edify digital

Nos formations en cybersécurité

L'expertise à portée de Clic

Les cursus métiers

Comme son nom l'indique, un cursus-métier est un ensemble de formations qui, une fois accompli, donne une qualification-métier à l'apprenant.

En suivant un cursus de formations, vous pourrez apprendre un nouveau métier ou développer de nouvelles compétences professionnelles dans des délais relativement réduits.

Les cursus EdLearn ont été créés sur la base de nos partenariats avec les plus grands éditeurs mondiaux de solutions tels que Cisco ou encore Microsoft, etc. De quoi voir son avenir professionnel avec confiance et enthousiasme !

Comme une bonne nouvelle n'arrive jamais seule, en vous inscrivant à un cursus métier d'Edlearn, bénéficiez d'une réduction pouvant aller jusqu' à -25% sur le coût total de chaque formations du cursus achetées individuellement

CYBER SECURITY SPECIALIST

CODE	FORMATIONS/CERTIFICATIONS	DURÉE
SEC01	SECURITY +	40h
SEC02	ETHICAL HACKING	40h
SEC04	CYBEROPS	36h
SEC02	NETWORK SECURITY	24h
GOV01	ISO 27001	24h
SEC03	INTRO TO CLOUD SECURITY	24h
GOV02	ISO 27005	24h

ADMINISTRATEUR SYSTEME NIVEAU 2

CODE	FORMATIONS/CERTIFICATIONS	DURÉE
MS05	AZURE 104	40h
VM02	VMware Certified PROFESSIONNAL (VCP)	40h
LP02	LPIC2	36h
MS06	AZURE 800	24h
MS07	MICROSOFT 365 SECURITY ADMINISTRATOR MS 500	24h
LP03	RHCSA	24h
CL01	AWS SYS OS	24h

ADMINISTRATEUR RESEAU HYBRIDE

CODE	FORMATIONS/CERTIFICATIONS	DURÉE
NT05	CCNP ENCOR	40h
NT06	CCNP ENARSI	40h
SEC03	NETWORK SECURITY	36h
MS05	AZURE 104	24h
CL02	AWS CLOUD PRACTIONNER	24h
CL03	DOCKER DCA	24h
CL04	KUBERNETE KCNA	24h
CL05	KUBERNETE CKA	

Les cursus métiers

SECURITY ARCHITECT		
CODE	FORMATIONS/CERTIFICATIONS	DURÉE
HD02	NETWORK SECURITY	40h
NT05	CCNP 350-701 SCORE	40h
SEC05	PANORAMA DES SOLUTIONS DE SECURITES RESEAU	36h
SEC06	CCNP FIREPOWER	24h
SEC07	CISSP	24h
SEC08	AWS SECURITY SPECIALIST	24h
SEC09	AZURE 500	24h

ANALYSTE DE CYBERSECURITE		
CODE	FORMATIONS	DURÉE
RHLABS01	Fondamentaux de la Cybersécurité	40h
RHLABS02	Théorie de la connaissance et introduction au métier d'analyste	40h
RHLABS03	Introduction à sécurité opérationnelle des SI	40h
RHLABS04	Supervision, analyse et gestion des incidents de sécurité	40h
RHLABS05	Etude des stratégies d'attaque et de défense	40h
RHLABS06	Renseignement et investigation sur les menaces cyber	40h
RHLABS07	Gestion des projets	40h

L'importance d'un cursus métier

Les nouvelles technologies, l'évolution des méthodes de travail et de management font évoluer nos métiers. Suivre les cursus métiers d'Edify, c'est se maintenir formé et informé pour assurer sa performance et sa réussite. Nos formations spécifiques à chaque métiers vous permettent de valider et de renforcer vos compétences afin d'être plus efficace. De courtes durées, nos cursus professionnels sont conçus pour répondre de façon concrète à vos besoins professionnels immédiats. Ils sont enrichis et mis à jour de manière constante.

40H CODE : SECO1

Objectifs

- Maîtriser les concepts fondamentaux de la sécurité informatique.
- Acquérir les compétences nécessaires pour mettre en œuvre et gérer des systèmes de sécurité efficaces

Débouchées

- Technicien en sécurité informatique
- Analyste de la sécurité
- Spécialiste de la réponse aux incidents
- sécurité et restauration des systèmes.
- Consultant en sécurité

Prérequis

- CCNA ou notions équivalentes

Programme S+

Module 1 : Les fondamentaux de la sécurité

Définition de la sécurité informatique
Types de menaces (malware, phishing, etc.)
Vulnérabilités courantes
Les principes de la sécurité (CIA : confidentialité, intégrité, disponibilité)
Risques et gestion des risques:
Analyse des risques
Plans de continuité d'activité
Gestion des incidents
Législation et conformité:
Réglementations en matière de sécurité des données (RGPD, etc.)
Audits de sécurité

Module 2 : Architecture et conception des systèmes sécurisés

Protocoles sécurisés (HTTPS, VPN, etc.)
Firewalls–IDS/IPS
Segmentation de réseau
Sécurité des systèmes d'exploitation:
Configuration sécurisée de Windows et Linux
Gestion des privilèges
Patch management
Sécurité des applications:
Développement sécurisé
Tests d'intrusion
Protection contre les injections SQL et XSS

Module 3 : Cryptographie et gestion des identités

Algorithmes de chiffrement
Gestion des clés
Signatures numériques
Gestion des identités et des accès (IAM):
Authentification (mot de passe, biométrie)
Autorisation
Contrôle d'accès basé sur les rôles (RBAC)

Module 4 : Sécurité des systèmes d'information cloud et mobiles

Modèles de déploiement cloud (IaaS, PaaS, SaaS)
Sécurité des données dans le cloud
Sécurité des appareils mobiles:
Gestion des appareils mobiles (MDM)
Sécurité des applications mobiles

Module 5 : Réponse aux incidents et analyse numérique

Identification-Confinement-Éradication-Récupération
Analyse numérique:
Collecte d'évidences
Analyse des logs
Investigation d'incidents

Take this course to level up your Network Security skills and get ready for in-demand security job roles. You'll get lots of practice, with 45 hands-on labs. Build your skills in implementing security measures, detecting vulnerabilities, and responding to incidents while ensuring network integrity. This comprehensive course helps you develop a deep understanding of Network Security and build expertise in designing, implementing, and supporting secure networks and data protection.

