ANSSI
AGENCE NATIONALE DE LA SÉCURITÉ
DES SYSTÈMES D'INFORMATION
CÔTE D'IVOIRE

CATALOGUE
DES FORMATIONS

CENTRE DE FORMATION
ANSSI CI

Agréé
FDFP
Fonds de Développement de la Formation Professionnelle

SOMMAIRE

PRÉSENTATION DU CFSSI

La transformation numérique des organisations ouvre de nouvelles perspectives de développement, d'innovation et d'amélioration des services. Elle s'accompagne toutefois d'une exposition croissante à des cybermenaces de plus en plus nombreuses, sophistiquées et complexes à maîtriser. Dans ce contexte, la cybersécurité s'impose comme un enjeu stratégique de souveraineté, de résilience et de confiance numérique, face aux risques d'interruption d'activité, de pertes financières, de fuite de données et d'atteinte à la réputation.

La technologie, à elle seule, ne suffit pas à garantir cette protection. La sécurité des systèmes d'information repose avant tout sur des professionnels qualifiés, capables d'anticiper les menaces, de prévenir les attaques, de détecter les vulnérabilités et de réagir efficacement aux incidents.

C'est pour répondre à cet impératif que **l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)** a créé **le Centre de Formation à la Sécurité des Systèmes d'Information (CFSSI).**

Agréé par le Fonds de Développement de la Formation Professionnelle (FDFP), le CFSSI a pour mission de former, certifier et rendre opérationnels les acteurs de la cybersécurité en Côte d'Ivoire.

En 2026, le CFSSI propose trois parcours complémentaires :

- **Des formations techniques courtes (2 à 3 jours),** destinées aux techniciens portent sur les menaces et les technologies de sécurité;
- **Des formations certifiantes fondées sur le RGSSI,** destinées aux professionnels chargés de sa mise en œuvre au sein des organisations, ainsi qu'aux auditeurs chargés d'évaluer la conformité des systèmes d'information aux exigences de ce référentiel;
- **Des Masters en cybersécurité,** organisés en partenariat avec l'ESATIC, dans les domaines de la sécurité des systèmes d'information et de la criminalistique numérique. Ce nouveau programme n'est pas encore intégré au présent catalogue.

Pourquoi choisir le CFSSI ?

- De formateurs et d'encadreurs qualifiés, reconnus pour leur expertise en cybersécurité;
- De programmes conçus en fonction des réalités opérationnelles et réglementaires de la Côte d'Ivoire;
- De formations alignées sur le RGSSI et sur les standards internationaux;
- D'un environnement technique et pédagogique adapté à l'apprentissage et à la mise en pratique;
- De parcours progressifs permettant d'acquérir, de renforcer et de certifier des compétences de haut niveau;
- D'un centre agréé par le FDFP et adossé à l'autorité nationale de cybersécurité.

Notre engagement : Vous former, vous rendre opérationnels et faire de vous des relais de l'ANSSI.

FORMATIONS CERTIFIANTES

CENTRE DE FORMATION ANSSI CI

Agréé FDFP

1. CERTIFICATION DES EXPERTS AUDITEURS DU RGSSI

Durée : 05 jours

Devenez un acteur clé de la conformité des systèmes d'information aux exigences du RGSSI en Côte d'Ivoire. Fondée sur le Référentiel Général de Sécurité des Systèmes d'Information (RGSSI), cette formation certifiante vous prépare à conduire des audits réglementaires auprès des organisations établies sur le territoire national et atteste votre capacité à les réaliser avec l'éthique et conformement au décret n° 2021-917.

OBJECTIFS

- Maîtriser et interpréter les exigences du RGSSI, du PPIC et de la PSSI, ainsi que le cadre réglementaire applicable à la sécurité des systèmes d'information;
- Planifier, conduire et clôturer un audit réglementaire selon une méthodologie structurée, rigoureuse et impartiale, conformément aux exigences du décret n° 2021-917;
- Évaluer la conformité des organisations, formaliser les constats d'audit et formuler des recommandations construtives dans un rapport structuré.

CONDITIONS D'ACCÈS

- Diplôme Bac +2 en Technologies de l'Information;
- Au moins 1 an d'expérience en management des systèmes d'information;
- Bonne connaissance des systèmes informatiques, des politiques de sécurité SI et du RGSSI;
- Maîtrise des outils bureautiques et d'Internet;
- Bonne connaissance de la protection des données à caractère personnel;
- Excellentes capacités relationnelles, organisationnelles et rédactionnelles.

PUBLIC CONCERNÉ

- Professionnels souhaitant réaliser et diriger des audits de sécurité selon le RGSSI;
- Personnes chargées de maintenir la conformité RGSSI au sein d'une organisation;
- Experts techniques se préparant à l'audit du système de gestion de la sécurité de l'information;
- Conseillers experts en gestion de la sécurité de l'information.

