DIRECTION GENERALE DE L'ECOLE DES METIERS DU NUMERIQUE

APPEL A CANDIDATURE

POUR LE RECRUTEMENT DE FORMATEURS DANS LE CADRE DU DEPLOIEMENT DE LA FORMATION EN « ANALYSTE EN CYBERSÉCURITÉ »

Septembre 2025

Contexte

L'accélération de la transformation digitale au Bénin et dans la sous-région s'accompagne de nouveaux défis en matière de sécurité numérique. La protection des systèmes d'information, des données sensibles et des infrastructures critiques est devenue une priorité stratégique pour les États, les entreprises et les citoyens.

Dans ce cadre, l'École des Métiers du Numérique (EMN), institution publique créée par décret n°2020-492 et spécialisée dans les formations certifiantes aux métiers du numérique, a pour mission de préparer une main-d'œuvre qualifiée répondant aux besoins croissants du marché.

Afin de renforcer son offre, l'EMN déploie une formation certifiante en « **Analyste en cybersécurité** », destinée à doter les apprenants de compétences pratiques et opérationnelles dans ce domaine en pleine expansion. Pour assurer la qualité de ce programme, l'école lance le présent appel à candidatures en vue du recrutement de formateurs expérimentés capables d'accompagner efficacement les apprenants dans leur parcours.

Modules de formation

La formation en « Analyste en Cybersécurité » de l'École des Métiers du Numérique (EMN) prépare les apprenants à relever les défis de la sécurité numérique au sein des organisations.

Elle combine bases théoriques, études de cas et mises en pratique pour développer des compétences opérationnelles immédiatement mobilisables. Structuré autour de modules clés tel que :

- Introduction à la cybersécurité ;
- Réponses aux incidents ;
- Gouvernance de la cybersécurité ;
- Cyberattaque et défense en entreprise ;
- Réseautique et sécurité.

Ce parcours offre une vision complète et intégrée des enjeux, des outils et des stratégies de protection dans un monde numérique en constante évolution.

Les modules de formation ainsi que les profils de formateurs recherchés sont présentés dans le tableau ci-après :

MODULES ET DESCRIPTIONS	MISSIONS	PROFILS RECHERCHÉS
INTRODUCTION À LA CYBERSÉCURITÉ L'enseignant(e) en Introduction à la Cybersécurité sera responsable de la conception et de l'animation de cours visant à initier les étudiants aux fondamentaux de la cybersécurité. Il/elle jouera un rôle crucial dans la formation de la prochaine génération de professionnels de la sécurité informatique.	- Concevoir et dispenser des cours d'introduction à la cybersécurité pour des étudiants de niveau débutant à intermédiaire. - Initier les étudiants aux principes fondamentaux de la cybersécurité (confidentialité, intégrité, disponibilité). - Former aux bases de la cryptologie et à la modélisation des menaces. - Encadrer des exercices pratiques avec des outils d'analyse de vulnérabilités. - Sensibiliser aux enjeux éthiques et réglementaires de la cybersécurité, notamment au RGPD et aux normes ISO 27001. - Développer et mettre à jour régulièrement le contenu des cours pour refléter les dernières tendances et menaces en cybersécurité. - Évaluer les progrès des étudiants et fournir des retours constructifs.	- Diplôme de niveau Bac+5 minimum en informatique avec une spécialisation en cybersécurité. - Minimum 5 ans d'expérience récente dans la cybersécurité avec des projets probants. - Connaissance approfondie des risques cyber et des mesures de protection. - Maîtrise des outils et technologies de sécurité informatique (pare-feu, antivirus, cryptage, etc.). - Expérience en audit de sécurité informatique et en proposition de solutions d'amélioration. - Maîtrise des fondamentaux de la cybersécurité, incluant la gestion des risques et les politiques de sécurité. - Connaissance approfondie des architectures de sécurité, des protocoles et des systèmes d'exploitation.

