Alta formazione in Apprendistato a.a. 2023/2024

Master in
CYBERSECURITY
www.mastercybersecuritytorino.it

Dati dell'impresa

Ragione Sociale: HWG Sababa srl

Sede Azienda: Milano
Sede Operativa: Torino

Sito web azienda:www.hwgsababa.com

Breve descrizione dell'azienda: HWG Sababa è un provider di cybersecurity che offre una suite completa di soluzioni strategiche di sicurezza, servizi gestiti e consulenza.
Orgogliosamente "Made in Italy", l'azienda opera a livello globale in oltre 20 Paesi, proteggendo le infrastrutture digitali di organizzazioni che operano in vari settori – tra cui finance, banche centrali, energy & utilities, infrastrutture critiche, automotive, fashion e telco – e fornendo supporto lungo l'intera catena del valore.

Ruolo previsto in azienda per il candidato:

- Supporto alle attività di Governance della Compliance di Information Security (PCI-DSS, ISO 27001)
  - Gestione richieste utenze privilegiate (anche a fini norma Amministratori di Sistema)
  - Revisione utenze e profili di operatività utenti privilegiati ADS
  - Gestione attività di formazione ed awareness Cyber Security e Amministratori di Sistema (gestione dei corsi, proposta nuovi corsi, mail di awareness, campagne di simulazione phishing)
  - Predisposizione, aggiornamento e revisione policy, procedure e linee guida di Information Security e Cyber Security (l'azienda sta portando avanti una iniziativa di certificazione ISO 27001)
  - Analisi del rischio GDPR e ISO 27001
  - Valutazione soluzioni di supporto alla Governance
- Supporto alle attività di Governance di Cyber Security
  - Vulnerability Management (monitoraggio vulnerabilità, supporto alla remediation)
  - Verifica delle attività di Penetration Testing e delle relative attività di remediation infrastrutturale e applicativa
  - Verifica delle segnalazioni di eventi di Sicurezza (phishing, data breach, falsi positivi, anomalie)

- Verifica attività anomale e segnalazioni su piattaforma SIEM
- Valutazione dell'adeguatezza dei fornitori (sulla base della Checklist Cyber Security)
- Verifica di adeguatezza delle misure di sicurezza previste per nuovi progetti (o aggiornamenti di piattaforme preesistenti)
- Valutazione nuove soluzioni di Cyber Security
- Categorie di strumenti utilizzati: vulnerability management, email protection, network traffic anomaly detection, piattaforma SIEM per threat e anomaly detection, XDR, strumenti di pentesting, cloud security posture management, external surface monitoring

Area aziendale a cui afferisce il candidato: Offence/Defence

Profilo richiesto:

- Competenze tecniche su IT e Cyber Security (derivanti da percorsi di studio quali Scienze dell'Informazione, Ingegneria Informatica, etc)
- Mente brillante, curiosità e voglia di imparare
- Buona conoscenza dell'inglese

Competenze che il candidato raggiungerà alla fine del percorso formativo:

fornisce al partecipante una overview molto ampia e ricca delle tematiche di Information Security e Cyber Security