Analyste Cybersécurité

Inscrit au répertoire spécifique des certifications professionnelles

Code RS : 6092
Code CPF : 235779
Code Certif Info : N°114031

CYBER

diplome.m2iformation.fr

Le métier d'Analyste Cybersécurité

L'Analyste Cybersécurité aide à protéger une organisation en utilisant une gamme de technologies et de processus pour prévenir, détecter et gérer les cybermenaces. Il(Elle) est en mesure de mener des audits de sécurité et de détecter des failles et des faiblesses dans le système d'information de l'entreprise. Il(Elle) fait une synthèse des résultats, est capable de mettre des solutions en place, d'organiser l'entreprise autour de ses préconisations à condition d'avoir défendu son projet devant la Direction.

L'Analyste Cybersécurité est chargé de mettre en place des protections et d'assurer la surveillance des systèmes informatiques.

Il(Elle) maîtrise :

+ L'organisation des entreprises du point de vue sécurité informatique
+ La construction de plans d'affaires visant à organiser la sécurité informatique dans l'entreprise
+ La présentation orale de son expertise auprès des décideurs
+ La rédaction d'un plan d'action et la présentation de son rapport de fin de mission
+ Les évolutions réglementaires et techniques de son domaine ; assurer les relations avec les acteurs de son secteur d'activité autour de la cybersécurité

Le dispositif de formation

Public concerné

Toute personne en reconversion professionnelle ou souhaitant monter en compétences. Niveau BAC+2 en informatique (réseaux, systèmes...) et une expérience professionnelle en milieu informatique (TSSR, Développeur) souhaités.

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

Métier visés / Passerelles et poursuite d'études

Métiers accessibles*

+ Administrateur(trice) Sécurité
+ Technicien(ne) Sécurité
+ Spécialisation Gestion de crise sécurité
+ Consultant(e) Sécurité organisationnelle
+ Evaluateur(trice) Sécurité
+ Analyste Cybersécurité

Passerelles et poursuite d'études possibles**

Expert en sécurité des systèmes d'information ou en cybersécurité
Architecte sécurité
Spécialiste en développement sécurité

* Liste non-exhaustive
** La formation vise l'insertion directe en emploi. Une poursuite de parcours peut néanmoins être envisageable avec des exemples indiqués.

Prérequis et modalités d'accès

Connaissances générales en maintenance, support, système, réseau. Notions en sécurité informatique souhaitées.

Entrée en formation soumise à :

+ Entretien(s) avec un(e) Conseiller(e) Formation visant à démontrer la cohérence du projet professionnel en adéquation avec la formation visée
+ Positionnement via une plateforme de test
+ 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).

Méthodes mobilisées

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 longduparcours, comme en présentiel
+ Modalités : théorie, pratique, travaux de groupes, individuels, réalisation de projets

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
+ Être muni d'un casque audio/micro
+ PC/MAC i5, SSD, 16 Go de RAM
+ Configuration nécessaire pour travailler sur des environnements virtualisés

Pédagogie

Un 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 collectif et individuels (espaces d'échanges et de partage en ligne, salles virtuelles, supports de cours, TP, exercices)

Le dispositif de formation
(suite)

Modalités d'évaluation

+ Evaluation des acquis tout au long du parcours, tests d'acquisition des savoirs et mesures des savoir-faire lors de situations de mise en application pratique (TPs, exercices, projets)
+ Fin de formation : attestation de fin de formation
+ Projet professionnel : à partir d'un cas d'entreprise réelle ou fictive, le/la candidat(e) doit produire une liste d'incidents redoutés et développer une stratégie de collecte d'événements correspondante
+ Mise en situation professionnelle : sous la forme d'une mise en situation professionnelle, le/la candidat(e) doit programmer des règles imposées de collecte des événements

La Certification

« Réaliser des tests d'intrusion (Sécurité Pentesting) » Certification déposée au Répertoire Spécifique des certifications professionnelles de France Compétence (RS6092).

