Cyberini

Cybersécurité et Hacking éthique

PROGRAMME DE FORMATION

Date de création du document :
28/09/2021 (modifié le 28/11/2022 – v7).

https://cyberini.com

FAITES CERTIFIER VOS COMPÉTENCES EN CYBERSÉCURITÉ

6 MODULES

20H* SOUS 30 JOURS

100% EN LIGNE

NIVEAU DÉBUTANT

Bénéficiez d'un accès illimité à la plateforme et d'un apprentissage 100% en ligne à votre rythme.

* : Durée minimale à passer en ligne pour valider administrativement la formation. Avec les missions et la pratique les stagiaires passent 35h en moyenne. Accès sans limite de temps après les 30 jours initiaux.

OBJECTIFS PÉDAGOGIQUES

- Savoir réagir en cas de cyberattaque en milieu professionnel.
- Sécuriser des systèmes informatiques clients et adopter les bons réflexes.

PRÉREQUIS

- Avoir une connexion à Internet
- Webcam et micro pour l'examen.

CYBERSÉCURITÉ & HACKING ÉTHIQUE

Cette formation certifiante répond aux réalités métiers pour améliorer l'employabilité du candidat. Quelle que soit votre situation professionnelle ou votre âge, Cyberini© vous permet d'acquérir des compétences prisées dans le monde de la cybersécurité. La formation est basée sur des référentiels reconnus (ANSSI) et le support personnalisé est inclus. Elle vous permet aussi d'apprendre à créer votre activité en tant qu'indépendant(e) dans le domaine.

PUBLIC CONCERNÉ

Personnel en reconversion, salarié, indépendant, demandeur d'emploi.

SUIVI D'APPRÉCIATION

Le candidat recevra un questionnaire de satisfaction en fin de formation.

FORMATEUR

Michel KARTNER, formateur cybersécurité depuis 2013, diplômé d'un master en réseaux informatiques.

TARIFS & LIEN

1500€ TTC par personne.
Accéder à la formation.

LIEU DE FORMATION

100% en ligne avec un compte sur https://cyberini.com
Format **FOAD** collectif (e-learning) asynchrone (le stagiaire étudie à son rythme en accès illimité).

DATES ET DURÉE

20h pendant une session de 30 jours consécutifs. Dates à sélectionner sur la page d'inscription. Accès sans limite de temps et 24/7. Ensuite, 3 mois pour passer l'examen en ligne (durée 1h).

La formation inclut un droit de passage à l'examen de certification en ligne « **TOSA CyberCitizen** »

Proposée en partenariat avec Isograd SAS

TAUX D'OBTENTION DE LA CERTIFICATION : N/A
VALIDATION DE BLOCS DE COMPETENCES : N/A
ÉQUIVALENCE ET PASSERELLES : N/A
SUITE DE PARCOURS : N/A


TOSA

CERTIFICATION
Tosa CyberCitizen

Nous soussignés, Marc Alpérovitch Président de la société Isograd, éditeur du Tosa et Clément Hammel, Responsable pédagogique, certifions que :

Prénom NOM

a passé la Certification Tosa CyberCitizen, le 19 novembre 2021 via le centre de passage Cyberini et a obtenu le score de 883/1000 points correspondant à un niveau Expert.

CLÉMENT HAMMEL
RESPONSABLE PÉDAGOGIQUE

MARC ALPÉROVITCH
LE PRÉSIDENT

MODALITÉS DE FORMATION

MÉTHODES PÉDAGOGIQUES

Vidéos, mises en pratique (exercices, simulations et missions).

MODALITÉS D'ÉVALUATION

Une évaluation diagnostic est réalisée en début de formation. L'acquisition ou l'amélioration de compétences sont évaluées à travers des QCM de fin de module, et en fin de formation.

MODALITÉS ET DÉLAIS D'ACCÈS

Le délai d'accès varie entre 11 et 30 jours selon situation.

MOYENS TECHNIQUES

Un compte Cyberini permettra au stagiaire de suivre la formation dans son intégralité. Supports de formation inclus.

