Alta formazione in Apprendistato a.a. 2025/2026

Master in
CYBERSECURITY
www.mastercybersecuritytorino.it

Dati dell'impresa

Ragione Sociale: **NEXT G CLOUD TECHNOLOGIES S.R.L.**

Sede Azienda: Torino, Via Garibaldi 18/4, 10122

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

Breve descrizione dell'azienda: Next G Cloud Technologies S.r.l. è una società innovativa con sede a Torino specializzata nello sviluppo di soluzioni cloud sicure, sovrane e orientate ai settori regolamentati. L'azienda supporta imprese e organizzazioni nella protezione dei carichi di lavoro mission-critical attraverso tecnologie avanzate di cloud computing, cybersecurity, confidential computing, edge computing e architetture cloud di nuova generazione. La proposta di valore si basa sui principi di Security by Design, conformità normativa e sovranità del dato, con soluzioni progettate per favorire l'aderenza a normative come GDPR, NIS2, DORA e AI Act europeo. Next G Cloud promuove un approccio modulare e interoperabile, offrendo servizi gestiti che consentono alle aziende di mantenere il controllo delle proprie infrastrutture e dei propri dati, garantendo al contempo elevati standard di sicurezza, flessibilità e preparazione alle sfide tecnologiche future.

Ruolo previsto in azienda per il candidato: Junior Cyber Security Architect, inserito nel Dipartimento IT & TECH a supporto dei Senior Architect. Mansioni e responsabilità principali:

- Supporto architetturale alla progettazione e implementazione di architetture di sicurezza cloud ibride e multi-cloud (AWS, Azure, Google Cloud).
- Supporto all'implementazione e alla gestione operativa di tecnologie di sicurezza: Identity and Access Management (IAM), crittografia, firewall e sistemi SIEM.
- Attività di vulnerability e risk management: valutazione dei rischi, threat modeling e analisi delle vulnerabilità sulle infrastrutture dei clienti.
- Adozione di un approccio DevSecOps, integrando controlli di sicurezza nei processi di sviluppo e deployment (CI/CD) in collaborazione con cloud engineer, team DevOps e IT.
- Contributo alla stesura di policy e documentazione tecnica per la conformità normativa (GDPR, NIS2, SOC2, HIPAA) e agli standard di settore (ETSI, GSMA, CAMARA, CRA).
- Aggiornamento continuo su threat intelligence, strumenti e framework cloud-native.

Smart working: previsto, con modalità di lavoro flessibile/ibrido e base a Torino.

Area aziendale a cui afferisce il candidato: Dipartimento IT & TECH

Profilo richiesto: Laurea (Triennale o Magistrale) in Informatica, Sicurezza Informatica/Cybersecurity, Ingegneria o discipline affini. Esperienza di 1–3 anni (inclusi stage o progetti accademici rilevanti) in ambito sicurezza informatica o cloud engineering. Comprensione dei principi fondamentali di cybersecurity e dei principali framework (NIST, CIS, ISO 27001); conoscenza di base di almeno una piattaforma cloud (AWS, Azure, GCP) e dei relativi servizi di sicurezza; familiarità con protocolli di rete, RESTful API e sicurezza applicativa. Ottima padronanza dell'italiano e buona conoscenza dell'inglese tecnico. *Titoli preferenziali:* esperienza con Infrastructure as Code (Terraform, Ansible), Docker e Kubernetes; certificazioni di settore (AWS Certified Security Specialty,

Azure Security Engineer Associate o equivalenti); conoscenze di base su Kernel Linux/eBPF, Confidential Computing, Incident Response, Cloud Forensics o modelli Zero Trust; partecipazione a progetti di ricerca europei/nazionali.

Soft skills: Forte propensione all'apprendimento continuo, curiosità tecnologica e mentalità critica e analitica; attitudine al problem-solving e attenzione ai dettagli in contesti complessi; capacità di lavorare in team interfunzionali e di comunicare tematiche tecniche in modo chiaro; proattività e adattabilità in un settore in rapida evoluzione.

Ruoli con cui il candidato dovrà interfacciarsi: Team IT

Competenze che il candidato raggiungerà alla fine del percorso formativo: Al termine del percorso il candidato sarà in grado di progettare e contribuire autonomamente all'implementazione di architetture di sicurezza cloud ibride e multi-cloud, gestire operativamente i principali strumenti di sicurezza (IAM, crittografia, firewall, SIEM), condurre attività di threat modeling, risk assessment e vulnerability analysis, applicare metodologie DevSecOps all'interno di pipeline CI/CD e garantire la conformità a normative e standard di settore (GDPR, NIS2, SOC2, ISO 27001), acquisendo le basi per evolvere verso un ruolo di Security Architect senior.