Alta formazione in Apprendistato a.a. 2021/2022

Master in CYBERSECURITY
www.mastercybersecuritytorino.it

Dati dell'impresa

Ragione Sociale: Shielder Srl

Sede Azienda: Pinerolo (TO)

Sito web azienda: https://www.shielder.it

Ruolo previsto in azienda per il/la candidato/a:
Il/La candidato/a verrà inserito/a all'interno del *team* di *Offensive Security* di Shielder.

Il *team* si occupa di diverse attività, tra le quali:

- *Web Application Penetration Test*
- *Mobile Application Penetration Test*
- *Embedded Systems Penetration Test*
- *Hardware Penetration Test*
- *Secure Code Review*
- *Red Teaming Operations*

Shielder ha come visione quella di diventare una *boutique* nell'ambito della *CyberSecurity*, di conseguenza è alla ricerca costante di talenti da integrare nel proprio *team* e cerca di supportare le propensioni personali dei componenti dello stesso, supportandoli con tutti i propri strumenti. Nel tentativo di raggiungere al meglio questo obiettivo la risorsa sarà inserita su attività che rispecchino i suoi interessi.

La risorsa potrà inoltre godere su richiesta di momenti dedicati alla ricerca, durante i quali potrà cercare nuove classi di vulnerabilità, vulnerabilità in

servizi critici o di largo utilizzo, sviluppare *tool* per automatizzare fasi dei test, ecc. Maggior informazioni sull'impegno dell'azienda in attività di ricerca possono essere trovate nella sezione *Advisory* (https://www.shielder.it/advisories/) e *Blog* (https://www.shielder.it/blog/) del sito aziendale.

Profilo richiesto:
Il/la candidato/a ideale si emoziona a ogni *core dump*, comunica solo con persone di cui ha la chiave pubblica, ordina il piatto -1'or(user())like/**/0x7225-- quando va a mangiare sushi e gli avanza sempre una vite.

Costituiscono elementi preferenziali:

- Partecipazione a competizioni di tipologia *Capture the Flag* (CTF);
- Pubblicazioni di *tool* orientati al mondo dell'*offensive security*;
- Qualsiasi esperienza comprovabile (*bug hunting*, *blog post*, certificazioni) attinenti.
- Ottima padronanza della lingua inglese parlata e scritta.

Competenze che il/la candidato/a dovrà aver raggiunto alla fine del percorso formativo:
Il/la candidato/a acquisirà competenze di *Offensive Security* in linea con lo stato dell'arte, non solo sulle principali tecnologie, ma anche su quelle moderne (cloud, linguaggi di programmazioni *memory-safe*, classi di vulnerabilità meno note, ecc.). Tali competenze potranno essere usate per costruire una carriera da *Penetration Tester*, *Security Engineer*, *Security Researcher*.

Diverse opportunità di confronto con esperti del settore e clienti in diversi settori (Digitale, Telecomunicazioni, Finanziario, ecc.) permetteranno al/alla candidato/a di migliorare le proprie *soft-skill* e di sperimentare opportunità, difficoltà e scenari stimolanti.