Association
Des
Neticiens

Pour que chacun.e puisse développer ses compétences en numérique et cybersécurité.

PRÉSENTATION DE LA FORMATION EN ALTERNANCE

INGÉNIEUR SYSTÈMES, RÉSEAUX ET CYBERSÉCURITÉ

TITRE PROFESSIONNEL
Niveau 7 - équivalent Bac +5
RNCP 38105

Emploi métier de rattachement suivant la nomenclature ROME :

- M1803 - Direction des systèmes d'information
- M1806 - Conseil et maîtrise d'ouvrage en systèmes d'information
- M1805 - Études et développement informatique
- M1802 - Expertise et support en systèmes d'information

I -PRÉSENTATION GÉNÉRALE

L'Association des Neticiens

L'ÉQUIPE DE L'ADN

Christophe Dolinsek

Président

Directeur Cisco Networking Academy

Michel Tabouret

Vice-président

Ingénierie pédagogique ADN et réseau IUT

Frédéric Géraud

Secrétaire

Responsable des affaires publiques Google Cloud France

Didier Jehl

Trésorier

Ingénierie pédagogique ADN et réseau IUT

Kaya Issiakou

Directrice de coordination

Référente qualité

Laetitia Jean

Trésorière adjointe

Responsable administrative

Elodie Brosset

Responsable communication

Réseau des formateurs ADN

400 Enseignants en IUT Réseaux & Télécoms et professionnels du secteur

Pour les questions liées à l'accompagnement des Personnes en Situation de Handicap, nous vous invitons à contacter **Laëtitia JEAN** (référente handicap et mobilité) ou **Kaya ISSIAKOU** (référente suppléante).

I -PRÉSENTATION GÉNÉRALE

L'Association des Neticiens

MISSIONS ET VALEURS

MISSIONS

- Être une passerelle entre les futurs professionnels et les entreprises
- Rendre l'accès aux métiers et formations du numérique et de la cybersécurité accessible au plus grand nombre

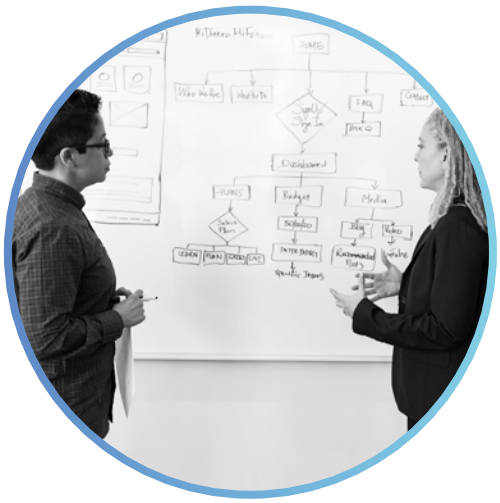
VALEURS

- Égalité femmes/hommes, féminisation de l'IT
- Qualité de la formation et du suivi
- Ecoute des besoins et adaptabilité de la formation
- Transmission de compétences opérationnelles

I -PRÉSENTATION GÉNÉRALE

L'ingénieur systèmes, réseaux, cybersécurité

L'ingénieur systèmes, réseaux et cybersécurité (ISRC) est capable de concevoir, mettre en oeuvre et maintenir l'architecture du système d'information d'une structure en prenant en compte tous les aspects liés au projet à savoir : techniques et technologiques, juridiques, sécuritaires et organisationnels.



Il est en mesure de gérer un projet international dans sa globalité en prenant en compte les indicateurs pertinents, les risques potentiels liés au projet et sait maitriser le planning et les coûts liés au projet.

Il est capable d'identifier les problèmes à l'origine du besoin et de cerner les exigences du client. Il met en lumière les contraintes techniques et juridiques afin de choisir les technologies les plus adaptées.

Il est capable de concevoir l'architecture générale d'un système d'information ou d'un ICS (Industrial Control System) comme de rédiger la documentation opérationnelle ou d'organiser et animer des formations de prise en main du système. Il maitrise entre autres choses le déploiement automatique de solutions, le cloud, la gestion des flux réseaux (QoS), le SD-WAN, les solutions VOIP et/ou TOIP et la msie en place d'un SOC (Security Operation Center).