PROGRAMME (7 modules)

- Écosystème des agences et institutions de cybersécurité en Côte d'Ivoire;
- Cadre juridique international de la sécurisation des SI;
- Référentiel Général de Sécurité des Systèmes d'Information (RGSSI);
- Politique de Sécurité des Systèmes d'Information (PSSI);
- Plan de Protection des Infrastructures Critiques (PPIC);
- Procédure d'audit, de contrôle et de certification des SI.
- cybercriminalité et ingénierie sociale

COMPÉTENCES ACQUISES

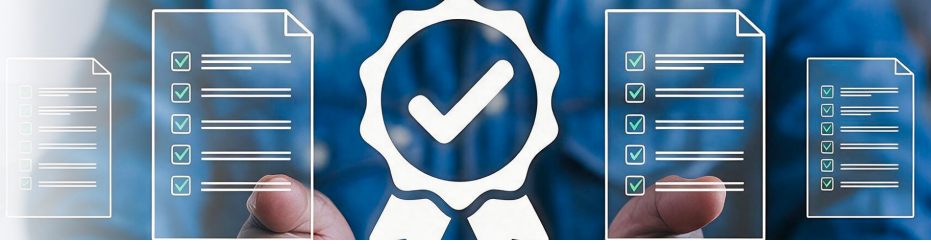
- Maîtriser du cadre réglementaire et de la préparation du périmètre d'un audit de conformité en définissant les objectifs, les critères et le programme de travail selon les risques et les ressources.
- Conduite et formalisation de l'audit en collectant les preuves, en évaluant les mesures de sécurité et en qualifiant les conformités, non-conformités et axes d'amélioration.

DÉBOUCHÉS PROFESSIONNELS

- Auditeur RGSSI certifié;
- Responsable conformité SI;
- Consultant en audit de sécurité;
- Référent conformité au sein d'une DSI / RSSI.

DOSSIER D'INSCRIPTION

- Fiche d'inscription (retrait au CF-SSI de l'ANSSI ou en ligne;
- Photocopie de la CNI (Ivoiriens) ou photocopie légalisée d'un titre de séjour valide (non-Ivoiriens);
- Photocopie légalisée du dernier diplôme obtenu en lien avec la formation;
- Casier judiciaire datant de moins de 3 mois;
- Reçu de paiement des frais;
- Curriculum vitae certifié sincère;
- 3 photos d'identité récentes, de même tirage;
- Le registre des inscriptions est ouvert au CF-SSI dans les délais fixés par l'ANSSI. Le dépôt des dossiers se fait sur rendez-vous. Seuls les dossiers complets sont acceptés.



2. CERTIFICATION DES EXPERTS EN INTEGRATION DU RGSSI : NIVEAU 1

Durée : 05 jours

Vos systèmes d'information, vos collaborateurs et vos partenaires sont au cœur de votre activité, mais constituent également des cibles privilégiées pour les cybercriminels. Décideurs comme experts IT, cette formation certifiante vous donne les clés pour maîtriser le cadre juridique national. Comprendre le paysage national de la cybersécurité, bâtir une gouvernance robuste, anticiper les risques pesant sur l'information et prioriser vos efforts de protection de vos actifs informationnels.

OBJECTIFS

- Maîtriser les concepts fondamentaux de la cybersécurité;
- Comprendre les menaces, vulnérabilités et mécanismes d'attaque;
- Structurer une gouvernance de cybersécurité efficace;
- Anticiper les risques cyber et mesurer leurs impacts financiers, juridiques et réputationnels;
- Prendre des décisions éclairées en situation de cyber crise;
- Favoriser la collaboration entre les métiers, d'une organisation d'une institution.

CONDITIONS D'ACCÈS

- Bonne connaissance des systèmes informatiques, des politiques de sécurité SI et du RGSSI;
- Maîtrise des outils bureautiques et d'Internet;
- Bonne connaissance de la protection des données à caractère personnel;
- Excellentes capacités relationnelles, organisationnelles et rédactionnelles.

PUBLIC CONCERNÉ

- Cadres, responsables IT, DG, DRH, DAF et directeurs d'exploitation impliqués dans les décisions de sécurité;
- RSSI et spécialistes de la sécurité des SI;
- Auditeurs et responsables de conformité;
- Chefs de projets digitaux;
- Responsables de Gestion de risques ou de conformité.

PROGRAMME (9 modules)

- Module inaugural de la formation;
- Cadre juridique de la cybersécurité;
- Introduction à la cybersécurité et paysage national;
- Gouvernance et pilotage de la sécurité;
- Sécurité des ressources humaines;
- Gestion des actifs, menaces et risques informatiques;
- Gouvernance de la gestion des accès;
- Gestion des vulnérabilités et incidents;
- Gestion des fournisseurs et des changements.

COMPÉTENCES ACQUISES

- Maîtrise du cadre réglementaire et des principales cybermenaces nationales.
- Pilotage d'une gouvernance de sécurité intégrant les ressources humaines et la protection des actifs informationnels.

