FICHES DE POSTE DÉTAILLÉES - CAMPAGNE DE RECRUTEMENT ANSI 2025

Architecte Sécurité et Gouvernance

Positionnement hiérarchique

Rattaché directement à la Direction de la Sécurité des Systèmes d'Information, l'Expert en Architecture sécurité occupe une position stratégique au sein de l'ANSI. Il travaille en étroite collaboration avec l'ensemble des départements techniques et entretient des relations privilégiées avec les institutions nationales de sécurité, notamment l'Agence Nationale de Cybersécurité et le futur CERT national.

Mission principale

L'Expert en architecture sécurité est garant de la sécurité du cyberespace national et de la protection des infrastructures numériques critiques du Niger. Il conçoit et est garant de l'architecture de l'ensemble des dispositifs de sécurité nécessaires à la protection des systèmes d'information gouvernementaux contre les menaces cybernétiques en constante évolution. Sa mission consiste aussi en la définition des politiques et procédures de sécurité à la gestion opérationnelle des incidents, en passant par la sensibilisation des utilisateurs.

Activités et responsabilités principales

Dans le cadre de ses fonctions, l'Expert effectue régulièrement des audits de sécurité et des analyses de vulnérabilités de l'architecture en place, permettant d'identifier et de corriger proactivement les failles potentielles. L'architecte s'assure que les choix technologiques respectent les standards internationaux en matière de sécurité. Il doit également s'assurer que les solutions d'infrastructures réseaux ainsi que les logiciels sont adaptés aux besoins. Ce qui fait de lui un acteur important pour tout projet de transformation numérique. Le suivi d'obsolescence et de renouvellement de licence constitue un pan important de ses activités.

L'expert développe, vulgarise et veille à la mise à jour des politiques et procédures de sécurité. Il participe activement dans les cellules de crise en cas d'attaque majeure. Il assure la veille technologique sur les menaces émergentes, analyse les tendances du cybercrime et adapte constamment les défenses en conséquence. La formation et la sensibilisation des utilisateurs constituent également une part importante de ses activités, en contribuant à l'organisation de sessions de formation, la rédaction de guides de bonnes pratiques et la conduite de campagnes de sensibilisation.

Profil recherché

Le candidat idéal possède un diplôme d'ingénieur (BAC+5) en informatique, télécommunications ou cybersécurité, complété par des certifications professionnelles reconnues telles que CISSP, CISA ou équivalent. Une expérience minimale de 2 ans dans le domaine de la cybersécurité est exigée. La maîtrise des frameworks de sécurité

internationaux (ISO 2700X, NIST, COBIT) est indispensable, ainsi qu'une connaissance approfondie des technologies de sécurité modernes : firewalls nouvelle génération, systèmes de détection et prévention d'intrusion, solutions SIEM, technologies de chiffrement et authentification forte. Le candidat dispose d'une bonne connaissance des équipements réseaux (routeurs, switch, FW, SIEM, DNS, mail server,). Un bon niveau d'anglais (écrit et parlé) est requis pour ce poste.

Qualités personnelles requises

L'Expert en architecture sécurité doit faire preuve d'une intégrité irréprochable et d'une éthique professionnelle exemplaire, compte tenu de la sensibilité des informations qu'il sera amené à manipuler. Une capacité d'analyse exceptionnelle, couplée à un esprit de synthèse permettant de communiquer efficacement avec des interlocuteurs non techniques, est essentielle. La gestion du stress et la capacité à prendre des décisions rapides en situation de crise sont des qualités indispensables. L'expert doit également démontrer une curiosité intellectuelle constante et une passion pour l'apprentissage continu dans un domaine en perpétuelle évolution.

Conditions de travail et évolution

Le poste implique une disponibilité étendue avec des déplacements fréquents sur l'ensemble du territoire national sont à prévoir pour les audits de sites distants. L'environnement de travail est moderne et stimulant, avec accès aux technologies de pointe et aux formations continues. Les perspectives d'évolution incluent la possibilité d'accéder au poste de Directeur de la Sécurité des Systèmes d'Information (DSSI) ou de Chief Information Security Officer (CISO) au sein de l'ANSI ou d'autres institutions nationales.

