Devenir Analyste Cybersécurité

Document mis à jour le 25/11/2026

Dispositif de formation : **Parcours Métier Diplômants**
Durée de la formation : **700 heures**
Date de formation : **Du 7 septembre 2026 au 6 avril 2027**

Alors que les volumes de données et les équipements connectés sont l'objet d'une croissance exponentielle, la Cybersécurité est plus que jamais un enjeu stratégique, en lien étroit avec la performance économique des organisations.

Les analystes Cybersécurité sont rares et les entreprises n'hésitent plus à recruter ces compétences pour sécuriser leur patrimoine numérique.

Alliant expertise technique, rigueur et méthodologie, la formation diplômante Analyste Cybersécurité vous prépare aux métiers les plus demandés tels que Administrateur Sécurité, Spécialiste en Gestion de Crise ou Consultant en Sécurité Organisationnelle.

Attention : Cette formation nécessite des prérequis et des compétences techniques préalables.

Métiers visés / Passerelles et poursuites d'études

Métiers accessibles*

Administrateur Sécurité
Technicien Sécurité
Spécialiste Gestion de crise sécurité
Consultant Sécurité organisationnelle
Evaluateur Sécurité
Analyste Cybersécurité

Passerelles et poursuite d'études possibles**
Expert en sécurité des systèmes d'information ou en cyber sécurité
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.*

OBJECTIFS DE FORMATION

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

Certification professionnelle de « Réaliser des tests d'intrusion (Sécurité Pentesting) » inscrite au RS par France Compétences lors de la commission du 29/09/2022, sous le code RS7394, code NSF 326. Certification sous l'autorité et délivrée par M2i. Date d'échéance de l'enregistrement: 29/09/2025.

Elle s'adresse aux professionnels de la sécurité informatique et permet d'acquérir toutes les compétences indispensables pour effectuer des tests qui consistent à examiner tous les réseaux et les systèmes informatiques en simulant les actions d'un intrus potentiel à l'intérieur de leur environnement de travail : analyse des flux, analyse des espaces de stockage, analyse de sécurité spécifique au terminal utilisé.

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

- C.1.1 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.
- C.1.2 Appliquer une méthodologie de test d'intrusion claire et reproductible afin de pouvoir restituer des éléments comparables dans leurs approches.
- C.1.3 Concevoir et réaligner des outils d'intrusion dans l'objectif de répondre aux différents besoins d'un test d'intrusion.
- C.1.4 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.
- C.1.5 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.

EN SAVOIR PLUS

PRÉREQUIS

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

Entrée en formation soumise à :

- Entretien(s) avec un Conseiller 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).

PUBLIC CONCERNÉ ET FINANCEMENT

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.

COMPÉTENCES ET TECHNOLOGIES ABORDÉES

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

Surveillance SI sur des critères de sécurité :

- Analyse et évaluation globale de la vulnérabilité du système d'information
- Stratégie de collecte d'événements en provenance du système d'information
- Stratégie de veille technologique pour renforcer la gestion des risques

Technologies

INFORENSIC :

- Distribution orientée forensic (SIFT, CAINE)
- Script développé en Python
- Volatility
- NirSoft
- Suite Sysinternals

PENTESTING :

- Outils OWASP
- Nmap
- Metasploit
- Python
- Kali
- PowerShell Empire

ANALYSTE :

- L'analyse des métiers du commanditaire et l'évaluation globale de la vulnérabilité de son système d'information
- L'élaboration et la mise en œuvre d'une stratégie de collecte d'évènements en provenance du système d'information du commanditaire
- L'élaboration et la mise en œuvre d'une stratégie de veille technologique pour renforcer la gestion des risques

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants. Consultez-nous pour obtenir le programme détaillé, module par module.

DIPLÔME

Certification professionnelle de « Réaliser des tests d'intrusion (Sécurité Pentesting) » inscrite au RS par France Compétences lors de la commission du 29/09/2022, sous le code RS7394, code NSF 326.
Certification sous l'autorité et délivrée par M2i.
Date d'échéance de l'enregistrement : 29/09/2025.

