



COHORTE 2 — 2026

Programme d'Excellence en Cybersécurité

APSI-NE x ACRC — Partenariat Officiel — Former la prochaine génération de défenseurs du numérique africain

8

Modules

De formation intensive

27

Semaines

De mai à novembre 2026

500

Talents

Formés en cybersécurité

16+1

Pays + Haïti

Afrique francophone



Sommaire

01

Découvrir l'APSI-NE

Mission et modalités du programme de formation en cybersécurité

→ 2 sections

02

Le Parcours de Formation

Module socle + 7 spécialisations + CTF pratique

→ 8 modules

03

Projet de Fin de Formation

Mise en pratique encadrée par un mentor expert

→ 1 projet

04

Votre Plateforme & Communauté

Moodle, WhatsApp, Forums et Talent Pool

→ 3 outils



+ TALENT POOL

Insertion professionnelle garantie

2026

CHAPITRE 01

01

Découvrir l'APSI-NE

Notre mission et notre vision pour la cybersécurité au Niger

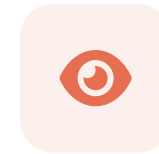
À la découverte de l'APSI-NE

Notre mission



Renforcer la culture de sécurité numérique

Accompagner les organisations dans leur transformation digitale tout en assurant une protection optimale de leurs actifs numériques.



Anticiper les menaces

Fournir à nos membres des alertes, outils et ressources pour rester en avance sur les cybermenaces émergentes.



Soutenir l'innovation locale

Encourager les initiatives et les talents locaux en cybersécurité pour positionner le Niger comme un hub régional.



Préparer la prochaine génération de leaders

Former et inspirer les jeunes talents pour qu'ils deviennent les piliers de l'Afrique numérique de demain.



L'APSI-NE s'engage à bâtir un écosystème de cybersécurité robuste et inclusif pour l'Afrique francophone.

Modalités du Programme

Tout ce que vous devez savoir pour rejoindre la Cohorte 2



Durée

Programme intensif de **6 mois** de formation, de mai à novembre 2026



Format

100% en ligne via Moodle & Zoom — accessible de partout



Évaluations

Quiz hebdomadaires et projets pratiques — **évaluation continue**



Attestation

Attestation officielle délivrée par l'APSI-NE à la validation du programme



Calendrier du programme

M

Mai – Août 2026

Sessions formation en ligne

S

Sept – Nov 2026

Projets & Attestations

N

Nov 2026

Talent Pool actif & diplômes

PARTENARIAT OFFICIEL

ACRC

— AFRICA CYBERSECURITY RESOURCE CENTRE

Partenaire Sponsor Principal

Consortium panafricain en partenariat public-privé — Plus de 500 experts — Membre du GFCE

6M

FCFA

Financement stratégique

500+

Experts

Au sein du consortium

150

Certifications AFP

Offertes aux meilleurs



Partenariat ACRC × APSI-NE

Cohorte 2, Session 2026

contact@apsi.ne

apsi.ne

Africa Cybersecurity Resource Centre

Consortium en partenariat public-privé à but non lucratif — Membre du GFCE — 1er financement BAD-ADFI



LHC Luxembourg

Agence de cybersécurité du Ministère de l'Économie du Luxembourg



35 experts

Équipe dédiée cybersécurité



CERT CIRCL

Centre de réponse aux incidents



MISP

Plateforme de partage de menaces



SnT / Université du Luxembourg

Centre de recherche en cybersécurité



300+ chercheurs

Experts en cybersécurité



Priorité stratégique

Recherche & innovation



Thalès Cyber Solution

Leader européen en cybersécurité



174+ experts

Équipe cybersécurité



SOC & TCS CERT

Opérations de sécurité



Suricate Solutions

1er SOC de l'UEMOA depuis 2016



Dakar, Sénégal

Siège régional Afrique de l'Ouest



20+ experts

Inclusion financière & sécurité



Partenaire Sponsor Principal

Contribution de l'ACRC

Un partenariat stratégique de 6M FCFA pour la cybersécurité africaine

Financement Stratégique 6M FCFA

Soutien de 6M FCFA au déploiement global du programme : labs pratiques, plateforme CTF, cérémonie de clôture et récompenses.

