



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: <https://www.nais.ai/it>

Breve descrizione dell'azienda: Nais, fondata a Torino nel 1998, specializza infrastrutture IT per difesa 24/7 da cyber-attacchi per aziende medie e grandi. Il suo Cyber Fusion Center combina Cybersecurity e AI, posizionandola come leader nazionale. Offre servizi di eccellenza in IT e Cybersecurity grazie a un team di 100 esperti e Competence Center avanzati.

Ruolo previsto in azienda per il candidato: Stiamo cercando un/una Technical Account Manager (TAM) Junior che sarà il punto di riferimento tecnico e relazionale per i clienti assegnati sui servizi di Security Operations Center.

Il/la candidato/a avrà la responsabilità di garantire la qualità del servizio erogato, presidiare le esigenze del cliente e assicurare l'evoluzione continua delle soluzioni SOC, operando come interfaccia tra cliente, SOC, Service Manager e team tecnici interni.

Il ruolo richiede una forte combinazione di competenze tecniche, capacità di governance del servizio e attitudine consulenziale.

Area aziendale a cui afferisce il candidato: Security Operation Center

Profilo richiesto:



- 1 anno di esperienza in ambito cybersecurity, SOC o IT infrastrutturale oppure formazione in discipline tecniche (Informatica, Ingegneria, Cybersecurity) con forte interesse per il ruolo
- Conoscenza base di concetti di sicurezza informatica (SIEM, incident response, networking, firewall, ecc.)
- Buone capacità analitiche e organizzative
- Ottime doti comunicative e relazionali
- Attitudine consulenziale e orientamento al cliente
- Interesse a crescere in un ruolo ibrido tecnico-relazionale
- Buona conoscenza della lingua inglese
- Scripting in Python

Soft skills:

- Curiosità tecnica: voglia di approfondire e comprendere i meccanismi della sicurezza informatica.
- Orientamento al cliente: capacità di ascolto e comprensione delle esigenze.
- Responsabilità e proattività: desiderio di mettersi in gioco.
- Team working: collaborazione costante con figure tecniche e di delivery

Ruoli con cui il candidato dovrà interfacciarsi: Responsabili IT dei nostri clienti

Competenze che il candidato raggiungerà alla fine del percorso formativo:

- Gestione tecnica dei clienti in ambito SOC, garantendo continuità, qualità e miglioramento del servizio
- Supervisione dei servizi SOC erogati (monitoraggio, incident handling, escalation)
- Coordinamento tecnico in caso di incidenti critici e gestione delle escalation
- Conduzione di meeting periodici (SAL, QBR) con il cliente, con presentazione di KPI e reportistica



- Analisi dei trend di sicurezza e proposta di improvement plan
- Supporto nell'evoluzione delle architetture SOC (SIEM, SOAR, XDR, ecc.)
- Collaborazione con il team commerciale per attività di upselling e cross-selling tecnico
- Raccolta requisiti e definizione di use case di monitoraggio personalizzati
- Supporto alla definizione di playbook e processi di risposta agli incident