APSI-NE

ASSOCIATION DES PROFESSIONNELS DE LA SÉCURITÉ DE L'INFORMATION DU NIGER

ENSEMBLE POUR UN NIGER PLUS SÛR ET CONNECTÉ

Programme Excellence en Cybersécurité APSI-NE

INTRODUCTION

Dans un contexte où la menace cybernétique ne cesse de croître en Afrique et dans le monde, il est impératif de former des professionnels qualifiés et opérationnels pour faire face à ces défis. Malgré une demande croissante de spécialistes en cybersécurité, l'offre de formation pratique et adaptée aux réalités du terrain reste insuffisante.

L'APSI-NE (Association des Professionnels de la Sécurité de l'Information du Niger) lance donc le programme Excellence en Cybersécurité, une initiative 100% en ligne, afin de combler ce fossé et de répondre aux besoins du marché. Ce programme vise à :

- Offrir aux étudiants et aux professionnels un apprentissage concret des métiers de la cybersécurité.
- Accompagner les talents dans leur insertion professionnelle grâce à un suivi mentoré.
- Permettre une reconversion efficace vers la cybersécurité en six mois avec une attestation de bonne exécution.

L'approche 100% en ligne garantit l'accessibilité à tous, indépendamment des contraintes géographiques, et s'appuie sur des outils interactifs ainsi qu'un mentorat rapproché. Ces programmes sont ouverts aux Nigériens, avec une première promotion de 30 étudiants et 20 professionnels souhaitant se reconvertir.

AXE 1 : PROGRAMME D'OPÉRATIONALISATION (PROJETS DE FIN D'ÉTUDES MENTORÉS)

Ce programme vise à aider les étudiants en fin de cycle à réaliser un projet de fin d'études (PFE) en lien avec un domaine concret de la cybersécurité. L'objectif est de permettre aux apprenants d'acquérir une expertise pratique sous l'encadrement d'experts du domaine.

Thématiques et sujets de PFE (75 sujets par thématique)

SOC (Security Operations Center) et Surveillance des Menaces

1. Implémentation d'une solution SIEM open-source (ex : Wazuh, ELK).
2. Automatisation de la détection des menaces avec SOAR.
3. Analyse des attaques courantes sur un SOC : étude de cas.
4. Mise en place d'un honeypot pour la surveillance des menaces.
5. Analyse forensique d'un incident de cybersécurité.
6. Gestion des logs et corrélation des événements de sécurité.
7. Réponse à incident : élaboration d'un playbook opérationnel.
8. Implémentation de MITRE ATT&CK dans un SOC.
9. Etude sur l'impact de l'IA dans les SOC.
10. Simulation d'attaques réelles et réactions du SOC.
11. Surveillance des cybermenaces en temps réel avec Threat Intelligence.
12. Comparaison des différentes solutions SIEM disponibles sur le marché.
13. Détection et analyse des ransomwares en environnement SOC.
14. Sécurisation des environnements OT/SCADA dans un SOC.
15. Gestion des incidents en entreprise : études de cas réels.

Pentesting et Test d'Intrusion

1. Audit de sécurité d'une application web avec OWASP ZAP.
2. Test d'intrusion sur un réseau d'entreprise avec Kali Linux.
3. Exploitation de vulnérabilités sur Active Directory.
4. Sécurisation d'une API REST contre les attaques courantes.
5. Techniques avancées de phishing et contremesures.
6. Utilisation de Metasploit pour des tests d'intrusion.
7. Audit de sécurité sur un système embarqué.
8. Red Teaming : simulation d'une attaque APT.

9. Exploitation de vulnérabilités zero-day en environnement contrôlé.

10. Analyse des failles de sécurité dans les applications mobiles.

11. Pentesting sur les objets connectés (IoT).

12. Évaluation des failles dans les systèmes d'authentification multifactorielle.

13. Attaques sur les infrastructures Cloud et méthodes de protection.

14. Sécurité des réseaux sans fil : tests et recommandations.

15. Étude de la sécurité des smart contracts et blockchain.

Gestion des Risques et Gouvernance

1. Mise en place d'un cadre de gouvernance cybersécurité ISO 27001.
2. Analyse des risques cyber dans une PME.
3. Conception d'un plan de continuité d'activité (PCA/PRA).
4. Etude sur la cyber-résilience des infrastructures critiques.
5. Implémentation d'une politique de gestion des accès et des identités.
6. Sensibilisation à la cybersécurité en entreprise.
7. Cartographie des menaces sectorielles en Afrique.
8. Audit de conformité RGPD/NIST.
9. Analyse des cyberattaques les plus récentes et leurs impacts.
10. Gouvernance de la cybersécurité dans le cloud.
11. Modélisation des menaces dans les systèmes industriels.
12. Évaluation des risques cyber dans le secteur financier.
13. Étude d'impact des cyberattaques sur les infrastructures gouvernementales.
14. Protection des données personnelles et conformité aux normes internationales.
15. Éthique et cybersécurité : enjeux et responsabilités.

