ITS Group Benelux

Formation – Consultant en cybersécurité

Module 1 - Administration de systèmes en environnements Linux & Windows - 20 jours

- Windows 10/11 - Installation & Administration
- Windows 10/11 - Administration avancée
- Windows Server 2022 - Mise en œuvre & administration
- Infrastructure hybride en entreprise avec Microsoft
- Linux - Mise en œuvre
- Linux – Administration

Module 2- Fonctionnement et configuration basique des réseaux informatiques, des éléments qui les composent et des protocoles les plus courants – 8 jours

- Orienté théorie, présentation générale du modèle OSI, type de réseau, raccordement
- Mix théorie/pratique, couche média détaillé (Ethernet, 802.11, IP, ARP), TP mise en œuvre basique notion d'adressage/routage
- Orienté pratique, présentation d'équipement réseaux, TP routage VLAN
- Orienté Théorie, couche hôte TCP, DNS, SSH, HTTP(S), FTP
- Orienté pratique, Analyse de protocole avec wireshark
- Mix pratique théorie, protégé son réseau, firewall, VPN, isolation, TP VPN & firewall
- Pratique au choix : application des notions vu en explorant DNS64, NAT64 et DoH ou pratique sur des routeur/switch émulé

Module 3 - Fondamentaux en programmation – Python – 6 jours

- Théorie, présentation générale du langage, manipulation avec l'interpréteur, premier programme –
- TP guidé, entrée sortie, opérateur, variables, string, fonctions
- TP guidé, module, fichiers, donné complexe
- TP guidé, Classe Programmation Objet
- TP Use Case, keylogger, gestion des exceptions, logging
- TP Use Case keylogger, lint, effacer ses traces, séparation en classe, unit-test

Module 4 : Introduction au Cloud & à ses services – 3 jours

- Cloud - Solutions Architect
- Cloud - Solutions Architect DevOps – Initiation

Module 5 - Cadre légal & méthodologie – 7 jours

- Présentation des normes les plus courantes - ISO 27001
- Présentation des normes les plus courantes - ISO 27005
- RSSI - Présentation des métiers
- RSSI - Directive EU NIS1-NIS2
- RSSI - Présentation des différents métiers de la cybersécurité par les étudiants aux choix
- RSSI - présentation par des étudiants d'un cas concret de cyberattaque, comprenant une explication détaillée de l'attaque, des lacunes identifiées ainsi que des propositions de mesures de sécurité techniques ou organisationnelles qui auraient pu être mises en œuvre
- Introduction à la gestion de crise IT

Module 6 - Attaques & vulnérabilité courantes – 13 jours

- Cybersécurité - Parcours introductif
- Sécurité - Système & réseaux
- Sécurité - Applications web

Module 7 - Protocoles & outils de sécurisation – 10 jours

- Cryptographie
- PKI
- TLS/SSL
- Firewalls
- Sécurité applicative
- Systèmes de Détection et prévention d'intrusions
- Monitoring de sécurité

Module 8 - Analyse et tests de pénétration – 7 jours

- Hacking & Sécurité - Niveau 1 - Fondamentaux techniques
- Forensic – Fondamentaux

Module 9 - Préparation à la certification Security+ - 5 jours