40H CODE : SECO3

Objectifs

Comprendre et prévenir les menaces et attaques réseau.
Mettre en œuvre des mesures de sécurité robustes pour protéger les réseaux.
Configurer et gérer des dispositifs de sécurité réseau (firewalls, VPN, etc.).
Développer des compétences pratiques en matière de sécurité réseau

Débouchées

- Technicien en sécurité informatique
- Analyste de la sécurité
- Spécialiste de la réponse aux incidents
- sécurité et restauration des systèmes.
- Consultant en sécurité

Prérequis

- CCNA ou notions équivalentes

NETWORK SECURITY

Module 1 : Introduction à la sécurité réseau
Concepts fondamentaux de la sécurité réseau (CIA : confidentialité, intégrité, disponibilité)
Types de menaces et attaques (malware, attaques DDoS, phishing, etc.)
Vulnérabilités communes (erreurs de configuration, failles logicielles, etc.)
Principes de défense en profondeur

Module 2 : Sécurité des périphériques réseau
Gestion et surveillance sécurisée des périphériques réseau (SNMP, syslog)
Configuration des niveaux de privilège et des commandes CLI basées sur les rôles
Mise en œuvre de l'authentification, de l'autorisation et de la comptabilité (AAA) (RADIUS, TACACS+)

Module 3 : Filtrage de trafic et pare-feu
Listes de contrôle d'accès (ACL) : configuration et utilisation
Pare-feu basés sur les zones (ZBF) : configuration et utilisation
Comparaison des différents types de pare-feu (stateless, stateful)

Module 4 : Systèmes de prévention des intrusions (IPS)
Principes de fonctionnement des IPS
Types d'IPS (NIPS, HIPS)
Configuration et gestion des IPS

Module 5 : Sécurité des points d'extrémité
Vulnérabilités des points d'extrémité (ordinateurs, appareils mobiles)
Méthodes de protection des points d'extrémité (antivirus, anti-malware, firewalls logiciels)
Gestion des correctifs et des mises à jour

Module 6 : Sécurité de la couche 2
Semaine 6 :
Attaques de la couche 2 (attaques ARP, attaques de diffusion)
Méthodes de mitigation des attaques de la couche 2 (VLAN, STP)

Module 7 : Cryptographie
Concepts de base de la cryptographie (chiffrement, hachage, signatures numériques)
Algorithmes de chiffrement symétrique et asymétrique
Infrastructure à clé publique (PKI)

Module 8 : VPN
Protocoles VPN (IPsec, SSL/TLS)
Configuration d'un VPN IPsec site-à-site
Utilisation des VPN pour l'accès à distance

Module 9 : Cisco ASA
Présentation du Cisco ASA
Configuration du pare-feu ASA à l'aide de la CLI et de l'ASDM
Fonctionnalités avancées du Cisco ASA

Module 10 : Tests de sécurité
Méthodes de test de sécurité (tests d'intrusion, analyse des vulnérabilités)
Outils de test de sécurité (nmap, Wireshark)
Analyse des résultats des tests de sécurité

40H CODE : SECO4

Objectifs

- Identifier et analyser les menaces cybernétiques: Détecter les incidents de sécurité, comprendre les techniques d'attaque et évaluer les risques.
- Mettre en œuvre des mesures de sécurité: Configurer et gérer les systèmes de sécurité réseau, tels que les IDS/IPS, les firewalls et les systèmes de prévention des intrusions.
- Réagir aux incidents de sécurité: Suivre les procédures d'incident, mener des investigations et mettre en œuvre des mesures correctives.
- Collaborer au sein d'une équipe de sécurité: Communiquer efficacement avec les autres membres de l'équipe et contribuer à l'amélioration continue des processus de sécurité.

Débouchées

- Analyste de la sécurité: Surveillance des événements de sécurité, détection des incidents.
- Ingénieur de la sécurité
- Responsable de la sécurité:
- Consultant en sécurité:

Prérequis

- Connaissances de base en réseau: TCP/IP, routage, commutation.
- Expérience avec les systèmes d'exploitation: Windows, Linux

CYBER OPS 200-201

Module 1 : Fondamentaux de la Sécurité Cybernétique

Cycle de vie d'un incident de sécurité: Détection, analyse, réponse, récupération.

Menaces courantes: Malware, attaques par déni de service, piratage, ingénierie sociale.

Vulnérabilités: Failles logicielles, erreurs de configuration.

Contrôles de sécurité: Authentification, autorisation, chiffrement.

Module 2 : Technologies de Sécurité Réseau

IDS/IPS: Fonctionnement, signature, anomalies.

Firewalls: Stateful, NGFW, WAF.

VPN: IPsec, SSL.

EDR: Endpoint Detection and Response.

SIEM: Security Information and Event Management.

Module 3 : Analyse des Menaces et Incidents

Techniques d'attaque: Exploitation de vulnérabilités, attaques par force brute, phishing.

Outils d'analyse: Wireshark, Snort, SIEM.

Investigation d'incidents: Collecte d'évidences, analyse forensique.

Module 4 : Réponse aux Incidents

Plans de réponse aux incidents: Élaboration et mise en œuvre.

Gestion de crise: Communication, escalade, coordination.

Restauration des systèmes: Sauvegardes, récupération.

Module 5 : Automatisation et Orchestration

SOAR: Security Orchestration, Automation and Response.

Intégration des outils de sécurité: API, scripts.

Module 6 : Pratiques Meilleurs et Tendances

Frameworks de sécurité: NIST CSF, CIS Controls.

Sécurité cloud: IaaS, PaaS, SaaS.