	Participer aux réunions pédagogiques et contribuer à l'amélioration continue du programme de formation.	- Expertise en cryptographie et en techniques de protection des données. - Familiarité avec les outils d'analyse de vulnérabilités et de tests d'intrusion.
RÉPONSES AUX INCIDENTS L'enseignant(e) en Réponse aux Incidents de Cybersécurité sera responsable de former les étudiants aux aspects théoriques et pratiques de la gestion des incidents de sécurité informatique. Ce rôle est crucial pour préparer la prochaine génération de professionnels capables de détecter, analyser et répondre efficacement aux cybermenaces.	- Concevoir et dispenser des cours couvrant toutes les phases du processus de réponse aux incidents : préparation, détection, analyse, confinement, éradication et rétablissement. - Former les étudiants à l'utilisation d'outils d'analyse tels que IDS, SIEM, Wireshark, Snort ou Zeek. - Encadrer des projets pratiques pour la conception et l'implémentation d'architectures de sécurité réseau. - Évaluer les compétences des apprenants à travers des études de cas et des travaux diriges. - Développer des scenarios d'incidents réalistes pour des exercices de simulation. - Enseigner les meilleures pratiques pour la rédaction de rapports d'incidents et la communication avec les parties prenantes. - Sensibiliser les étudiants aux aspects éthiques et légaux de la réponse aux incidents.	- Diplôme de niveau Bac+5 minimum en informatique avec une spécialisation en cybersécurité - Minimum 5 à 7 ans d'expérience active et récente en gestion des incidents de sécurité - Justificatifs de missions/projets significatifs dans le secteur de la cybersécurité. - Certifications pertinentes (ex : CISSP, GIAC Certified Incident Handler, CompTIA Security+) appréciées. - Maîtrise approfondie des processus de réponse aux incidents et des méthodologies associées. - Expertise dans l'utilisation d'outils de détection et d'analyse des incidents (IDS, SIEM, etc.). - Connaissance approfondie des architectures de sécurité réseau et des protocoles. - Compétences en analyse de logiciels malveillants et en forensique numérique ;

	- Maintenir à jour le contenu des cours en fonction de l'évolution des menaces et des technologies de sécurité.	- Familiarité avec les cadres règlementaires en matière de cybersécurité (ex : RGPD, NIS2).
GOUVERNANCE DE LA CYBERSÉCURITÉ L'enseignant(e) en Gouvernance de la Cybersécurité sera responsable de former les étudiants aux aspects stratégiques et organisationnels de la sécurité des systèmes d'information. Ce rôle est crucial pour préparer la prochaine génération de professionnels capables de concevoir, mettre en œuvre et évaluer des politiques de cybersécurité efficaces au sein des organisations.	- Former sur les cadres de gouvernance et la gestion des risques en cybersécurité. - Encadrer l'élaboration de politiques de sécurité et l'évaluation de la posture de cybersécurité. - Assurer une maîtrise des standards de conformité internationaux (ISO 27001, NIST Cyber Security Framework). - Superviser des projets pratiques sur les diagnostics de cybersécurité organisationnelle. - Enseigner les principes de l'analyse et du traitement des problématiques de cybersécurité, notamment pour les Opérateurs de Services Essentiels (OSE). - Former à la conduite de projets de cybersécurité, de la conception à la mise en œuvre. - Sensibiliser aux enjeux juridiques et règlementaires de la cybersécurité (RGPD, NIS2, etc.) ; - Développer des cours sur l'audit des systèmes d'information et l'analyse des risques.	- Cybersécurité niveau Bac+5 minimum en informatique avec une spécialisation en cybersécurité. - Minimum 5 ans d'expérience active en gouvernance et sécurité de l'information. - Justification de missions/projets significatifs alignés sur des standards internationaux. - Certifications pertinentes (ex : CISSP, CISM, ISO 27001) appréciées. - Maîtrise approfondie des cadres de gouvernance en cybersécurité (ISO 27001, NIST CSF). - Expertise en gestion des risques de sécurité et en élaboration de politiques de sécurité. - Connaissance des architectures de sécurité et des mécanismes de protection des données ; - Compréhension des enjeux de la cybersécurité pour différents secteurs d'activité.

