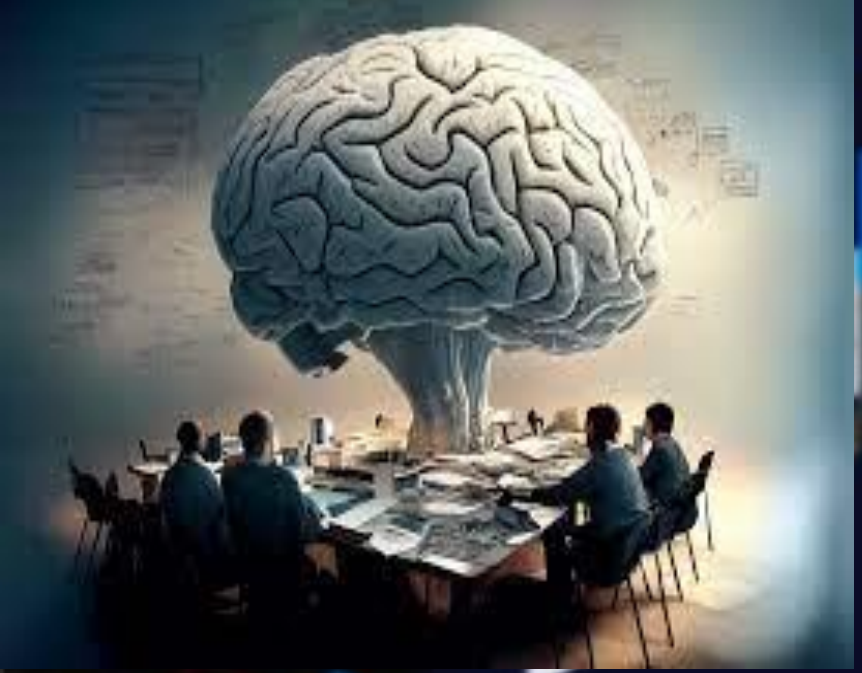


FORMATIONS CERTIFIANTES

CATALOGUE 2023-2024

POURQUOI SE CERTIFIER ?

L’expérience est un atout indéniable, mais comment démontrer vos connaissances et compétences auprès d’employeurs ?

GRACE A LA CERTIFICATION !

De nos jours, il est primordial d’être capable de rallier à son diplôme un métier ; Ainsi, En obtenant une certification, vous démontrez votre expertise et prouvez votre capacité à vous différencier des autres sur le marché du travail de plus en plus concurrentiel d’aujourd’hui.

La certification apporte de la crédibilité à votre curriculum vitae, ce qui vous ouvre d’importantes possibilités d’évolution de carrière.
C’est un facteur clé de succès pour obtenir des opportunités d’emploi mieux rémunérées et une reconnaissance accrue.

Avantages :

- ❑ Amélioration de l’employabilité et de meilleures opportunités d’emploi.
- ❑ Emplois mieux rémunérés avec en prime augmentation de salaires
- ❑ Reconnaissance de carrière au sein de l’entreprise et auprès de ses pairs
- ❑ Accroissement de la crédibilité et de la notoriété
- ❑ Permet de booster des carrières et etre plus compétitif

TABLE INDEX DES FORMATIONS CERTIFIANTES

REFERENCE	INTITULE DE LA FORMATION	ORGANISME DE CERTIFICATION	PARTENAIRE TECHNIQUE
INFORMATIQUE & CYBERSÉCURITÉ			
Certification Cisco Débutant			
SI-CCS	Cisco Certified Support Technician Cybersecurity	**CISCO**	
SI-CCN	Cisco Certified Support Technician Networking		
Certification Cisco Associé			
SI-CNA	Cisco Certified Network Associate	**CISCO**	
SI-CDA	Cisco Certified DevNet Associate		
SI-CCA	Cisco Certified CyberOps Associate		
Certification Cisco Professionnelle			
SI-NPE	Cisco Certified Network Professional Enterprise	**CISCO**	
SI-NPS	Cisco Certified Network Professional Security		
SI-NPC	Cisco Certified Network Professional Collaboration		

REFERENCE	INTITULE DE LA FORMATION	ORGANISME DE CERTIFICATION	PARTENAIRE TECHNIQUE
INFORMATIQUE & CYBERSÉCURITÉ			
Certification Cisco Professionnelle			
SI-NPP	Cisco Certified Network Professional Service Provider	**CISCO**	
SI-NPD	Cisco Certified Network Professional Data Center		
SI-CDP	Cisco Certified DevNet Professional		
SI-CCP	Cisco Certified CyberOps Professional		
Certification Cisco Expert			
SI-EEI	Cisco Certified Internetwork Expert Enterprise Infrastructure	**CISCO**	
SI-ESP	Cisco Certified Internetwork Expert Service Provider		
SI-IES	Cisco Certified Internetwork Expert Security		
SI-EEW	Cisco Certified Internetwork Expert Enterprise Wireless		

REFERENCE	INTITULE DE LA FORMATION	ORGANISME DE CERTIFICATION	PARTENAIRE TECHNIQUE
INFORMATIQUE & CYBERSÉCURITÉ			
Certification Cisco Expert			
SI-EDC	Cisco Certified Internetwork Expert Data Center	**CISCO**	
SI-IEC	Cisco Certified Internetwork Expert Collaboration		
SI-CDE	Cisco Certified Design Expert		
SI-DNE	Cisco Certified DevNet Expert		

PROGRAMMES DÉTAILLÉS DES FORMATIONS

SECURITE INFORMATIQUE ET CYBERSÉCURITÉ : Certifications Cisco Professionnelle

Référence : **SI-NPC**	Intitulé de la formation certifiante : **Cisco Certified Network Professional Collaboration**		
Durée : 180*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert CISCO de JFN

Description et objectif :

Se connecter de partout, travailler n'importe où. Les technologies de collaboration nous permettent de vivre et de travailler à distance. L'obtention de la certification CCNP Collaboration prouve que vous avez ce qu'il faut pour construire les solutions qui permettent à notre monde hybride de s'épanouir.

Testez vos connaissances et vos compétences sur les technologies de collaboration telles que la passerelle Cisco Internetwork Operations System XE, le contrôle des appels, la qualité de service et bien plus encore lors de l'examen CLCOR et mettez en avant votre spécialité avec un examen de concentration de votre choix. Réussissez les deux examens pour obtenir votre certification.
Cet examen teste vos connaissances sur la mise en œuvre des technologies de collaboration de base, notamment :

- Infrastructure et conception
- Protocoles, codecs et points d'extrémité
- Passerelle Cisco IOS XE et ressources média
- Contrôle des appels
- QoS
- Applications de collaboration

Prérequis :
Il n'y a pas de prérequis formels pour le CCNP collaboration.
Les candidats CCNP ont généralement trois à cinq ans d'expérience dans la mise en œuvre de solutions de sécurité.

Cible :
Professionnels utilisant les produits CISCO
Ingénieur réseau et télécommunications

Débouchés :
Les professions possibles :

- Administrateur de la collaboration
- Ingénieur en solutions de collaboration
- Architecte de solutions de collaboration

Programme :

Infrastructure et conception
1.1 Décrire les éléments de conception des solutions de collaboration sur site, hybrides et en nuage de Cisco décrits dans le SRND/PA.
1.2 Décrire l'utilité des équipements de périphérie dans l'architecture de collaboration de Cisco, tels que Expressway et Cisco Unified Border Element.
1.3 Configurer ces composants de réseau pour soutenir les solutions de collaboration de Cisco
1.4 Dépanner ces composants réseau dans une solution de collaboration Cisco
1.5 Expliquer ces composants pour soutenir les solutions de collaboration de Cisco
1.6 Décrire les fonctionnalités de Webex Control Hub

Protocoles, codecs et points d'extrémité

2.1 Dépanner les éléments d'une conversation SIP
2.2 Identifier les codecs de collaboration pour un scénario donné
2.3 Déployer des points d'extrémité SIP2.4 Dépannage des terminaux SIP
2.5 Décrire SIP OAuth sur Cisco UCM

Référence : **SI-NPC**	Intitulé de la formation certifiante : **Cisco Certified Network Professional Collaboration**

Durée : 180 *H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert CISCO de JFN

Passerelle Cisco IOS XE et ressources média
3.1 Configuration des éléments de la passerelle vocale
3.2 Dépannage des lignes ISDN PRI/BRI
3.3 Identifier les ressources média IOS XE appropriées
3.4 Décrire les passerelles locales hybrides appelées "cloud

Contrôle des appels
4.1 Décrire le processus d'analyse des chiffres de Cisco UCM
4.2 Mettre en œuvre la prévention de la fraude au péage sur Cisco UCM
4.3 Configurer le routage d'appel globalisé dans Cisco UCM
4.4 Décrire l'accès mobile et distant (MRA)
4.5 Décrire les fonctions du plan de numérotation de Webex Calling