Méthode de sélection

Phase 1 : Présélection sur la base des qualifications
Phase 2 : Test Ecrit + Pratique
Phase 3 : Test Oral pour les trois (3) premiers issus de la Phase 2

Auditeur Sécurité

Positionnement hiérarchique

Rattaché directement à la Direction de la Sécurité des Systèmes d'Information, l'Expert en Audit sécurité occupe une position stratégique au sein de l'ANSI. Il travaille en étroite collaboration avec l'ensemble des départements techniques et entretient des relations privilégiées avec les institutions nationales de sécurité, notamment l'Agence Nationale de Cybersécurité et le futur CERT national.

Mission principale

L'Expert en Audit sécurité est garant de la sécurité du cyberespace national et de la protection des infrastructures numériques critiques du Niger. Il conçoit, déploie et supervise l'ensemble des dispositifs de sécurité nécessaires à la protection des systèmes d'information gouvernementaux contre les menaces cybernétiques en constante évolution. Sa mission s'étend de la définition des politiques de sécurité à la gestion opérationnelle des incidents, en passant par la sensibilisation des utilisateurs et l'accompagnement des projets de transformation numérique dans leur volet sécurité.

Activités et responsabilités principales

Dans le cadre de ses fonctions, l'Expert effectue régulièrement des audits de sécurité approfondis, incluant des tests d'intrusion et des analyses de vulnérabilités, permettant d'identifier et de corriger proactivement les failles potentielles. L’expert contribue en la maturité du Security Operations Center (SOC) en renforçant les règles d’alertes sécurité par l’envoi de logs pertinents facilitant la détection des comportements anormaux et la contention rapide des incidents sécurité.

L'expert contribue au développement et à la mise à jour des politiques et procédures de sécurité. Il participe activement dans les cellules de crise en cas d'attaque majeure. Il assure la veille technologique sur les menaces émergentes, analyse les tendances du cybercrime et adapte constamment les défenses en conséquence. La formation et la sensibilisation des utilisateurs constituent également une part importante de ses activités, en contribuant à l'organisation de sessions de formation, la rédaction de guides de bonnes pratiques et la conduite de campagnes de sensibilisation.

Profil recherché

Le candidat idéal possède un diplôme d'ingénieur (BAC+5) en informatique, télécommunications ou cybersécurité, complété par des certifications professionnelles reconnues telles que CISSP, CEH, CISA ou équivalent. Une expérience minimale de 2 ans dans le domaine de la cybersécurité est exigée. La maîtrise des frameworks de sécurité

internationaux (ISO 27001, NIST, OWASP) est indispensable, ainsi qu'une connaissance approfondie des technologies de sécurité modernes : firewalls nouvelle génération, systèmes de détection et prévention d'intrusion, solutions SIEM, technologies de chiffrement et authentification forte. Le candidat dispose d'une bonne connaissance des équipements réseaux (routeurs, switch) et la maîtrise des langages de programmation (PHP, Java, C, SQL, Python,…) est un atout. Un bon niveau d'anglais (écrit et parlé) est requis pour ce poste.

Qualités personnelles requises

L'Expert en audit sécurité doit faire preuve d'une intégrité irréprochable et d'une éthique professionnelle exemplaire, compte tenu de la sensibilité des informations qu'il sera amené à manipuler. Une capacité d'analyse exceptionnelle, couplée à un esprit de synthèse permettant de communiquer efficacement avec des interlocuteurs non techniques, est essentielle. La gestion du stress et la capacité à prendre des décisions rapides en situation de crise sont des qualités indispensables. L'expert doit également démontrer une curiosité intellectuelle constante et une passion pour l'apprentissage continu dans un domaine en perpétuelle évolution.

Conditions de travail et évolution

Le poste implique une disponibilité étendue avec des astreintes régulières pour assurer la continuité de la surveillance des systèmes. Des déplacements fréquents sur l'ensemble du territoire national sont à prévoir pour les audits de sites distants. L'environnement de travail est moderne et stimulant, avec accès aux technologies de pointe et aux formations continues. Les perspectives d'évolution incluent la possibilité d'accéder au poste de Directeur de la Sécurité des Systèmes d'Information (DSSI) ou de Chief Information Security Officer (CISO) au sein de l'ANSI ou d'autres institutions nationales.

Méthode de sélection

Phase 1 : Présélection sur la base des qualifications
Phase 2 : Test Ecrit + Pratique
Phase 3 : Test Oral pour les trois (3) premiers issus de la Phase 2