Devenir Spécialiste en Cybersécurité

En partenariat avec :

Document mis à jour le 16/09/2025

Dispositif de formation :	**Programme Régional de Formation (PRF)**
Date de formation :	**Du 29 avril au 6 octobre 2025**
Période de stage :	**Du 8 septembre au 3 octobre 2025**
Lieu(x) de formation :	**Orléans**
Réunion d'Information :	**Le 11 mars 2025 ou le 25 mars 2025**
Date limite d'envoi de candidature :	**Le 20 avril 2025**

M2I Scribtel en partenariat avec la Région Centre Val de Loire et France Travail dans le cadre du Plan Régional de Formation, recherche pour avril 2025 des demandeurs d'emploi souhaitant se spécialiser en Cybersécurité.

Cursus à temps plein en présentiel du 29 avril 2025 au 06 octobre 2025.

Formation indemnisée / rémunérée selon profil.

Formation avec période der stage en entreprise (544 heures en centre de formation et 140 heures en entreprise) avec à l'issue le passage de la certification Pentester (soutenance) et l'examen de validation Inforensic.

L'examen de validation « Réaliser une investigation numérique (Sécurité Inforensic) » s'adresse aux professionnels de la sécurité informatique et permet d'acquérir les compétences pour identifier et évaluer l'ensemble des méthodes de rétrospection faisant suite à une menace de sécurité, afin de préconiser les mesures d'urgence pour en limiter la propagation. Le stagiaire pourra ainsi collecter et analyser l'information se trouvant dans un programme informatique pour retrouver les traces des activités d'utilisateurs et prouver un délit numérique.

La certification « Réaliser des tests d'intrusion (Sécurité Pentesting) » 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 stockages, analyse de sécurité spécifique au terminal utilisé.

Réunions d'Information Collective sur inscription les 11 et 25 mars 2025 de 9h30 à 12h00 en distanciel.

OBJECTIFS DE FORMATION

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

– Utiliser des méthodologies d'investigations numériques dans l'objectif d'un recours judiciaire futur en s'appuyant sur les éléments recueillis
– Mener une investigation numérique au sein d'un système d'information afin d'en identifier les différentes traces laissées par un attaquant
– Analyser les traces recueillies dans l'objectif de pouvoir recréer le scénario d'attaque initial en identifiant l'origine potentiel de celui-ci
– 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

PRÉREQUIS

– 16 ans et plus
– Inscrit ou en cours d'inscription auprès de France Travail
– Bonne compréhension de la langue française (lu - écrit - parlé)
– Bon niveau d'anglais
– Spécialiste en sécurité informatique, systèmes, réseaux et infrastructure globale
– Avoir une appétence pour les différents systèmes d'exploitation et une compréhension globale de la sécurité informatique et les infrastructures SI
– Parcours en en systèmes et réseaux et/ou programmation recommandée
– Expérience en systèmes et réseaux et/ou programmation recommandée

PUBLIC CONCERNÉ ET FINANCEMENT

Cette formation financée à 100%* est à destination des demandeur·se·s d'emploi inscrit·e·s à France Travail en Région Centre-Val-de-Loire.

COMPÉTENCES ET TECHNOLOGIES ABORDÉES

Module	Durée (en heures)
Voyage dans le Cyber espace	21
Python par la pratique	35
Techniques de hacking	35
Tests d'intrusion en python	28
Investigation numérique - Computer Forensics	56
Durcissement Windows	28
Durcissement Linux	28
Durcissement réseau	21
Analyse de risques- EBIOS	21
SOC et SIEM	35
Les essentiels de Splunk	35
Modules transverses (remise à niveau, communication, anglais professionnel, gestion du temps, égalité F-H, laïcité, sexisme & harcèlement, transition énergétique et écologique, usage des IA génératives, ateliers TRE, savoir transmettre...), visite d'entreprises partenaires, mentorat, révisions, examens, entretiens individuels, bilans...	201
Stage en entreprise	140

Programme donné à titre indicatif et pouvant évoluer.

DIPLÔME

Certification M2i "Réaliser des tests d'intrusion (Sécurité Pentesting)" RS6092.

À PROPOS DES CERTIFICATIONS

Certification M2i "Réaliser des tests d'intrusion (Sécurité Pentesting)" enregistrée au répertoire spécifique de France Compétences sous le numéro RS6092 le 29/09/2022.

Objectifs et contexte de la certification :

La certification « Réaliser des tests d'intrusion (Sécurité Pentesting) » 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 stockages, analyse de sécurité spécifique au terminal utilisé.

Compétences attestées :

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.

LES PLUS DE M2I FORMATION

Microsoft Teams Education, un outil de suivi et d'animation en présentiel et à distance :

- Espace de stockage collaboratif pour accéder aux différents supports de cours et cahiers d'exercices
- Fonctionnalités pour gérer des sessions à distance

La playlist e-learning : tous les apprenants ont accès avant, pendant et après le cursus à notre plateforme e-learning M2i Learning pour :

- Acquérir les connaissances prérequises avant de démarrer (sous condition de l'existence des modules pour combler les lacunes)
- Utiliser les modules conseillés par les formateurs pour faire de l'ancrage mémoriel sur des sujets abordés pendant la formation
- Revenir sur un sujet après la formation pour continuer à s'auto-former

MODALITÉS, MOYENS ET MÉTHODES PÉDAGOGIQUES

Formation délivrée en présentiel.

