Alta formazione in Apprendistato a.a. 2022/2023

Master in
INNOVAZIONE DIGITALE E LEGAL COMPLIANCE
www.masterlegalinnovation.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 specializzata in SECURITY ADVISORY, SYSTEM INTEGRATION e OPERATIONS, che fornisce servizi completi di consulenza e soluzioni integrate.
Supportiamo i nostri clienti nell'applicazione di metodologie e strumenti di sicurezza pervasivi in tutte le diverse fasi del percorso di trasformazione digitale, proteggendo le organizzazioni 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:

- Disegno, implementazione e mantenimento di sistemi di gestione di Information Security, Cybersecurity e Data Protection in linea con i principali standard e normative pertinenti (e.g. ISO/IEC 27001, NIST CSF, ISO/SAE 21434, TISAX, ...)
- Supporto nel raggiungimento della conformità a standard e normative
- Definizione di policy, line guida, procedure in ambito cybersecurity
- Sviluppo di proposte di formazione e sensibilizzazione sulle tematiche di cybersecurity
- Coordinamento e gestione di progetti di cybersecurity

Profilo richiesto:

Il candidato ideale di Spike Reply deve avere la passione e la voglia di approfondire le tematiche di Cyber Security anche da un punto di vista tecnico, una buona padronanza della lingua inglese e uno

spirito innovativo e curioso. Il candidato ideale è in possesso di una laurea in Informatica o ingegneria, quali ingegneria informatica, 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;
- gli standard e le best practice per proteggere i sistemi aziendali e i relativi dati;
- le principali normative di riferimento;
- le principali dinamiche della sicurezza applicate in contesti aziendali ampi e strutturati (es. Supply Chain & Manufacturing Security, Risk management, business resilience, 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.