CONTACT ET ASSISTANCE TECHNIQUE

Le formateur Michel KARTNER est joignable par e-mail à l'adresse support@cyberini.com ou sur https://cyberini.com/contact durant toute la durée de la formation et cela du lundi au vendredi 9h – 16h hors jours fériés et congés.
Délai de réponse : 48h.

Accessibilité aux personnes en situation de handicap

Si vous êtes en situation de handicap, merci de nous le préciser en nous contactant avant votre entrée en formation. Nous nous assurons de l'adéquation du dispositif de formation à travers un questionnaire. Pour cela, nous pouvons également nous appuyer sur un réseau de partenaires nationaux préalablement identifiés.

PLAN DE FORMATION

MODULE 1 : CYBERSÉCURITÉ – CONTEXTE, ENJEUX ET ACTEURS

Évaluez vos compétences avant de commencer
Faisons connaissance ! Rencontrez les autres étudiants
CHAPITRE 1 : Le "Hacking" de 1960 à Maintenant
CHAPITRE 2 : Hacking éthique : modéliser l'attaque
CHAPITRE 3 : Comprendre la Cyber kill chain
CHAPITRE 4 : Maîtriser la Défense en profondeur
CHAPITRE 5 : Critères fondamentaux de la Cybersécurité
CHAPITRE 6 : Guerre de l'information et cyber stratégies
CHAPITRE 7 : Classifier les Cyberattaques
CHAPITRE 8 : Gérer et Traiter des cyber risques
CHAPITRE 9 : Reconnaître les acteurs pour Détecter et Gérer des incidents cybersécurité
CHAPITRE 10 : 6 étapes pour élaborer un plan de reprise d'activité
CHAPITRE 11 : Renseignement et investigation numérique
CHAPITRE 12 : MISSION 1 : Renseignement
CHAPITRE 13 : Réponse à la mission 1
CHAPITRE 14 : Connaître les Organisations françaises et européennes
CHAPITRE 15 : PROJET : Améliorez votre CV en participant à des événements
CHAPITRE 16 : Rôles et métiers de la cybersécurité
CHAPITRE 17 : Comprendre la méthode EBIOS Risk Manager
QCM MODULE 1

MODULE 2 : GOUVERNANCE ET MAÎTRISE DES SYSTÈMES

CHAPITRE 1 : Définir une stratégie de la Cybersécurité
CHAPITRE 2 : Piloter la Cybersécurité
CHAPITRE 3 : Définir une stratégie de communication sur la Cybersécurité
CHAPITRE 4 : Disposer des ressources humaines nécessaires
CHAPITRE 5 : Comprendre la gestion des permissions en pratique
CHAPITRE 6 : Inclure la Cybersécurité dans les contrats
CHAPITRE 7 : Connaître ses systèmes
CHAPITRE 8 : Maîtriser ses systèmes tout au long de leur cycle de vie

PLAN DE FORMATION (suite)

CHAPITRE 9 : Maîtriser les accès systèmes
CHAPITRE 10 : Utiliser des composants sécurisés
CHAPITRE 11 : Protéger physiquement ses systèmes d'information
CHAPITRE 12 : Protéger logiquement ses systèmes d'information
CHAPITRE 13 : MISSION 2 : Piloter la sécurité lors d'une transformation numérique
CHAPITRE 14 : Réponse à la mission 2
QCM MODULE 2

