Cybersécurité

Responsable en sécurité des systèmes d'information

Mettez en œuvre une stratégie de cybersécurité dans votre entreprise et déployez-la en continu

Durée de la formation
1135 heures

à temps plein
12 mois

Master's-level diploma *

*Master - Ingénierie des systèmes complexes - code NSF 110 - Master's-level diploma - certification professionnelle enregistrée au Répertoire National des Certifications Professionnelles (RNCP) par décision de France compétences publiée le 01/09/2019

OPENCLASSROOMS

Formation mise à jour le 19 juin 2024

Projet 1 - 10 heures

Démarrez votre formation de Responsable en sécurité des Systèmes d'information

Mettez-vous dans les meilleures conditions pour réussir votre parcours : projetez-vous dans votre formation, définissez votre planning et appropriez-vous les outils essentiels pour apprendre.

Compétences cibles

- Définir le cadre de votre formation

Cours associés

Engagez-vous dans votre formation OpenClassrooms

Facile 2 heures

Prenez en main votre parcours OpenClassrooms et réalisez votre premier projet en suivant ce cours conçu pour vous accompagner dans ces premières étapes de formation.

Projet 2 - 10 heures

24h dans la peau d'un Responsable en sécurité des Systèmes d'information

A partir de témoignages, vous découvrirez les missions au quotidien d'un RSSI et commencerez à clarifier votre projet professionnel

Compétences cibles

- Construire pas à pas son projet professionnel
- Identifier vos compétences existantes et vos motivations pour ce métier

Cours associés

Construisez votre projet professionnel

Facile 6 heures

Vous souhaitez booster votre carrière ? Construisez votre projet pas à pas et ouvrez-vous de nouvelles perspectives professionnelles !

Découvrez l'univers de la cybersécurité

Facile 4 heures

Comprenez le déroulement des cyberattaques, enjeu majeur de société, et découvrez l'ensemble des métiers qui participent à la cybersécurité. Peut-être vous demain ?

Optimisez votre apprentissage avec l'Intelligence Artificielle

Facile 6 heures

Utiliser l’IA en gardant un esprit critique, pour acquérir plus rapidement des compétences, gagner en productivité et mieux organiser votre planning d’apprentissage.

Projet 3 - 50 heures

Sécurisez l'infrastructure SI d'une entreprise

À partir d'une demande d'un client, vous proposerez une architecture SI sécurisée.

Compétences cibles

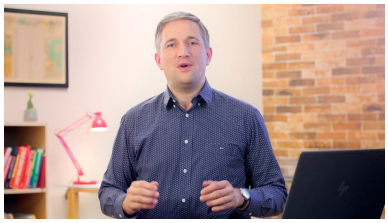
- Sécuriser un serveur web Apache
- Sécuriser Windows avec Active Directory
- Configurer des VLAN avec un switch
- Configurer un pare-feu
- Installer une infrastructure virtuelle
- Configurer un serveur Linux sécurisé

Cours associés

Centralisez et sécurisez votre annuaire Active Directory

Moyenne 8 heures

Avec ce cours, apprenez à maîtriser Active Directory. Ce service d'annuaire basé sur LDAP vous aidera à centraliser l'identification et l'authentification des ressources.



Sécurisez vos infrastructures

Difficile 10 heures

Apprenez à sécuriser vos infrastructures des attaques physiques mais aussi des cyber attaques grâce aux protocoles, firewalls et autres techniques ! Dans ce cours, vous aborderez les types de hacking les plus connus et comment vous en protéger.

Initiez-vous à Linux

Facile 8 heures

Dans ce cours débutant, découvrez Linux : un système d'exploitation gratuit et fascinant qui vous donnera un contrôle sans précédent sur votre ordinateur ! Créé par des passionnés d'informatique, Linux est un vecteur important de la philosophie du libre et l'alternative parfaite à Windows ou macOS.

Simulez le schéma de votre réseau avec Cisco Packet Tracer

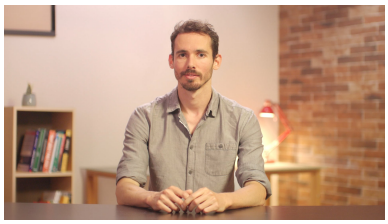
Moyenne 12 heures

Apprenez à simuler votre schéma de réseau d'entreprise avec l'outil Cisco Packet Tracer : configurez et sécurisez votre réseau.