Labs pratiques

Plateforme CTF

Cérémonie

150 Certifications AFP

150 certifications Associé Forensic Pro (AFP) offertes aux meilleurs apprenants de la cohorte. Certification reconnue internationalement.

Sélection par performance

Reconnue internationalement

Expertise de Haut Niveau Masterclass & Interventions

Masterclass et interventions par des experts certifiés de l'ACRC tout au long du programme. Partage d'expérience internationale.

LHC Luxembourg

Thalès

SnT

Suricate

Prix Innovation Récompenses & Visibilité

Récompenses pour les 3 meilleurs projets de fin de formation — soutien aux talents et à l'innovation. Rayonnement via le réseau ACRC.

3 meilleurs projets

Co-branding APSI-NE × ACRC



Partenariat ACRC × APSI-NE

Programme porté par l'APSI-NE avec le soutien de l'ACRC

Cohorte 2 — Session 2026

contact@apsi.ne apsi.ne

CHAPITRE 02

02 Le Parcours de Formation

Module socle, 7 spécialisations, CTF, projet final et diplôme

★ NOUVEAU IA 2026

Module Socle — Bases Cyber

Fondamentaux de la cybersécurité sur 4-5 semaines (3-5h/semaine)

MODULE OBLIGATOIRE POUR TOUS

Les 9 séquences du module

0 Bienvenue

Orientation & présentation

1 Intro Cyber

Cybersécurité fondamentale

2 Linux

Commandes essentielles

3 Réseaux

OSI/TCP-IP, protocoles

4 Programmation

Python & Bash

5 Bases SQL

SQL & injection SQL

6 Hacking éthique

Pentest, Nmap, Metasploit

7 CTF

Apprendre en jouant

8 Red/Blue Team

Les 3 voies + GRC

🎯 Ce que vous apprendrez

- ✓ Concepts fondamentaux : CIA, vocabulaire, acteurs, menaces
- ✓ Types d'attaques : phishing, malware, ransomware, ingénierie sociale
- ✓ Linux : commandes essentielles et environnement
- ✓ Réseaux : modèles OSI/TCP-IP, adressage, protocoles
- ✓ Programmation : Python & Bash pour la cybersécurité
- ✓ Bases de données SQL et injection SQL
- ✓ Hacking éthique : phases du pentest, outils (Nmap, Metasploit)
- ✓ CTF : challenges pratiques Capture The Flag
- ✓ Les 3 voies : Red Team, Blue Team, GRC
- ✓ Bonnes pratiques et cadre légal/éthique

Gouvernance & Gestion des Risques (GRC)

La gouvernance, c'est le pilotage stratégique de la cybersécurité dans l'organisation.

🎯 Objectifs

- ✓ Apprendre à anticiper, détecter, réagir et gérer les incidents
- ✓ Comprendre les enjeux juridiques, stratégiques et opérationnels
- ✓ Intégrer les bonnes pratiques dans un contexte de transformation digitale
- ✓ Structurer une gouvernance alignée avec les normes internationales

📅 GRC en résumé

- 🏰 Piloter la stratégie cybersécurité
- 👥 Répartir les responsabilités
- ⚖️ Assurer transparence et conformité
- 🛡️ Suivre la stratégie de sécurité
- ⚙️ Aligner avec les normes ISO 27001, NIST, etc.