DÉBOUCHÉS PROFESSIONNELS

- RSSI adjoint;
- Chargé de la sécurité des systèmes d'information;
- Référent cybersécurité;
- Coordinateur conformité RGSSI.

DOSSIER D'INSCRIPTION

- Fiche d'inscription (retrait au CF-SSI de l'ANSSI ou en ligne;
- Photocopie de la CNI (Ivoiriens) ou photocopie légalisée d'un titre de séjour valide (non-Ivoiriens);
- Photocopie légalisée du dernier diplôme obtenu en lien avec la formation;
- Casier judiciaire datant de moins de 3 mois;
- Reçu de paiement des frais;
- Curriculum vitae certifié sincère;
- 3 photos d'identité récentes, de même tirage;
- Le registre des inscriptions est ouvert au CF-SSI dans les délais fixés par l'ANSSI. Le dépôt des dossiers se fait sur rendez-vous. Seuls les dossiers complets sont acceptés.

3. CERTIFICATION DES EXPERTS EN INTEGRATION DU RGSSI : NIVEAU 2

Durée : 05 jours

Passez du niveau fondamental au niveau expert. Réservée aux professionnels déjà certifiés Niveau 1, cette formation vous apprend à piloter un programme de conformité RGSSI complet, à mobiliser les parties prenantes, à gérer les risques, à définir prioriser et suivre les actions de sécurisation et à inscrire durablement la protection des systèmes d'information dans une démarche d'amélioration continue.

OBJECTIFS

- Traduire les exigences du RGSSI en mesures de sécurité concrètes, adaptées aux risques et aux enjeux de l'organisation;
- Évaluer le niveau de conformité existant, et définir les priorités de mise en conformité;
- Concevoir, déployer, piloter et améliorer un programme complet de conformité au RGSSI;
- Préparer l'organisation aux audits de conformité, et piloter les actions correctives;
- Mobiliser et coordonner les parties prenantes impliquées dans la sécurité des systèmes d'information.

CONDITIONS D'ACCÈS

- Diplôme Bac +3 en Technologies de l'Information;
- Certificat Niveau 1 « EXPERT EN INTEGRATION DU RGSSI »;
- Au moins 1 an d'expérience en management des systèmes d'information;
- Bonne connaissance des systèmes informatiques, des politiques de sécurité SI et du RGSSI;
- Maîtrise des outils bureautiques et d'Internet, notions en protection des données personnelles;
- Excellentes capacités relationnelles, organisationnelles et rédactionnelles.

PUBLIC CONCERNÉ

- Cadres et professionels IT,
- RSSI, DSI;
- Auditeurs et responsables de conformité.

PROGRAMME (9 modules)

- Module inaugural de la formation;
- Infractions spécifiques aux TIC;
- Matrice des méthodes et techniques d'attaques;
- Protection des infrastructures physiques;
- Mesures techniques de sécurité;
- Planification de la mise en œuvre des mesures SSI;
- Mise en œuvre des mesures SSI;
- Suivi, amélioration et préparation de l'audit;
- Cas pratique.

COMPÉTENCES ACQUISES

- Identification et définition d'un plan de sécurisation conforme au RGSSI, adapté aux risques et aux responsabilités juridiques.
- Pilotage, documentation et évaluation la mise en œuvre des mesures de sécurité, suivre les actions correctives et préparer les audits de conformité

DÉBOUCHÉS PROFESSIONNELS

- RSSI;
- Consultant en systèmes de management de la sécurité;
- Auditeur interne;
- Chef de projet conformité SI.

DOSSIER D'INSCRIPTION

- Identifiant du certificat Niveau 1;
- Fiche d'inscription (retrait au CF-SSI de l'ANSSI ou en ligne);
- Photocopie de la CNI (Ivoiriens) ou photocopie légalisée d'un titre de séjour valide (non-Ivoiriens);
- Photocopie légalisée du dernier diplôme obtenu en lien avec la formation;
- Casier judiciaire datant de moins de 3 mois;
- Reçu de paiement des frais;
- Curriculum vitae certifié sincère;
- 3 photos d'identité récentes, de même tirage;
- Le registre des inscriptions est ouvert au CF-SSI dans les délais fixés par l'ANSSI. Les candidats sont informés. Le dépôt des dossiers se fait sur rendez-vous. Seuls les dossiers complets sont acceptés.

FORMATIONS AUX APTITUDES TECHNIQUES

4. POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION (PSSI)

Durée : 02 jours

La PSSI, annexée au décret n°2021-915, est le cadre de référence des mesures de securité protection des systèmes d'information de l'administration publique ivoirienne, bâtie sur le RGSSI. En deux jours, appropriez-vous ses principes, ses règles et ses mécanismes de gouvernance pour bâtir la stratégie de sécurisation de votre propre organisation.