Sécurité IoT: Vulnérabilités et défis

40H CODE : SECO3

CCNP SCNF 300-710

Objectifs

Maîtriser le Cisco Firepower: Acquérir une connaissance approfondie des fonctionnalités avancées du Cisco Firepower en tant que pare-feu nouvelle génération.
Mettre en œuvre des politiques de sécurité: Configurer des règles de sécurité complexes, des contrôles d'accès et des politiques de VPN.
Gérer les menaces: Identifier, analyser et répondre aux menaces en utilisant les fonctionnalités IPS et Threat Intelligence.
Optimiser les performances: Configurer et ajuster le Cisco Firepower pour garantir des performances optimales dans différents environnements.
Intégrer le Cisco Firepower dans une architecture de sécurité globale: Comprendre comment le Cisco Firepower s'intègre avec d'autres produits Cisco et tiers

Débouchées

- Ingénieur sécurité réseau: Conception, mise en œuvre et maintenance de solutions de sécurité réseau
- Administrateurs réseaux
- Architectes réseau: Pour concevoir des architectures de sécurité robustes et évolutives.
- Consultants en sécurité

Prérequis

- CCNP SECURITY CORE ou notions équivalentes

<u>Module 1 : Introduction au Cisco Firepower</u>

Architecture du Cisco Firepower: Composants, fonctionnement.

Fonctionnalités clés: Pare-feu, IPS, VPN, WAF.

Intégration avec d'autres produits Cisco: ISE, Prime Infrastructure.

<u>Module 2 : Configuration de Base</u>

Interface utilisateur: FMC (Firepower Management Center)

Objets de sécurité: Groupes d'accès, réseaux, services.

Politiques de sécurité: Règles d'accès, NAT, VPN.

<u>Module 3 : Système de Prévention des Intrusions (IPS)</u>

Signatures IPS: Types de signatures, mise à jour.

Configuration des règles IPS: Adaptation aux besoins spécifiques.

Gestion des fausses alertes.

<u>Module 4 : Sécurité des Applications Web (WAF)</u>

Protection contre les attaques web: XSS, SQL injection, etc.

Configuration des règles WAF: Protection des applications web.

<u>Module 5 : VPN</u>

IPsec VPN: Configuration de tunnels site-à-site et de télétravail.

SSL VPN: Accès distant sécurisé.

<u>Module 6 : Gestion des Menaces</u>

Threat Intelligence: Sources d'information, intégration dans le Cisco Firepower.

Analyse des événements: Corrélation des événements, investigation des incidents.

Automatisation des réponses: Playbooks, orchestration.

<u>Module 7 : Optimisation des Performances</u>

Dimensionnement du Cisco Firepower: Calcul des capacités.

Optimisation des règles: Éviter les goulots d'étranglement.

Dépannage: Outils et techniques.

<u>Module 8 : Intégration Avancée</u>

Intégration avec SIEM: Corrélation des événements de sécurité.

Automatisation: Ansible, Python.

Cette formation certifiante est la porte d'entrée de la filière sécurité de Cisco. Elle compose l'un des deux prérequis pour devenir CCNP Security. En la suivant, vous apprendrez à maîtriser les compétences et les technologies nécessaires pour implémenter les principales solutions de sécurité Cisco afin d'assurer une protection avancée contre les attaques de cyber sécurité. Durant la formation vous développerez vos connaissances dans la mise en œuvre et l'exploitation des technologies de sécurité de base, notamment la sécurité des réseaux, la sécurité dans les cloud, la sécurité du contenu, la protection et la détection des points d'extrémité, l'accès sécurisé aux réseaux, la visibilité et l'application. Cette formation vous prépare également à réussir l'examen de certification SCOR (350 -701)

40H CODE : SECO4

Objectifs

- Connaitre les concepts et les stratégies de sécurité de l'information au sein du réseau
- Comprendre les attaques TCP/IP courantes, les applications réseau et les points d'extrémité
- Savoir décrire comment les différentes technologies de sécurité des réseaux fonctionnent ensemble pour se protéger contre les attaques
- Savoir mettre en place un contrôle d'accès sur les équipements Cisco ASA et le pare-feu Cisco Firepower
- Connaitre et mettre en œuvre les caractéristiques et les fonctions de sécurité du contenu web fournies par le Cisco Web Security Appliance
- Maitriser les capacités de sécurité de Cisco Umbrella, les modèles de déploiement, la gestion des politiques et la console Investigate
- Connaitre les VPN et savoir décrire les solutions et les algorithmes de cryptographie
- Savoir mettre en œuvre les solutions de connectivité d'accès à distance sécurisé Cisco et savoir décrire comment configurer l'authentification 802.1X et EAP, etc.

Débouchées

- Technicien en sécurité informatique
- Analyste de la sécurité
- Spécialiste de la réponse aux incidents
- sécurité et restauration des systèmes.
- Consultant en sécurité

Prérequis

- CCNA + Network security ou notions équivalentes

CCNP SCOR 350-701

Module 1 : Fondamentaux de la Sécurité Réseau

Concepts de base: Définition de la sécurité réseau, menaces courantes, bonnes pratiques.

Protocoles de sécurité: TCP/IP, SSL/TLS, VPN, IPSec.

Architecture de sécurité: DMZ, pare-feu, systèmes de prévention d'intrusion.

Module 2 : Technologies de Sécurité Cisco

Cisco Firepower: Configuration et gestion, règles de sécurité, fonctionnalités avancées.

Cisco Identity Services Engine (ISE): Authentification, autorisation, comptabilité (AAA), gestion des politiques.

Cisco Secure Email: Protection contre les menaces par e-mail, filtrage du contenu.

Module 3 : Sécurité du Cloud et des Centres de Données

Sécurité dans les environnements cloud: AWS, Azure, GCP.

Sécurité des conteneurs: Docker, Kubernetes.

Sécurité des données au repos et en transit.