👜 Les débouchés en GRC



CISO / RSSI

Chief Information Security Officer



Risk Manager

Gestionnaire des risques



Auditeur SSI

Auditeur en sécurité des systèmes d'information



Compliance Officer

Responsable conformité



Consultant(e) GRC

Consultant en gouvernance et gestion des risques



Analyste continuité d'activité

Business Continuity Analyst

Pentest — Tests d'intrusion

Simulation d'attaque informatique visant à identifier et corriger les vulnérabilités d'un système

Types de Pentest

Externe

Attaque depuis l'extérieur (internet)

Interne

Simulation depuis l'intérieur

Applicatif

Web, mobile ou API

Red/Blue Team

Exercices de simulation poussés

Compétences clés

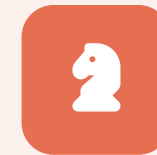
Réseaux, systèmes, développement Python/PHP, scripting, connaissance des frameworks d'attaque (Metasploit, Burp Suite)

Débouchés Pentest



Penetration Tester

Testeur d'intrusion professionnel



Red Teamer

Simulateur d'attaques avancées



Security Engineer

Ingénieur en sécurité informatique



Bug Bounty Hunter

Chasseur de vulnérabilités rémunéré

 Objectif : évaluer la sécurité d'un réseau, site web ou application

SOC — Security Operations Center

La tour de contrôle de la cybersécurité — surveillance, détection, analyse et réponse en temps réel

☰ Missions du SOC

-  **Surveiller**
En temps réel les systèmes d'information et les alertes
-  **Détecter**
Les menaces et incidents de sécurité
-  **Réagir**
Rapidement pour limiter les impacts des attaques
-  **Anticiper**
Veille constante pour anticiper les nouvelles attaques

🎓 Prérequis utiles

Bases en réseaux, systèmes et cybersécurité. Compréhension des attaques courantes. Maîtrise d'outils **SIEM**, **EDR**. Capacité à analyser des logs.

🧰 Débouchés SOC

-  **Analyste SOC (N1, N2, N3)**
Analyste de niveau 1, 2 ou 3
-  **Threat Hunter**
Chasseur de menaces
-  **SOC Manager**
Responsable du SOC
-  **Analyste Cyber Threat Intelligence**
Analyste en renseignement sur les menaces
-  **Consultant SOC**
Consultant en opérations de sécurité

IoT et Systèmes Industriels

La cybersécurité des objets connectés et des systèmes industriels est devenue critique

Chiffres clés

21B+

objets IoT actifs en
2025

35–40B

projection horizon
2030

IoT

rarement durcis dès la
conception

Concepts clés

- ✓ Architecture IoT/OT : pile IoT et modèle de Purdue
- ✓ Protocoles IoT/OT : Modbus, MQTT, LoRaWAN, NB-IoT
- ✓ Sécurité IoT : OWASP Top 10, firmware, UART/JTAG
- ✓ Sécurité OT : segmentation, supervision, contrôle des accès
- ✓ Attaques industrielles : Stuxnet, Industroyer, TRITON
- ✓ Référentiels : ETSI EN 303 645 & IEC 62443



Prérequis : Réseaux, Cloud, Linux/Scripting, bases en sécurité informatique.
Exercices en environnement émulé — aucun matériel physique obligatoire.

Débouchés IoT / IIoT



Spécialiste cybersécurité IoT/IIoT
Expert en sécurité des objets connectés



Ingénieur/Consultant IoT
Conception et sécurisation des solutions IoT



Chef de projet IoT/IIoT
Gestion de projets connectés sécurisés



Architecte Solutions IoT
Architecture sécurisée des systèmes connectés



Pen Tester IoT
Tests d'intrusion sur objets connectés

Analyse Forensique

L'enquête post-cyberattaque — comprendre ce qui s'est passé, comment, quand, et parfois par qui

🔍 Ce que vous ferez

-  **Retrouver les traces**
Laissées après une cyberattaque
-  **Collecter et analyser**
Les preuves numériques (PC, mobiles, logs)
-  **Comprendre le "Comment"**
Et le "Pourquoi" d'un incident
-  **Produire des rapports**
Exploitable en entreprise ou devant un tribunal

🎓 Prérequis

Aisance sur Windows et Android, connaissances en ligne de commande, **curiosité + rigueur + sens du détail**. Pas besoin d'être développeur pro.