DevSecOps et Sécurité des Développements

1. Utilisation des outils SAST et DAST (SonarQube, OWASP ZAP, Snyk) dans les pipelines CI/CD.
2. Sécurisation des conteneurs Docker et Kubernetes.
3. Automatisation des déploiements sécurisés avec Terraform.
4. Audit et conformité avec Open Policy Agent (OPA).
5. Sécurité applicative en amont : pratiques et outils pour éliminer les menaces dès la conception.
6. Expérimentation avec des applications vulnérables comme DVWA pour l'apprentissage.
7. Sécurisation des chaînes CI/CD avec des outils comme GitLab CI/CD et Jenkins.
8. Sécurité des artefacts avec Artifactory et Nexus.
9. Intégration de GitOps et sécurité des configurations avec FluxCD et ArgoCD.
10. Sécurisation des infrastructures cloud AWS avec Terraform.
11. Détection et correction des vulnérabilités dans les infrastructures IaC (Infrastructure as Code).
12. Renforcement des stratégies RBAC (Role-Based Access Control) dans Kubernetes.
13. Sécurisation des secrets et gestion des credentials dans les pipelines DevSecOps.
14. Détection des comportements anormaux dans les environnements DevOps avec ML et IA.
15. Étapes et méthodologie d'accompagnement pour une mise en œuvre réussie de DevSecOps.

Cybersécurité Industrielle et IoT

1. Sécurisation des protocoles industriels (Modbus, OPC-UA, SCADA).
2. Analyse des menaces sur les objets connectés (IoT) et leur impact.
3. Sécurisation des systèmes embarqués et firmware security.
4. Test d'intrusion sur des équipements industriels et IoT.
5. Détection des cyberattaques sur les infrastructures critiques.
6. Protection des réseaux industriels contre les attaques APT.
7. Sécurisation des communications IoT avec TLS et certificats X.509.
8. Évaluation de la conformité des équipements IoT aux normes de cybersécurité.
9. Mise en place d'une architecture Zero Trust pour les infrastructures critiques.
10. Étude des attaques physiques sur les systèmes embarqués et techniques de mitigation.
11. Sécurisation des infrastructures énergétiques (smart grids, centrales électriques).
12. Protection contre les attaques par injection dans les systèmes industriels.
13. Analyse forensique sur les équipements IoT après une cyberattaque.
14. Sécurité des mises à jour logicielles des objets connectés.
15. Modélisation des risques et évaluation des impacts d'une cyberattaque sur les systèmes critiques.

AXE 2 : (6 mois, sanctionné par une attestation de bonne exécution)

Ce programme s'adresse aux professionnels souhaitant se reconvertir en cybersécurité. Pendant six mois, les participants travailleront sur des projets appliqués et réaliseront une mission complète en lien avec leur spécialisation.

Sujets de projets pour la reconversion (20 sujets)

1. Mise en place d'une solution SOC open-source (SIEM, IDS, SOAR).
2. Développement d'un script d'automatisation pour l'analyse de logs.
3. Analyse d'une attaque ransomware et recommandations de rémédiation.
4. Configuration et durcissement d'un serveur Linux pour une entreprise.
5. Audit et sécurisation des accès cloud (AWS, Azure, GCP).
6. Mise en place d'une politique de gestion des mots de passe d'entreprise.
7. Analyse des vulnérabilités d'un site web et correctifs.
8. Conception d'un programme de sensibilisation à la cybersécurité.
9. Simulation d'une attaque phishing et analyse des réactions.
10. Développement d'un outil de gestion des incidents de cybersécurité.
11. Sécurisation des bases de données en entreprise.
12. Étude et mise en place de solutions Zero Trust Architecture.
13. Surveillance des cybermenaces via Threat Intelligence Platforms.
14. Conception et déploiement d'une politique de sécurité pour une entreprise.
15. Sécurisation des applications mobiles contre les attaques courantes.
16. Étude et implémentation des solutions d'authentification biométrique.
17. Implémentation de solutions de chiffrement des données.
18. Sécurisation des infrastructures industrielles (SCADA, ICS).
19. Étude et mise en place d'un cadre de gestion des incidents cyber.
20. Déploiement d'une infrastructure PKI et gestion des certificats numériques.

Ces projets permettront aux participants de démontrer leurs compétences et d'obtenir une attestation de bonne exécution, facilitant leur insertion professionnelle