Administrez un système Linux

Moyenne 10 heures

Initiez-vous à l'administration d'un serveur Linux : utilisez le terminal et le shell, manipulez des fichiers, configurez un réseau et surveillez l'activité du système !



Virtualisez votre architecture et vos environnements de travail

Facile 6 heures

Découvrez la virtualisation et les machines virtuelles. Distinguez les types d'hyperviseurs et virtualisez vos environnements de test et l'architecture de vos systèmes d'information !

Projet 4 - 50 heures

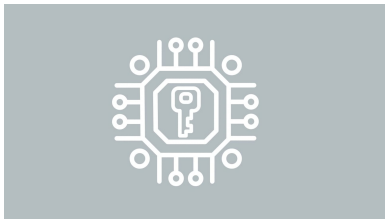
Sécurisez une application du SI

Afin d'aider votre entreprise à réaliser une application web sécurisée pour accéder à son SI existant, vous proposerez la liste des vulnérabilités et rédigerez votre proposition pour présenter votre solution technique.

Compétences cibles

- Rédiger des tests de sécurité
- Détecter les vulnérabilités dans le code
- Définir les exigences de sécurité

Cours associés



Sécurisez vos données avec la cryptographie

Moyenne 8 heures

Maîtrisez les bases de la cryptographie afin de chiffrer vos données et ainsi, développer par exemple des signatures électroniques, des certificats, hacher les mots de passe, faire de la communication sécurisée, etc.

Sécurisez vos applications

Moyenne 10 heures

Les applications sont vulnérables aux cyber-attaques. Dans ce cours, vous apprendrez à identifier les vulnérabilités et à proposer des bonnes pratiques à vos développeurs pour vous en protéger : mécanismes d'authentification, échappements de caractères, TLS...

Sécurisez vos applications web avec l'OWASP

Moyenne 10 heures

Pour créer une application de qualité, vous devez définir son modèle de sécurité ! Apprenez à appliquer les techniques de OWASP, une communauté qui fournit des outils inestimables pour réduire les risques de sécurité dans le développement web.

Projet 5 - 60 heures

Auditez la sécurité SI de l'entreprise

A partir de l'architecture SI de l'entreprise et de la politique SSI, vous proposerez un plan d'audit de sécurité contenant un audit externe et un audit interne.

Compétences cibles

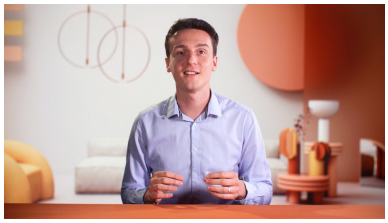
- Conduire des tests d'intrusion
- Rédiger un plan d'audit

Cours associés

Construisez votre stratégie d'audits et de contrôles cybersécurité

Moyenne 6 heures

Cartographiez les différentes typologies d'audits et contrôles existants, et construisez sur cette base une stratégie d'audits adaptée à vos besoins.



Réalisez un test d'intrusion web

Moyenne 10 heures

Mettez-vous dans la peau d'un attaquant et réalisez un test d'intrusion de A à Z sur une application web, grâce à la méthode et aux outils d'un pentester professionnel !

Planifiez une politique d'audit au sein de votre entreprise

Difficile 8 heures

Déterminez une stratégie d'audit, puis planifiez les audits, préparez-les et réalisez-les pour apporter de la valeur à votre entreprise.

Projet 6 - 50 heures

Mettez en place la surveillance de la sécurité SI

A partir de l'architecture Si d'une entreprise, vous proposerez une architecture de surveillance SI, ses règles et des procédures de traitement d'alertes.

Compétences cibles

- Configurer la journalisation des éléments du SI
- Proposer des scénarios de corrélation
- Concevoir une architecture de surveillance de la sécurité SI

Cours associés

Optimisez la sécurité informatique grâce au monitoring

Difficile 8 heures

Apprenez à sécuriser votre système d'information en optimisant la collecte et la remontée de logs pour en tirer des scénarios de corrélation pertinents.

Simulez le schéma de votre réseau avec Cisco Packet Tracer

Moyenne 12 heures

Apprenez à simuler votre schéma de réseau d'entreprise avec l'outil Cisco Packet Tracer : configurez et sécurisez votre réseau.