L'ingénieur systèmes, réseaux et cybersécurité est capable de maintenir le système en condition opérationnelle et de sécurité. Il peut mettre en place un SMSI (Système de Management de la Sécurité Informatique), réalise des analyses de risques de sécurité (EBIOS ou ISO 27005), et définit la stratégie de maintenance préventive et curative du système.

II -PRÉSENTATION DE LA FORMATION ISRC

Modalité de formation

Titre professionnel de niveau 7, (bac +5)

Ingénieur Systèmes, Réseaux et Cybersécurité

52 semaines :

d'octobre 2023 à octobre 2024

560 heures de formation

Nombre de places disponibles :

12 apprentis

Rythme d'alternance :

1 semaine en formation, 3 semaines en entreprise

Lieu de regroupement :

Ile-de-France

5 semaines en présentiel sur l'année, le reste des cours étant suivi à distance

Accessibilité :

En présentiel : Locaux pouvant accueillir les personnes en situation de handicap

En distanciel : Accessible à toute personne pouvant manipuler un ordinateur

Formateurs :

enseignants du réseau des IUT Réseaux & Télécoms et professionnels du domaine

Recrutement des apprentis :

réseaux des IUT Réseaux & Télécoms, Cisco Networking Academy et entreprises

Points forts :

- Tous les blocs de compétences techniques sont abordés **pendant les 3 premiers mois**
- **Suivi rigoureux**, en partenariat avec le tuteur en entreprise
- **Ingénierie pédagogique éprouvée**
- Evaluation et suivi des apprentis au début et tout au long de la formation *(voir III - document d'évaluation et de suivi)*

Coûts pédagogiques :
Dans le cadre du contrat d'apprentissage ou de professionnalisation, la formation est gratuite et rémunérée pour l'apprenant.Prix de la formation : 12500€ TTC, majoritairement pris en charge par les OPCO.

Admission :
Sur dossier (CV, lettre de motivation, derniers bulletins de notes) et après entretien. Pré-requis : Titre professionnel de niveau 6 ou diplôme de niveau Bac+4 (Master 1) en Réseaux et Télécommunications.

Dépôt du dossier de candidature :
Sur le site : www.formations-neticiens.net
Par mail : contact@adn-neticien.net

II -PRÉSENTATION DE LA FORMATION ISRC

N° semaine calendaire	Semaine du	Période Entreprise / Période Formation
40	02/10/2023	
41	09/10/2023	1- Présentiel
42	16/10/2023	2- Distanciel
43	23/10/2023	
44	30/10/2023	
45	06/11/2023	
46	13/11/2023	3 - Distanciel
47	20/11/2023	
48	27/11/2023	
49	04/12/2023	
50	11/12/2023	4 - Distanciel
51	18/12/2023	
52	25/12/2023	
1	01/01/2024	
2	08/01/2024	5 - Distanciel
3	15/01/2024	
4	22/01/2024	6 - Présentiel
5	29/01/2024	
6	05/02/2024	
7	12/02/2024	7 - Distanciel
8	19/02/2024	
9	26/02/2024	
10	04/03/2024	
11	11/03/2024	8 - Distanciel
12	18/03/2024	
13	25/03/2024	
14	01/04/2024	9 - Distanciel

N° semaine calendaire	Semaine du	Période Entreprise / Période Formation
15	08/04/2024	
16	15/04/2024	
17	22/04/2024	10 - Présentiel
18	29/04/2024	
19	06/05/2024	
20	13/05/2024	
21	20/05/2024	
22	27/05/2024	11 - Distanciel
23	03/06/2024	
24	10/06/2024	
25	17/06/2024	12 - Présentiel
26	24/06/2024	13 - Distanciel
27	01/07/2024	
28	08/07/2024	
29	15/07/2024	
30	22/07/2024	
31	29/07/2024	
32	05/08/2024	
33	12/08/2024	
34	19/08/2024	
35	26/08/2024	14 - Distanciel
36	02/09/2024	
37	09/09/2024	
38	16/09/2024	15 - Distanciel
39	23/09/2024	16 - Présentiel
40	30/09/2024	
41	07/10/2024	

II -PRÉSENTATION DE LA FORMATION ISRC

La formation se compose de 5 blocs de compétences dont 3 autour de compétences techniques comme détaillé ci-après.