CYBERATTAQUE ET DÉFENSE EN ENTREPRISE L'enseignant(e) en Cyberattaque et Défense sera responsable de former les étudiants aux aspects théoriques et pratiques des cyberattaques et des stratégies de défense. Ce rôle est crucial pour préparer la prochaine génération de professionnels capables de comprendre, détecter et contrer les menaces cybernétiques avancées.	- Former à l'analyse des cyberattaques : reconnaissance, exploitation, mouvements latéraux, etc. - Enseigner l'utilisation d'outils de détection avances (EDR, SIEM) et l'analyse des logs. - Superviser la conception d'architectures défensives adaptées aux entreprises. - Organiser des simulations pratiques pour renforcer les compétences des apprenants. - Développer des cours sur les techniques de mouvement latéral et les stratégies de détection associées. - Enseigner les principes de la réponse aux incidents et de l'analyse forensiques. - Former à l'utilisation d'outils d'analyse comme Wireshark, Snort ou Zeek. - Sensibiliser aux enjeux éthiques et légaux des tests d'intrusion et de la défense en cybersécurité.	- Diplôme de niveau Bac+5 minimum en informatique avec une spécialisation en cybersécurité. - Minimum 7 ans d'expérience récente et significative dans la gestion des cyberattaques et la sécurité informatique. - Justificatifs de projets complexes ou de postes à responsabilité dans le domaine. - Certifications pertinentes (ex: OSCP, GIAC, CEH) appréciées. - Maîtrise approfondie des techniques de cyberattaque et des stratégies de défense. - Expertise dans l'utilisation d'outils de détection et d'analyse des menaces. - Connaissance approfondie des architectures de sécurité réseau et des protocoles. - Compétences en analyse de logiciels malveillants et en investigation numérique (forensiques). - Veille technologique active sur les nouvelles menaces et techniques de défense.

RÉSEAUTIQUE ET SÉCURITÉ L'enseignant(e) en Réseautique et Sécurité sera responsable de former les étudiants aux aspects théoriques et pratiques des architectures réseau et de leur sécurisation. Ce rôle est crucial pour préparer la prochaine génération de professionnels capables de concevoir, mettre en œuvre et sécuriser des infrastructures réseau complexes.	- Former sur les architectures réseau et leurs principes de sécurité (zoning, segmentation, IPv6). - Encadrer l'analyse et la sécurisation des équipements réseau et protocoles. - Superviser des travaux pratiques sur la détection des logiciels malveillants et l'analyse réseau. - Sensibiliser aux normes, standards et lois en matière de réseautique. - Enseigner l'utilisation d'outils d'analyse réseau comme Wireshark, Snort et Zeek. - Développer des cours sur les protocoles de sécurité réseau (TCP/IP, DNS, HTTP, etc.). - Former à la mise en place et à la gestion de dispositifs de sécurité tels que les pares-feux, les systèmes de détection d'intrusion (IDS/IPS) et les VPN. - Organiser des simulations pratiques pour renforcer les compétences des apprenants en matière de détection et de réponse aux incidents de sécurité réseau.	- Diplôme de niveau Bac+5 minimum en informatique avec une spécialisation en réseaux. - Minimum 5 à 7 ans d'expérience active dans la conception et la sécurisation des infrastructures réseau. - Participation à des projets significatifs dans le domaine de la réseautique. - Certifications pertinentes (ex : CCNA, CCNP, CISSP) appréciées. - Maitrise approfondie des architectures réseau et des protocoles de communication. - Expertise dans la configuration et la sécurisation des équipements réseau (routeurs, commutateurs, pare-feu). - Connaissance approfondie des menaces de sécurité réseau et des stratégies de défense. - Compétences en analyse de trafic réseau et en détection d'anomalies. - Veille technologique active sur les évolutions en matière de réseautique et de sécurité.

Modalités de candidature

Les candidats intéressés sont invités à soumettre :

- Un CV détaillé mettant en avant les expériences pertinentes en rapport avec le module choisi ;
- Une lettre de motivation précisant clairement le module, la disponibilité, l'expérience en cybersécurité et en enseignement ;
- Les justificatifs des diplômes et expériences ainsi que tout autre document pertinent (certificats, lettres de recommandation, etc.) ;

Les dossiers de candidature doivent être envoyés par courrier électronique à l'adresse : contact@ecolenumerique.bj, au plus tard le 28 septembre 2025 à 23h59 (heure locale).

Issiakou SOULEYMANE
Directeur Général