**CORSO SOC ANALYST JUNIOR I° LIVELLO-CYBER SECURITY**

**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 Corso è progettato per aspirare a divenire un analista di I° Livello. Ha l’obiettivo di fornire le competenze necessarie per lavorare in un Security Operations Center.

Il Corso copre i fondamenti delle diverse operazioni di un SOC e permette ai partecipanti di apprendere e gestire i vari processi.

Come durata complessiva l’intero precorso formativo prevede:

* **240 ore** di sessioni teoriche e pratiche inerenti ai moduli oggetto della seguente proposta
* **80** **ore** di stage “*learning by doing”* in azienda.

**Tool e ambienti software utilizzati**

* Distribuzioni Linux orientate alla security
* Cisco Packet Tracer (Design e simulazione di reti)
* Wireshark (Analisi di rete, sniffing, scomposizione data frame)
* NMAP (Identificazione Host e analisi dei servizi)
* IP Tables (Creazione e simulazione policy di firewalling)
* Saranno predisposte opportune sessioni *hands-on* su ambienti SIEM, SOAR e IAM le cui piattaforme di riferimento saranno identificate durante lo svolgimento del programma di formazione

**Modulo 1 - Linux OS**

*Obiettivo di questo modulo è fornire le informazioni per installare, configurare e amministrare un sistema Linux. Fornire inoltre una base di preparazione sistemistica orientata ad amministratori di sistema, affrontare problematiche reali, confrontare Linux con altri sistemi operativi e fare diretti riferimenti al mondo Internet.*

**Contenuti:**

**Fondamenti di Linux**

* Introduzione al SO.
* Connessione SSH e cenni di crittografia.
* Comandi Linux.
* Bash scripting.
* User profilig, permissions e attributes.
* Editing e manipolazione di testi.
* Gestione dei processi.
* Gestione aggiornamenti e pacchetti.
* Servizi (SSH, FTP, Apache).

**MODULO 2** – **Infrastrutture di networking**

*Obiettivo di questo modulo e fornire tutte le competenze necessarie a supportare e implementare architetture di sistemi e reti aziendali operativamente sostenibili, altamente disponibili e soprattutto sicure. Verranno forniti gli strumenti per identificare e tradurre i requisiti in un'architettura tecnica completa. Durante tutto il modulo sarà posto sempre un particolare accento nell’ambito dell’identificazione e risoluzione degli incident di sicurezza. Verranno infine illustrate le metodologie di monitoraggio, di misurazione e il reporting delle prestazioni e della capacità dei sistemi aziendali.*

**Contenuti:**

**Foundamentals**

* Networking Basics
* Network Architecture
* TCP-IP/OSI Model
* Comparison Between TCP-IP/OSI Model
* Binary To Decimal Conversion
* Introduction To Ipv6
* Classfull Ip Address
* Introduction To Tcp-Ip First Lvl
* Computer Cables Intoduction
* Unshielded Twisted Pair Cable
* Network Devices Introduction Switch & Router
* Static Routing Theory
* Lab: Configure Static Routing Ipv4

**Routing & switching**

* Administrative Distance
* Dynamic Routing
* Protocol
* Interior Routing Protocol
* Link State
* Basi di Ospf
* Vlan
* Subnet

**Advanced Routing & switching**

* Distance Vector
* Routing Information Protocol
* Introduction To Cisco Packet Tracer
* Lab: Cisco Packet Tracer
* Nat/Pat
* Lab: Vlan Trunking

**Application layer**

* Arp, Icmp, Tcp
* Dns
* Dhcp
* Http/Https
* Ftp/Ftps
* Introduction To Virtualization
* Introduction To Windows
* Lab: Windows Networking

**Principi di network & infrastructure security**

* Computer Security: History
* Computer Security: Principles
* Mobile Security
* Introduction To Cryptography
* Symmetric Cryptography
* Lab: Sym Crypto
* Asymmetric Cryptography
* Lab: Asym Crypto
* Hash Function
* Lab: Hash Function
* Proxy
* Vpn
* Remote Access Vpn
* Site-To-Site Vpn

