**Alta formazione in Apprendistato a.a. 2021/2022**

**Master in CYBERSECURITY**
**www.mastercybersecuritytorino.it**

## Dati dell'impresa

**Ragione Sociale**: NAIS SRL

**Sede Azienda:** Torino

**Sito web azienda**: https://www.nais-net.it/

## Ruolo previsto in azienda per il candidato:

- Gestire gli eventi individuati dai sistemi automatici e dal primo livello e lavorando alla loro remediation, attraverso gli strumenti del SOC
- Analizzare criticità e rischi collaborando con i clienti nella gestione della sicurezza delle informazioni
- Supportare i processi ed il modello operativo del SOC
- Riconoscere i potenziali tentativi di intrusione, effettuati e mancati attraverso la review e l'analisi di informazioni dettagliate relative agli eventi
- Lavorare con l'obiettivo di individuare potenziali comportamenti anomali che possano rappresentare minacce non ancora note e quindi non rilevabili dagli ordinari controlli di sicurezza
- Supportare l'evoluzione degli strumenti del SOC
- Redigere i relativi report da condividere con il team
- Supporto a Security Analyst e il Security Architect nella ricerca di soluzioni appropriate

## Profilo richiesto:

Laurea informatica/ICT
Conoscenza base reti e sistemi
Scripting
SIEM
Active directory
Azure
Microsoft 365 defender

## Competenze che il candidato dovrà aver raggiunto 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 in commercio (Es: IBM QRadar, SPlunk, Microsoft Sentinel)
- Conoscenza ambiente Microsoft Active Directory, Microsoft Azure, Powershell.
- Capacità di eseguire analisi sulle vulnerabilità emerse, in particolare quelle sistemistiche e applicative, e di proporre contromisure adeguate per mitigare e risolvere i problemi
- Capacità di eseguire le attività tecniche secondo gli standard e le metodologie richieste
- Capacità di controllare e coadiuvare le azioni di rientro a seguito di eventi, incidenti e generici gap di sicurezza
- Supporto a Security Analyst e il Security Architect nella ricerca di soluzioni appropriate
- Realizzazione reportistica dei risultati raggiunti nell'ambito dei diversi interventi di cui è responsabile
- Conoscenza della normativa in materia di trattamento dei dati e privacy