OBJECTIFS

- Comprendre les concepts fondamentaux de la PSSI de l'administration ivoirienne;
- Formaliser les règles, les pratiques et les procédures de gestion de la sécurité de l'information;
- Mettre en place une organisation et un schéma de gouvernance clairs et approuvés;
- Expliquer et appliquer les approches et techniques de mise en œuvre et de gestion des mesures de sécurité.

CONDITIONS D'ACCÈS

- Connaissances fondamentales en cybersécurité;
- Connaissance des mesures techniques de sécurité de l'information.

PUBLIC CONCERNÉ

- Responsables de la sécurité des systèmes d'information;
- Directeurs des systèmes d'information;
- Personnes en charge de la sécurité, de la conformité, du risque ou de la gouvernance;
- Professionnels de l'informatique et consultants souhaitant renforcer leurs compétences en sécurité de l'information.

PROGRAMME (2 modules)

- Principes et règles des thèmes 1 à 7;
- Principes et règles relatives aux domaines 12 à 16.

COMPÉTENCES ACQUISES

- Élaboration et formalisation d'une PSSI;
- Gouvernance de la sécurité des SI en administration publique.

DÉBOUCHÉS PROFESSIONNELS

- Référent PSSI;
- RSSI et ASSI;
- Consultant en gouvernance SSI pour le secteur public.

DOSSIER D'INSCRIPTION

- Fiche d'inscription (retrait au CF-SSI de l'ANSSI ou en ligne;
- Photocopie de la CNI (Ivoiriens) ou photocopie légalisée d'un titre de séjour valide (non-Ivoiriens);
- Photocopie légalisée du dernier diplôme obtenu en lien avec la formation;
- Casier judiciaire datant de moins de 3 mois;
- Reçu de paiement des frais;
- Curriculum vitae certifié sincère;
- 3 photos d'identité récentes, de même tirage;
- Le registre des inscriptions est ouvert au CF-SSI dans les délais fixés par l'ANSSI. Le dépôt des dossiers se fait sur rendez-vous. Seuls les dossiers complets sont acceptés.

CENTRE DE FORMATION ANSSI CI

Agréé FDFP

5. COMPRENDRE ET CONTRER LA DÉSINFORMATION EN LIGNE

Durée : 03 jours

Une rumeur virale peut ruiner en quelques heures une réputation construite en des années. Face à la multiplication des campagnes de désinformation sur les réseaux sociaux, forums et messageries, le CFSSI forme les professionnels de la communication à identifier les contenus trompeurs, modérer efficacement les espaces numériques et préserver la confiance du public.

OBJECTIFS

- Renforcer les capacités de détection et de vérification des fausses informations;
- Gérer les fausses informations circulant sur les réseaux sociaux, forums et messageries;
- Protéger la réputation des institutions et préserver la confiance du public;
- Maintenir des espaces d'échange fiables et sains.

CONDITIONS D'ACCÈS

- Connaissance générale de l'usage d'Internet et des réseaux sociaux niveau utilisateur.

PUBLIC CONCERNÉ

- Directeurs et responsables de communication;
- Agents et journalistes de presse;
- Administrateurs et animateurs de communauté en ligne;
- Marketeurs et distributeurs en ligne.

PROGRAMME (5 modules)

- Introduction à la désinformation;
- Typologie des fausses informations;
- Cadre légal de la lutte contre la désinformation;
- Bonnes pratiques de prévention et de gestion de la désinformation;
- Outils et méthodes de vérification des fake news.

COMPÉTENCES ACQUISES

- Détection et vérification de fausses informations;
- Gestion de crise informationnelle;
- Modération d'espaces numériques.

DÉBOUCHÉS PROFESSIONNELS

- Responsable de veille informationnelle;
- Community manager institutionnel;
- Chargé de communication de crise;
- Analyste désinformation.

DOSSIER D'INSCRIPTION

- Fiche d'inscription (retrait au CF-SSI de l'ANSSI ou en ligne);
- Photocopie de la CNI (Ivoiriens) ou photocopie légalisée d'un titre de séjour valide (non-Ivoiriens);
- Photocopie légalisée du dernier diplôme obtenu en lien avec la formation;
- Casier judiciaire datant de moins de 3 mois
- Reçu de paiement des frais;
- Curriculum vitae certifié sincère;
- 3 photos d'identité récentes, de même tirage;
- Le registre des inscriptions est ouvert au CF-SSI dans les délais fixés par l'ANSSI. Les candidats sont informés. Le dépôt des dossiers se fait sur rendez-vous. Seuls les dossiers complets sont acceptés.

6. MÉTHODOLOGIE DE RECHERCHE ET DE COLLECTE EN RÉSEAUX SOCIAUX (OSINT)

Durée : 03 jours

Les réseaux criminels organisés exploitent chaque jour les réseaux sociaux (trafics, traite des personnes, migration irrégulière, vol de données ...). Le Centre de lutte informationnelle forme les enquêteurs à des méthodologies éprouvées de recherche et de collecte en sources ouvertes (OSINT), adaptées aux réalités numériques du terrain. Enquêtez plus vite, plus loin et en toute sécurité.