Les compétences constituant la certification visent à exercer les activités suivantes :

+ 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.

L'examen final permettant de valider la certification professionnelle se fera sur l'un de nos sites avec :

1. Réalisation d'un mini projet dans le cadre d'une étude de cas.
2. Mise en situation professionnelle : sélectionner les outils et exploiter les différentes vulnérabilités pour effectuer un test d'intrusion.

TARIF & FINANCEMENT

Tarif
Taux horaire de 16€ TTC.
Demandeurs d'emploi ou financement personnel :
Tarifs spécifiques à consulter auprès du centre concerné pour un accompagnement personnalisé.

Financement
Quel que soit votre statut (salarié du secteur privé ou public, demandeur d'emploi...), des dispositifs de financement vous aident à réaliser votre projet de formation.

Toutes nos formations sont éligibles au CPF.

Descriptif des activités de la certification

Inforensic

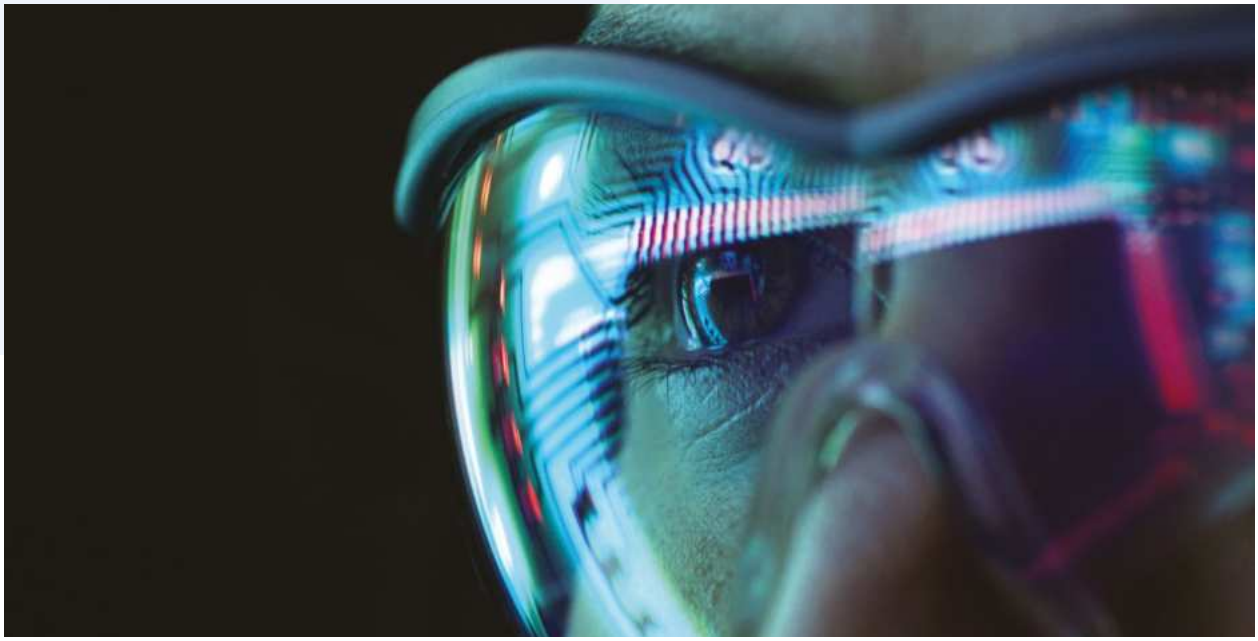
+ Application d'une démarche de sécurisation suivant une méthodologie
+ Sécurisation d'un système d'information