👜 Débouchés Forensique

-  **Analyste forensique**
Analyse numérique post-incident
-  **Investigateur en incident response**
Réponse aux incidents de sécurité
-  **Expert judiciaire**
Expertise légale en cybersécurité
-  **Consultant en gestion de crise cyber**
Accompagnement en cas d'attaque
-  **Threat Intelligence Analyst**
Analyste en renseignement sur les menaces

DevSecOps

Intégrer la sécurité à chaque étape du cycle de vie du développement logiciel

∞ Les 3 piliers



Dev
Développement



Sec
Sécurité



Ops
Opérations

☰ Missions & Tâches

- ✓ Intégrer des tests de sécurité dans les pipelines CI/CD
- ✓ Automatiser la détection des vulnérabilités
- ✓ Gérer les politiques de sécurité cloud/infrastructure
- ✓ Assurer une veille continue sur les menaces
- ✓ Travailler avec les devs pour corriger le code

✂ **Compétences:** Git, Docker, Jenkins, CI/CD, SonarQube, Trivy, Snyk, Kubernetes, AWS/Azure

🧰 Débouchés DevSecOps



DevSecOps Engineer
Ingénieur sécurité intégrée au développement



Cloud Security Engineer
Sécurité des infrastructures cloud



Security Automation Specialist
Spécialiste en automatisation de la sécurité



Platform Engineer Security
Ingénieur plateforme sécurisée



SRE (Site Reliability Engineer)
Ingénieur de fiabilité des systèmes

IA & Cybersécurité

★ NOUVEAU 2026

Comment l'intelligence artificielle transforme la cybersécurité — outil d'attaque ET outil de défense

IA pour la détection des menaces

Machine learning appliqué à la détection d'anomalies, SIEM intelligents, threat hunting automatisé

Attaques assistées par IA

Deepfakes, phishing ciblé par LLM, génération automatique de malwares — comprendre pour mieux défendre

Sécurité des systèmes IA

Adversarial attacks, empoisonnement de modèles, protection des pipelines ML/AI

IA générative & SOC

Automatisation des réponses aux incidents, copilotes de cybersécurité, réduction du temps de réponse

Débouchés IA & Cybersécurité

 **AI Security Analyst**
Analyste en sécurité IA

 **ML Security Engineer**
Ingénieur sécurité ML

 **Threat Intelligence Analyst**
Analyste en renseignement

 **AI Red Teamer**
Attaquant IA éthique

 **Consultant IA & Cybersécurité**
Consultant spécialisé

 **SOC Analyst IA-augmented**
Analyste SOC augmenté par IA

 Un domaine en pleine explosion, incontournable pour les professionnels de demain

CHAPITRE 03

03

Projet de Fin de Formation

Mettez en pratique vos compétences sur un projet réel, encadré
par un mentor

Projet de fin de formation

Réalisez un projet individuel ou en binôme sur un thème de cybersécurité, encadré par un mentor

Processus en 4 étapes

1

Choix du thème

Vous choisissez votre sujet ou votre mentor vous en propose un adapté à votre spécialisation et à vos intérêts.

2

Travail encadré

Vous travaillez sur le projet durant la phase finale (Sept-Nov 2026), encadré par un mentor expert de l'APSI-NE.

3

Présentation finale

Vous présentez votre projet devant un jury. C'est l'occasion de démontrer vos compétences et de valoriser votre expertise.

4

Portfolio & Attestation

Le projet alimente votre portfolio professionnel et contribue à l'obtention de votre attestation APSI-NE.

Idées de projets



Audit de sécurité d'une application web



Mise en place d'un SOC miniature



Analyse forensique d'un incident simulé



Pipeline CI/CD sécurisé avec DevSecOps



Modèle ML de détection d'anomalies



Framework de conformité ISO 27001



Sécurisation d'un réseau IoT domestique



Le sujet de votre choix !

CHAPITRE 04

04 Votre Plateforme & Communauté

Moodle, WhatsApp, Forums et le Talent Pool

Moodle — Votre espace d'apprentissage

Votre plateforme d'apprentissage en ligne (LMS) pour la Cohorte 2



Moodle

Learning Management System

C'est ici que vous trouverez tous vos **cours**, **ressources pédagogiques**, **évaluations** et le suivi de votre progression.