Bloc de compétences et compétences:

Gérer un projet international

A1.1 Initialiser le projet	A1.2 Conduire le projet	A1.3 Clore le projet	
✓			Identifier les parties prenantes
✓			Choisir la méthode de gestion de projet adaptée
✓			Identifier la Core Team (équipe projet minimale)
✓			Rédiger le plan de management de projet
✓			Réaliser un planning de projet
✓			Définir le coût prévisionnel estimé du projet
✓			Définir les indicateurs suivis
✓			Identifier les risques projet afin de sécuriser ce dernier
✓			Rédiger les fiches de risques
✓			Organiser une réunion de lancement afin de partager la vision du projet
✓			Conduire, indifféremment en français ou en anglais, la réunion de lancement
	✓		Comprendre et s'exprimer en anglais sans problème dans un contexte professionnel
	✓		Accepter et exécuter les directives de sa direction
	✓		S'adapter lors d'interactions avec des personnes de cultures différentes afin d'accroitre sa créativité
	✓		Gérer les conflits au sein de l'équipe
	✓		Renforcer la cohésion d'équipe afin de gagner en productivité
	✓		Gérer les relations humaines afin de maintenir une efficience au sein du projet
	✓		Animer les revues de projet, indifféremment en français ou en anglais
	✓		Suivre les dépenses budgétaires
	✓		Communiquer de manière aisée à l'écrit comme à l'oral, en français comme en anglais
	✓		Suivre et analyser les dérives du projet afin de réduire les écarts à échéance

	✓		Gérer avec calme les événements inattendus afin de satisfaire et rassurer le client
	✓		Négocier avec professionnalisme afin de construire une relation client gagnant/gagnant
	✓		Gérer la sous-traitance afin de s'assurer de ne pas avoir de non- conformités ou de dérives à terminaison
		✓	Gérer son équipe projet afin de s'assurer de ne pas avoir de non-conformités ou de dérives aux termes du projet
		✓	Mesurer la satisfaction des parties prenantes afin de déterminer les axes d'amélioration
		✓	Analyser le déroulement du projet afin de déterminer les erreurs qui ont eu lieu durant le projet
		✓	Rédiger un rapport de clôture

Bloc de compétences et compétences:

Recueillir et analyser les exigences du client

A2.1 Recueillir les exigences du client	A2.2 Réaliser l'analyse technique et fonctionnelle	
✓		Identifier les problèmes ou manques à l'origine du besoin
✓		Identifier les différents types d'utilisateurs
✓		Extraire d'un cahier des charges les exigences du client
✓		Identifier les enjeux afin de mieux cerner la problématique du client
✓		Identifier les exigences connexes afin de répondre au besoin du client
✓		Identifier, gérer et suivre les contraintes qualité
✓		Identifier, gérer et suivre les contraintes juridiques et légales
✓		Reformuler la demande afin de s'assurer de la bonne compréhension du besoin
✓		Rédiger les documents formalisant les exigences
	✓	Rédiger les spécifications fonctionnelles du besoin
	✓	Rédiger les spécifications techniques du besoin
	✓	Effectuer des tests exploratoires afin de valider les solutions techniques envisagées
	✓	Choisir les technologies appropriées afin de réaliser l'ensemble des exigences client au mieux et au moindre coût
	✓	Exposer la solution aux parties prenantes afin de partager les solutions techniques envisagées
	✓	Identifier les fonctions représentatives des solutions techniques retenues afin de les mettre en application sur une maquette

	☑	Formaliser les cas d'utilisation de chaque fonction retenue pour la maquette, afin de définir une manière de l'utiliser pour chacune d'elles
	☑	Réaliser des maquettes afin de vérifier et prouver le bon fonctionnement de la solution technique retenue
	☑	Rédiger un cahier de recette afin de permettre la validation de chaque fonction de la maquette
	☑	Conduire une recette afin de prouver au client le bon fonctionnement des solutions techniques retenues

Bloc de compétences et compétences:

Concevoir l'architecture, réaliser et déployer la solution technique

A3.1 Concevoir l'architecture de la solution	A3.2 Sécuriser des systèmes industriels	A3.3 Réaliser et déployer la solution	
☑			Concevoir de manière autonome, une architecture générale sécurisée (MFA, Workload, DMZ, gestion des identités, etc.) d'un système d'informations
☑			Concevoir, de manière autonome, une architecture générale sécurisée d'un ICS (Industrial Control System) en réseau (HAN, NAN, BLÊME)
☑			Intégrer des objets connectés (IOT) sécurisés dans une architecture ICS afin d'obtenir des données plus riches
☑			Identifier, au sein d'une architecture de SI, les données et services critiques afin de déterminer lesquels peuvent être externalisés (IaaS, PaaS, SaaS, CaaS)
☑			Adapter en CLOUD (privé, public, hybride et multicloud) une architecture existante afin d'externaliser une architecture «On Premise»
☑			Prendre en compte les spécifications non techniques (contraintes, normes) afin de garantir l'utilisation ultérieure du système informatique
☑			Réaliser les schémas d'architecture, notamment à l'aide de méthodes comme Merise, UML, AXIAL ou encore IDEF afin de donner une représentation fonctionnelle de celui-ci
☑			Rédiger les documents formalisant l'architecture afin de produire la documentation du projet
☑			Définir les impacts des changements afin de préparer la conduite du changement indispensable
☑			Communiquer les décisions d'architecture afin de partager les choix architecturaux avec le client

A3.1 Concevoir l'architecture de la solution	A3.2 Sécuriser des systèmes industriels	A3.3 Réaliser et déployer la solution	
✓			Définir les régles de gestion des flux réseau (QoS : Quality Of Services) afin de garantir le bon fonctionnement des différents services mis à disposition de l'utilisateur final du système informatique
✓			Définir la politique de virtualisation du système informatique afin de détailler la stratégie d'automatisation du système informatique et de réduction des coûts de l'entreprise
✓			Concevoir une fabric pour pouvoir intégrer le SDN (Software Defined Network) au sein de l'architecture afin de gagner en nombre de manipulations nécessaires pour configurer les équipements
✓			Dissocier, à l'aide du SDS (Software Defined Storage) la gestion du stockage à l'aide d'un logiciel d'un système informatique de la partie matérielle afin d'offrir plus de flexibilité à ce dernier
✓			Rédiger la PSSI (Politique de Sécurité du Système Informatique) afin de définir et expliquer la vision stratégique en termes de sécurité du système informatique
	✓		Adapter son architecture de sécurité à l'utilisation des capteurs et des actionneurs afin de sécuriser un système SCADA (ICS)
	✓		Implémenter un système PAM (Privileged Access Management) dans une architecture ICS afin de limiter les risques de cybersécurité en gérant le contrôle des accès administratifs à l'ICS
		✓	Définir une organisation afin d'assurer le fonctionnement optimal du système informatique et son évolution, en respectant la structure existante et les contraintes qui lui sont liées
		✓	Mettre en œuvre une méthode adaptée, en fonction du SI, de restitution des failles de sécurité, en signalant des recommandations plausibles, selon le contexte de l'entreprise afin de garantir le maintien en condition de sécurité du système informatique
		✓	Intégrer la virtualisation des services au sein de l'architecture afin de réduire les équipements physiques nécessaires
		✓	Mettre en œuvre le NFV (Network function virtualization) afin d'accélérer le déploiement de nouveaux services réseaux et de réduire le nombre d'équipements réseau nécessaires
		✓	Intégrer des solutions de conteneurisation de l'architecture afin de migrer les applications vers des conteneurs
		✓	Intégrer l'orchestration des conteneurs au sein de l'architecture afin d'automatiser le déploiement, la montée en charge et la mise en œuvre de conteneurs d'application sur des clusters

A3.1 Concevoir l'architecture de la solution	A3.2 Sécuriser des systèmes industriels	A3.3 Réaliser et déployer la solution	
		✓	Mettre en œuvre l'IBN (Intent-Based-Networking) afin de réaliser une mise en réseau basée sur les objectifs, de déterminer via l'IA (Intelligence Artificielle) comment exécuter et automatiser les tâches requises pour exploiter un réseau et de superviser l'architecture
		✓	Intégrer le SDN (Software Defined Network) au sein de l'architecture afin de programmer les équipements actifs et donc de réduire les temps de déploiement
		✓	Intégrer le SD-WAN (Software-defined wide-area-network) afin de déporter des services dans le CLOUD, de soulager ou remplacer les liaisons MPLS trop onéreuses pour l'entreprise et de conférer davantage d'agilité et de flexibilité
		✓	Implémenter une solution de gestion du stockage (SDS) des données, transparente pour l'utilisateur final afin de gagner en agilité dans la gestion du système informatique
		✓	Mettre en place une architecture de supervision de sécurité : un SOC (Security Operation Center) qui puisse détecter et filtrer les programmes malveillants, afin de lutter contre les menaces persistantes avancées
		✓	Implémenter une solution de VOIP (Voix sur IP) et/ou de TOIP (Téléphonie sur IP) afin de fournir au système informatique des fonctionnalités de communications unifiées
		✓	Implémenter une solution de MDM afin de gérer l'ensemble des périphériques mobiles de l'entreprise
		✓	Intégrer l'ensemble des éléments réalisés séparément afin de vérifier qu'ils communiquent correctement et qu'ils fonctionnent ensemble
		✓	Rédiger la documentation technique afin de produire la documentation du projet