OBJECTIFS

- Renforcer vos capacités de recherche en sources ouvertes;
- Collecter des informations pertinentes sur les réseaux sociaux;
- Documenter et analyser des activités criminelles en ligne.

CONDITIONS D'ACCÈS

- Connaissance générale de l'usage d'Internet et des réseaux sociaux (niveau utilisateur).

PUBLIC CONCERNÉ

- Analystes et enquêteurs souhaitant renforcer leurs compétences de recherche, de collecte et d'analyse d'informations issues des réseaux sociaux;
- Avocats, commissaires de justice, professionnels du droit, experts judiciaires.

PROGRAMME (5 modules)

- Généralités sur les enquêtes en ligne et les réseaux sociaux;
- Sécurité opérationnelle de l'enquêteur;
- Collecte et conservation des preuves numériques;
- Création et gestion de comptes;
- Techniques de recherche et de collecte.

COMPÉTENCES ACQUISES

- Méthodologie OSINT;
- Sécurité opérationnelle en enquête numérique;
- Collecte et conservation de preuves numériques.

DÉBOUCHÉS PROFESSIONNELS

- Enquêteur cyber;
- Analyste OSINT;
- Chargé d'enquête numérique;
- Analyste sécurité / veille.

DOSSIER D'INSCRIPTION

- Fiche d'inscription (retrait au CF-SSI de l'ANSSI ou en ligne;
- Photocopie de la CNI (Ivoiriens) ou photocopie légalisée d'un titre de séjour valide (non-Ivoiriens);
- Photocopie légalisée du dernier diplôme obtenu en lien avec la formation;
- Casier judiciaire datant de moins de 3 mois;
- Reçu de paiement des frais;
- Curriculum vitae certifié sincère;
- 3 photos d'identité récentes, de même tirage;
- Le registre des inscriptions est ouvert au CF-SSI dans les délais fixés par l'ANSSI. Le dépôt des dossiers se fait sur rendez-vous. Seuls les dossiers complets sont acceptés.

7. PRÉVENTION ET DÉTECTION DES ATTAQUES DE PHISHING

Durée : 03 jours

Un seul clic sur un courriel piégé peut compromettre toute une organisation. Le phishing reste l'une des menaces les plus répandues et les plus dévastatrices. Cette formation transforme vos agents en première ligne de défense: en leur offrant la capacité de détecter, d'analyser et de réagir efficacement face aux courriels frauduleux et à l'hameçonnage.

OBJECTIFS

- Comprendre en profondeur les mécanismes et objectifs des attaques par phishing;
- Identifier les différentes formes de courriels piégés et les techniques d'ingénierie sociale;
- Acquérir des méthodes concrètes de détection et de validation des e-mails suspects;
- Mettre en œuvre des stratégies de protection à plusieurs niveaux;
- Réagir efficacement en cas d'incident grâce à des procédures adaptées.

CONDITIONS D'ACCÈS

- Agents publics ou personnels manipulant des courriels professionnels sensibles;
- Responsables ou référents en sécurité informatique;
- Avoir idéalement suivi une formation de sensibilisation à la sécurité numérique de base.

PUBLIC CONCERNÉ

- Toute personne amenée à manipuler, traiter ou sécuriser des informations par voie électronique, en particulier les profils exposés au phishing, à l'ingénierie sociale et aux cyberattaques ciblées.

PROGRAMME (4 modules)

- Comprendre le phishing et ses mécanismes;
- Techniques d'hameçonnage ciblé et détection;
- Prévention, protection et réaction;
- Exercices et outils pratiques.

COMPÉTENCES ACQUISES

- Détection des e-mails frauduleux;
- Réponse à incident phishing;
- Sensibilisation et réflexes de cybersécurité.

DÉBOUCHÉS PROFESSIONNELS

- Référent sécurité informatique;
- Agent support IT;
- Chargé de sensibilisation cybersécurité.

DOSSIER D'INSCRIPTION

- Fiche d'inscription (retrait au CF-SSI de l'ANSSI ou en ligne;
- Photocopie de la CNI (Ivoiriens) ou photocopie légalisée d'un titre de séjour valide (non-Ivoiriens);
- Photocopie légalisée du dernier diplôme obtenu en lien avec la formation;
- Casier judiciaire datant de moins de 3 mois;
- Reçu de paiement des frais;
- Curriculum vitae certifié sincère;
- 3 photos d'identité récentes, de même tirage;
- Le registre des inscriptions est ouvert au CF-SSI dans les délais fixés par l'ANSSI. Le dépôt des dossiers se fait sur rendez-vous. Seuls les dossiers complets sont acceptés.

8. TECHNIQUES DE TRAÇAGE ET D'ANALYSE D'ADRESSES IP MALVEILLANTES

Durée : 03 jours

Derrière chaque intrusion, scan, botnet ou campagne de phishing se cache une adresse IP. Encore faut-il savoir la faire parler. Cette formation résolument pratique vous donne les méthodes et les outils pour identifier, tracer et analyser les activités malveillantes associées à une adresse IP et transformer vos constats en rapports techniques exploitables.