QoS
5.1 Décrire les problèmes qui peuvent entraîner une mauvaise qualité de la voix et de la vidéo
5.2 Décrire les exigences de qualité de service pour la voix et la vidéo
5.3 Décrire les modèles de classe pour fournir la QoS sur un réseau5.4 Décrire l'objectif et la fonction de ces valeurs DiffServ en ce qui concerne la collaboration
5.5 Décrire les limites de confiance de la QoS et leur importance dans la classification et le marquage basés sur le LAN
5.6 Décrire et déterminer les exigences de bande passante CAC basées sur la localisation
5.7 Configurer LLQ (carte de classe, carte de politique, politique de service)

Applications de collaboration
6.1 Configurer la boîte aux lettres et le MWI de Cisco Unity Connection
6.2 Configurer les options d'intégration SIP de Cisco Unity Connection pour le contrôle des appels
6.3 Décrire les gestionnaires d'appels de Cisco Unity Connection

SECURITE INFORMATIQUE ET CYBERSÉCURITÉ : Certifications Cisco Professionnelle

Référence **SI-NPP**	Intitulé de la formation certifiante **: Cisco Certified Network Professional Service Provider**		
Durée : 180*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert CISCO de JFN

Description et objectif :

L'examen Implementing and Operating Cisco Service Provider Network Core Tech (SPCOR 350-501) est un examen de 120 minutes associé aux certifications CCNP Service Provider, CCIE Service Provider et Cisco Certified Specialist - Service Provider Core.
Cet examen teste les connaissances du candidat en matière de mise en œuvre des technologies de réseau des fournisseurs de services, notamment l'architecture de base, les services, la mise en réseau, l'automatisation, la qualité des services, la sécurité et l'assurance du réseau. Le cours Implementing and Operating Cisco Service Provider Network Core Technologies aide les candidats à se préparer à cet examen.

Prérequis :
Il n'y a pas de prérequis formels pour le CCNP Service Provider. Néammoins, une expérience dans la mise en œuvre de solutions pour fournisseurs de services est un avantage

Cible :
Administrateur réseau, ingénieur réseau junior, architecte réseau, ingénieur télécoms

Débouchés :
- Concepteur de réseau
- Ingénieur réseau senior
- Gestionnaire de réseau senior
- Ingénieur système senior
- Administrateur réseau senior

Programme :

l'architecture de base, les services
1.1 Décrire les architectures des fournisseurs de services1.2 Décrire l'architecture logicielle du réseau Cisco
1.3 Décrire la virtualisation des fournisseurs de services
1.4 Décrire l'architecture de la qualité de service
1.5 Configurer et vérifier la sécurité du plan de contrôle
1.6 Décrire la sécurité du plan de gestion
1.7 Mise en œuvre de la sécurité du plan de données

3.1 Mise en œuvre de MPLS
3.2 Décrire l'ingénierie du trafic
3.3 Décrire le routage par segment

4.1 Décrire les services VPN
4.2 Configurer L2VPN et Carrier Ethernet
4.3 Configurer L3VPN4.4 Mettre en œuvre des services multicast
4.5 Mise en œuvre des services de qualité de service (QoS)

5.1 Décrire les API programmables utilisées pour inclure les périphériques Cisco dans l'automatisation du réseau.
5.2 Interpréter un script externe pour configurer un périphérique Cisco à l'aide d'une API REST
5.3 Décrire le rôle de l'orchestration des services réseau (NSO)
5.4 Décrire les principes de haut niveau et les avantages d'un langage de modélisation des données, tel que YANG

5.5 Comparer les outils de gestion de configuration avec ou sans agent, tels que Chef, Puppet, Ansible et SaltStack
5.6 Décrire l'analyse des données et la télémétrie pilotée par les modèles chez les fournisseurs de services
5.7 Configurer les flux de télémétrie dial-in/out en utilisant gRPC
5.8 Configurer et vérifier NetFlow/IPFIX
5.9 Configurer et vérifier NETCONF et RESTCONF
5.10 Configurer et vérifier SNMP (v2c/v3)

SECURITE INFORMATIQUE ET CYBERSÉCURITÉ : Certifications Cisco Professionnelle

Référence : **SI-NPD**	Intitulé de la formation certifiante : **Cisco Certified Network Professional Data Center**		
Durée : 180*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert CISCO de JFN

Description et objectif :
Implementing Cisco Data Center Core Technologies v1.1 (DCCOR 350-601) est un examen de 120 minutes associé aux certifications CCNP et CCIE Data Center. Cet examen certifie les connaissances du candidat en matière de mise en œuvre des technologies de base des centres de données, notamment :
le réseau, le calcul, le réseau de stockage, l'automatisation et la sécurité. Cette formation aide les candidats à se préparer à cet examen. Elle teste les connaissances en matière de mise en œuvre des technologies de base des centres de données

Prérequis :
pas de prérequis formels pour le CCNP data center.

Cible :
Architecte réseau
Ingénieur réseau et télécoms
Analyste de données

Débouchés :
Les métiers possibles après la formation(sans être exhaustif) :

- Concepteur principal de réseaux
- Administrateur de réseau
- Ingénieur principal de centre de données
- Ingénieur conseil en systèmes

Programme :

1.1 Appliquer les protocoles de routage
1.2 Appliquer les protocoles de commutation tels que RSTP+, LACP et vPC
1.3. Appliquer les protocoles de superposition tels que VXLAN EVPN
1.4 Appliquer les concepts ACI
1.5 Analyser le flux de paquets (unicast, multicast et broadcast)
1.6 Décrire les modèles de services et de déploiement du Cloud (NIST 800-145)
1.7 Décrire les mises à jour logicielles et leurs impacts
1.8 Mettre en œuvre la gestion de la configuration du réseau
1.9 Mettre en œuvre la surveillance de l'infrastructure telle que NetFlow et SPAN
1.10 Expliquer les concepts d'assurance réseau tels que la télémétrie en continu

2.1 Mettre en œuvre les serveurs en rack de Cisco Unified Compute System
2.2 Mettre en œuvre le châssis de lames du système unifié de calcul de Cisco (Cisco Unified Compute System Blade Chassis)
2.3 Expliquer les concepts et les avantages de l'infrastructure HyperFlex (architecture Edge et hybride vs all-flash)
2.4 Décrire les mises à jour du firmware et du logiciel et leurs impacts sur les serveurs B-Series et C-Series
2.5 Mettre en œuvre la gestion de la configuration informatique (sauvegarde et restauration)
2.6 Mettre en œuvre la surveillance de l'infrastructure telle que SPAN et Cisco Intersight

Référence : **SI-NPD**	Intitulé de la formation certifiante : **Cisco Certified Network Professional Data Center**		
Durée : 180*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert CISCO de JFN

3.2 Implémenter la structure unifiée FCoE 3.3 Décrire les concepts NFS et NAS 3.4 Décrire les mises à jour logicielles et leurs impacts (perturbateur/non perturbateur et EPLD) 3.5 Mettre en œuvre la surveillance de l'infrastructure3.1 Mise en œuvre de Fibre Channel 4.1 Mise en œuvre d'outils d'automatisation et de script 4.2 Évaluer les technologies d'automatisation et d'orchestration 5.1 Appliquer la sécurité du réseau 5.2 Appliquer la sécurité informatique 5.3 Appliquer la sécurité du stockage	14

SECURITE INFORMATIQUE ET CYBERSÉCURITÉ : Certifications Cisco Professionnelle

Référence : **SI-CDP**	Intitulé de la formation certifiante : **Cisco Certified DevNet Professional**

Durée : 180*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert CISCO de JFN

Description et objectifs :

Pour obtenir la certification DevNet Professional ou DevNet Expert, vous devez réussir l'examen DEVCOR 350-901 Cet examen teste vos connaissances en matière de développement et de conception de logiciels, notamment :

- l'utilisation des API
- Les plateformes Cisco
- Déploiement d'applications et sécurité
- Infrastructure et automatisation

Cible :
Tout professionnel informatique
Développeur web
Ingénieur informaticien
Développeur front-end et back-end

Prerequis :
Aucun exigé

Débouchés :

Développeur d'applications senior
Concepteur de logiciel

Programme :

