Dipartimento
Management
"Valter Cantino"

UNIVERSITÀ
DI TORINO

SAA
School of Management

Alta formazione in Apprendistato a.a. 2025/26

Master in
CYBERSECURITY
www.mastercybersecuritytorino.it

Dati dell'impresa

Ragione Sociale: N&C S.p.A.

Sede Azienda: Orbassano (TO)

Sito web azienda: https://www.nectlc.com/

Breve descrizione dell'azienda:
N&C S.p.A. è un System Integrator italiano fondato nel 1982 a Veglie (LE), specializzato nella progettazione, realizzazione e gestione di soluzioni ICT integrate.

Nel corso degli anni, l'azienda ha consolidato la propria presenza sul territorio nazionale, sviluppando una rete di sedi in diverse città italiane, tra cui Roma, Torino, Napoli, Bologna e Milano, e ampliando la propria presenza anche a livello internazionale.

N&C opera in diversi ambiti tecnologici, tra cui Cybersecurity & Security, IT System & Cloud, Networking, Software e AI, Managed Services, Cabling & Infrastructure, Data Center e Digital Workspace & Collaboration, offrendo soluzioni integrate a supporto dei processi di innovazione e trasformazione digitale di aziende private e Pubbliche Amministrazioni.

Ruolo previsto in azienda per il candidato:
Il candidato sarà inserito nel Team Cyber Security con il ruolo di **Junior Cyber Security Analyst** e si occuperà di:

- Monitoraggio degli eventi e degli alert di sicurezza attraverso strumenti SIEM, EDR/XDR e SOAR.
- Supporto nell'analisi degli alert e nell'identificazione di potenziali minacce informatiche.

- Collaborazione nelle attività di gestione e classificazione degli incidenti di sicurezza, contribuendo alle fasi di analisi, escalation e risposta.
- Supporto nella raccolta e nell'analisi dei log provenienti da sistemi e infrastrutture IT.
- Supporto nella predisposizione di report e dashboard relativi agli eventi di sicurezza e alle attività di monitoraggio.

È previsto un percorso di formazione e affiancamento on the job, finalizzato allo sviluppo progressivo delle competenze tecniche e dell'autonomia operativa.

Modalità di lavoro: è previsto lo smart working per 2 giorni alla settimana.

Area aziendale a cui afferisce il candidato:
SOC - Security Operations Center Team

Profilo richiesto:
Il profilo ideale è un candidato interessato ad approfondire il mondo della Cyber Security, motivato a sviluppare competenze tecniche nell'ambito del monitoraggio e della gestione degli eventi di sicurezza informatica.
È preferibile una laurea in Informatica, Ingegneria Informatica, Cyber Security o discipline affini.
Sono considerate preferenziali:

- Conoscenze di base di reti informatiche, protocolli TCP/IP e sistemi operativi.
- Familiarità con i principi fondamentali della sicurezza informatica e delle principali minacce cyber.
- Conoscenze introduttive di strumenti SIEM, EDR/XDR e analisi dei log.
- Eventuali esperienze formative, progetti universitari, tirocini o certificazioni in ambito Cyber Security.
- Buona conoscenza della lingua inglese, preferibilmente almeno a livello B2.

Non è richiesta una consolidata esperienza professionale: il percorso è rivolto a profili junior interessati a crescere attraverso la formazione e l'esperienza sul campo.

Soft skills:

- Capacità di analisi e problem solving;
- Capacità di organizzare le attività e gestire le priorità.
- Precisione e attenzione al dettaglio;
- Capacità di lavorare in team;
- Buone capacità comunicative e relazionali;
- Curiosità, interesse e attitudine all'apprendimento continuo;
- Proattività, affidabilità e senso di responsabilità;

Ruoli con cui il candidato dovrà interfacciarsi:
Il candidato collaborerà principalmente con i Cyber Security Analyst e gli altri professionisti del Team SOC, confrontandosi con figure tecniche specializzate nella gestione delle infrastrutture e dei servizi di sicurezza informatica.
In funzione delle attività e dei progetti, potrà inoltre interfacciarsi con il Project Manager, il Service Manager, i referenti tecnici delle infrastrutture IT e i referenti dei clienti.

Competenze che il candidato raggiungerà alla fine del percorso formativo:
Al termine del percorso, il candidato avrà acquisito competenze di base e operative nell'ambito della Cyber Security, con particolare riferimento alle attività di monitoraggio, analisi e gestione degli eventi di sicurezza informatica.