62.50% des personnes ayant passé l'examen dans le cadre de leur formation M2i ont obtenu la certification ACS (16 candidats inscrits).*

**Taux moyen constaté sur les parcours ACS suivis chez M2i Formation Diplômante sur l'ensemble de nos centres sur la période 2023-2024.*
Réussite totale : le candidat a obtenu le titre complet. En détail, 62.50% en validation totale, 0% en validation partielle et 37.50% en refus.

Les indicateurs de résultats chiffrés sur le niveau de performance et d'accomplissement des prestations, selon la nature des prestations et des publics accueillis, sont disponibles à la demande.
Taux de retour à l'emploi : 62.50%*
Taux de retour à l'emploi dans le métier ACS : 80%*
Taux de poursuite des études : le nombre de répondant à cette question n'est pas suffisant pour permettre une publication significative.
**Taux calculé sur la base de 8 répondants à 6 mois post-formation.*

LES PLUS DE M2I

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).

MODALITÉS, MOYENS ET MÉTHODES PÉDAGOGIQUES

Formation en distanciel synchrone (classe virtuelle en temps réel)

- 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

Prérequis techniques fortement conseillés pour suivre cette formation à distance

- Connexion internet « Haut débit », 15 mégabits par seconde minimum
- Fibre non obligatoire
- Être muni d'un casque audio/micro
- PC/MAC i7, SSD, 32 Go de RAM.
  Configuration nécessaire pour travailler sur des environnements virtualisés

FINANCEMENT

Tarif :
Taux horaire de 16 euros TTC (soit 11200 euros*).
Demandeurs d'emploi ou financement personnel :
Tarifs spécifiques à consulter auprès du centre concerné pour un accompagnement personnalisé.

**Coût total calculé selon le nombre d'heures théoriques référencé sur le planning de la formation.*

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.

MODALITÉS D'ACCÈS

Nos équipes accorderont toute leur attention au traitement de votre candidature et s'engagent à vous faire un premier retour dans un délai de 7 jours.

ADMISSION

- Dossier de candidature
- Test de vérification des prérequis
- Entretien
- Validation et éligibilité France Travail (dans le cas de certains dispositifs)

Le groupe M2I s'engage pour faciliter l'accessibilité de ses formations. Les détails de l'accueil des personnes en situation en handicap sont consultables sur la page Politique Handicap.

POURQUOI CHOISIR M2I ?

- Un apprentissage métier proactif axé sur l'emploi et basé sur le faire avec l'accompagnement de nos formateurs tout au long du parcours.
- Un accès à des experts : bénéficiez de l'expertise de nos formateurs.
- En présentiel ou à distance : 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 si en présentiel ou à distance, supports de cours, TP, exercices).

MODALITÉS D'ÉVALUATION

Certification professionnelle de « Réaliser des tests d'intrusion (Sécurité Pentesting) » inscrite au RS par France Compétences lors de la commission du 29/09/2022, sous le code RS7394, code NSF 326. Certification sous l'autorité et délivrée par M2i. Date d'échéance de l'enregistrement: 29/09/2025.

Mise en situation professionnelle en temps limité et d'une durée de 4h à partir d'un besoin exprimé ou généré.

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

Après l'étude de cas de 4h le candidat présentera un rapport au jury qu'il défendra à l'oral durant un temps maximum de 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.

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.