Module 1 : Développement et conception de logiciels

1.1 Décrire les applications distribuées en rapport avec les concepts de front-end, back-end et équilibrage de charge.
1.2 Évaluer la conception d'une application en tenant compte de l'évolutivité et de la modularité
1.3 Évaluer la conception d'une application en tenant compte de la haute disponibilité et de la résilience (y compris sur site, hybride et dans le nuage)
1.4 Évaluer la conception d'une application en tenant compte de la latence et de la limitation du débit
1.5 Évaluer la conception et la mise en œuvre d'une application en tenant compte de la maintenabilité
1.6 Évaluer la conception et la mise en œuvre d'une application en tenant compte de l'observabilité
1.7 Diagnostiquer les problèmes d'une application à partir de logs relatifs à un événement
1.8 Évaluer le choix des types de bases de données en fonction des exigences de l'application (relationnelles, documentaires, graphiques, en colonnes, séries temporelles, etc.)
1.9 Expliquer les modèles architecturaux (monolithique, orienté services, microservices et orienté événements)
1.10 Utiliser les opérations avancées de contrôle de version avec Git
1.11 Expliquer les concepts d'empaquetage des versions et de gestion des dépendances
1.12 Construire un diagramme de séquence qui inclut les appels API

SECURITE INFORMATIQUE ET CYBERSÉCURITÉ : Certifications Cisco Professionnelle

Référence **SI-CDP**	Intitulé de la formation certifiante : **Cisco Certified DevNet Professional**		
Durée : 180*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert CISCO de JFN

Module 2

2.1 Mise en œuvre d'une gestion robuste des erreurs de l'API REST pour les délais et les limites de débit
2.2 Mise en œuvre du flux de contrôle du code du consommateur pour les erreurs REST API irrécupérables
2.3 Identifier les moyens d'optimiser l'utilisation de l'API par le biais de contrôles du cache HTTP
2.4 Construire une application qui consomme une API REST qui prend en charge la pagination
2.5 Décrire les étapes du flux d'octroi de code d'autorisation à trois branches OAuth2

Module 3

3.1 Construire des requêtes API pour mettre en œuvre des chatops avec l'API Webex Teams
3.2 Construire des requêtes API pour créer et supprimer des objets à l'aide de la gestion des dispositifs Firepower (FDM)
3.3 Construire des requêtes API à l'aide de la plateforme Meraki pour accomplir ces tâches
3.4 Construire des appels API pour récupérer les données d'Intersight
3.5 Construire un script Python utilisant les API UCS pour provisionner un nouveau serveur UCS à partir d'un modèle.
3.6 Construire un script Python utilisant les API du centre ADN de Cisco pour récupérer et afficher des informations sur la santé du réseau sans fil.
3.7 Décrire les capacités d'AppDynamics lors de l'instrumentation d'une application
3.8 Décrire les étapes de la construction d'un tableau de bord personnalisé pour présenter les données collectées à partir des API de Cisco

Module 4

4.1 Diagnostiquer une défaillance du pipeline CI/CD (comme une dépendance manquante, des versions incompatibles de composants et des tests échoués)
4.2 Intégrer une application dans un environnement CD préconstruit en s'appuyant sur Docker et Kubernetes
4.3 Décrire les avantages des tests continus et de l'analyse statique du code dans un pipeline CI
4.4 Utiliser Docker pour conteneuriser une application
4.5 Décrire les principes de l'"application à 12 facteurs".
4.6 Décrire une stratégie de journalisation efficace pour une application
4.7 Expliquer les problèmes de confidentialité des données liés au stockage et à la transmission des données
4.8. Identifier l'approche de stockage secret adaptée à un scénario donné
4.9 Configurer des certificats SSL spécifiques à l'application
4.10 Mettre en œuvre des stratégies d'atténuation des menaces OWASP (telles que XSS, CSRF et injection SQL)
4.11 Décrire comment les principes de chiffrement de bout en bout s'appliquent aux API

Module 5

5.1 Expliquer les considérations relatives à la télémétrie pilotée par un modèle (y compris la consommation et le stockage des données)
5.2 Utiliser RESTCONF pour configurer un périphérique réseau, y compris les interfaces, les routes statiques et les VLAN (IOS XE uniquement)
5.3 Construire un flux de travail pour configurer les paramètres du réseau avec :
5.4 Identifier une solution de gestion de configuration pour répondre aux exigences techniques et commerciales
5.5 Décrire comment héberger une application sur un équipem[illegible] compris les équipements Catalyst 9000 et Cisco Ios)

SECURITE INFORMATIQUE ET CYBERSÉCURITÉ : Certifications Cisco Professionnelle

Référence **SI-CCP**	Intitulé de la formation certifiante : **Cisco Certified CyberOps Professional**		
Durée : 180*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert CISCO de JFN

Description et objectif :

Performing CyberOps Using Cisco Security Technologies v1.1 (CBRCOR 350-201) est un examen de 120 minutes qui est associé à la certification professionnelle Cisco CyberOps.
Cet examen permet de tester les connaissances et les compétences des candidats en matière d'opérations de CYBERSÉCURITÉ de base :

- les principes fondamentaux
- les techniques
- les processus
- l'automatisation

Prérequis :
Il n'y a pas de prérequis formels pour le CyberOps Professional. Une expérience dans la mise en œuvre de solutions de réseau d'entreprise est bénéfique

Cible :
Tout professionnel informatique
Professionnel de la CYBERSÉCURITÉ
Administrateur de base de données
Ingénieur informaticien

Débouchés :

- Ingénieur en CYBERSÉCURITÉ
- Enquêteur en CYBERSÉCURITÉ
- Gestionnaire d'incidents
- Intervenant en cas d'incident

Programme :

Module 1 :
L. Interpréter les composants d'un cahier de jeu
2. Déterminer les outils nécessaires sur la base d'un scénario de livre de jeu
3. Appliquer le cahier de jeu à un scénario courant (par exemple, élévation non autorisée des privilèges, DoS et DDoS, défiguration de sites web).
4. Déduire l'industrie pour diverses normes de conformité (par exemple, PCI, FISMA, FedRAMP, SOC, SOX, PCI, GDPR, Data Privacy, et ISO 27101).
5. Décrire l'objectif de l'assurance contre les cyber-risques
6. Analyser les éléments d'une analyse de risque (combinaison d'actifs, de vulnérabilités et de menaces)
7. Appliquer le processus de réponse aux incidents
8. Décrire les caractéristiques et les domaines d'amélioration à l'aide des mesures communes de réponse aux incidents
9. Décrire les types d'environnements en nuage
10. Comparer les considérations relatives aux opérations de sécurité des plateformes en nuage (par exemple, IaaS, PaaS)

Module 2 :
1. Recommander des techniques d'analyse de données pour répondre à des besoins ou à des questions spécifiques
2. Décrire l'utilisation du durcissement des images machine pour le déploiement
3. Décrire le processus d'évaluation de la posture de sécurité d'un bien
4. Évaluer les contrôles de sécurité d'un environnement, diagnostiquer les lacunes et recommander des améliorations
5. Déterminer les ressources pour les normes industrielles et les recommandations pour le renforcement des systèmes

SECURITE INFORMATIQUE ET CYBERSÉCURITÉ : Certifications Cisco Professionnelle

Référence **SI-CCP**	Intitulé de la formation certifiante : **Cisco Certified CyberOps Professional**		
Durée : 180*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert CISCO de JFN

6. Déterminer les recommandations en matière de correctifs, en fonction d'un scénario
7. Recommander des services à désactiver, en fonction d'un scénario
8. Appliquer la segmentation à un réseau
9. Utiliser les contrôles réseau pour le renforcement du réseau
10. Déterminer les recommandations SecDevOps (implications)
11. Décrire l'utilisation et les concepts liés à l'utilisation d'une plateforme de renseignement sur les menaces (TIP) pour automatiser le renseignement.
12. Appliquer le renseignement sur les menaces à l'aide d'outils
13. Appliquer les concepts de perte de données, de fuite de données, de données dans la lune, de données en cours d'utilisation et de données au repos sur la base de normes communes.
14. Décrire les différents mécanismes de détection et d'application des techniques de prévention des pertes de données 15. Recommander de régler ou d'adapter les dispositifs et les logiciels en fonction des règles, des filtres et des politiques
16. Décrire les concepts de gestion des données de sécurité
17. Décrire l'utilisation et les concepts des outils d'analyse des données de sécurité
18. Recommander un flux de travail à partir du problème décrit jusqu'à l'escalade et l'automatisation nécessaire à la résolution.
19. Appliquer les données du tableau de bord pour communiquer avec les parties prenantes techniques, les dirigeants ou les cadres.
20. Analyser les comportements anormaux des utilisateurs et des entités (UEBA)
21. Déterminer l'action suivante sur la base des alertes relatives au comportements utilisateurs
22. Décrire les outils et leurs limites pour l'analyse des réseaux (par exemple, les outils de capture de paquets, les outils d'analyse du trafic, les outils d'analyse des journaux de réseau)
23. Évaluer les artefacts et les flux dans un fichier de capture de paquets
24. Dépanner les règles de détection existantes

Module 3 :

1. Analyser les composants d'un modèle de menace
2. Déterminer les étapes de l'enquête sur les types de cas les plus courants
3. Appliquer les concepts et la séquence des étapes du processus d'analyse des logiciels malveillants : 4. Interpréter la séquence des événements au cours d'une attaque sur la base de l'analyse des schémas de trafic
5. Déterminer les étapes à suivre pour enquêter sur une intrusion potentielle au niveau des terminaux sur différents types de plateformes (par exemple, ordinateur de bureau, ordinateur portable, IoT, appareils mobiles).
6. Déterminer les indicateurs de compromission (IOC) et les indicateurs d'attaque (IOA) connus.
7. Déterminer les IOC dans un environnement sandbox (y compris la génération d'indicateurs complexes).
8. Déterminer les étapes pour enquêter sur la perte potentielle de données à partir d'une variété de vecteurs de modalité (par exemple, nuage, point d'extrémité, serveur, bases de données, application).
9. Recommander les mesures générales d'atténuation pour résoudre les problèmes de vulnérabilité.
10. Recommander les étapes suivantes pour le triage des vulnérabilités et l'analyse des risques en utilisant les systèmes de notation de l'industrie (par exemple, CVSS) et d'autres techniques.

