



**Alta formazione in Apprendistato a.a. 2021/2022**

**Master in CYBERSECURITY**  
[www.mastercybersecuritytorino.it](http://www.mastercybersecuritytorino.it)

**Dati dell'impresa**

**Ragione Sociale: Cybertech S.R.L.**

**Sede azienda: Torino**

**Sito azienda: <https://www.cybertech.eu/>**

**Ruolo previsto in azienda per il candidato: Analista SOC I° livello**

**Lauree preferenziali: Ing. Informatica, Informatica, Laurea Magistrale in Cyber Security.**

**Profilo richiesto:**

Analista SOC I livello

**Compiti**

Inserito in turnistica H24, svolge attività di monitoraggio e analisi di I° livello SOC con l'utilizzo di piattaforme SIEM (Security information and event management) al fine di prevenire attacchi informatici.

Sotto la supervisione del Team Coordinator:

- esegue modifiche ordinarie e straordinarie alle configurazioni dei sistemi gestiti;
- effettua interventi manutentivi e evolutivi, iniziative progettuali, campagne di phishing, gestione di problemi e incidenti ed esecuzione di servizi di Vulnerability Assessment.

**Competenze:**

Conoscenze sui principali Sistemi Operativi (Windows, Linux).

Conoscenze relative ai flussi di rete (Networking) e dei principali protocolli utilizzati

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

Conoscenze basi su Sistemi, Networking, Penetration Test. Introduzione all'analisi di I e II livello SOC. Monitoraggio e classificazione degli incidenti o dei potenziali incidenti di sicurezza, analisi



approfondita degli eventi (nonché la correlazione tra gli stessi) nella definizione e conferme relative ad attacchi informatici (o potenziali), falsi positivi, azioni sospette. Introduzione alla fase di escalation verso il gruppo di competenza relativo ad eventi sospetti o incidenti confermati.

La configurazione delle tecnologie di interesse, l'installazione di upgrade o patch, o la redazione di report di eventi di sicurezza.

Buona conoscenza dell'inglese scritto e parlato.

Conoscenze relative alle infrastrutture e all'architettura orientata alla Security

Conoscenze degli attacchi informatici più comuni e frequenti (Penetration Test)

Conoscenze relative ai principali tools utilizzati in ambito SOC (SIEM, piattaforme di Threat intelligence e Threat Hunting, Sandbox, ecc.)