**Cyber attacks – Analisys**

* Introduzione al *Blue Teaming*
* Sw/Network Vulnerabilities & Threats
* Osi Lvl 2/3: Attacks
* Lab: Lvl 2/3 Attacks
* Dns Attacks
* Lab: Dns Attacks
* Linux Security: Os, Access Control Policy
* Windows Security: Os, Access Control Policy

**Cyber attacks – Mitigation**

* Malware Overview
* Malware Analysis/Threat Hunting
* Tcp/Udp Attacks
* Lab: Tcp/Udp Attacks
* Web Application Attacks
* Lab: Web Applications
* Linux Security: Os, Access Control Policy
* Windows Security: Os, Access Control Policy

**Defensive Hardware & Software - fondamenti**

* Secure Network Infrastructure
* Waf
* Mitigation And Remediation
* Balancer
* Firewall Introduction
* Ids/Ips Introduction
* Piattaforme di *logging* e monitoraggio

**Analisi e trattamento dei Data Breach**

* gdpr introduction and privacy concerns
* risk assessment
* data protection and impact assessment
* dealing with data breaches
* cloud introduction
* cloud security (Backup)
* gdpr: dealing with data in cloud
* penalties for non-compliance
* Configuration, Provisioning & Fine Tuning
* Logging And Advanced Troubleshooting

**MODULO 3** – **Alert Analysis**

*Durante lo svolgimento di questo modulo verranno sviluppati i temi relativi all’analisi di 1° e 2° livello relativamente ai concetti di base della gestione del rischio in un contesto infrastrutturale complesso. Obiettivo è descrivere l’architettura SOC, la tassonomia degli incidenti e illustrare le procedure di gestione degli eventi. Dettagliare i controlli di sicurezza, le logiche di gestione degli incidenti di sicurezza IT e Service Level Agreement (SLA) correlati. Verrà fornita inoltre una panoramica delle policy aziendali in merito a: l’utilizzo corretto delle risorse IT, la navigazione Web, le best practice e DO’s & DONT’s.*

**Contenuti:**

**Protocolli applicativi e porte**

* Tipologia di porte e loro caratteristiche
* Principali protocolli
* Porte note
* IANA
* HTTP/S
* FTP/S
* SSH
* Cenni sul funzionamento e sulla sicurezza della posta elettronica
  + SMTP
  + IMAP\POP3
  + SPF
  + DKIM
  + DMARC

**Strutture dati e piattaforme SO**

* Dati non strutturati in ambiente Windows.
* Elementi di amministrazione e profilazione in ambiente Windows.
* Linux architetture & file system.
* Gestione dati non strutturati in ambiente Linux.
* Elementi di amministrazione e profilazione in ambiente Linux.

**Modello di architettura e ruoli**

* 3-Tiers *architecture model*
* Introduzione alle web application
* Front End
* Back End
* Client
* DataBase
* CMS
* DBMS

**Tipologie di attacchi**

* Malware
* Adware
* Cookies Attacks
* Applications DDos
* Volumetrics DDos
  + DNS Amplification
  + IP Fragmented
  + NTP Amplifications
  + Memcached Amplifications
  + SSDP Amplifications
* Phishing
* SQL Injection
* Cross-site scripting
* Sniffing
* Brute force attack
* User enumeration
* Social engineering
* Remote code execution

**Defensive Hardware & Software**

* Apparati Firewall
* Apparati IDS/IPS
* Antivirus
* ACL
* DMZ
* Proxy
* Balancer
* VPN

**Detection, analysis e Recovery**

* Piattaforme di monitoraggio e supporto (SIEM, SOAR, …)
* Breach and log analysis
* Threat Analysis
* Incident Response
* Ruoli e responsabilità, procedure di escalation e profili di intervento