Module 4 : Gestion des Événements de Sécurité

Systèmes de détection d'intrusion (IDS/IPS): Configuration et analyse des alertes.

Gestion des logs: Collecte, analyse, corrélation.

Incident response: Plans d'urgence, procédures d'investigation.

Module 5 : Automatisation et Orchestration

Ansible: Automatisation des tâches de configuration et de maintenance.

Intégration avec d'autres outils: SIEM, SOAR.

70H CODE : SECO6

INTRO TO CLOUD SECURITY

Objectifs

- Comprendre les concepts fondamentaux du cloud computing et ses modèles de service (IaaS, PaaS, SaaS).
- Identifier les menaces et les vulnérabilités spécifiques au cloud.
- Connaître les principaux domaines de la sécurité du cloud : sécurité des données, sécurité des identités et des accès, sécurité des infrastructures, conformité et gouvernance.
- Comprendre le modèle de responsabilité partagée dans le

Débouchées

Chefs de projet

Responsables métiers

Professionnels des achats et des contrats

Toute personne souhaitant évoluer

Prérequis

Connaissances de base en informatique

Notions élémentaires de sécurité informatique

Toute personne souhaitant évo-

Module 1 : Introduction au Cloud Computing

Qu'est-ce que le cloud computing ? Définition, avantages, inconvénients.

Les modèles de service cloud : IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service).

Les modèles de déploiement cloud : public, privé, hybride.

Concepts clés : virtualisation, élasticité, scalabilité, haute disponibilité.

Module 2 : Menaces et Vulnérabilités dans le Cloud

Menaces spécifiques au cloud : accès non autorisés, violations de données, attaques DDoS, vulnérabilités des API, etc.

Les risques liés à la virtualisation et à la multi-location.

Les défis de la sécurité dans un environnement partagé.

Module 3 : Le Modèle de Responsabilité Partagée

Explication détaillée du modèle de responsabilité partagée entre le fournisseur de services cloud et le client.

Clarification des responsabilités de chacun en matière de sécurité pour les différents modèles de service (IaaS, PaaS, SaaS).

Importance de la configuration et de la gestion de la sécurité côté client.

Module 4 :Sécurité des Données dans le Cloud

Chiffrement des données au repos et en transit.

Gestion des clés de chiffrement.

Contrôle d'accès aux données.

Protection contre la perte et la corruption de données

Module 5 :Sécurité des Identités et des Accès

Gestion des identités et des accès (IAM).

Authentification multi-facteurs (MFA).

Contrôle d'accès basé sur les rôles (RBAC).

Gestion des identités fédérées.

Module 6 :Sécurité de l'Infrastructure Cloud

Sécurité des réseaux virtuels (VPC).

Groupes de sécurité et pare-feu.

Sécurité des instances virtuelles.

Module 7:Conformité et Gouvernance dans le Cloud

Normes et certifications de sécurité du cloud (ISO 27001, SOC 2, etc.).

Exigences réglementaires et juridiques.

Audit et conformité dans le cloud.

Module 8 : Bonnes Pratiques et Outils de Sécurité du Cloud

Principes de sécurité Zero Trust.

Sécurité par conception (Security by Design).

Outils de sécurité cloud natifs et tiers.

Automatisation de la sécurité.

70H CODE : SECO6

PANORAMA DU TOP 5 DES EDITEURS DE SECURITE

Objectifs

Comprendre les fondamentaux de la sécurité réseau
Comparer et contraster les solutions de sécurité réseau proposées par Cisco, Palo Alto, Fortinet, Checkpoint et F5. Analyser les forces et les faiblesses de chaque solution en fonction des besoins spécifiques d'une organisation.
Évaluer les exigences de sécurité, les contraintes budgétaires et les caractéristiques techniques.
Configurer les fonctionnalités clés, surveiller la performance et répondre aux incidents.
S'adapter aux évolutions technologiques en matière de sécurité réseau: Rester informé des dernières tendances et des nouvelles menaces

Débouchées

Ingénieur sécurité réseau: Conception, mise en œuvre et maintenance de solutions de sécurité réseau
Administrateurs réseaux: Pour enrichir leurs compétences et choisir les meilleures solutions pour sécuriser leurs infrastructures.
Architectes réseau: Pour concevoir des architectures de sécurité robustes et évolutives.
Consultants en sécurité: Pour conseiller leurs clients sur les solutions de sécurité les plus adaptées.

Prérequis

CCNA ou notions équivalentes

<u>Module 1 : Fondamentaux de la Sécurité Réseau</u>
Les enjeux de la sécurité dans un environnement numérique en constante évolution
Principes de défense en profondeur:
Normes et certifications:
ISO 27001, NIST Cybersecurity Framework
Certifications professionnelles (CISSP, CCSP)

<u>Module 2 : Présentation des Principaux Éditeurs</u>
Cisco:
Cisco ASA, FTD, Firepower
IPS, VPN, NGFW
Intégration avec d'autres produits Cisco
Palo Alto:
Pare-feu nouvelle génération
Prévention des intrusions
Analyse des menaces
Fortinet:
FortiGate
FortiClient
FortiAnalyzer
Checkpoint:
Pare-feu nouvelle génération
Threat Prevention
SandBlast
F5:
BIG-IP
Load balancing, WAF, DDoS protection

<u>Module 3 : Comparaison des Solutions</u>
Tableau comparatif des fonctionnalités:
NGFW, IPS, VPN, WAF, Sandboxing
Gestion unifiée des menaces
Intégration avec d'autres solutions de sécurité

Cas d'utilisation:
Protection des réseaux d'entreprise
Sécurité des datacenters
Sécurité du cloud

Critères de sélection:
Taille de l'entreprise
Budget
Exigences réglementaires
Compétences internes

<u>Module 4 : Mise en œuvre et Gestion Configuration de base</u>:
Création de zones de sécurité
Définition de règles de pare-feu
Configuration de VPN

Gestion des événements de sécurité:
Systèmes de détection d'intrusion (IDS/IPS)
Gestion des logs
Réponse aux incidents