Module 4 :

1. Comparer les concepts, les plateformes et les mécanismes d'orchestration et d'automatisation
2. Interpréter des scripts de base (par exemple, Python)

Référence **SI-CCP**	Intitulé de la formation certifiante **: Cisco Certified CyberOps Professional**		
Durée : 180*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert CISCO de JFN

3. Modifier un script fourni pour automatiser une tâche d'opérations de sécurité
4. Reconnaître les formats de données courants (par exemple, JSON, HTML, CSV, XML)
5. Déterminer les possibilités d'automatisation, d'orchestration et d'apprentissage automatique.
6. Déterminer les contraintes lors de la consommation d'API (par exemple, taux limité, délais et charge utile).
7. Expliquer les codes de réponse HTTP courants associés aux API REST
8. Évaluer les parties d'une réponse HTTP (code de réponse, en-têtes, corps)
9. Interpréter les mécanismes d'authentification de l'API : basic, custom token, et API keys
10. Utiliser les commandes Bash (gestion des fichiers, navigation dans les répertoires et variables d'environnement)
11. Décrire les composants d'un pipeline CI/CD
12. Appliquer les principes des pratiques DevOps
13. Décrire les principes de l'Infrastructure as Code

SECURITE INFORMATIQUE ET CYBERSÉCURITÉ : Certification Cisco débutant

Référence : **SI-CCS**	Intitulé de la formation certifiante : **Cisco Certified Support Technician Cybersecurity**		
Durée : 192 *H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert en CYBERSÉCURITÉ(CISCO) de JFN

Description et objectif :

La certification Cisco Certified Support Technician (CCST) Cybersecurity valide les compétences et les connaissances d'un candidat dans les concepts et les sujets de CYBERSÉCURITÉ de niveau débutant, notamment :
les principes de sécurité, la sécurité réseau et les concepts de sécurité des terminaux, l'évaluation des vulnérabilités et la gestion des risques, ainsi que la gestion des incidents.
La certification CCST Cybersecurity est également une première étape vers la certification CyberOps Associate.

Prérequis :
Pas de prérequis.

Cible :
- Techniciens de support informatique
- Administrateurs de réseau débutants
- Analystes de la sécurité débutants
- Professionnels de la sécurité informatique débutants
- Étudiants des filieres informatiques
- Professionnels des secteurs réseaux et télécommunications

- **Débouchés :**
- Technicien en CYBERSÉCURITÉ
- Analyste junior en sécurité informatique
- Analyste junior en CYBERSÉCURITÉ
- support du service d'assistance
- Analyste de la securite des operations
-

Programme :

1- Principes de sécurité essentiels
1.1. principes essentielles de sécurité
1.2. Menaces et vulnérabilités courantes
1.3. Principes de gestion des accès
1.4. Méthodes et applications de chiffrement

2- Concepts de base de la sécurité réseau
2.1. Vulnérabilités des protocoles TCP/IP
2.2. Impact des adresses réseau sur la sécurité
2.3. Infrastructure et technologies réseau
2.4. Configuration d'un réseau SoHo sans fil sécurisé
2.5. Mise en place de technologies d'accès sécurisées

3- Concepts de sécurité des points de terminaison
3.1. Concepts de sécurité des systèmes d'exploitation
3.2. Outils d'évaluation de la sécurité des endpoints
3.3. Vérification de la conformité des systèmes endpoints aux politiques de sécurité
3.4. Mise en place de mises à jour logicielles et matérielles
3.5. Interprétation des journaux système
3.6. Suppression des malwares

4- Évaluation des vulnérabilités et gestion des risques
4.1. Gestion des vulnérabilités
4.2. Utilisation de techniques de renseignement sur les menaces pour identifier les vulnérabilités réseau
4.3. Gestion des risques
4.4. Importance de la planification de la reprise après sinistre et de la continuité des activités

Référence : **SI-CCS**	Intitulé de la formation certifiante : **Cisco Certified Support Technician Cybersecurity**

Durée : 192*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert en CYBERSÉCURITÉ(CISCO) de JFN

5- Gestion des incidents

5.1. Surveillance des événements de sécurité et identification des cas nécessitant une escalade

5.2. Explication de la cyber forensique et des processus d'attribution des attaques

5.3. Impact des cadres de conformité sur la gestion des incidents de CYBERSÉCURITÉ

5.4. Description des éléments de la réponse aux incidents de CYBERSÉCURITÉ

SECURITE INFORMATIQUE ET CYBERSÉCURITÉ : Certification Cisco débutant

Référence **SI-CCN**	Intitulé de la formation certifiante **: Cisco Certified Support Technician Networking**		
Durée : 192*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert CISCO de JFN

Description et objectif :

La certification Cisco Certified Support Technician (CCST) Networking valide les compétences et les connaissances d'un individu dans les concepts et les sujets de base en matière de réseautage. elle démontre une connaissance et des compétences fondamentales nécessaires pour comprendre le fonctionnement des réseaux, y compris les appareils, les supports et les protocoles qui permettent les communications réseau.
CCST Networking est également une première étape vers la certification CCNA.

Prérequis : Il n'y a pas de prérequis formels pour obtenir cette certification

Cible : Tous ceux qui souhaitent acquérir des connaissances et des compétences de base dans le domaine du réseautage.

Débouchés : une fois la certification obtenue, les apprenants peuvent occupés les postes suivants : Technicien réseau ; Administrateur réseau ; Technicien de support technique ; Analyste de réseau

Programme :

1- Normes et concepts
1.1. Identifier les éléments conceptuels fondamentaux des réseaux.
1.2. Différencier la bande passante et le débit.
1.3. Différencier entre LAN, WAN, MAN, CAN, PAN et WLAN.
1.4. Comparer et contraster les applications et services cloud et sur site.
1.5. Décrire les applications et protocoles réseau courants.
2- Adresses et formats de sous-réseau
2.1. Comparer les adresses privées et les adresses publiques.

3- Points de terminaison et types de supports
3.1. Identifier les câbles et connecteurs couramment utilisés dans les réseaux locaux.
3.2. Différencier les technologies de réseau Wi-Fi, cellulaire et filaire.
3.3. Décrire les dispositifs de point d'extrémité.
3.4. Démontrer comment configurer et vérifier la connectivité réseau sur Windows, Linux, Mac OS, Android et Apple iOS..

4- Infrastructures
4.1. Identifier les voyants d'état sur un appareil Cisco lorsqu'on reçoit des instructions d'un ingénieur.
4.2. Utiliser un schéma réseau fourni par un ingénieur pour connecter les câbles appropriés.
4.3. Identifier les différents ports sur les appareils réseau.
4.4. Expliquer les concepts de base du routage.
4.5. Expliquer les concepts de base de la commutation.
Diagnostic des problèmes
5.1. Démontrer des méthodologies de dépannage efficaces et les meilleures pratiques du service d'assistance, y compris la gestion des tickets, la documentation et la collecte d'informations.

5.2. Effectuer une capture de paquets avec Wireshark et l'enregistrer dans un fichier.
5.3. Exécuter des commandes de diagnostic de base et interpréter les résultats.
5.4. Différencier les différentes façons d'accéder et de collecter des données sur les appareils réseau.
5.5. Exécuter des commandes d'affichage de base sur un appareil réseau **Cisco.**

Sécurité
6.1. Décrire le fonctionnement des pare-feu pour filtrer le trafic.
6.2. Décrire les concepts de sécurité fondamentaux.
6.3. Configurer la sécurité sans fil de base sur un routeur domestique (WPAx)

SECURITE INFORMATIQUE ET CYBERSÉCURITÉ : Certification Cisco Associé

Référence **SI-CNA**	Intitulé de la formation certifiante **: Cisco Certified Network Associate**		
Durée : 192*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert CISCO de JFN

Description et objectif :

La certification Cisco Certified Network Associate (CCNA) est une certification reconnue mondialement qui atteste des connaissances et compétences fondamentales dans le domaine des réseaux informatiques. Cette certification vise à former des professionnels capables d'installer, configurer, exploiter et résoudre les problèmes des réseaux de taille moyenne, qu'ils soient câblés ou sans fil. Les titulaires de la certification CCNA sont en mesure de comprendre le fonctionnement des réseaux de données, d'appliquer les principes de base de la commutation et du routage, de configurer des réseaux locaux et étendus, et de mettre en œuvre des mesures de sécurité pour protéger les réseaux.