A3.4 Mettre en place une conduite du changement	A3.5 Industrialiser la solution	
✓		Rédiger la documentation à destination des opérationnels afin de faciliter l'utilisation du système informatique et leur adhésion à celui-ci
✓		Comprendre les causes des résistances afin de pouvoir mieux les contourner
✓		Identifier les porteurs du changement afin de créer un réseau de relais pour porter le changement localement
✓		Communiquer les changements afin d'avertir tous les utilisateurs de l'arrivée prochaine du système informatique et des apports de celui-ci.

A3.4 Mettre en place une conduite du changement	A3.5 Industrialiser la solution	
✓		Préparer des supports de formations afin de pouvoir les remettre aux apprenants lors des sessions de formation au système informatique
✓		Organiser et animer des formations afin de faciliter la prise en main du système informatique
	✓	Mettre en œuvre l'intégration continue afin de vérifier que le résultat des modifications du système informatique ne produit pas de régression
	✓	Industrialiser le déploiement de la solution afin de simplifier l'opération pour le client, notamment à l'aide de différents outils DEVOPS (par exemple : ANSIBLE, PUPPET, CHEF, …)
	✓	Automatiser le déploiement, par le biais de scripting, de programmation d'équipements actifs, de provisioning afin de réduire les coûts et les risques d'erreurs humaines

Bloc de compétences et compétences:

Maintenir le système en condition opérationnelle et de sécurité

A4.1 Gérer les faits techniques et les évolutions	A4.2 Mettre en place une démarche d'amélioration continue	A4.3 Maintenir en condition opérationnelle et de sécurité	A4.4 Mettre en place une gouvernance de sécurité	
✓				Définir et rédiger la stratégie de maintenance curative
✓				Mettre en œuvre des outils de suivi des faits techniques et des demandes d'évolution afin de suivre les futures modifications à réaliser
✓				Corriger des faits techniques afin d'améliorer la qualité du système informatique
✓				Proposer des solutions de contournement à des faits techniques
✓				Maintenir une base de connaissances
✓				Réaliser une veille technologique
✓				Communiquer les modifications
	✓			Déterminer les indicateurs de qualité
	✓			Analyser les indicateurs de qualité afin de palier certaines dérives
	✓			Améliorer la qualité du système informatique
	✓			Mettre en œuvre des méthodes de suivi afin de garantir la traçabilité de toutes les actions réalisées

A4.1 Gérer les faits techniques et les évolutions	A4.2 Mettre en place une démarche d'amélioration continue	A4.3 Maintenir en condition opérationnelle et de sécurité	A4.4 Mettre en place une gouvernance de sécurité	
	✓			Adopter une démarche d'amélioration continue de la sécurité afin de respecter les soucis de performances économiques de l'entreprise
		✓		Définir et rédiger la stratégie de maintenance préventive
		✓		Identifier et mettre en œuvre les outils de supervision de système et réseau (NOC : Network Operation Center)
		✓		Réaliser les requêtes corrélées d'analyse de sécurité afin de garantir la détection des attaques du système informatique
		✓		Rédiger l'ensemble des documents de sureté de fonctionnement du SI, en se conformant aux règles d'hygiène informatique édictées par l'ANSSI (Agence Nationale de Sécurité des SI)
		✓		Mettre en place un SMSI (Système de Management de la Sécurité Informatique) conforme à l'ISO 27001
		✓		Réaliser une analyse des risques de sécurité (EBIOS ou ISO 27005) afin de mieux sécuriser le système informatique.
		✓		Mettre en œuvre une démarche d'urbanisation de système informatique afin de transformer ce dernier, et de prévoir les plans d'évolution à moyen terme (2-5 ans)
		✓		Mettre en œuvre la PSSI afin d'appliquer la stratégie de sécurité de l'entreprise
		✓		Gérer les droits d'accès aux différentes ressources du système informatique en appliquant le principe du moindre privilége
		✓		Garantir l'intégrité des données du système informatique afin de se prémunir contre toute manipulation de celles-ci
		✓		Mettre en oeuvre une politique de routage adaptée au besoin de l'entreprise afin de d'optimiser la gestion des flux au sein de l'architecture
		✓		Assurer une veille de sécurité afin d'éviter les attaques de type zéro day

