Alta formazione in Apprendistato a.a. 2022/2023

Master in CYBERSECURITY
www.mastercybersecuritytorino.it

Dati dell'impresa

Ragione Sociale: DBLC S.r.l.
Sede Azienda: Torino (TO)
Sito web azienda: https://www.dblc.it

Ruolo previsto in azienda per il candidato:
La risorsa verrà inserita in un nuovo team aziendale di Cybersecurity e parteciperà alla creazione di un SOC (Security Operation Center), svolgendo attività di monitoraggio e analisi di primo livello SOC con l'utilizzo delle più importanti piattaforme tecnologiche di sicurezza, tra cui Microsoft 365 Defender e Microsoft Sentinel. Imparerà a gestire tecnologie quali EDR/XDR (endpoint detection response, e extended detection and response) e SIEM (Security information and event management) al fine di monitorare, analizzare, prevenire e contrastare attacchi informatici.

In particolare, la risorsa si occuperà di diverse attività, tra le quali:
- Attività di progettazione, implementazione e configurazione, di soluzioni di sicurezza utilizzate presso i clienti attraverso tecnologie Microsoft e altri vendor alternativi
- Attività di Risk, Threat and Vulnerability Assessment (EDR/XDR, SIEM, IPS, WAF, Firewall, Cloud Security) che portino alla creazione di procedure di security conformi con gli standard e le policy di settore quali ISO27001 e GDPR
- attività di Penetration Test su web, infrastrutture e applicazioni, con l'obiettivo di identificare vulnerabilità applicative, vulnerabilità delle reti e dei sistemi.
- Attività di Triage di primo livello SOC, attraverso le tecnologie Microsoft e alternative
- Attività di Incident Response e Forensic, ovvero analisi forense sugli alert e incident rilevati dalle piattaforme, reverse engineering, IOC e remediation.
- Attività di Threat Intelligence
- Attività di formazione (security awarness)

Profilo richiesto:
Di seguito indicazione del profilo richiesto:
- Laurea in Informatica o Ingegneria Informatica;
- Buona conoscenza della lingua inglese (ottima conoscenza costituirà un plus)
- Passione per la Cybersecurity e forte attitudine alla curiosità verso le tematiche collegate
- Costituisce titolo preferenziale pregressa conoscenza o esperienza in ambito System e Network Administration: Microsoft Active Directory, networking, router, firewall (IPS/IDP/WAF), switch, bilanciatori

Competenze che il candidato dovrà aver raggiunto alla fine del percorso formativo:
- Conoscenza dei principali standard di riferimento (ISO27001, ITIL, NIST, GDPR, etc.)
- Conoscenza delle principali metodiche, tecnologie e capacità di progettare ed eseguire attività inerenti risk, threat and vulnerability management
- Conoscenza e capacità di analisi e implementazione procedure di security, gestione incidenti, security e privacy assessment
- Conoscenza e capacità di implementare attività di vulnerability assessment e penetration test
- Capacità di gestire e attuare attività di triage, incident response e forensic, threat intelligence.