Intégration avec d'autres systèmes:
SIEM, SOAR
Orchestration de la sécurité

<u>Module 5 : Tendances et Perspectives</u>
Sécurité cloud:
Sécurité des applications cloud
Sécurité des données dans le cloud

Sécurité IoT:
Protection des appareils connectés

IA et machine learning en sécurité:
Détection des menaces avancées
Automatisation de la réponse aux incidents

70H CODE : NTO5

CCNP ENTERPRISE ADVANCED ROUTING

Objectifs

Le cours CCNP ENARSI vise à doter les professionnels de la réseau des compétences nécessaires pour :

- Configurer, optimiser et dépanner des réseaux d'entreprise complexes.
- Mettre en œuvre des technologies de routage avancées.
- Assurer la haute disponibilité et la performance des réseaux.
- Sécuriser les réseaux d'entreprise.
- Automatiser des tâches de configuration et de gestion de réseau.

Compétences clés à acquérir :

- Routage avancé: EIGRP, OSPF, BGP, ISIS
- VPN: IPsec, DMVPN, GRE
- Services de qualité de service (QoS): Classification, marquage, gestion de la congestion
- Protocoles de routage multicast: PIM, DVMRP
- Technologies de virtualisation: VXLAN, NVGRE
- Automatisation: Ansible, Python
- Sécurité: ACL, IPS, Firewall

Débouchées

- Ingénieur réseau senior: Conception, implémentation et maintenance de réseaux d'entreprise complexes.
- Architecte réseau: Conception de solutions réseau à grande échelle.
- Spécialiste de la sécurité réseau: Mise en œuvre de mesures de sécurité pour protéger les réseaux.
- Consultant réseau: Fourniture de conseils et d'expertise aux entreprises.

Module 1 : Fondamentaux du Routage Avancé

EIGRP: Concepts de base, métriques, auto-summarisation
Configuration avancée (stub areas, route summarization)
OSPF: Types d'areas, LSA, SPF
Configuration avancée (virtual links, OSPFv3)
BGP: Attributs BGP, AS path, route reflectors
Configuration de routage inter-domaine

Module 2 : VPN et Services de Tunnel

IPsec: Encapsulation, modes de transport et tunnel
Configuration de VPN site-à-site
DMVPN: Hub and spoke, full mesh
Configuration et gestion de DMVPN
GRE: Encapsulation générique
Utilisation de GRE pour les tunnels VPN

Module 3 : QoS et Multicast

QoS: Classification, marquage, gestion de la congestion
Configuration de QoS sur les routeurs et commutateurs
Multicast: PIM, DVMRP :Configuration de routage multicast

Module 4 : Technologies de Virtualisation

VXLAN: Encapsulation VXLAN, VTEP
Intégration avec les réseaux physiques
NVGRE: Comparaison avec VXLAN
Cas d'utilisation spécifiques

Module 5 : Automatisation et Programmation Réseau

Ansible: Playbooks, modules
Automatisation de tâches de configuration
Python: Programmation réseau avec Python
Intégration avec les API des équipements réseau

Module 6 : Sécurité Réseau

ACL: Configuration d'ACL étendues et standard
IPS: Déploiement et configuration d'un système de prévention des intrusions
Firewall: Configuration de règles de pare-feu

Module 7 : Haute Disponibilité et Redondance

HSRP, VRRP : Protocoles de routage de secours
CARP: Protocole de clustering pour les commutateurs
Clustering de routeurs: Configuration de clusters de routeurs

Module 8 : Dépannage Avancé

Outils de dépannage:
Debug, show commands
Méthodologie de dépannage
Analyse de traces

Module 9 : Labos Pratiques

Configuration de scénarios réseau complexes
Résolution de problèmes réels

CISSP (Certified Information Systems Security Professional)

40H CODE : SECO3

Certified Information Systems Security Professional)

Objectifs

- Maîtriser les huit domaines du CBK du CISSP :
- Comprendre les concepts, les principes et les meilleures pratiques de la sécurité de l'information.
- Développer une approche holistique de la sécurité des systèmes d'information.
- Préparer efficacement l'examen de certification CISSP.

Débouchées

- Directeur de la sécurité des systèmes d'information (DSSI/CISO).
- Responsable de la sécurité de l'information.
- Architecte de sécurité.
- Consultant en sécurité.

Prérequis

- Expérience professionnelle significative dans le domaine de la sécurité de l'information (comme mentionné ci-dessus).
- Connaissances générales en informatique et en réseaux.

Module 1 : Sécurité et gestion des risques (Security and Risk Management)

Concepts de base de la sécurité de l'information.

Gestion des risques : identification, analyse, évaluation, traitement et surveillance.

Cadres de gestion des risques (NIST, ISO 31000).

Politiques, normes, procédures et directives de sécurité.

Lois, réglementations et conformité (RGPD, HIPAA, etc.).

Éthique professionnelle.

BCP/DRP (Business Continuity Planning/Disaster Recovery Planning).

Module 2 : Sécurité des actifs (Asset Security)

Classification des informations.

Propriété des données.

Protection de la vie privée.

Gestion du cycle de vie des informations.

Module 3 :Ingénierie de sécurité (Security Architecture and Engineering)

Principes de conception sécurisée.

Modèles de sécurité.

Architecture des systèmes de sécurité.

Sécurité des systèmes embarqués et des systèmes de contrôle industriel (ICS).

Cryptographie : concepts, algorithmes, implémentations.

Module 4 :Sécurité des communications et des réseaux (Communication and Network Security)

Modèles de réseau (OSI, TCP/IP).

Protocoles réseau et sécurité des protocoles.

Conception et implémentation de réseaux sécurisés (pare-feu, VPN, IDS/IPS).

Sécurité des réseaux sans fil.

Module 5 : Gestion des identités et des accès

Identification et authentification.

Autorisation.

Gestion du cycle de vie des identités.

Types de contrôles d'accès.