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

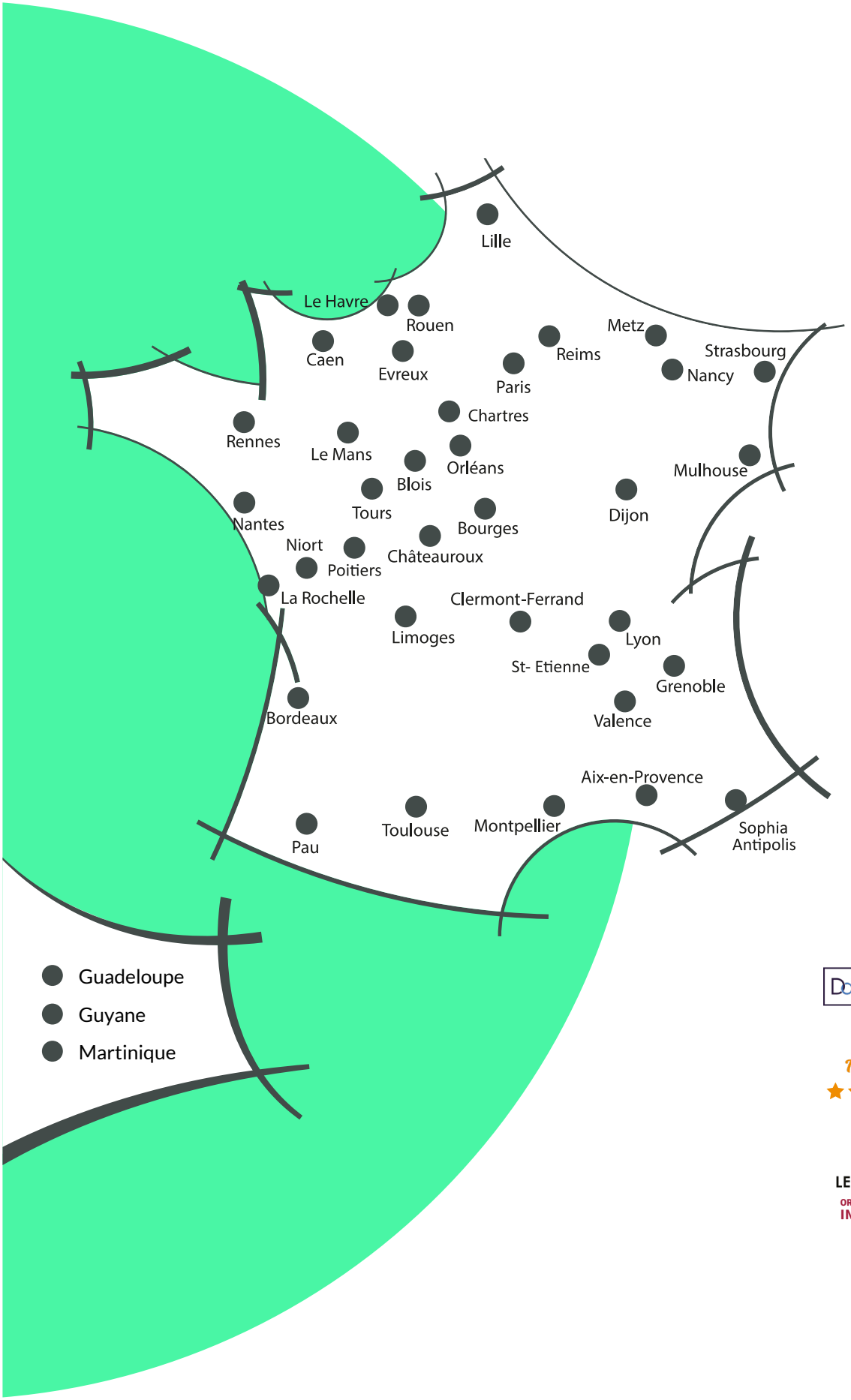
du consentement légal
– Appliquer une méthodologie de test d'intrusion claire et reproductible afin de pouvoir restituer des éléments comparables dans leurs approches
– Concevoir et réaligner des outils d'intrusion dans l'objectif de répondre aux différents besoins d'un test d'intrusion
– Identifier 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 avec :

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

MaCarrière

m2i Formation



Datadock

Avis Vérifiés 4,6/5

LEADERS LEAGUE
ORGANISME DE FORMATION INCONTOURNABLE

© Ma Carrière M2i Formation - Crédits photos : Getty Images - Document non contractuel - Les informations contenues dans ce document peuvent être modifiées sans préavis - NE PAS JETER SUR LA VOIE PUBLIQUE