



Alta formazione in Apprendistato a.a. 2020/2021

Master in CYBERSECURITY
www.mastercybersecuritytorino.it

Dati dell'impresa

Ragione Sociale: Security Reply Srl con Socio Unico

Sede operativa: Torino (TO)

Sito azienda: <https://www.reply.com/spike-reply>

Ruolo previsto in azienda per il candidato:

Spike Reply è la società del Gruppo Reply focalizzata sulla cybersecurity e sulla protezione dei dati personali. La sua missione è quella di salvaguardare i valori e la privacy delle persone, delle aziende e dei processi al fine di sostenere la crescita di un mondo digitale globale attraverso l'innovazione. Riservatezza, integrità e disponibilità dei sistemi sono priorità assolute. Insieme ai suoi partner e senza alcun vincolo sulle tecnologie in gioco, l'azienda fornisce servizi di consulenza per aiutare le imprese a sviluppare una cultura orientata alla sicurezza.

Il portafoglio dei servizi di sicurezza di Spike Reply è in continua evoluzione per garantire una protezione completa e il candidato dovrà confrontarsi con uno o più dei temi seguenti:

- SICUREZZA DEL CLOUD
- SICUREZZA INDUSTRIALE E IOT
- SICUREZZA DELLA RETE E DELL'INFRASTRUTTURA
- SICUREZZA DELLE APPLICAZIONI (es. DEVSECOPS)
- GESTIONE DELLE IDENTITÀ E DEGLI ACCESSI
- DATA SECURITY
- GOVERNANCE, RISCHIO E COMPLIANCE



- VALUTAZIONE E TEST DI SICUREZZA
- AUTOMOTIVE CYBERSECURITY

Lauree preferenziali:

Informatica, Telecomunicazioni, Gestionale e CyberSecurity

Profilo richiesto:

Il candidato ideale di Spike Reply deve avere la passione e la voglia di approfondire le tematiche di Sicurezza Informatica, una buona padronanza della lingua inglese e uno spirito innovativo e curioso.

Competenze che il candidato dovrà aver raggiunto alla fine del percorso formativo:

Il candidato, al termine del percorso formativo in CyberSecurity, conoscerà:

- Le minacce informatiche e le loro conseguenze;
- le best practice per proteggere una rete aziendale e i suoi 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.