Pentesting

+ Utilisation des méthodologies d'hacking
+ Application des tests d'intrusion

Surveiller un système d'information sur des critères de sécurité informatique

+ Évaluer la criticité des risques liés aux métiers du commanditaire sur le système d'information en exploitant des méthodologies d'identification et de classification des risques
+ Analyser l'architecture d'un système d'information et des protocoles de sécurité du commanditaire à l'aide de la documentation existante afin d'évaluer les risques de sécurité potentiels et leurs impacts éventuels
+ Élaborer une stratégie de collecte d'événement provenant d'un système d'information comprenant la collecte, le stockage, les règles de filtres et l'exploitation des données dans le respect des lois et réglementations en vigueur
+ Programmer les règles de filtre du collecteur permettant la collecte des évènements à surveiller de manière à alimenter l'application de détection des incidents
+ Concevoir un système de veille technologique permettant de collecter, classifier, analyser et diffuser l'information liés à la cybersécurité aux différents acteurs de l'organisation/du commanditaire afin d'améliorer la sécurité du SI du commanditaire



Contenu de la formation

1. 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 pare-feu ASA
+ Chiffrement symétrique et asymétrique

2. 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

3. Sécurité Mobile

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

4. 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

5. VPN

+ Les fondamentaux du VPN
+ Présentation et mise en œuvre d'un VPN PPTP
+ Présentation d'un VPN L2TP
+ Principe du protocole ipsec et mise en œuvre
+ Principe des protocoles SSL/TLS

6. Mise en œuvre PKI

+ Cryptographie
+ Type de chiffrement
+ Certificats, Clés publique / 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

7. Techniques de Hacking

+ Veille sécurité informatique
+ Organisation de la SSI
+ Normes et référentiels
+ Aspects juridiques
+ Les techniques de hacking & contremesures
+ 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

8. 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

9. Audit et Méthode EBIOS

+ Maîtriser les notions de base relatives à la sécurité
+ Connaitre les objectifs de la sécurité et les mécanismes à mettre en place pour assurer la sécurité des systèmes d'information
+ Connaitre 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

Contenu de la formation

10. Programmation en Python

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

11. Inforensic

+ Les différents types de Forensic
+ Modèles d'investigation
+ Démarrage d'une enquête
+ Collecte de données
+ Images système
+ Forensics de fichiers
+ La base de registre
+ Collecte de données
+ Dump
+ Le rapport

12. Sécurité sous Android

+ Présentation du système d'exploitation Android
+ Configuration de la plate-forme de Pentesting
+ Haking Android avec APK
+ Forensic Android
+ Les Droits sous Android

13. Security Information and Event Management (SIEM)

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

14. 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
+ Retro-ingénierie

15. Inforensic réseaux et Wireshak

+ Éléments 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

16. 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
+ Élaboration de la liste des incidents redoutés et des impacts associés
+ Élaboration d'une échelle de gravité des incidents redoutés
+ Analyse de l'architecture réseau
+ Analyse des protocoles de sécurité en place
+ Élaboration de la liste des incidents redoutés et des impacts associés
+ Élaboration d'une échelle de gravité des incidents redoutés

17. Élaboration et mise en œuvre 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
+ Élaboration des méthodes de collecte (protocoles, applications, propriétés de sécurité, etc.) 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 identifiées
+ Stockage des événements collectés
+ Détection d'incidents

18. Élaboration et mise en œuvre 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