Le formateur alterne entre des méthodes démonstratives et actives (via des travaux pratiques et/ou des mises en situation).
La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.

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 Accueil PSH.

POURQUOI CHOISIR M2I FORMATION ?

– 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).

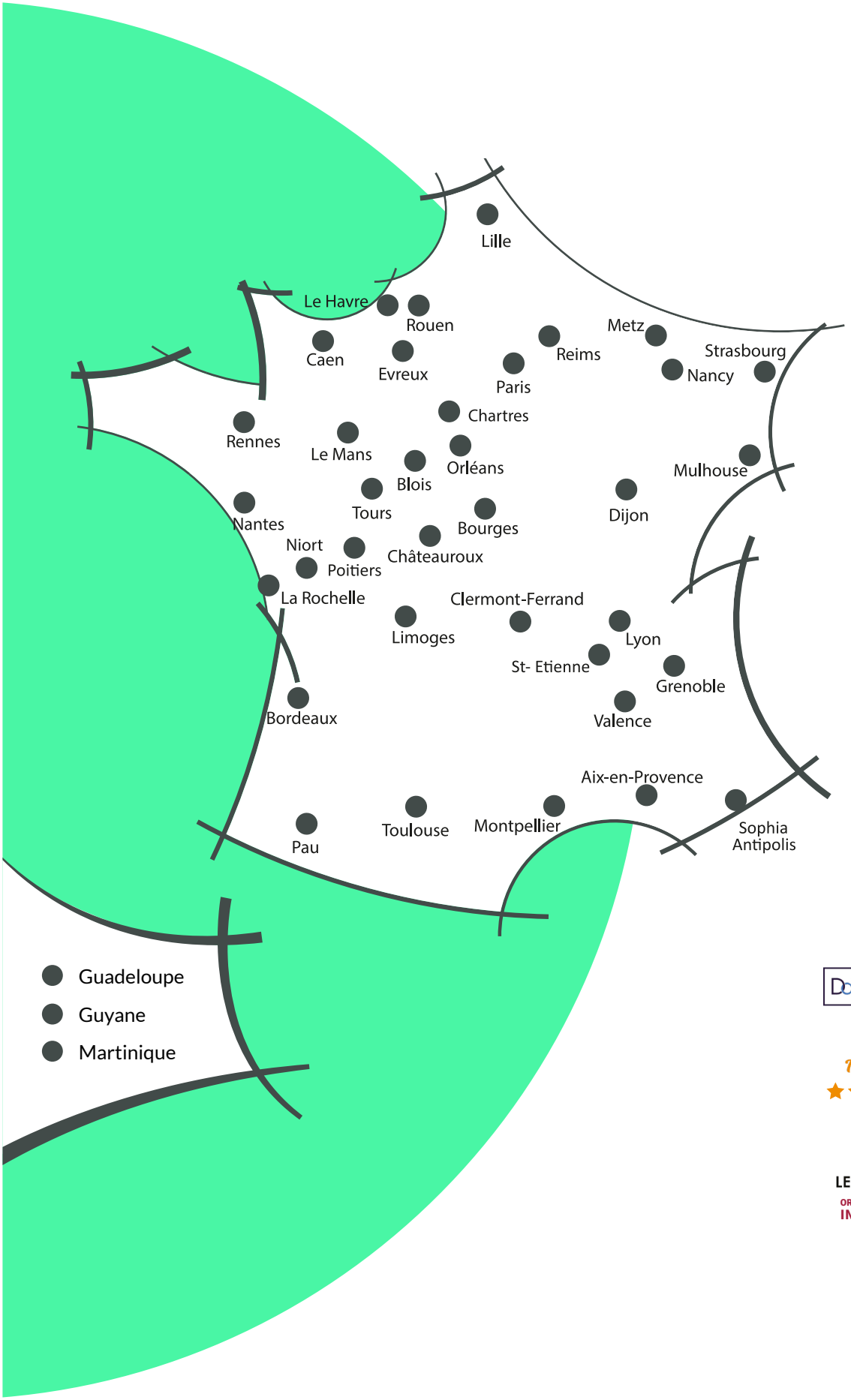
MODALITÉS D'ÉVALUATION

Exemples de validation des acquis de formation :

– Travaux dirigés dans chaque module
– Mise en situation via des cas pratiques et un mini projet
– Certification (si prévue dans le programme de formation)
– Soutenance devant un jury de 30 à 40 min

MaCarrière

m2i Formation



Datadock

Avis Vérifiés 4,6/5

LEADERS LEAGUE
ORGANISME DE FORMATION INCONTOURNABLE