OBJECTIFS

- Comprendre l'utilisation des adresses IP dans les attaques informatiques;
- Maîtriser des outils d'analyse essentiels (WHOIS, BGP, ASN, géolocalisation);
- Mettre en œuvre une méthodologie de traçage pour identifier l'origine d'une activité suspecte;
- Croiser et interpréter des informations issues de sources publiques;
- Rédiger un rapport technique d'analyse clair, structuré et exploitable.

CONDITIONS D'ACCÈS

- Connaissance générale des réseaux TCP/IP;
- Notions en administration des systèmes et des réseaux;
- Capacité à utiliser la ligne de commande sous Linux ou Windows.

PUBLIC CONCERNÉ

- Tout professionnel de l'informatique souhaitant acquérir des compétences en traçage et analyse d'adresses IP malveillantes.

PROGRAMME (6 modules)

- Introduction aux adresses IP et aux menaces associées;
- Méthodes et outils de traçage;
- Exploitation de bases publiques;
- Atelier pratique - analyse d'IP malveillantes;
- Bonnes pratiques de restitution.

COMPÉTENCES ACQUISES

- Usage des outils WHOIS / BGP / ASN / géolocalisation;
- Méthodologie de traçage d'IP;
- Rédaction de rapports techniques d'analyse.

DÉBOUCHÉS PROFESSIONNELS

- Analyste SOC;
- Analyste threat intelligence;
- Enquêteur cyber;
- Administrateur réseau sécurité.

DOSSIER D'INSCRIPTION

- Fiche d'inscription (retrait au CF-SSI de l'ANSSI ou en ligne;
- Photocopie de la CNI (Ivoiriens) ou photocopie légalisée d'un titre de séjour valide (non-Ivoiriens);
- Photocopie légalisée du dernier diplôme obtenu en lien avec la formation;
- Casier judiciaire datant de moins de 3 mois;
- Reçu de paiement des frais;
- Curriculum vitae certifié sincère;
- 3 photos d'identité récentes, de même tirage;
- Le registre des inscriptions est ouvert au CF-SSI dans les délais fixés par l'ANSSI. Le dépôt des dossiers se fait sur rendez-vous. Seuls les dossiers complets sont acceptés.

9. SÉCURISATION DES INFRASTRUCTURES DE MESSAGERIE ÉLECTRONIQUE

Durée : 02 jours

La messagerie électronique est la porte d'entrée préférée des attaquants : phishing, BEC, usurpation d'identité, malwares. Cette formation vous apprend à bâtir une infrastructure de messagerie réellement sécurisée, appuyée sur des politiques solides, les bonnes pratiques du domaine et les protocoles de référence (SPF, DKIM, DMARC, TLS).

OBJECTIFS

- Comprendre les menaces spécifiques ciblant la messagerie;
- Appliquer les meilleures pratiques de sécurisation des serveurs et services de messagerie;
- Mettre en œuvre les protocoles d'authentification et de protection des e-mails (SPF, DKIM, DMARC, TLS);
- Déployer des solutions de filtrage et de détection avancée (antispam, sandbox, passerelles sécurisées);
- Développer une approche de résilience et sensibiliser les utilisateurs finaux.

CONDITIONS D'ACCÈS

- Connaissances générales en administration système (Windows / Linux);
- Notions de réseaux informatiques (TCP/IP, DNS, pare-feu);
- Connaissances générales des certificats SSL/TLS et de la gestion des identités numériques.

PUBLIC CONCERNÉ

- Administrateurs systèmes et réseaux;
- Gestionnaires messagerie;
- Responsables et ingénieurs sécurité (SOC, RSSI, CSIRT);
- Équipes d'exploitation IT en charge des services de communication;
- Responsables de la continuité de service et de la reprise après incident (PRA/PCA).

PROGRAMME (2 modules)

- Compréhension des menaces et mise en place d'une infrastructure de messagerie sécurisée;
- Protection opérationnelle, gestion des incidents et sensibilisation.

COMPÉTENCES ACQUISES

- Configuration SPF / DKIM / DMARC / TLS;
- Filtrage antispam et sandboxing;
- Résilience et continuité de la messagerie.

DÉBOUCHÉS PROFESSIONNELS

- Administrateur de messagerie sécurisée;
- Ingénieur sécurité SOC / CSIRT;
- Référent PRA/PCA messagerie.

DOSSIER D'INSCRIPTION

- Fiche d'inscription (retrait au CF-SSI de l'ANSSI ou en ligne;
- Photocopie de la CNI (Ivoiriens) ou photocopie légalisée d'un titre de séjour valide (non-Ivoiriens);
- Photocopie légalisée du dernier diplôme obtenu en lien avec la formation;
- Casier judiciaire datant de moins de 3 mois;
- Reçu de paiement des frais;
- Curriculum vitae certifié sincère;
- 3 photos d'identité récentes, de même tirage;
- Le registre des inscriptions est ouvert au CF-SSI dans les délais fixés par l'ANSSI. Le dépôt des dossiers se fait sur rendez-vous. Seuls les dossiers complets sont acceptés.