A4.1 Gérer les faits techniques et les évolutions	A4.2 Mettre en place une démarche d'amélioration continue	A4.3 Maintenir en condition opérationnelle et de sécurité	A4.4 Mettre en place une gouvernance de sécurité	
		✓		Vérifier par le biais de sites spécialisés (CERT, NIST, CVE, etc.) que de nouvelles failles de sécurité n'ont pas été détectées sur des composants de l'architecture du système informatique
		✓		Mettre en place un plan de continuité d'activité et de reprise d'activité afin de minimiser les temps d'interruption du système informatique conformément à la norme ISO 22301
		✓		Réaliser des analyses de contenu approfondies (DLP : Data Loss Prevention) afin d'identifier, de contrôler et de protéger l'information
		✓		Calculer le RTO (Recovery Time Objective) et le RPO (Recovery Point Objective) afin de calculer les coûts associés à ces mesures et de garantir les performances économiques de l'entreprise
		✓		Implémenter des solutions de résilience des infrastructures du système informatique afin de garantir une disponibilité optimale de celui-ci
		✓		Mettre en œuvre une gestion de crise afin de s'assurer que les dispositifs mis en place sont opérationnels et en mesure de faire face à tous types de situations de crise informatique.
			✓	Prendre en compte la LPM (Loi de Programmation Militaire) afin de garantir que les OIV (Organismes d'Intérêts Vitaux) mettent en place des mesures techniques et organisationnelles garantissant un niveau de sécurité conforme
			✓	Prendre en compte le RGS (Référentiel Général de Sécurité) afin de renforcer la confiance des usagers
			✓	Prendre en compte le RGPD (Règlement Général sur la Protection des Données)
			✓	Mettre en place le standard UL 2900 spécifiant les exigences de cybersécurité
			✓	Comprendre les obligations réglementaires de sécurité liées au domaine d'activité d'une entreprise (COB [Commission des Opérations de Bourse], HDS [Hébergement Données Santé], etc.) afin d'être en conformité

A4.5 Réaliser une analyse médico-légale après un crime informatique	A4.6 Réaliser un audit sécurité	A4.7 Réaliser un anti-virus	A4.8 Communiquer sur la cybersécurité	
✓				Maitriser les techniques de Forensic numérique
✓				Définir la timeline du crime informatique afin de comprendre les différentes étapes et les vecteurs d'attaque
✓				Savoir comment conserver les preuves de l'attaque afin de pouvoir les utiliser lors d'un procès
✓				Savoir expliquer à son équipe les principes d'une analyse médico-légale après un crime informatique
	✓			Savoir expliquer ce qu'est un audit de sécurité
	✓			Savoir identifier et utiliser les failles de sécurité réseau afin de pénétrer un système informatique et de proposer des solutions de remédiation
	✓			Savoir identifier et utiliser les failles de sécurité humaines
	✓			Savoir rédiger un rapport d'audit afin de le rendre compréhensible par les non-initiés
	✓			Réaliser des tests de pénétration et de vulnérabilités afin de vérifier la bonne sécurisation du système informatique
	✓			Réaliser un audit de code afin de vérifier que le code développé (applications mobile et Web) ne présente pas de failles de sécurité, conformément à la méthodologie OWASP
	✓			Réaliser le fuzzing d'un logiciel afin d'injecter des données aléatoires dans ses entrées et de vérifier ainsi si il y a des défauts de sécurité à corriger
	✓			Calculer le CVSS (Common Vulnerability Scoring System) afin d'évaluer la criticité des vulnérabilités
	✓			Déterminer le risque financier des vulnérabilités en fonction du CVSS afin de d'identifier les coûts associés à celles-ci
		✓		Faire du reverse engineering sur un virus afin de comprendre son fonctionnement
		✓		Définir les algorithmes à même de contrer le mode de fonctionnement d'un virus afin de créer un antivirus
		✓		Développer des tests unitaires, des tests d'intégration et des tests d'acceptations
			✓	Sensibiliser les utilisateurs du système informatique à l'hygiène informatique et aux risques liés à la cybersécurité