Module 6 : Évaluation et tests de sécurité (Security Assessment and Testing)

Types de tests de sécurité (tests de pénétration, analyses de vulnérabilités).

Méthodologies de test.

Outils de test de sécurité.

Audit de sécurité.

Module 7 :Opérations de sécurité (Security Operations)

Gestion des incidents de sécurité.

Gestion des changements.

Gestion des vulnérabilités.

Surveillance et journalisation de la sécurité.

Sécurité physique.

Sensibilisation et formation à la sécurité.

40H CODE : SECO3

AWS Certified Security – Specialty

Objectifs

- Maîtriser les concepts et les services AWS liés à la sécurité.
- Être capable de concevoir et de mettre en œuvre des solutions de sécurité robustes sur AWS.
- Comprendre les meilleures pratiques en matière de sécurité, de conformité et de gestion des risques sur AWS.
- Savoir automatiser les tâches de sécurité et répondre aux incidents de sécurité.

Débouchées

- Ingénieur sécurité cloud.
- Architecte sécurité cloud.
- Consultant en sécurité AWS.
- Spécialiste en réponse aux incidents sur

Prérequis

- Expérience pratique avec les services AWS (au moins 2 ans).
- Connaissances solides en sécurité informatique (réseaux, systèmes d'exploitation, cryptographie).
- Certification AWS Certified Cloud Practitioner ou AWS Certified Solu-

Module 1 : Réponse aux incidents

Planification de la réponse aux incidents.

Détection et analyse des incidents de sécurité.

Confinement, éradication et reprise après incident.

Utilisation des services AWS pour la réponse aux incidents (AWS Security Hub, Amazon GuardDuty, AWS Config, AWS CloudTrail, Amazon CloudWatch).

Automatisation de la réponse aux incidents avec AWS Lambda et AWS Systems Manager.

Module 2 :Surveillance et journalisation

Collecte et analyse des journaux (AWS CloudTrail, Amazon CloudWatch Logs, VPC Flow Logs, AWS Config).

Surveillance des métriques de sécurité (Amazon CloudWatch Metrics).

Utilisation des services de sécurité pour la surveillance (Amazon GuardDuty, AWS Security Hub, Amazon Inspector).

Création d'alertes et de tableaux de bord de sécurité.

Centralisation de la gestion des journaux avec Amazon S3 et Amazon Athena.

Module 3 :Sécurité de l'infrastructure

Sécurité des réseaux : VPC, sous-réseaux, groupes de sécurité, Network ACLs, AWS Network Firewall, AWS Transit Gateway.Sécurité des instances EC2 : durcissement des instances, gestion des accès, utilisation d'AMIs sécurisées.

Sécurité des conteneurs : ECS, EKS, Fargate, sécurité des images Docker.

Sécurité du serverless : AWS Lambda, API Gateway.

Sécurité du stockage : S3, EBS, EFS, Glacier, chiffrement des données au repos et en transit.

Module 4 : Gestion des identités et des accès (IAM)

IAM : utilisateurs, groupes, rôles, politiques, identités fédérées.

Stratégies de moindre privilège.

Gestion des clés d'accès.

AWS Organizations : gestion multi-comptes et contrôle d'accès centralisé.

AWS Single Sign-On (SSO).

Intégration avec des fournisseurs d'identité externes.

Module 5 : Protection des données

Chiffrement des données : KMS, CloudHSM, chiffrement côté client et côté serveur.

Gestion des clés de chiffrement.

Protection contre la perte de données : sauvegardes, restauration, réplication.

Conformité aux réglementations sur la protection des données (RGPD, HIPAA, etc.).Classification et étiquetage des données.AWS Data Loss Prevention

ISO 27001

70H CODE : GOVO1

Objectifs

Comprendre les principes fondamentaux de la norme ISO 27001 et son importance pour la sécurité de l'information.

- Acquérir les connaissances nécessaires pour planifier, mettre en œuvre, maintenir et améliorer un SMSI conforme à la norme.
- Identifier et évaluer les risques liés à la sécurité de l'information.
- Mettre en place des mesures de sécurité appropriées pour protéger les informations sensibles.
- Préparer un organisme à la certification ISO

Débouchées

- Responsable de la sécurité des systèmes d'information (RSSI) / Chief Information Security Officer (CISO)
- Auditeur interne ISO 27001
- Auditeur externe ISO 27001 (Lead Auditor)
- Consultant en sécurité de l'information

Prérequis

Formation d'initiation (sensibilisation)

Formation d'implémentation (Lead

<u>Introduction à la sécurité de l'information et à la norme ISO 27001 :</u>

Concepts clés de la sécurité de l'information : confidentialité, intégrité, disponibilité.
Menaces et vulnérabilités des systèmes d'information.
Présentation de la norme ISO 27001 : historique, objectifs, structure.
Liens avec d'autres normes (ISO 27002, ISO 27005, ISO 22301, etc.).
Les bénéfices de la certification ISO 27001 pour une organisation.

<u>Exigences de la norme ISO 27001</u>

Analyse détaillée des exigences de la norme :
Contexte de l'organisme.
Leadership.
Planification (analyse des risques, objectifs de sécurité).
Support (ressources, compétences, sensibilisation, communication, informations documentées).
Réalisation des activités opérationnelles (maîtrise des risques).
Évaluation des performances (surveillance, mesure, analyse et évaluation, audit interne, revue de direction).
Amélioration.
Exercices pratiques d'interprétation des exigences.

<u>Analyse et traitement des risques</u>

Méthodologies d'analyse des risques (ISO 27005, EBIOS RM).
Identification des actifs informationnels.
Identification des menaces et des vulnérabilités.
Évaluation des risques (impacts et probabilités).
Options de traitement des risques : éviter, transférer, atténuer, accepter.
Mise en place des mesures de sécurité (contrôles de l'Annexe A de l'ISO 27001).
Exercices pratiques d'analyse et de traitement des risques.

