Alta formazione in Apprendistato a.a. 2022/2023

Master in
CYBERSECURITY
www.mastercybersecuritytorino.it

Dati dell'impresa

Ragione Sociale: Security Reply Srl con Socio Unico

Sede Azienda: Torino (TO)

Sito web azienda: https://www.reply.com/spike-reply

Ruolo previsto in azienda per il candidato:

Spike Reply è la società di cybersecurity del Gruppo Reply specializzata in SECURITY ADVISORY, SYSTEM INTEGRATION e OPERATIONS, che fornisce servizi completi di consulenza e soluzioni integrate.
La nostra missione è supportare i nostri clienti nell'applicazione di metodologie e strumenti di sicurezza in tutte le diverse fasi del percorso di trasformazione digitale, proteggendoli dagli attacchi informatici attraverso metodi avanzati e innovativi per identificare e analizzare rischi, vulnerabilità e minacce.
Questo approccio consente alle aziende di migliorare il proprio livello di sicurezza continuando a operare in condizioni ottimali.

Il portafoglio dei servizi di sicurezza di Spike Reply è in continua evoluzione per garantire una protezione completa, senza alcun vincolo sulle tecnologie in gioco. Il candidato dovrà confrontarsi con uno o più dei temi seguenti:

- SICUREZZA DEL CLOUD
- SICUREZZA INDUSTRIALE E IOT
- SICUREZZA DELLE RETI E DELLE INFRASTRUTTURE
- SICUREZZA DELLE APPLICAZIONI (es. DEVSECOPS)
- GESTIONE DELLE IDENTITÀ E DEGLI ACCESSI
- DATA SECURITY
- GOVERNANCE, RISCHIO E COMPLIANCE

- VALUTAZIONE E TEST DI SICUREZZA
- AUTOMOTIVE CYBERSECURITY

Profilo richiesto:
Il candidato ideale di Spike Reply deve avere la passione e la voglia di approfondire le tematiche di Cyber Security, una buona padronanza della lingua inglese e uno spirito innovativo e curioso. Il candidato ideale è in possesso di una laurea in Informatica, Telecomunicazioni, Gestionale o CyberSecurity.

Competenze che il candidato dovrà aver raggiunto alla fine del percorso formativo:
Il candidato, al termine del percorso formativo in CyberSecurity, conoscerà:

- le principali minacce informatiche e i relativi impatti sul business;
- le best practice per proteggere i sistemi aziendali e i relativi dati;
- le soluzioni tecnologiche principali (es. WAF/IPS/DAMP, PKI/HSM, S-IoT, SASE, EDR, DLP etc.)
- le dinamiche della sicurezza applicate in contesti aziendali ampi e strutturati (es. Metodologia DevSecOps, Anti-Fraud Systems, Data Loss Prevention & Encryption, Supply Chain & Manufacturing Security, Connected Vehicles, etc.)

Imparerà a conoscere le dinamiche di business (es. riferite ai clienti Automotive, Manufacturing, Finance, Utilities) e i relativi processi per gestire progetti complessi di sicurezza informatica.

Il candidato imparerà anche a integrarsi con un team di lavoro di esperti di Cyber Security dove potrà condividere esperienza e problematiche, potrà acquisire la capacità della gestione delle priorità e della condivisione dei risultati.