CENTRE DE FORMATION ANSSI CI

Agréé FDFP

10. IDENTIFICATION ET PRÉVENTION DES VULNÉRABILITÉS WEB : INJECTIONS SQL ET XSS

Durée : 03 jours

Les injections SQL et les failles XSS figurent, année après année, parmi les vulnérabilités web les plus exploitées au monde. Cette formation vous place des deux côtés de la barrière : identifier ces failles, les exploiter en environnement contrôlé pour en comprendre la mécanique, puis déployer les mesures préventives adaptées selon les bonnes pratiques OWASP.

OBJECTIFS

- Identifier les vulnérabilités de type injection SQL et XSS;
- Exploiter ces vulnérabilités en environnement contrôlé;
- Mettre en place des mesures préventives efficaces;
- Réaliser un audit de sécurité web;
- Appliquer les bonnes pratiques OWASP.

CONDITIONS D'ACCÈS

- Connaissances de base en développement web;
- Notions de HTML, JavaScript et SQL;
- Compréhension générale des architectures web.

PUBLIC CONCERNÉ

- Développeurs web;
- Administrateurs systèmes;
- Auditeurs sécurité;
- Testeurs QA;
- RSSI.

PROGRAMME (3 modules)

- Sécurité web et injections SQL;
- Défense contre les injections SQL et introduction au XSS;
- Prévention du XSS et audit final.

COMPÉTENCES ACQUISES

- Exploitation contrôlée des failles SQL / XSS;
- Audit de sécurité applicative web;
- Application des bonnes pratiques OWASP.

DÉBOUCHÉS PROFESSIONNELS

- Développeur sécurisé (secure coding);
- Pentester junior;
- Auditeur en sécurité applicative;
- RSSI / référent sécurité web.

DOSSIER D'INSCRIPTION

- Fiche d'inscription (retrait au CF-SSI de l'ANSSI ou en ligne;
- Photocopie de la CNI (Ivoiriens) ou photocopie légalisée d'un titre de séjour valide (non-Ivoiriens);
- Photocopie légalisée du dernier diplôme obtenu en lien avec la formation;
- Casier judiciaire datant de moins de 3 mois;
- Reçu de paiement des frais;
- Curriculum vitae certifié sincère;
- 3 photos d'identité récentes, de même tirage;
- Le registre des inscriptions est ouvert au CF-SSI dans les délais fixés par l'ANSSI. Le dépôt des dossiers se fait sur rendez-vous. Seuls les dossiers complets sont acceptés.

11. BONNES PRATIQUES DE SÉCURISATION DES SERVICES DNS ET DES SERVEURS WEB

Durée : 02 jours

Le DNS et les serveurs web sont les fondations critiques et pourtant souvent négligées de toute infrastructure numérique. Cette formation vous apprend à identifier les menaces qui les ciblent et à déployer une méthodologie de défense en profondeur pour les durcir et les sécuriser durablement.

OBJECTIFS

- Identifier les menaces pesant sur les services DNS et les serveurs web;
- Configurer et durcir les services DNS et web pour réduire les risques;
- Déployer les meilleures pratiques de sécurisation;
- Utiliser des outils d'audit et de monitoring;
- Appliquer une méthodologie de défense en profondeur.

CONDITIONS D'ACCÈS

- Connaissances de base en administration système;
- Notions de réseaux (TCP/IP, DNS, HTTP/HTTPS);
- Compréhension des architectures web.

PUBLIC CONCERNÉ

- Administrateurs systèmes;
- Ingénieurs réseaux;
- Exploitants DNS / Web;
- RSSI.

PROGRAMME (2 modules)

- Sécurisation des services DNS;
- Sécurisation des serveurs web.

COMPÉTENCES ACQUISES

- Durcissement des services DNS et web;
- Audit et monitoring de sécurité;
- Méthodologie de défense en profondeur.

DÉBOUCHÉS PROFESSIONNELS

- Administrateur systèmes et réseaux;
- Ingénieur infrastructure / exploitant DNS-Web;
- Référent sécurité technique;
- Auditeur technique junior.

DOSSIER D'INSCRIPTION

- Fiche d'inscription (retrait au CF-SSI de l'ANSSI ou en ligne;
- Photocopie de la CNI (Ivoiriens) ou photocopie légalisée d'un titre de séjour valide (non-Ivoiriens);

DOSSIER D'INSCRIPTION

- Photocopie légalisée du dernier diplôme obtenu en lien avec la formation;
- Casier judiciaire datant de moins de 3 mois;
- Reçu de paiement des frais;
- Curriculum vitae certifié sincère;
- 3 photos d'identité récentes, de même tirage;
- Le registre des inscriptions est ouvert au CF-SSI dans les délais fixés par l'ANSSI. Le dépôt des dossiers se fait sur rendez-vous. Seuls les dossiers complets sont acceptés.