Prérequis :

Aucun prérequis formel, mais il est recommandé d'avoir une ou plusieurs années d'expérience dans la mise en œuvre et l'administration de solutions Cisco.

Cible :

Débutant en réseaux informatiques
Étudiants en informatique

Débouchés :

- Administrateur réseau
- Ingénieur réseau
- Administrateur système
- Ingénieur système

Programme :

1- Fondamentaux du réseau

1.1 Expliquer le rôle et la fonction des composants réseau
1.2 Décrire les caractéristiques des architectures de topologie réseau
1.3 Comparer les types d'interfaces physiques et de câblage
1.4 Identifier les problèmes d'interface et de câble (collisions, erreurs, duplex et/ou vitesse non correspondants)
1.5 Comparer TCP à UDP
1.6 Configurer et vérifier l'adressage IPv4 et le sous-réseau
1.7 Expliquer la nécessité de l'adressage IPv4 privé
1.8 Configurer et vérifier l'adressage IPv6 et le préfixe
1.9 Décrire les types d'adresses IPv6
1.10 Vérifier les paramètres IP pour les systèmes d'exploitation clients (Windows, Mac OS, Linux)
1.11 Décrire les principes du sans fil
1.12 Expliquer les fondamentaux de la virtualisation (virtualisation de serveur, conteneurs et VRF)
1.13 Décrire les concepts de commutation

2- Accès au réseau

2.1 Configurer et vérifier les VLAN (plage normale) sur plusieurs commutateurs
2.2 Configurer et vérifier la connectivité entre les commutateurs
2.3 Configurer et vérifier les protocoles de découverte de couche 2 (Cisco Discovery Protocol et LLDP)
2.4 Configurer et vérifier EtherChannel (LACP) (couche 2/couche 3)
2.5 Décrire la nécessité et les opérations de base du protocole Spanning Tree Rapid PVST+ et identifier les opérations de base

SECURITE INFORMATIQUE ET CYBERSÉCURITÉ : Certification Cisco Associé

Référence : **SI-CNA**	Intitulé de la formation certifiante : **Cisco Certified Network Associate**		
Durée : 192*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert CISCO de JFN

2.6 Comparer les architectures sans fil Cisco et les modes AP
2.7 Décrire les connexions d'infrastructure physique des composants WLAN (AP, WLC, ports d'accès/trunk et LAG)
2.8 Décrire les connexions d'accès à la gestion des AP et des WLC (Telnet, SSH, HTTP, HTTPS, console et TACACS+/RADIUS)
2.9 Configurer les composants d'un accès LAN sans fil pour la connectivité client en utilisant uniquement l'interface graphique utilisateur (GUI), tels que la création de WLAN, les paramètres de sécurité, les profils QoS et les paramètres WLAN avancés

3- Connectivité IP
3.1 Interpréter les composants de la table de routage
3.2 Déterminer comment un routeur prend une décision de transfert par défaut
3.3 Configurer et vérifier le routage statique IPv4 et IPv6
3.4 Configurer et vérifier OSPFv2 à zone unique
3.5 Décrire l'objectif, les fonctions et les concepts des protocoles de redondance de la première étape

4- Services IP
4.1 Configurer et vérifier la translation d'adresse réseau (NAT) interne à l'aide de statique et de pools
4.2 Configurer et vérifier le fonctionnement de NTP en mode client et serveur
4.3 Expliquer le rôle de DHCP et DNS dans le réseau
4.4 Expliquer la fonction de SNMP dans les opérations réseau
4.5 Décrire les fonctionnalités de syslog, y compris les installations et les niveaux
4.6 Configurer et vérifier le client DHCP et le relais DHCP
4.7 Expliquer le comportement de transfert par saut (PHB) pour la QoS, tels que la classification, le marquage, l'ordonnancement, la congestion, le contrôle et le façonnage
4.8 Configurer les périphériques réseau pour un accès distant en utilisant SSH
4.9 Décrire les capacités et les fonctions de TFTP/FTP dans le réseau

5- Fondamentaux de la sécurité
5.1 Définir les concepts clés de la sécurité (menaces, vulnérabilités, exploits et techniques d'atténuation)
5.2 Décrire les éléments d'un programme de sécurité (sensibilisation des utilisateurs, formation et contrôle d'accès physique)
5.3 Configurer et vérifier le contrôle d'accès aux périphériques en utilisant des mots de passe locaux
5.4 Décrire les éléments des politiques de mots de passe de sécurité, tels que la gestion, la complexité et les alternatives aux mots de passe (authentification multifactorielle, certificats et biométrie)
5.5 Décrire l'accès distant IPsec et les VPN site à site
5.6 Configurer et vérifier les listes de contrôle d'accès
5.7 Configurer les fonctionnalités de sécurité de couche 2 (DHCP snooping, inspection dynamique ARP et sécurité de port)
5.8 Différencier les concepts d'authentification, d'autorisation et de comptabilité
5.9 Décrire les protocoles de sécurité sans fil (WPA, WPA2 et WPA3)
5.10 Configurer un WLAN utilisant WPA2 PSK en utilisant l'interface graphique utilisateur (GUI)

6- Automatisation et programmabilité
6.1 Expliquer comment l'automatisation impacte la gestion des réseaux
6.2 Comparer les réseaux traditionnels avec les réseaux basés sur un contrôleur
6.3 Décrire les architectures basées sur un contrôleur et définies par logiciel (superposition, sous-couche et tissu)
6.4 Comparez la gestion traditionnelle des appareils sur le campus avec la gestion des appareils activée par Cisco DNA Center.
6.5 Décrivez les caractéristiques des API basées sur REST (CRUD, verbes HTTP et encodage des données).
6.6 Reconnaissez les capacités des mécanismes de gestion de la configuration tels que Puppet, Chef et Ansible.

SECURITE INFORMATIQUE ET CYBERSÉCURITÉ : Certification Cisco Associé

Référence **SI-CDA**	Intitulé de la formation certifiante : **: Cisco Certified DevNet Associate**		
Durée : 192*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert CISCO de JFN

Description et objectif :

La certification Cisco DevNet Associate est une formation d'entrée de gamme qui permet d'acquérir une compréhension approfondie de la sécurité, de l'automatisation et des infrastructures réseau. On peut apprendre les meilleures pratiques du développement logiciel moderne, DevOps, et comment interagir en toute sécurité avec les interfaces de programmation d'applications (API) pour automatiser les processus manuels existants avec la formation DevNet.

Prérequis :
Compréhension de base de l'industrie informatique
1 à 2 ans d'expérience dans le développement et la maintenance d'applications Cisco
Connaissance fondamentale du langage de programmation

Cible :
La formation est destinée aux développeurs de logiciels, ingénieurs réseau, gestionnaires de centres de données et professionnels de l'informatique pour valider les compétences et les connaissances requises dans le domaine des réseaux Cisco

Débouchés :
Cette certification enrichie le CV et peut ouvrir les portes à des postes tels que développeur de logiciels, professionnel du réseau, ingénieur en CYBERSÉCURITÉ, analyste de sécurité des informations, gestionnaire d'incidents, et bien d'autres encore

Programme :

Module 1 Développement et Conception de Logiciels
Comparer les formats de données
Contrôle de version / Git

Module 2: Comprendre et utiliser les API
Construire et appeler l'API REST
Identifier et dépanner la réponse HTTP

Module 3 Plateformes Cisco et Développement
Comprendre les capacités des différentes plates-formes responsable de la communication ed, y compris AXL
Utiliser un SDK Cisco
Programmabilité du réseau Cisco et DevNet écosystème
Construction de code pour une opération

Module 4 Développement d'Applications et Sécurité
Comprendre le déploiement des applicationsExplorer l'outil DockerSécurité et Déploiement des Applications

Module 5 Infrastructure et Automatisation
Automatisation de l'Infrastructure et Pratiques DevOps
Explorer le travailutomatisation des flux
Interpréter les codes / modèles et revoir le processus

Module 6 : Principes fondamentaux du réseau
Comprendre les bases des concepts de réseautage
Comprendre les services/protocoles IP et les problèmes de réseau

SECURITE INFORMATIQUE ET CYBERSÉCURITÉ : Certification Cisco Associé

Référence **SI-CCA**	Intitulé de la formation certifiante : **Cisco Certified CyberOps Associate**		
Durée : 192*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert CISCO de JFN

Description et objectif :

Pour obtenir votre certification CyberOps Associate, vous devez réussir l'examen 200-201 CBROPS. Cet examen de 120 minutes teste vos connaissances sur :
- Concepts de sécurité
- Surveillance de la sécurité
- Analyse basée sur l'hôte
- Analyse des intrusions réseau
- Politiques et procédures de sécurité

Prérequis :

aucun prérequis spécifique pour l'obtention. Ce qui signifie que les professionnels de la CYBERSÉCURITÉ peuvent se lancer dans cette certification sans avoir à remplir des conditions préalables particulières

Cible :

La formation est destinée aux professionnels de la CYBERSÉCURITÉ qui souhaitent valider leurs compétences dans des domaines tels que la surveillance de la sécurité, l'analyse des intrusions réseau, les politiques et procédures de sécurité, et d'autres concepts essentiels liés à la CYBERSÉCURITÉ.

