Alta formazione in Apprendistato a.a. 2021/2022

Master in CYBERSECURITY
www.mastercybersecuritytorino.it

Dati dell'impresa

Ragione Sociale: Security Reply Srl con Unico Socio

Sede Azienda: Torino (TO)

Sito web azienda: http://www.communicationvalley.it

Ruolo previsto in azienda per il candidato:
Il candidato ideale andrà a ricoprire un ruolo di Cybersecurity Analyst nel contesto del Cyber Security Operation Center di Communication Valley Reply.
Dopo un periodo di affiancamento iniziale in modalità training on the job, il profilo in questione sarà inserito nel team di Tier1 che opera su turnistica H24 all'interno del CSOC ed il ruolo affidato prevedrà attività di monitoraggio, identificazione e analisi di attacchi attraverso l'utilizzo dei principali tool di detection e correlazione (es. SIEM). Successivamente all'identificazione delle minacce, in base al livello di maturità ed esperienza sulle singole tecnologie, potrà essere inoltre previsto il supporto ai team specialistici per supportare le fasi successive di contenimento e risposta agli incidenti informatici.

Profilo richiesto:

- Laurea in informatica, sicurezza informatica, scienze e tecnologie informatiche, Ingegneria Informatica o delle Telecomunicazioni.
- Buona conoscenza della lingua inglese scritta e parlata.
- Conoscenza di concetti fondamentali di Networking (es. TCP/IP e protocolli) e delle principali metodologie e tecniche di attacco in ambito Cyber.

- Forte capacità di problem solving e spiccata passione e curiosità per i temi di Sicurezza Informatica

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

Il candidato dovrà raggiungere l'autonomia nelle attività di analisi di attacchi informatici grazie all'ausilio di tecnologie SIEM e principali strumenti di monitoraggio e protezione in ambito CyberSecurity .

Nello specifico, si elencano a seguire le competenze attese al termine del percorso formativo:

1. conoscenza delle tecniche e metodologie di analisi di attacchi di sicurezza, che includano la correlazione ed approfondimento di eventi critici, analisi ed individuazione di IOC, una corretta classificazione e prioritizzazione degli incidenti.
2. conoscenza delle principali soluzioni di sicurezza e tecnologie a supporto;
3. conoscenza dei sistemi di Security Monitoring e dei principali tool a supporto (EDR , Antispam, AV, etc.);
4. capacità di tuning delle soluzioni di Security Monitoring, ed in particolare delle regole di correlazione eventi;
5. conoscenza delle principali componenti di Network Security, in particolar modo firewall e IDS/IPS;
6. conoscenza di tecniche e metodologie OSINT in ambito Cyber;