

Corso formazione Tecnico Gestore di Reti e Sistemi Digitali

Prerequisiti

I candidati, per la selezione e partecipazione al corso di formazione, dovranno essere in possesso di laurea e/o diploma e che abbiano una conoscenza base dell'ambito IT e conoscenza della lingua inglese.

Obiettivi

Il piano di formazione oggetto del presente documento è orientato a fornire ai candidati le competenze necessarie al fine di poter essere introdotti in un ambito lavorativo per la gestione delle tematiche di sicurezza legati ad un contesto infrastrutturale/logico/applicativo complesso.

Come durata complessiva l'intero percorso formativo prevede:

- **280 ore** di sessioni teoriche e pratiche inerenti ai moduli oggetto della seguente proposta
- **320** di stage "*learning by doing*" in azienda.

Modulo 1 – Cenni di Networking

Contenuti:

Elementi fondamentali

Dispositivi di Rete

Protocolli di Rete

Implementazioni Architetture

Sicurezza & Troubleshooting

Modulo 2 – Introduzione ai Sistemi Linux

Contenuti:

Fondamenti dei Sistemi Linux

- Architettura del Sistema Operativo Linux
- Comandi Principali dei sistemi Linux

Sicurezza dei Sistemi Linux

- Firewalling nei Sistemi Linux
- Hardening dei Sistemi Linux

Modulo 3 – Introduzione ai Sistemi Windows

Contenuti:

Fondamenti dei Sistemi Windows

- Architettura del Sistema Operativo Windows
- Configurazione Active Directory e servizi accessori

Sicurezza dei Sistemi Windows

- Firewalling nei Sistemi Windows
- Hardening dei Sistemi Windows

Modulo 4 – Introduzione agli ambienti Cloud

Contenuti:

Introduzione agli ambienti Cloud

- Presentazione dei principali ambienti Cloud
- Utilizzo dei servizi principali nel cloud Amazon AWS

Sicurezza degli ambienti Cloud

- Network Security nel cloud Amazon AWS
- Utilizzo dei *Security Group* & NACL

Modulo 5 – Firewalling

Contenuti:

Local Firewalling

- Firewalling nei Sistemi Linux
- Firewalling nei Sistemi Windows

Network Firewalling

- Modalità di installazione di un firewall
- Configurazioni di base
- NAT & Traffic Shaping
- Failover & Load Balancing
- Web Proxing

- **NIDS/NIPS**

Cloud Firewalling:

- **Tecniche di Firewalling negli ambienti Cloud**
- **Configurazione e utilizzo di un firewall nel Cloud**

Modulo 6 – Blue Teaming (Defensive Security)

Contenuti:

Defensive Hardware & Software

Cyber-attacks – Analysis

Cyber-attacks – Mitigation

Malware Analysis

Alert Analysis

Data Breach Management

MITRE ATT&CK® analysis

Modulo 7 – Red Teaming (Offensive Security)

Contenuti:

Layer 2 Attacks

Layer 3-4 Attacks

Layer 7 Attacks

Cloud Attacks

DDoS Attacks

DevSecOps & Container Attacks

Social Engineering Attacks