Débouchés :

Cette certification peut ouvrir des opportunités professionnelles dans le domaine de la CYBERSÉCURITÉ. Les professionnels certifiés peuvent viser des postes tels que analyste en CYBERSÉCURITÉ, ingénieur en sécurité des informations, spécialiste en sécurité réseau, et d'autres rôles liés à la CYBERSÉCURITÉ au sein d'organisations variées

Programme :

Module 1 : Concepts de sécurité

1. Décrire la triade de la CIA
2. Comparer les déploiements de sécurité3. Décrire les termes relatifs à la sécurité
4. Comparer les concepts de sécurité5. Décrire les principes de la stratégie de défense en profondeur
6. Comparer les modèles de contrôle d'accès
8. Identifier les défis liés à la visibilité des données (réseau, hôte et nuage) dans le cadre de la détection des menaces.
9. Identifier les pertes potentielles de données à partir des profils de trafic
10. Interpréter l'approche 5-tuple pour isoler un hôte compromis dans un ensemble groupé de logs
11. Comparer la détection basée sur des règles avec la détection comportementale et statistique

Module 2 : Surveillance de la sécurité

1. Comparer la surface d'attaque et la vulnérabilité
2. Identifier les types de données fournies par ces technologies
3. Décrire l'impact de ces technologies sur la visibilité des données
4. Décrire l'utilisation de ces types de données dans le cadre du contrôle de la sécurité
5. Décrire les attaques de réseau, telles que les attaques basées sur le protocole, les dénis de service, les dénis de service distribués et les attaques de type "man-in-the-middle".
6. Décrire les attaques contre les applications web, telles que les [illegible]ions SQL, les injections de commandes et les scripts intersites.

Référence : **SI-CCA**	Intitulé de la formation certifiante **: Cisco Certified CyberOps Associate**		
Durée : 192*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert CISCO de JFN

Module 3 : Analyse basée sur l'hôte

7. Décrire les attaques d'ingénierie sociale
8. Décrire les attaques basées sur les terminaux, telles que les débordements de mémoire tampon, la commande et le contrôle (C2), les logiciels malveillants et les logiciels rançonneurs.
9. Décrire les techniques d'évasion et d'obscurcissement, telles que les tunnels, le cryptage et les proxys.
10. Décrire l'impact des certificats sur la sécurité (y compris PKI, public/privé traversant le réseau, asymétrique/symétrique).
11. Identifier les composants du certificat dans un scénario donné

Module 4 : Analyse des intrusions réseau

1. Décrivez la fonctionnalité de ces technologies de point final en ce qui concerne la surveillance de la sécurité
2. Identifier les composants d'un système d'exploitation (tel que Windows et Linux) dans un scénario donné
3. Décrire le rôle de l'attribution dans une enquête
4. Identifier le type de preuves utilisées sur la base des registres fournis
5. Comparer une image de disque falsifiée et une image de disque non falsifiée
6. Interpréter les journaux du système d'exploitation, de l'application ou de la ligne de commande pour identifier un événement
7. Interpréter le rapport de sortie d'un outil d'analyse de logiciels malveillants tel qu'une chambre de détonation ou un bac à sable.

Module 5 : Politiques et procédures de sécurité

1. Décrire les concepts de gestion
2. Décrire les éléments d'un plan de réponse aux incidents tel qu'énoncé dans le document NIST.SP800-61.
3. Appliquer le processus de traitement des incidents tel que NIST.SP800-61 à un

4. Associer les éléments à ces étapes de l'analyse sur la base du document NIST.SP800-61
5. Dresser la carte des parties prenantes de l'organisation en fonction des catégories de RI du NIST (CMMC, NIST.SP800-61)
6. Décrire les concepts décrits dans le document NIST.SP800-86
7. Identifiez les éléments utilisés pour le profilage du réseau
8. Identifier les éléments utilisés pour le profilage des serveurs
9. Identifier les données protégées dans un réseau
10. Classer les événements d'intrusion dans les catégories définies par les modèles de sécurité, tels que le modèle de la chaîne de la mort cybernétique et le modèle diamant de l'intrusion.
11. Décrire la relation entre les mesures SOC et l'analyse du champ d'application (temps de détection, temps de confinement, temps de réponse, temps de contrôle).

SECURITE INFORMATIQUE ET CYBERSÉCURITÉ : Certification Cisco Professionnelle

Référence **SI-NPE**	Intitulé de la formation certifiante : **Cisco Certified Network Professional Enterprise**		
Durée : 192*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert CISCO de JFN

Description et objectif :

La certification est conçue pour les professionnels des réseaux qui se spécialisent dans l'infrastructure des réseaux au niveau de l'entreprise. Elle permet de valider leurs compétences et leurs connaissances en matière de mise en œuvre, de dépannage et d'optimisation de solutions réseau complexes
Pour obtenir la certification CCNP Enterprise, les candidats doivent réussir deux examens : l'examen Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR 350-401) et un examen de concentration de leur choix. L'examen ENCOR couvre un large éventail de sujets, notamment l'architecture, la virtualisation, les services d'infrastructure, la sécurité, l'automatisation, etc.
En revanche, les examens de concentration permettent aux candidats de se concentrer sur des domaines spécifiques tels que les réseaux sans fil ou les technologies de routage avancées, en fonction de leurs objectifs de carrière.
En obtenant la certification CCNP Enterprise, vous prouvez que vous êtes capable de faire évoluer et de maintenir les réseaux d'entreprise afin qu'ils puissent continuer à répondre à la demande croissante.

Prérequis :

Il n'y a pas de prérequis formels pour le CCNP enterprise. Les candidats ont souvent trois à cinq ans d'expérience dans la mise en œuvre de solutions de réseau d'entreprise.

Débouchés :

les rôles professionnels possibles sont :

- Administrateur de réseau
- Ingénieur système
- Technicien d'assistance réseau
- Ingénieur réseau de niveau intermédiaire

Cible :

La formation est destinée aux professionnels des réseaux et des systèmes qui souhaitent démontrer leur expertise dans la configuration, le dépannage et la gestion des réseaux d'entreprise. Elle est adaptée aux personnes occupant des postes tels que : administrateur réseau, ingénieur système, technicien de support réseau et ingénieur réseau de niveau intermédiaire.

Programme :

Pour obtenir votre certification CCNP Enterprise vous devez réussir l'examen 350-401 ENCOR qui teste vos connaissances dans les domaines suivants :

- l'architecture
- la virtualisation
- Infrastructure
- Assurance du réseau
- Sécurité des réseaux
- Automatisation
-

SECURITE INFORMATIQUE ET CYBERSÉCURITÉ : Certification Cisco Professionnelle

Référence **SI-NPE**	Intitulé de la formation certifiante **: Cisco Certified Network Professional Enterprise**

Durée : 192*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert CISCO de JFN

Module 1 : l'architecture
1.1 Expliquer les différents principes de conception utilisés dans un réseau d'entreprise
1.2 Décrire les principes de conception des réseaux sans fil
1.3 Expliquer les principes de fonctionnement de la solution SD-WAN de Cisco
1.4 Expliquer les principes de fonctionnement de la solution Cisco SD-Access
1.5 Interpréter les configurations QoS filaires et sans fil
1.6 Décrire les mécanismes de commutation matériels et logiciels tels que CEF, CAM, TCAM, FIB, RIB et les tables d'adjacence.