✓ Plateforme intuitive avec forum intégré

✓ Messagerie et calendrier pédagogique

✓ Bibliothèque de ressources complète

★ Ce que Moodle vous offre



Accès 24/7

Accédez à vos cours à tout moment, de n'importe où



Cours structurés

Par module avec vidéos et supports pédagogiques



Quiz et évaluations

Pour valider vos compétences en continu



Suivi de progression

En temps réel pour visualiser votre avancement

Plateforme CTF — Capture The Flag

PRATIQUE EN LIGNE

Apprenez en jouant sur ctf.apsi.ne — mettez en pratique vos compétences en cybersécurité

? Qu'est-ce qu'un CTF ?

Un **Capture The Flag** est un challenge de cybersécurité où vous devez résoudre des énigmes, exploiter des vulnérabilités, et trouver des "flags" (codes secrets) pour marquer des points.

🏆 C'est la meilleure façon d'apprendre la cybersécurité en s'amusant !

🚩 Catégories de défis



Web

Faibles applicatives



Crypto

Décryptage



Forensics

Investigation



Reverse

Rétro-ingénierie



Pwn

Exploitation binaire



OSINT

Recherche d'infos

★ Pourquoi les CTF ?



Apprentissage actif

Apprenez en faisant, pas seulement en lisant



Esprit compétitif

Challengez-vous avec la cohorte



Portfolio

Valorisez vos résultats et progrès



Fun & épanouissant

Apprendre en s'amusant, sans pression

ctf.apsi.ne

Votre terrain de jeu cybersécurité

Talent Pool APSI-NE

★ NOUVEAU 2026

Connecte les meilleurs diplômés avec les recruteurs et opportunités en cybersécurité



Le Mur de la Cohorte

PUBLIC

Flux public partageant les accomplissements collectifs de la cohorte : projets, défis relevés, et succès de la communauté.



Le Classement

PRIVÉ

Leaderboard privé d'émulation saine. Classement anonymisé basé sur la progression, l'engagement et les performances.



Registre des Diplômés

OPT-IN

Catalogue public des diplômés avec profils vérifiés. Mise en relation directe avec recruteurs et entreprises partenaires.

★ Pourquoi rejoindre le Talent Pool ?

- ✓ Annuaire des diplômés avec attestation APSI-NE
- ✓ Les meilleurs profils mis en avant
- ✓ Connexion avec opportunités au Niger
- ✓ Accès au réseau Afrique francophone
- ✓ Offres d'emploi et de stage exclusives
- ✓ Visibilité auprès des partenaires recruteurs
- ✓ Networking avec la communauté APSI-NE
- ✓ Reconnaissance de l'excellence

Communauté d'échanges

Restez connectés et échangez avec votre cohorte tout au long du programme

Groupe WhatsApp

- ✓ Canal de communication principal pour les échanges rapides
- ✓ Annonces importantes en temps réel
- ✓ Entraide entre participants
- ✓ Partage de ressources et d'actualités cybersécurité
- ✓ Coordination pour les sessions en groupe

Forums Moodle

- ✓ Discussions structurées par module de formation
- ✓ Questions-réponses avec les formateurs
- ✓ Espace de collaboration pour les projets
- ✓ Archive des discussions pour référence
- ✓ Support pédagogique structuré

Règles de la communauté

-  **Respect et bienveillance**
Obligatoires envers tous les membres
-  **Confidentialité**
Des informations partagées
-  **Entraide et collaboration**
Esprit de solidarité
-  **Participation active**
Encouragée pour tous

Comment ça marche ?

- 1 Connectez-vous sur Moodle**
Pour accéder à vos cours et ressources
- 2 Rejoignez le groupe WhatsApp**
Pour les échanges rapides et annonces
- 3 Utilisez les forums**
Pour poser vos questions et collaborer



Rejoignez l'Aventure !

Votre parcours vers l'excellence en cybersécurité commence maintenant !

Votre parcours en 5 étapes



Partenariat ACRC x APSI-NE

Programme porté par l'APSI-NE avec le soutien de l'ACRC

 contact@apsi.ne  apsi.ne  Cohorte 2, Session 2026