CALENDRIER 2026 DES FORMATIONS

FORMATIONS CERTIFIANTES		
THÈMES / ACTIVITÉS	**DATES**	**DURÉES**
Formation Auditeurs RGSSI 2025 (25 pers.)	**Du 31 août au 04 sept. 2026**	**05 jours**
Évaluations	08 et 11 sept. 2026	02 jours
Formation Auditeurs RGSSI 2025 (25 pers.)	Du 21 au 25 sept. 2026	05 jours
Évaluations	29 sept. et 02 oct. 2026	02 jours
Formation Auditeurs RGSSI 2025 (25 pers.)	Du 12 au 16 oct. 2026	05 jours
Évaluations	20 et 23 oct. 2026	02 jours
Formation RGSSI 2025 (25 pers.)	Du 02 au 06 nov. 2026	05 jours
Évaluations	10 et 13 nov. 2026	02 jours
Formation RGSSI 2025 (25 pers.)	Du 23 au 27 nov. 2026	05 jours
Évaluations	01 et 04 déc. 2026	02 jours
Formation Experts Intégration RGSSI N1 (25 pers.)	**Du 07 au 11 sept. 2026**	**05 jours**
Évaluations	15 et 18 sept. 2026	02 jours
Formation Experts Intégration RGSSI N1 (25 pers.)	Du 05 au 09 oct. 2026	05 jours
Évaluations	13 et 16 oct. 2026	02 jours
Évaluations	Du 02 au 06 nov. 2026	05 jours
Formation Experts Intégration RGSSI N1 (25 pers.)	10 et 13 nov. 2026	02 jours
Formation Experts Intégration RGSSI N1 (25 pers.)	Du 30 nov. au 04 déc. 2026	05 jours
Évaluations	08 et 11 déc. 2026	02 jours
Formation Experts Intégration RGSSI N2 (25 pers.)	Du 07 au 11 sept. 2026	05 jours
Évaluations	15 et 18 sept. 2026	02 jours
Formation Experts Intégration RGSSI N1 (25 pers.)	Du 05 au 09 oct. 2026	05 jours
Évaluations	13 et 16 oct. 2026	02 jours
Évaluations	Du 02 au 06 nov. 2026	05 jours
Formation Experts Intégration RGSSI N1 (25 pers.)	10 et 13 nov. 2026	02 jours
Formation Experts Intégration RGSSI N1 (25 pers.)	Du 30 nov. au 04 déc. 2026	05 jours
Évaluations	08 et 11 déc. 2026	02 jours

FORMATIONS AUX APTITUDES TECHNIQUES		
THÈMES / ACTIVITÉS	**DATES**	**DURÉES**
Prévention et détection des attaques de phishing	Du 01 au 03 sept. 2026	03 jours
Comprendre et contrer la désinformation en ligne	Du 14 au 16 sept. 2026	03 jours
Comprendre et contrer la désinformation en ligne	Du 28 au 30 sept. 2026	03 jours
Sécurisation des infrastructures de messagerie électronique	Du 01 au 02 oct. 2026	02 jours
Techniques de traçage et d'analyse d'adresses IP malveillantes	Du 05 au 06 oct. 2026	03 jours
Méthodologie de recherche et de collecte OSINT	Du 12 au 14 oct. 2026	03 jours
Identification et prévention des vulnérabilités web : injections SQL et XSS	Du 26 au 28 oct. 2026	03 jours
Bonnes pratiques de sécurisation des services DNS et des serveurs web	Du 02 au 03 nov. 2026	02 jours
Techniques de traçage et d'analyse d'adresses IP malveillantes	Du 16 au 18 nov. 2026	03 jours
Politique de Sécurité des Systèmes d'Information (PSSI)	Du 23 au 24 nov. 2026	02 jours
Identification et prévention des vulnérabilités web : injections SQL et XSS	Du 01 au 02 déc. 2026	03 jours
Méthodologie de recherche et de collecte OSINT	Du 14 au 16 déc. 2026	03 jours
Bonnes pratiques de sécurisation des services DNS et des serveurs web	Du 21 au 22 déc. 2026	02 jours
Prévention et détection des attaques de phishing	Du 28 au 30 déc. 2026	03 jours

ANSSI
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
CÔTE D'IVOIRE

marketing.commerce@anssi.gouv.ci

+225 07 59 00 66 00

551 rue J79 KOUAO Eugène Boka,
cocody vallon Sopim

NOS PARTENAIRES

ESATIC
ECOLE SUPÉRIEURE AFRICAINE DES TIC

ENSEA

CENTRE DE FORMATION ANSSI CI

Agréé FDFP
Fonds de Développement de la Formation Professionnelle