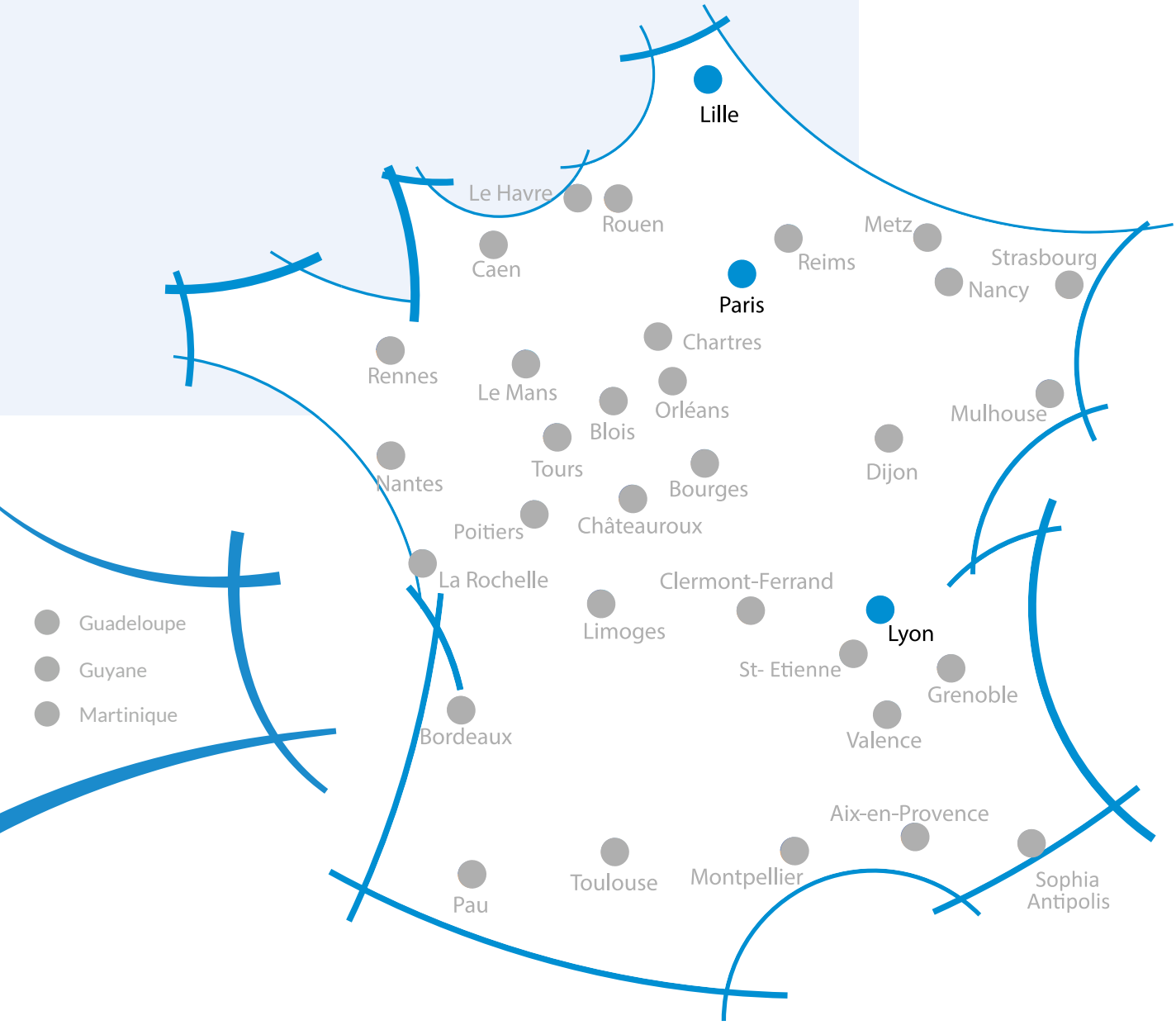
Modalités d'obtention des Certifications

A l'issue d'un parcours continu de formation correspondant au certificat visé, le candidat est évalué sur la base des éléments suivants :

+ Projet professionnel : à partir d'un cas d'entreprise réelle ou fictive, le/la candidat(e) doit produire une liste d'incidents redoutés et développer une stratégie de collecte d'évènements correspondante.

+ Mise en situation professionnelle : sous la forme d'une mise en situation professionnelle, le/la candidat(e) doit programmer des règles imposées de collecte des évènements.

M2i, LEADER DE LA FORMATION
IT, DIGITAL ET MANAGEMENT EN FRANCE



Retrouvez tous les détails de notre offre sur **diplome.m2iformation.fr**

Tél. Paris : 01 44 53 36 30 - Tél. Lyon : 04 78 02 38 90 - Tél. Lille : 03 20 19 07 19