematiche di sicurezza a livello sistemistico e applicativo.
- Interesse e motivazione a sviluppare competenze in ambito **cybersecurity** (incident discovery, network forensics, vulnerability assessment).
- Capacità di analisi e problem solving, con approccio metodico e orientato al dettaglio.
- Attitudine al lavoro in team e alla collaborazione con figure tecniche (Security Analyst, Security Architect).
- Buone capacità comunicative e predisposizione alla redazione di report tecnici.
- Precisione, affidabilità e curiosità, con forte desiderio di apprendere e crescere professionalmente.

Ruoli con cui il candidato dovrà interfacciarsi: Soc Manager, Senior Analyst, IRT, Developer ecc

Competenze che il candidato raggiungerà alla fine del percorso formativo:

Gestire **in autonomia eventi di sicurezza di base** (alert SIEM, EDR, IDS/IPS).
Distinguere **falsi positivi** da eventi potenzialmente reali.
Effettuare una **prima classificazione e prioritizzazione** degli incidenti.
Escalare correttamente i casi più complessi al livello superiore
Analizzare **log e eventi di sicurezza** per individuare:

- tentativi di intrusione
- attività sospette
- comportamenti anomali

Riconoscere **pattern di attacco comuni** (phishing, brute force, malware, lateral movement, ecc.).
Iniziare a sviluppare una **mentalità da threat analyst**, anche su minacce non ancora note.
Utilizzare con confidenza:

- SIEM
- sistemi di ticketing
- strumenti di correlazione e investigazione

Collaborare al **miglioramento delle regole di detection** (tuning di base).
Comprendere il flusso operativo degli strumenti di remediation.