Sécurité défensive

Analyste Cybersécurité

140 jours (980h00) | ★★★★½ 4,6/5 | FD-ACS | Code RS ou RNCP : RS6092 | Certification Réaliser des tests d'intrusion (Sécurité Pentesting) (incluse) | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Formations Informatique › Cybersécurité › Sécurité défensive

Contenu mis à jour le 13/10/2023. Document téléchargé le 30/05/2024.

Objectifs de formation

A l'issue de cette formation, vous serez capable de :

- Protéger une organisation en utilisant une gamme de technologies et de processus pour prévenir, détecter et gérer les cybermenaces
- Mener des audits de sécurité et détecter des failles et des faiblesses dans le système d'information de l'entreprise
- Faire une synthèse des résultats
- Mettre des solutions en place
- Organiser l'entreprise autour de vos préconisations à condition d'avoir défendu votre projet devant la Direction
- Mettre en place des protections et assurer la surveillance des systèmes informatiques
- Gérer l'organisation des entreprises du point de vue sécurité informatique
- Construire des plans d'affaires visant à organiser la sécurité informatique dans l'entreprise
- Présenter oralement votre expertise auprès des décideurs
- Rédiger un plan d'actions et présenter votre rapport de fin de mission
- Identifier les évolutions réglementaires et techniques de votre domaine
- Assurer les relations avec les acteurs de votre secteur d'activité autour de la cybersécurité
- Passer la certification "Réaliser des tests d'intrusion (Sécurité Pentesting)".

Compétences attestées par la certification

- Définir les enjeux et contraintes du test d'intrusion dans l'objectif de définir les scénarios les plus probables ainsi que l'obtention du consentement légal
- Appliquer une méthodologie de test d'intrusion claire et reproductible afin de pouvoir restituer des éléments comparables dans leurs approches
- Concevoir et réaligner des outils d'intrusion dans l'objectif de répondre aux différents besoins d'un test d'intrusion
- Identifier les différentes vulnérabilités présentes en réalisant les différentes phases des tests d'intrusion évoqués dans les enjeux initiaux dans le but de découvrir les points de faiblesses de l'organisation
- Remonter et restituer les différentes vulnérabilités identifiées ainsi qu'un plan d'actions contenant les mesures de sécurité permettant à l'organisation de corriger ses failles.

Lien pour visualiser le détail de la certification enregistrée au RS :
https://www.francecompetences.fr/recherche/rs/6092/

Modalités, méthodes et moyens pédagogiques

Formation en présentiel à distance

- 35 heures/semaine, du lundi au vendredi de 9h00 à 17h00
- Formation synchrone avec une équipe pédagogique dédiée tout au long du parcours, comme en présentiel
- Modalités : théorie, pratique, travaux de groupes, individuels, réalisation de projets
- La formation est composée d'une période théorique de 700 heures puis d'une période pratique en entreprise de 280 heures (durées moyennes données à titre indicatif)
- Compte-tenu de l'évolution du référentiel, des compétences métier, des logiciels, les éléments du programme ne sauraient être contractuels.

Prérequis techniques fortement conseillés pour suivre cette formation en présentiel à distance

- Connexion Internet "haut débit", 15 mégabits par seconde minimum
- Fibre non obligatoire
- Relier sa box à son ordinateur via un câble réseau
- Résider en France Métropolitaine
- Etre muni d'un casque audio / micro
- PC / MAC i5, SSD, 16 Go de RAM
- Configuration nécessaire pour travailler sur des environnements virtualisés.

Pédagogie

- Apprentissage métier proactif basé sur le "faire", avec l'accompagnement des formateurs tout au long du parcours
- Accès individuel aux ressources de formation et progression personnalisée si besoin
- Outils de suivi collectifs et individuels (espaces d'échanges et de partage en ligne, salles virtuelles, supports de cours, TP, exercices).

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

Prérequis

Avoir des connaissances générales en maintenance, support, système, réseau ainsi que des notions en sécurité informatique. Un niveau Bac +2 en informatique (réseaux, systèmes...) et une expérience professionnelle en milieu informatique (TSSR, développeur) sont souhaités. L'entrée en formation est soumise à un entretien avec un conseiller formation visant à démontrer la cohérence du projet professionnel en adéquation avec la formation visée, un positionnement via une plateforme de test et une validation du financement du parcours (délai d'accès variable selon le calendrier de la formation et le dispositif de financement mobilisé, entre 15 jours et 5 mois).