Bloc de compétences et compétences:

Opérer des bases de données

A5.1 Définir et automatiser la gestion des bases de données	
☑	Mettre en oeuvre différents types d'algorithme
☑	Créer, administrer et maintenir des bases de données
☑	Automatiser avec un langage de haut niveau la gestion de bases de données

III - CALENDRIER DE LA FORMATION ISRC

		Périodes de formation réparties sur 52 semaines														
Bloc de compétences		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Gérer un projet international	A1.1	☑	☑					☑		☑	☑	☑				☑
	A1.2	☑	☑					☑		☑	☑	☑				☑
	A1.3	☑	☑					☑			☑	☑				☑
Recueillir et analyser les exigences du client	A2.1	☑	☑					☑			☑	☑				☑
	A2.2	☑	☑					☑		☑	☑	☑				
Concevoir l'architecture, réaliser et déployer la solution technique	A3.1	☑			☑		☑		☑	☑					☑	
	A3.2	☑														
	A3.3	☑	☑		☑	☑	☑	☑	☑							
	A3.4	☑	☑							☑						
	A3.5		☑		☑											
Maintenir le système en condition opérationnelle et de sécurité	A4.1	☑	☑	☑			☑	☑						☑	☑	
	A4.2	☑					☑							☑		
	A4.3	☑			☑	☑	☑	☑	☑				☑	☑	☑	
	A4.4						☑					☑	☑			
	A4.5							☑						☑		
	A4.6							☑			☑	☑	☑			
	A4.7			☑								☑				
	A4.8		☑					☑			☑					
Opérer des bases de données	A5.1			☑												

III - CRITÈRES D'ÉVALUATION DE LA FORMATION ISRC

Un positionnement individuel sera demandé en début de formation en fonction des différents critères (voir l'exemple de grille d'évaluation ci-après).
Il y aura une évaluation continue des compétences en entreprise et en formation en vue de l'obtention du titre.
Il sera possible d'adapter la formation à l'entreprise si certains blocs de compétences sont déjà acquis par l'apprenti.

Exemple de grille d'évaluation en début de formation :

		Non acquis	Sous la responsabilité d'un expert	En autonomie	En tant qu'expert
A4.1	Définir et rédiger la stratégie de maintenance curative afin de garantir la gestion des dysfonctionnements du système informatique sur la durée"				
	Mettre en œuvre des outils de suivi des faits techniques et des demandes d'évolution afin de suivre les futures modifications à réaliser				
	Corriger des faits techniques afin d'améliorer la qualité du système informatique				
	Proposer des solutions de contournement à des faits techniques afin de permettre au client d'utiliser le système informatique lorsqu'une correction n'est pas possible ou pas réalisable rapidement				
	Maintenir une base de connaissances afin de partager les informations avec l'ensemble des parties prenantes				
	Réaliser une veille technologique afin de pouvoir proposer des évolutions pour le système informatique				
	Communiquer les modifications afin d'avertir le client de l'évolution et l'amélioration du système informatique				
	Niveau d'entrée				
	Compétences validées en entreprise				
	Compétences validées en formation				
	Taux de réussite				

Association
Des
Neticiens

CONTACTS

contact@adn-neticien.net

07 65 61 59 81

@ADN - Association des Neticiens

Pour que chacun.e puisse développer ses compétences en numérique et cybersécurité

UIMM PÔLE FORMATION Ile de France LA FABRIQUE DE L'AVENIR

GROUPE AFORP

Cette formation est délivrée en partenariat avec AFORP Formation, organisme ayant habilité l'ADN à préparer au titre déposé.

www.formations-neticiens.net

elodie-brosset.com / crédits photos : Tim Van Der Kuip, Christina Wocintechchat, Damir Kopezhanov, Kelly Sikkema - Unsplash | **Septembre 2023**