Module 2 : la virtualisation
2.1 Décrire les technologies de virtualisation des appareils
2.2 Configurer et vérifier les technologies de virtualisation du chemin de données
2.3 Décrire les concepts de virtualisation des réseaux

Module 3 : Infrastructure
3.1 Couche 2
3.2 Couche 3
3.3 Sans fil
3.4 Services IP

Module 4: Assurance du réseau
4.1 Diagnose network problems using tools such as debugs, conditional debugs, traceroute, ping, SNMP, and syslog
4.2 Configure and verify Flexible NetFlow
4.3 Configure SPAN/RSPAN/ERSPAN
4.4 Configure and verify IPSLA
4.5 Describe Cisco DNA Center workflows to apply network configuration, monitoring, and management
4.6 Configure and verify NETCONF and RESTCONF

Module 5: Sécurité des réseaux

5.1 Configurer et vérifier le contrôle d'accès à l'appareil
5.2 Configurer et vérifier les fonctions de sécurité de l'infrastructure
5.3 Décrire la sécurité de l'API REST
5.4 Configurer et vérifier les fonctions de sécurité sans fil
5.5 Décrire les composants de la conception de la sécurité du réseau

Module 6: Automatisation
6.1 Interpréter les composants et les scripts Python de base
6.2 Construire des fichiers JSON valides
6.3 Décrire les principes de haut niveau et les avantages d'un langage de modélisation des données, tel que YANG
6.4 Décrire les API pour Cisco DNA Center et vManage
6.5 Interpréter les codes de réponse de l'API REST et les résultats dans la charge utile en utilisant le Cisco DNA Center et RESTCONF
6.6 Construire une applet EEM pour automatiser la configuration, le dépannage ou la collecte de données
6.7 Comparer les outils d'orchestration avec ou sans agent, tels que Chef, Puppet, Ansible et SaltStack

SECURITE INFORMATIQUE ET CYBERSÉCURITÉ : Certification Cisco Professionnelle

Référence **SI-NPS**	Intitulé de la formation certifiante : **Cisco Certified Network Professional Security**

Durée : 192*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert CISCO de JFN

Description et objectif :

Les cybermenaces évoluent sans cesse, ce qui signifie que notre réponse doit également évoluer. En obtenant la certification CCNP Security, vous prouvez que vous pouvez entrer dans l'environnement de la CYBERSÉCURITÉ et protéger les réseaux et les données dont dépendent vos clients.

Mettez en avant vos connaissances en matière d'infrastructure d'entreprise, de virtualisation, d'assurance, de sécurité et d'automatisation lors de l'examen SCOR, puis démontrez vos compétences spécialisées lors de l'examen de concentration de votre choix. Réussissez les deux examens pour obtenir votre certification.

Prérequis :

Il n'y a pas de prérequis formels pour le CCNP sécurité. Les candidats ont souvent trois à cinq ans d'expérience dans la mise en œuvre de solutions de sécurité.

Cible :

La formation Cisco Certified Network Professional Security est destinée aux professionnels des réseaux et de la sécurité informatique qui souhaitent approfondir leurs compétences dans la conception, la mise en œuvre et la gestion de solutions de sécurité pour les réseaux d'entreprise. Cette formation est adaptée aux personnes occupant des postes tels que ingénieur réseau, administrateur de sécurité, analyste en sécurité des informations et tout professionnel souhaitant se spécialiser dans la sécurité des réseaux.

Débouchés :

Les postes possibles :
Ingénieur en sécurité associé
Ingénieur sécurité réseau

Programme :

Module 1 :Concepts de sécurité

1.1 Expliquer les menaces courantes contre les environnements sur site, hybrides et en nuage
1.2 Comparer les vulnérabilités de sécurité courantes telles que les bogues logiciels, les faiblesses et/ou les codes en dur
1.3 Décrire les fonctions des composants cryptographiques tels que le hachage, le cryptage, l'ICP, le SSL, l'IPsec, le NAT-T IPv4 pour l'IPsec, la clé prépartagée et l'autorisation basée sur un certificat.
1.4 Comparer les types et les composants de déploiement de VPN de site à site et d'accès à distance tels que les interfaces de tunnel virtuel, l'IPsec basé sur les normes, le DMVPN, le FlexVPN, et le Cisco Secure Client
y compris les considérations relatives à la haute disponibilité
1.5. Décrire la création, le partage et la consommation de renseignements de sécurité
1.6. Décrire les contrôles utilisés pour se protéger contre les attaques de phishing et d'ingénierie sociale
1.7 Expliquer les API North Bound et South Bound dans l'architecture SDN
1.8 Expliquer les API du Cisco DNA Center pour l'approvisionnement, l'optimisation, la surveillance et le dépannage du réseau
1.9 Interpréter les scripts Python de base utilisés pour appeler les API des appliances de sécurité Cisco

Module 2 : Sécurité des réseaux

2.1 Comparer les solutions de sécurité réseau qui offrent [illegible]nnalités de prévention des intrusions et de pare-feu

SECURITE INFORMATIQUE ET CYBERSÉCURITÉ : Certification Cisco Professionnelle

Référence **SI-NPS**	Intitulé de la formation certifiante **: Cisco Certified Network Professional Security**		
Durée : 192*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert CISCO de JFN

2.2 Décrire les modèles de déploiement des solutions de sécurité réseau et les architectures qui fournissent des fonctionnalités de prévention des intrusions et de pare-feu.
2.3 Décrire les composants, les capacités et les avantages des enregistrements NetFlow et Flexible NetFlow
2.4 Configurer et vérifier les méthodes de sécurité de l'infrastructure réseau
2.5 Mettre en œuvre la segmentation, les politiques de contrôle d'accès, l'AVC, le filtrage d'URL, la protection contre les logiciels malveillants et les politiques d'intrusion
2.6 Mettre en œuvre des options de gestion pour les solutions de sécurité réseau (gestionnaire unique ou multi-dispositifs, en bande ou hors bande, dans le nuage ou sur site)
2.7 Configurer l'AAA pour l'accès aux appareils et au réseau, comme TACACS+ et RADIUS
2.8 Configurer la gestion réseau sécurisée des dispositifs de sécurité périmétrique et d'infrastructure tels que SNMPv3, NetConf, RestConf, API, syslog sécurisé et NTP avec authentification.
2.9. Configurer et vérifier les VPN de site à site et d'accès à distance

Module 3 : Sécurisation du nuage
3.1 Identifier les solutions de sécurité pour les environnements cloud
3.2 Comparer les responsabilités en matière de sécurité pour les différents modèles de services cloud
3.3 Décrire le concept DevSecOps (pipeline CI/CD, orchestration de conteneurs et développement de logiciels sécurisés)
3.4 Mettre en œuvre la sécurité des applications et des données dans les environnements en nuage
3.5 Identifier les capacités de sécurité, les modèles de déploiement et la gestion des politiques pour sécuriser l'informatique en nuage
3.7 Décrire les concepts de sécurité des applications et des charges de travail