Public concerné

Toute personne en reconversion professionnelle ou souhaitant monter en compétences.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Contenu de la formation

Les bases sécurité réseau LAN

- Protection des équipements
- La sécurité des couches physiques et liaison
- Configuration d'un VPN
- La sécurité de la couche réseau via le pare-feu ASA
- Chiffrement symétrique et asymétrique

Sécurité systèmes et réseaux

- Généralités sur la sécurité des infrastructures
- Les types de pare-feux
- Les différents proxies
- Proxy HTTP et HTTPS via Squid
- Reverse proxy avec HAProxy
- Système de détection d'intrusion (IDS)
- Redondance de pare-feu

Sécurité mobile

- La sécurité dans le projet de mobilité
- Normes
- Mise en oeuvre de solutions techniques
- Le Cloud et la mobilité
- Panorama des solutions du marché
- Mise en place d'un MDM
- Géolocalisation d'utilisateurs

Linux

- Naissance de Linux à partir d'Unix
- L'histoire de l'Open Source
- Les différents types de distribution Linux
- Qu'est-ce que le Shell ?
- Les commandes de base
- Découverte de Sudo
- Utilisateurs et groupes
- Netfilter via iptables

VPN

- Les fondamentaux du VPN
- Présentation et mise en oeuvre d'un VPN PPTP
- Présentation d'un VPN L2TP
- Principe du protocole IPsec et mise en oeuvre
- Principe des protocoles SSL/TLS

Mise en oeuvre PKI

- Cryptographie
- Type de chiffrement
- Certificats, clés publiques / privées
- Autorité de certification entreprise
- Présentation d'une autorité de certification
- Révocation de certificats
- Chiffrement de fichiers EFS

- VPN implémentation de SSL avec SSTP
- Sauvegarde de l'AC
- Modèles de certificats

Techniques de hacking

- Veille sécurité informatique
- Organisation de la SSI
- Normes et référentiels
- Aspects juridiques
- Les techniques de hacking et contre-mesures
- Attaque MITM
- Redirection sur une fausse page Web
- Post exploitation
- Risques juridiques
- Introduction au Pentest
- Les méthodologies de Pentest
- Reconnaissance active avancée
- Utilisation de SearchSploit
- Social engineering

Sécurité Web

- Les différentes méthodologies
- Mise en place du lab
- Les basiques sur HTTP
- OWASP Top 10
- Scanning de base et énumération
- Outils scanning Proxy
- Injection SQL
- Injection de commandes

Audit et méthode EBIOS

- Maîtriser les notions de base relatives à la sécurité
- Connaître les objectifs de la sécurité et les mécanismes à mettre en place pour assurer la sécurité des systèmes d'information
- Connaître les notions de base relatives à l'audit informatique
- Sources de vulnérabilité des systèmes informatiques
- Types des menaces
- Origines et types des attaques
- Les effets d'une attaque
- Politique de sécurité
- Méthode EBIOS

Programmation en Python

- Langage Python 3, l'essentiel
- Les conditions dans Python
- Les boucles
- Les fonctions
- Programmation orientée système
- Création d'un programme qui calcule les hash
- Création de LS sous Python

Inforensic

- Les différents types de Forensic
- Modèles d'investigation
- Démarrage d'une enquête
- Collecte de données

- Images système
- Forensic de fichiers
- La base de registre
- Collecte de données
- Dump
- Le rapport

Sécurité sous Android

- Présentation du système d'exploitation Android
- Configuration de la plateforme de Pentesting
- Haking Android avec APK
- Forensic Android
- Les droits sous Android

Security Information and Event Management (SIEM)

- Définition du SIEM
- Avantages d'une solution SIEM
- Surveiller les données
- Splunk et sécurité
- Récolte de log avec Splunk
- Export des logs
  - Windows
  - Linux
- Analyse des logs
- Intégration de Splunk avec un pare-feu