Projet 7 - 60 heures

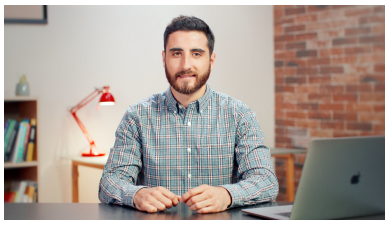
Investiguez un incident de sécurité

A partir de logs réseau, systèmes et applicatifs, vous effectuerez une analyse forensique pour détecter les attaques qui ont été menées et rédigerez un rapport d'incident qui évalue l'impact des attaques SI.

Compétences cibles

- Réaliser une analyse forensics
- Rédiger un rapport d'incident de sécurité

Cours associés



Menez une investigation d’incident numérique forensic

Difficile 20 heures

Menez une investigation numérique forensic suite à une cyber attaque. Identifiez vos indicateurs de compromission et rédigez des recommandations dans un rapport d'incident de sécurité.

Projet 8 - 10 heures

Créez et présentez votre CV pour un entretien

Dans ce projet, vous réalisez votre CV pour rechercher votre stage ou votre premier job dans la sécurité des SI !

Compétences cibles

- Réaliser un CV

Projet 9 - 90 heures

Gérez le risque SI d'une organisation

A partir des informations métier et organisationnelles d'une entreprise, du contexte des menaces et des obligations légales, vous identifierez les menaces sur la sécurité SI et évaluerez l'impact des attaques pour proposer une politique de sécurité.

Compétences cibles

- Analyser les risques SI
- Rédiger une Politique de Sécurité SI

Cours associés

Analysez et gérez des risques SI

Moyenne 4 heures

Grâce à ce cours, vous maîtriserez les différentes étapes d'analyse de risques de votre Système d'Information, de l'analyse de votre contexte à l'élaboration et la mise en œuvre d'un plan d'action. Vous découvrirez comment identifier, analyser et traiter les risques.

Définissez la politique de sécurité de votre entreprise

Difficile 8 heures

Mettez en place une politique de sécurité (PSSI) ! Découvrez les standards de sécurité, mettez en place un système de management de sécurité info (SMSI) et rédigez la politique de sécurité SI.

Gérez un projet digital avec une méthodologie en cascade

Facile 8 heures

Vivez la gestion de projet avec une méthodologie classique. Apprenez à gérer les 5 phases d'un projet en cascade : l'initialisation, le lancement, la conception, la production et l'exploitation.

Initiez-vous à la gestion de projet agile

Facile 6 heures

Formez votre équipe agile, prenez en compte le besoin des utilisateurs et développez des pratiques agiles comme le Planning Poker, les méthodes Kanban et Lean...

Mettez en place un plan de continuité d'activité (PCA)

Difficile 6 heures

Découvrez comment mettre en place un plan de continuité d'activité (PCA), en vous appuyant sur la norme ISO 22301, afin de réduire les impacts des sinistres et assurer une reprise d'activité efficace.

Maîtrisez les risques juridiques liés au numérique

Moyenne 12 heures

Mener un projet numérique nécessite de maîtriser certains risques juridiques, en particulier à l'heure du RGPD. Suivez ce cours pour mieux comprendre ces enjeux et connaître les fondamentaux pour ne pas faire de faux pas en droit du numérique !

Projet 10 - 10 heures

Réalisez une veille sur les menaces et les solutions

Réalisez une veille technologique sur les vulnérabilités, les attaques et la réglementation, et rédigez un rapport de veille en évaluant des produits de sécurité du marché.

Compétences cibles

- Effectuer une veille technologique, réglementaire, économique sur la sécurité des SI

Cours associés

Mettez en place un système de veille informationnelle

Facile 4 heures

Apprenez à faire de la veille pour vous adapter aux évolutions de votre métier et à utiliser des outils de veille informationnelle.

Projet 11 - 735 heures

Réalisez un stage (ou une mission en entreprise) dans la sécurité des systèmes d'information

Pour valider votre formation, vous allez devoir effectuer un stage de 6 mois (20 à 26 semaines) afin de mettre en pratique vos compétences de futur Responsable en sécurité des systèmes d'information.

Compétences cibles

- Effectuer un bilan de formation