Defensy

Formation Professionnalisante en Cybersécurité

Programme de 12 semaines I 350 Heures

- ✓ **Cours en ligne**
- ✓ **Certifications**
- ✓ **Formation Pratique**
  50%-75% Travail en Lab

OLiUM

+241-65727230 / 77676725
https://oliumgroup.com
Libreville, Gabon

Defensy

Contexte

La Cybersécurité est devenue une priorité essentielle dans notre société moderne en raison de l'omniprésence des technologies numériques dans tous les aspects de la vie quotidienne, professionnelle et gouvernementale. Parmi les raisons clés qui expliquent son importance, citons entre autre, la protection des données sensibles, l'augmentation des cyberattaques, la sécurité nationale, la protection de la vie privée, la conformité légale et réglementaire.
La réponse nécessite une prise de conscience collective, manadgériale, et une formation continue pour faire face aux cybermenaces.

Ce Que Vous Allez Avoir :

✓ Certifications les plus demandées

Acquisition de compétences applicables à des certifications: Network+, Linux+, Server+, Cloud+, certified Ethical Hacker (CEH),Pentest, CompTIA Security+, CySA+, CASP, PenTest+

✓ Apprentissage Pratique

Formation orientée projet avec utilisation d'outils comme Wireshark, Kali Linux, Metasploit, et plus pour le traitement de cas de sécurité informatique réels

✓ Instructeurs de Qualité

Un accompagnement exclusif et une supervision sur mesure, assurés par des experts de renom en cybersécurité, dotés d'une expérience approfondie et d'une expertise de pointe.

✓ Programme Exhaustif

Un programme complet couvrant les pratiques de gestion de la cybersécurité, incluant les tactiques offensives et défensives, le cadre de cybersécurité du NIST, ainsi que la gestion des événements et des incidents.

OLiUM

Defensy

Objectif de la Formation

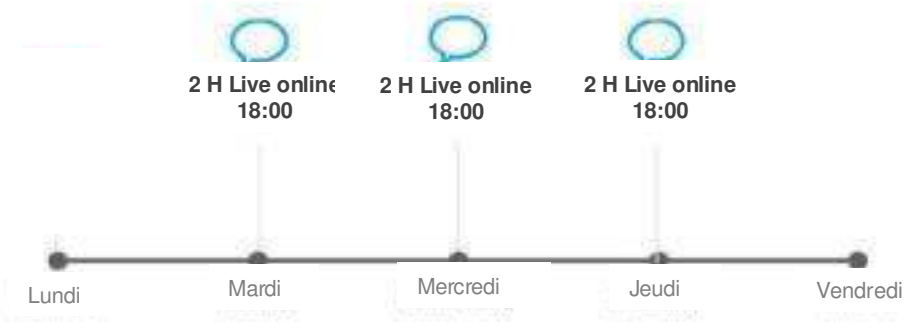
Cette formation, à la fois immersive et de haut niveau, permet aux apprenants de développer leur esprit critique et de renforcer leurs compétences en matière de gestion de l'information, de stratégies et de tactiques pour identifier et gérer les vulnérabilités des systèmes d'information. Ils apprendront à mettre en œuvre des mesures de cybersécurité préventives, défensives et offensives.

À l'issue de cette formation, les apprenants seront capables d'identifier, évaluer, reporter et gérer les risques de sécurité liés aux systèmes d'information et aux technologies.

Liste des certifications

Programme de 12 semaines qui peut être adapté aux besoins spécifiques

Planning de formation en ligne et en présentielle:



Projets et Exercices
20-25h par semaine

Intéraction avec le groupe

Instruction en ligne
6h par semaine

Les horaires et les jours sont flexibles selon le besoin

OLiUM

Defensy

Programme de la Formation

Semaine 1 à 2

Fondamentaux des réseaux

Architecture des réseaux, les modèles OSI, TCP/IP dans l'élaboration d'un réseau, les composantes et topologie des réseaux

Protocoles et infrastructure des réseaux

Principes de sécurité des réseaux: segmentation, isolation IPS/IDS, ACL

Fondamentaux de la sécurité

Concepts fondamentaux des menaces, risque, vulnérabilité et impact, confidentialité, intégrité et disponibilité (CIA)

Types de Cybermenaces: Virus, vers, chevaux de Troie, Phishing, Spear Phishing, Ransmomware et autres logiciels malveillants, attaques par déni de servoce (DoS/DDoS)

Labs:

- Configuration de VM
- Configuration des paramètres réseau
- Scanning des réseaux
- Capture de paquets
- Examen blanc CompTIA Security+

Semaine 3 à 4

Pentesting et Ethique du Hacking

Types et méthodes de Pentest et évaluation de vulnérabilité, process, CVE/CVSS

Définition de la portée, collecte d'information, environnement d'essai

Collecte d'information passive et active, scan de vulnérabilité, recherche en dark web, analyse du réseau

Attaques: service de réseau commun, outils metasploit, attaque des mots de passe, reverse shell (Linux, Windows, Bloodhoud, Wirnm)

Reporting; prises de notes et organisation, structure de rapport et rédaction de vulnérabilité

Labs:

- Exploration de vulnérabilité avec Metasploit
- Réalisation d'un Pentest sur un réseau vulnérable
- Rédaction d'un rapport de Pentest
- Examen blanc CompTIA PenTest+

OLiUM

Defensy

Programme de la Formation

Semaine 5 à 6

Sécurité applications et protection des données

Introduction aux applications web: architecture des applications web, composants des applications, modèles de développement web (MVC, SPA, …)

Utilisation des Proxys web: configuration et utilisation des proxys web (Burp, Suite, OWASP, ZAP), interception et modification des requêtes et réponses, analyses des flux de données

Attaque des applications web

Attaques par téléchargement de fichiers, Attaques côté serveur, Brute forcing des connections

Authentification défaillante, attaque web, inclusion de fichiers, sécurité des sessions, hacking des mots de passe

Labs:

- Analyse de sécurité d'application web avec OWASP ZAP
- Implémentation de mesures de protection des données
- Test d'intrusion sur une API REST

Semaine 7 à 8

Réponses aux incidents et analyse forensique

Détection et gestion des incidents.
Techniques d'analyse forensique : Collecte, préservation, analyse des preuves numériques.
Analyse des malwares et artefacts système.
Considérations légales et éthiques.

Labs:

- Mise en place d'un système SIEM (Elastic Stack ou Splunk).
- Simulation de réponse à un incident de sécurité.
- Analyse forensique sur une machine compromise.
- Examen blanc CompTIA CySa+

OLiUM

Defensy

Programme de la Formation

Semaine 9 à 10

Gestion des risques

Identification, évaluation, et priorisation des menaces.

Techniques de gestion des risques : ISO 27005, FAIR.

Utilisation d'un SIEM pour la surveillance proactive.

Planification de la continuité d'activité

Labs:

- Analyse des vulnérabilités avec Nessus.
- Création d'un plan de gestion des risques.
- Configuration d'un SIEM pour la surveillance des événements
- Projet : Préparation et défense d'un plan de gestion des risques pour une PME
- Examen blanc CompTIA CASP+

Semaine 11 à 12

Réglementation locale en cybersécurité

Exploration des régulations et exigences locales en matière de cybersécurité, en mettant l'accent sur les lois, normes et pratiques de sécurité applicables dans le contexte national.

Labs:

- Analyse de la conformité aux régulations locales.
- Ateliers pratiques sur la mise en œuvre de politiques de sécurité pour respecter les exigences légales.
- Études de cas pratiques concernant la gestion des données sensibles.
- Réponse aux audits de sécurité locaux et préparation de rapports de conformité.