Rétro-ingénierie des logiciels malfaisants

- Reconnaître un malware
- Préparation du lab
- Live Analyse
- Analyse statique
- Analyse dynamique - Analyse réseaux
- Analyse processus - Analyse de registre
- Trouver, isoler et éliminer
- Rétro-ingénierie

Inforensic réseaux et Wireshark

- Eléments clés de Wireshark et flux de trafic
- Personnaliser les vues et les paramètres de Wireshark
- Filtres de capture et d'affichage
- Colorer et exporter les paquets
- Réassembler le trafic
- Outils en ligne de commande

Analyse des métiers du commanditaire et évaluation globale de la vulnérabilité de son système d'information

- Sélection d'une méthodologie d'évaluation du risque
- Identification des risques liés aux métiers du commanditaire impactant le système d'information
- Elaboration de la liste des incidents redoutés et des impacts associés
- Elaboration d'une échelle de gravité des incidents redoutés
- Analyse de l'architecture réseau
- Analyse des protocoles de sécurité en place
- Elaboration de la liste des incidents redoutés et des impacts associés
- Elaboration d'une échelle de gravité des incidents redoutés

Elaboration et mise en oeuvre d'une stratégie de collecte d'évènements en provenance du système d'information du commanditaire

- Sélection des sources de collecte de données, des collecteurs et des événements à collecter
- Identification des règles de filtre
- Elaboration des méthodes de collecte (protocoles, applications, propriétés de sécurité...) et des fréquences de collecte
- Définition des règles de stockage des événements collectés : durée, quantité... dans le respect des lois / réglementations
- Installation et configuration de sondes dédiées
- Programmation de la collecte des évènements en provenance des équipements réseau identifiés
- Stockage des événements collectés
- Détection d'incidents

Elaboration et mise en oeuvre d'une stratégie de veille technologique pour renforcer la gestion des risques

- Sélection des sources d'information pertinentes
- Rédaction d'un état de l'art en français et anglais
- Collecte des données / informations liées à la cybersécurité en général et aux nouvelles vulnérabilités découvertes en particulier

Passage de la certification

Modalités d'obtention de la certification "Réaliser des tests d'intrusion (Sécurité Pentesting)"

- Le prix et le passage de la certification sont inclus dans ce parcours
- Une mise en situation professionnelle se déroulera sur 4h, à partir d'un besoin exprimé ou généré
- Après cette dernière, le candidat présentera un rapport au jury qu'il défendra à l'oral durant un temps maximum d'1h30 (en détaillant la méthode, les outils choisis ainsi que les contre-mesures adéquates vis-à-vis des menaces et vulnérabilités identifiées lors de son pentest)
- Une grille d'évaluation est complétée par le jury avec un score minimal de 70/100 pour la validation de l'ensemble des compétences de la certification

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités d’évaluation des acquis

- Au cours du parcours de formation, par des études de cas et/ou des travaux pratiques
- En fin de parcours de formation, par le passage de la certification "Réaliser des tests d'intrusion (Sécurité Pentesting)", pour laquelle le jury de certification sera composé de deux personnes minimum, dont au moins deux professionnels experts en sécurité, avec une expérience avérée de 2 ans
- La certification se compose d'une réalisation d'un mini projet dans le cadre d'une étude de cas et d'une mise en situation professionnelle où il faudra sélectionner les outils et exploiter les différentes vulnérabilités pour effectuer un test d'intrusion
- L'examen final permettant de valider la certification se fera sur l'un de nos 4 sites (Paris, Lille, Lyon, Bordeaux) ou à distance.

Les + de la formation

Toutes nos formations sont accessibles aux personnes en situation de handicap.

Métiers accessibles après la formation* : administrateur sécurité, technicien sécurité, spécialisation gestion de crise sécurité, consultant sécurité organisationnelle, évaluateur sécurité, analyste cybersécurité

* Liste non-exhaustive

Passerelles et poursuite d'études possibles** : expert en sécurité des sytèmes d'information ou en cybersécurité, architecte sécurité, spécialiste en développement sécurité

** La formation vise l'insertion directe en emploi. Une poursuite de parcours peut néanmoins être envisageable avec les exemples indiqués

Accessibilité de la formation

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Les détails de l'accueil des personnes en situation de handicap sont consultables sur la page Accueil et Handicap.

Modalités et délais d’accès à la formation

Les formations M2i sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.