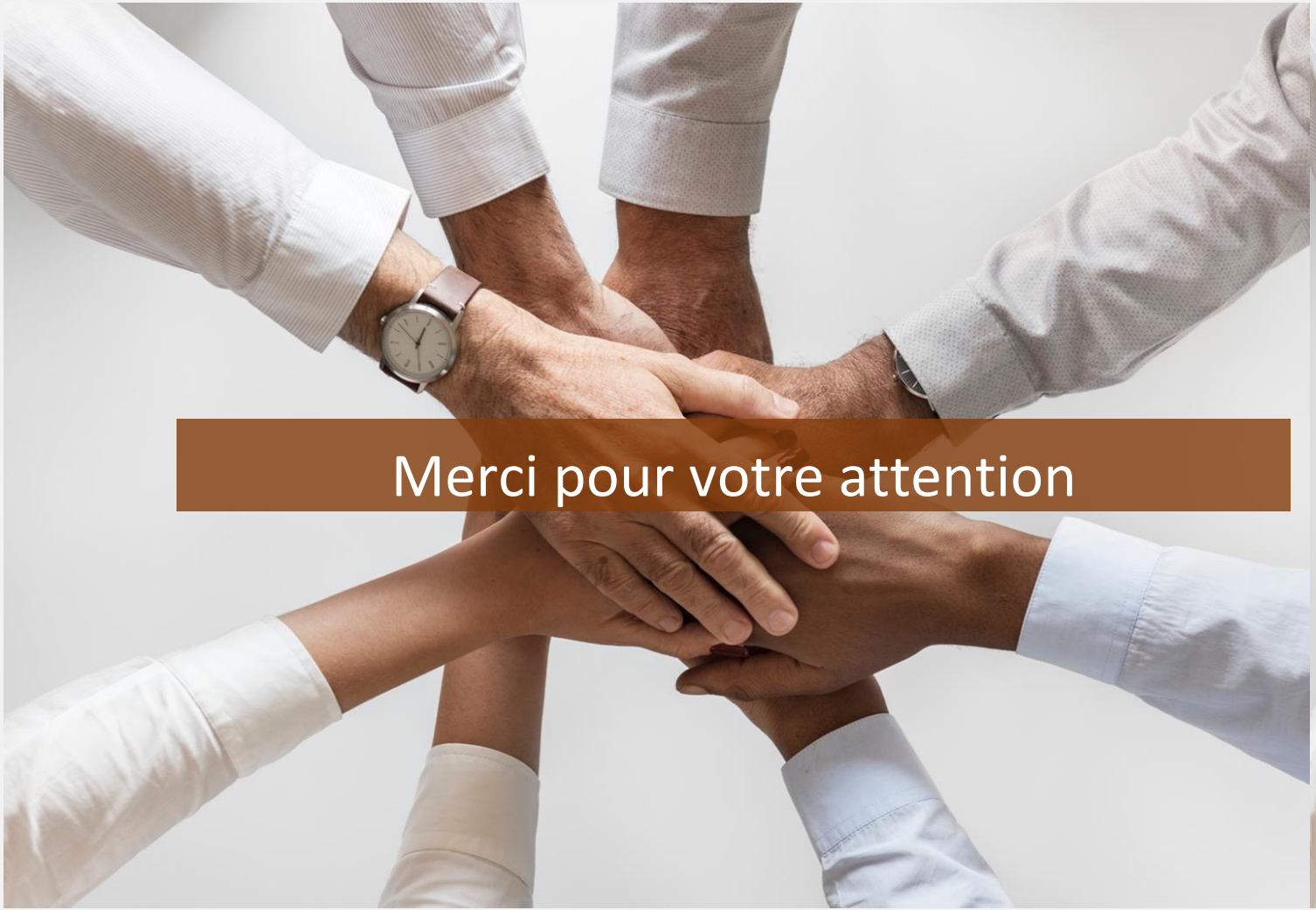
Module 4 : Sécurité du contenu
4.1 Mettre en œuvre des méthodes de redirection et de capture du trafic pour le proxy web
4.2 Décrire l'identité et l'authentification du proxy web, y compris l'identification transparente de l'utilisateur
4.3 Comparer les composants, les capacités et les avantages des solutions web et de messagerie sur site, hybrides et basées sur le cloud (Cisco Secure Email Gateway, Cisco Secure Email Cloud Gateway et Cisco Secure Web Appliance)
4.4 Configurer et vérifier les méthodes de déploiement de la sécurité du web et de la messagerie pour protéger les utilisateurs sur site, hybrides et distants
4.5 Configurer et vérifier les fonctions de sécurité de la messagerie telles que le filtrage SPAM, le filtrage antimalware, le DLP, la mise en liste de blocage et le cryptage de la messagerie.
4.6 Configurer et vérifier les fonctions de sécurité de Cisco Umbrella Secure Internet Gateway et du web telles que la mise en liste de blocage, le filtrage des URL, l'analyse des logiciels malveillants, la catégorisation des URL, le filtrage des applications web et le décryptage TLS.
4.7 Décrire les composants, les capacités et les avantages de Cisco Umbrella
4.8 Configurer et vérifier les contrôles de sécurité web sur Cisco Umbrella (identités, paramètres de contenu des URL, listes de destination et rapports)

Module 5 :Protection et détection des points finaux
5.1 Compare Endpoint Protection Platforms (EPP) and Endpoint Detection & Response (EDR) solutions
5.2 Configure endpoint antimalware protection using Cisco Secure Endpoint
5.3 Configure and verify outbreak control and quarantines to limit malware
5.4 Describe justifications for endpoint-based security
5.5 Describe the value of endpoint device management and asset inventory systems

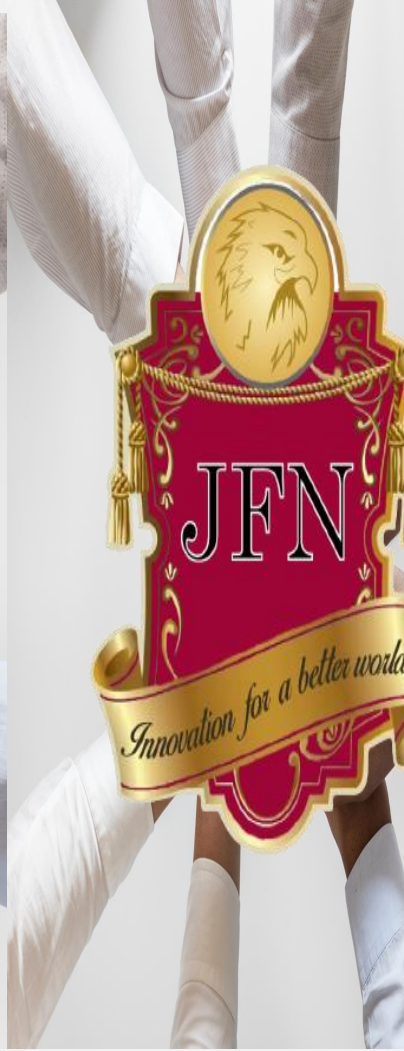
5.6 Describe the uses and importance of a multifactor authentication (MFA) strategy
5.7 Describe endpoint posture assessment solutions to ensure endpoint security
5.8 Explain the importance of an endpoint patching strategy

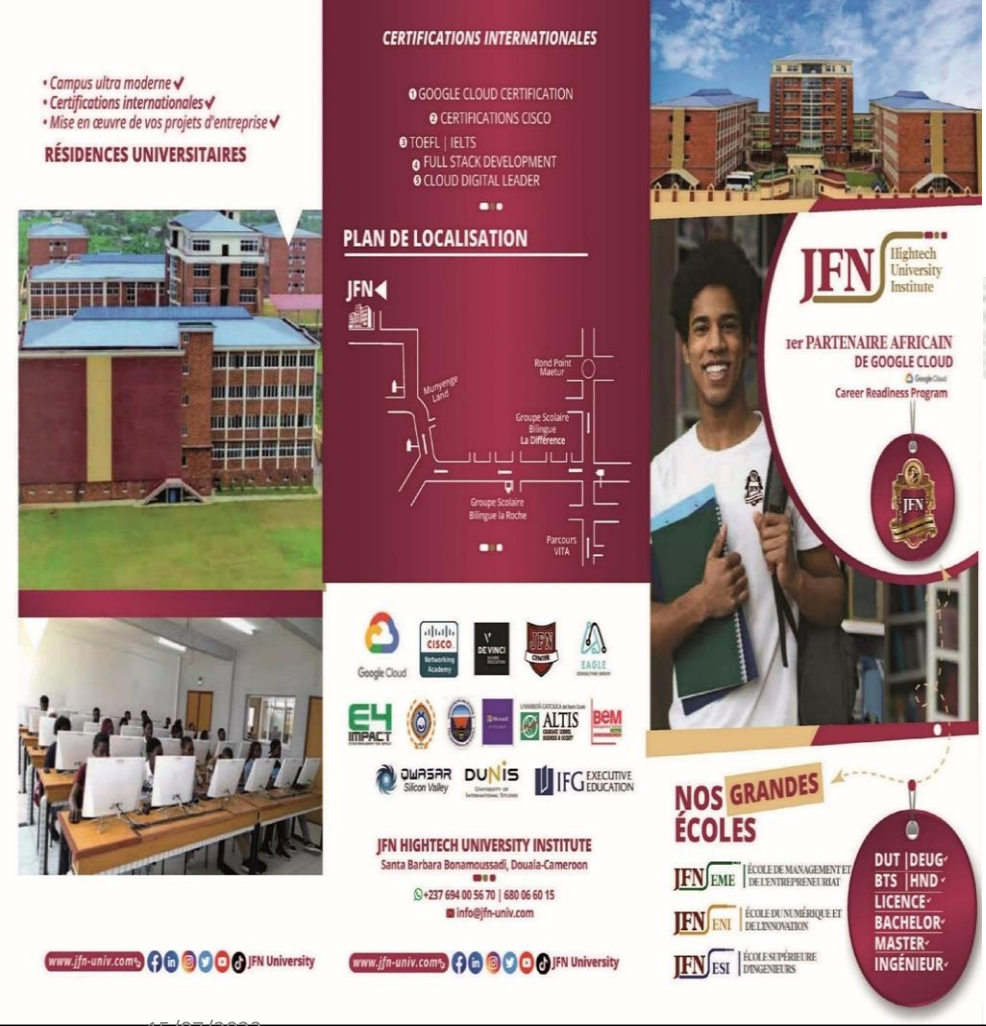
Module 6 : Accès sécurisé au réseau, visibilité et mise en œuvre

6.1 Describe identity management and secure network access concepts such as guest services, profiling, posture assessment and BYOD
6.2 Configure and verify network access control mechanisms such as 802.1X, MAB, WebAuth
6.3 Describe network access with CoA
6.4 Describe the benefits of device compliance and application control
6.5 Explain exfiltration techniques (DNS tunneling, HTTPS, email, FTP/SSH/SCP/SFTP, ICMP, Messenger, IRC, NTP)
6.6 Describe the benefits of network telemetry
6.7 Describe the components, capabilities, and benefits of these security products and solutions



Merci pour votre attention





- ☑ Innovation,
- ☑ Entrepreneuriat,
- ☑ Formation Professionnelle et Continue