<u>Mise en œuvre et maintenance d'un SMSI :</u>

Explication de l'importance de la Élaboration de la documentation du SMSI (politique de sécurité, procédures, instructions).
Mise en œuvre des mesures de sécurité.
Formation et sensibilisation du personnel.
Gestion des incidents de sécurité.
Surveillance et mesure de l'efficacité du SMSI.
Audits internes et revue de direction.
Amélioration continue du SMSI.
Préparation à l'audit de certification.

<u>Audit et certification ISO 27001 :</u>

Le processus de certification ISO 27001.
Le rôle de l'organisme certificateur.
Préparation et déroulement d'un audit de certification.
Gestion des non-conformités.
Maintien de la certification.
Expliquer les procédures de dépannage du système d'exploitation Microsoft Windows.

24H CODE : MSO6

Objectifs

- Déployer et gérer AD DS dans des environnements hybrides.
- Gérer des serveurs Windows et des charges de travail dans Azure.
- Gérer des machines virtuelles et des conteneurs dans un contexte hybride.
- Configurer et gérer une infrastructure réseau hybride.
- Gérer les services de stockage et de fichiers dans un environnement hybride.
- Utiliser les outils et les scripts

Débouchées

- Administrateur système hybride.
- Ingénieur cloud hybride.
- Spécialiste en infrastructure hybride.
- Consultant en migration vers le cloud

Prérequis

Notions en informatique et en réseau

Programme AZURE 800

Module 1 : Déployer et gérer Active Directory Domain Services (AD DS) dans des environnements locaux et cloud

Installation et configuration des contrôleurs de domaine AD DS.

Gestion des objets AD DS (utilisateurs, groupes, GPO).

Implémentation de l'intégration hybride avec Azure AD (Azure AD Connect, synchronisation du hachage de mot de passe, authentification directe).

Gestion des identités hybrides (authentification unique, authentification multifacteur).

Résolution des problèmes d'AD DS.

Module 2 : Gérer les serveurs et les charges de travail Windows Server dans un environnement hybride

Gestion des serveurs Windows Server sur site et dans Azure (machines virtuelles Azure).

Implémentation et gestion de Windows Admin Center.

Gestion des mises à jour des serveurs.

Migration des charges de travail vers Azure.

Module 3 : Gérer les machines virtuelles et les conteneurs

Déploiement et gestion des machines virtuelles Azure.

Configuration du stockage et du réseau pour les machines virtuelles.

Gestion des conteneurs avec Azure Kubernetes Service (AKS) et Azure Container Instances (ACI).

Implémentation de solutions de conteneurisation hybrides.

Module 4 : Implémenter et gérer une infrastructure réseau locale et hybride

Configuration des réseaux virtuels Azure et de la connectivité hybride (VPN, ExpressRoute).

Gestion de la résolution de noms (DNS) dans un environnement hybride.

Implémentation et gestion des services de routage et d'équilibrage de charge.

Configuration des pare-feu et de la sécurité réseau.

Module 4 : Gérer les services de stockage et de fichiers

Implémentation et gestion du stockage Azure (Stockage Blob,

24H CODE : MS07

Objectifs

- Mettre en œuvre et gérer les solutions d'identité et d'accès dans Microsoft 365.
- Déployer et gérer les solutions de protection contre les menaces de Microsoft 365.
- Implémenter et gérer la protection des informations dans Microsoft 365.
- Gérer la gouvernance et la conformité des données dans Microsoft 365.
- Utiliser les outils d'administration et de surveillance de la sécurité de Microsoft

Débouchées

- Administrateur de la sécurité Microsoft 365.
- Ingénieur en sécurité cloud.
- Analyste en sécurité.

Prérequis

- Une expérience pratique en administration de Microsoft 365.
- Une compréhension des concepts de sécurité réseau et des principes de sécurité informatique.
- Une familiarité avec les outils d'administration Microsoft, tels que PowerShell et le centre d'administration Microsoft 365.

Programme SECURITY ADMINISTRATOR MS 500

Module 1 : Implémenter et gérer l'identité et l'accès

Planifier et mettre en œuvre l'authentification et l'autorisation modernes (par exemple, Azure AD, authentification multifacteur, accès conditionnel).

Gérer les identités et les rôles dans Azure AD.

Mettre en œuvre et gérer la gouvernance des identités (par exemple, gestion du cycle de vie des identités, gestion des accès privilégiés).

Module 2 : Implémenter et gérer la protection contre les menaces

Planifier, mettre en œuvre et gérer Microsoft Defender pour Office 365 (protection contre les menaces par e-mail et collaboration).

Planifier, mettre en œuvre et gérer Microsoft Defender pour Identity (protection des identités sur site).

Planifier, mettre en œuvre et gérer Microsoft Defender pour point de terminaison (protection des appareils).

Gérer les alertes et les incidents de sécurité.

Module 3 : Implémenter et gérer la protection des informations

Planifier et mettre en œuvre la classification et l'étiquetage des données.

Mettre en œuvre et gérer la prévention de la perte de données (DLP).

Mettre en œuvre et gérer le chiffrement des données (par exemple, Azure Information Protection, chiffrement des messages Office 365).

Module 4 : Gérer la gouvernance et la conformité dans Microsoft 365

Planifier et mettre en œuvre la gouvernance des informations (par exemple, rétention, suppression, eDiscovery).

Gérer les audits et les rapports de

40H CODE : SECO3

ISO 27005

Objectifs

- Comprendre les concepts fondamentaux de la gestion des risques de sécurité de l'information selon la norme ISO 27005.
- Maîtriser les étapes du processus de gestion des risques : contexte, identification, analyse, évaluation, traitement, acceptation et communication.
- Être capable de mettre en œuvre une méthodologie d'analyse des risques adaptée à son organisation.
- Savoir identifier et évaluer les actifs informationnels, les menaces et les vulnérabilités.
- Déterminer les mesures de sécurité appropriées pour traiter les risques identifiés.

Débouchées

- Analyste des risques SSI
- Consultant en gestion des risques SSI
- Responsable de la sécurité des systèmes d'information (RSSI)

Prérequis

- Connaissances de base en sécurité de l'information.
- Familiarité avec la norme ISO

Module 1 : Module 1 : Introduction à la gestion des risques et à ISO 27005

Concepts clés de la gestion des risques : risque, menace, vulnérabilité, impact, probabilité.

Présentation de la norme ISO 27005 : historique, objectifs, structure, liens avec ISO 27001.

Importance de la gestion des risques pour la sécurité de l'information.

Les bénéfices d'une approche structurée de la gestion des risques.

Module 2 : Contexte et établissement des critères

Définir le contexte de la gestion des risques : objectifs, périmètre, parties prenantes.

Établir les critères d'acceptation des risques : niveaux de risque acceptables, échelles d'impact et de probabilité.

Définir les rôles et les responsabilités dans le processus de gestion des risques.

Module 3 : Identification des risques

Identification des actifs informationnels : données, logiciels, matériels, services, personnes.

Identification des menaces : sources de danger potentielles.

Identification des vulnérabilités : faiblesses exploitables par les menaces.

Techniques d'identification des risques : brainstorming, questionnaires, analyses de vulnérabilités, revues de documents.

Exercices pratiques d'identification des actifs, des menaces et des vulnérabilités

Module 4 : Analyse des risques

Évaluation des impacts : conséquences potentielles de la réalisation d'un risque.

Évaluation des probabilités : chance qu'une menace exploite une vulnérabilité.

Méthodes d'analyse des risques : qualitative, quantitative, semi-quantitative.

Utilisation de matrices de risques.

Exercices pratiques d'analyse des risques et de calcul des niveaux de risque.

Module 5 : Traitement des risques

Options de traitement des risques : éviter, transférer, atténuer, accepter.

Sélection des mesures de sécurité appropriées : contrôles techniques, organisationnels et physiques.

Élaboration d'un plan de traitement des risques.

40H CODE : SECO3

DOCKER DCA

Objectifs

- Comprendre les concepts fondamentaux de Docker et de la conteneurisation.
- Maîtriser l'installation, la configuration et l'utilisation de Docker Engine.
- Savoir créer, gérer et optimiser des images Docker.
- Comprendre le fonctionnement des réseaux et du stockage avec Docker.
- Être capable de déployer et d'orchestrer des applications conteneurisées avec Docker Swarm.
- Connaître les bonnes pratiques

Débouchées

- Administrateur système Docker.
- Ingénieur DevOps.
- Développeur d'applications conteneurisées.

Prérequis

- Connaissances de base des systèmes d'exploitation Linux ou Windows.
- Familiarité avec l'utilisation de la ligne de commande.

<u>Module 1 : Introduction à la conteneurisation et à Docker</u>

Les concepts de la conteneurisation : avantages par rapport à la virtualisation traditionnelle.

Présentation de Docker : historique, architecture, composants clés (Docker Engine, Docker Client, Docker Registry).

Installation et configuration de Docker Engine sur Linux et Windows.

Les commandes Docker de base : docker run, docker ps, docker stop, docker rm.

Premier contact avec les images et les conteneurs.

<u>Module 2 : Contexte et établissement des critères</u>

Les Dockerfiles : structure, instructions (FROM, RUN, COPY, CMD, ENTRYPOINT, etc.).

Création d'images Docker personnalisées.

Optimisation de la taille des images (multi-stage builds, .dockerignore).

Gestion des tags et des versions d'images.

Utilisation des registres Docker : Docker Hub, registres privés.

Les commandes **docker build, docker images, docker push, docker pull, docker rmi.**

<u>Module 3 :Gestion des conteneurs</u>

<u>Cycle de vie d'un conteneur.</u>

Configuration des conteneurs : variables d'environnement, ports, volumes.

Gestion des logs et du débogage des conteneurs.

Les commandes docker exec, docker logs, docker inspect, docker stats.

Utilisation de Docker Compose pour gérer des applications multi-conteneurs

<u>Module 4 : Réseaux Docker</u>

Les différents types de réseaux Docker : bridge, host, overlay, macvlan.

Configuration des réseaux Docker.

Communication entre les conteneurs.

Publication des ports des conteneurs.

Résolution de noms avec Docker.

<u>Module 5 : Stockage avec Docker</u>

Les différents types de stockage avec Docker : volumes, bind mounts, tmpfs mounts.

Gestion des volumes Docker.

Persistance des données.

Choix de la stratégie de stockage appropriée.

<u>Module 6 : Orchestration avec Docker Swarm</u>

Introduction à l'orchestration de conteneurs.

Création et gestion d'un cluster Swarm : managers et workers.

Déploiement de services sur Swarm.

Mise à l'échelle des services.

Gestion des mises à jour des services (rolling updates).

Gestion des secrets et des configurations avec Swarm.

Les commandes docker swarm, docker service, docker stack.

<u>Module 7 :Sécurité avec Docker</u>

Bonnes pratiques de sécurité pour les images Docker.

Nos partenaires technologiques

NDG

cisco

aruba

RHOPEN LABS

Microsoft

Ils nous font confiance

neeco
LOBAL ICT SERVICE

KONICA MINOLTA

ASTON ECOLE IT BY SQLI

E.S.I.C
Ecole Supérieure d'Informatique et de Commerce

m2i Formation

MOLIGE CAMEROUN
Industrie de fabrication des Produits Agroalimentaires

Où Nous trouver

CAMEROUN

Akwa 34 rue Boue lapeyrère ,
face hôtel planet

Tel : +237 670 556 187
+237 697 925 426
+237 656 019 902

CONGO BRAZAVILLE

Diata derrière le
stade Aphonse
Massamba Debat

Tel : +242 06 923 74 03

CANADA

102 Rue de Touraine, Lévis,
QC, G6J 2A8

Tel : +1 (581) 308-8186

FRANCE

30 Rue de Liège
75008 Paris, France
RCS Paris

Tel : +33(0) 920 303 773