MODULE 3 : NORMES, RÉGLEMENTATIONS ET IMPACTS

CHAPITRE 1 : Comprendre la Suite ISO/IEC 27000
CHAPITRE 2 : Reconnaître les Standards industriels et Normes métiers
CHAPITRE 3 : 5 étapes pour mettre en place une Politique de sécurité
CHAPITRE 4 : Identifier les enjeux d'un Plan d'Assurance Sécurité
CHAPITRE 5 : Comprendre le RGPD
CHAPITRE 6 : Comprendre les Lois Cybersécurité en France
CHAPITRE 7 : Mener un test d'intrusion – théorie
CHAPITRE 8 : Mener un test d'intrusion – reconnaissance
CHAPITRE 9 : Mener un test d'intrusion – scanning
CHAPITRE 10 : Mener un test d'intrusion – accès
CHAPITRE 11 : Pratiquer avec les CTF
CHAPITRE 12 : Améliorez votre CV : Faites des Projets cybersécurité
CHAPITRE 13 : Comprendre les impacts de la cybercriminalité
CHAPITRE 14 : MISSION 3 : Test d'intrusion en pratique
C**HAPITRE 15** : Réponse à la mission 3
QCM MODULE 3

MODULE 4 : HYGIÈNE INFORMATIQUE DES UTILISATEURS

CHAPITRE 1 : Tous piratés, tous concernés
CHAPITRE 2 : Bien comprendre l'Ingénierie sociale
CHAPITRE 3 : Reconnaître des tentatives de Phishing
CHAPITRE 4 : Choisir et sécuriser ses mots de passe
CHAPITRE 5 : Faire une Veille efficace

PLAN DE FORMATION (suite)

CHAPITRE 6 : PROJET : mettez en place votre agrégateur d'actualité
CHAPITRE 7 : Reconnaître les Arnaques en entreprise
CHAPITRE 8 : Sauvegarder et chiffrer des fichiers dans le Cloud
CHAPITRE 9 : Protéger sa vie privée efficacement
CHAPITRE 10 : Bonnes pratiques et hygiène informatique en entreprise
CHAPITRE 11 : MISSION 4 : Peut-on Vous pirater ?
CHAPITRE 12 : Réponse à la mission 4
QCM MODULE 4

MODULE 5 : SÉCURITÉ AU BUREAU ET EN DÉPLACEMENT

CHAPITRE 1 : Comprendre le fonctionnement des logiciels malveillants
CHAPITRE 2 : Savoir réagir en cas de cyberattaque
CHAPITRE 3 : Sécuriser son Identité numérique et authentification
CHAPITRE 4 : Sécuriser les accès physiques
CHAPITRE 5 : Stocker des données sensibles
CHAPITRE 6 : Comprendre les failles de sécurité
CHAPITRE 7 : Sécuriser ses équipements mobiles
CHAPITRE 8 : Éviter les risques avec les réseaux sans fils (Wi-Fi)
CHAPITRE 9 : Comprendre les menaces des clés USB
CHAPITRE 10 : MISSION 5 : Investiguer après un piratage
CHAPITRE 11 : Réponse à la mission 5
CHAPITRE 12 : PROJET : Créer un aide-mémoire cybersécurité (cheat sheet)
CHAPITRE 13 : PROJET : Créer un Script de détection de sites malveillants
QCM MODULE 5

MODULE 6 : PERSPECTIVES ET EMPLOYABILITÉ

Évaluez vos compétences en fin de formation
CHAPITRE 1 : Tout savoir sur la certification et son intérêt
CHAPITRE 2 : Plan d'action à suivre pour amorcer votre carrière en cybersécurité
CHAPITRE 3 : Conseils personnalisés sur votre CV
CHAPITRE 4 : Conseils généraux pour améliorer votre attractivité/employabilité
CHAPITRE 5 : Comprendre les bénéfices d'un travail indépendant dans le domaine

PLAN DE FORMATION (suite)

CHAPITRE 6 : Trouver sa voie dans son activité professionnelle
CHAPITRE 7 : Comprendre les compétences d'un(e) chef(fe) d'entreprise
CHAPITRE 8 : Se déclarer micro-entrepreneur
CHAPITRE 9 : Comprendre le régime fiscal et social de la micro-entreprise
CHAPITRE 10 : Comprendre les aides financières dédiées à la création d'entreprise
CHAPITRE 11 : Connaître le marché, trouver ses clients et pérenniser son activité
CHAPITRE 12 : Merci d'avoir suivi cette formation
CHAPITRE 13 : Je vous recommande personnellement

Accéder à la formation

INÉDIT SUR CYBERINI :

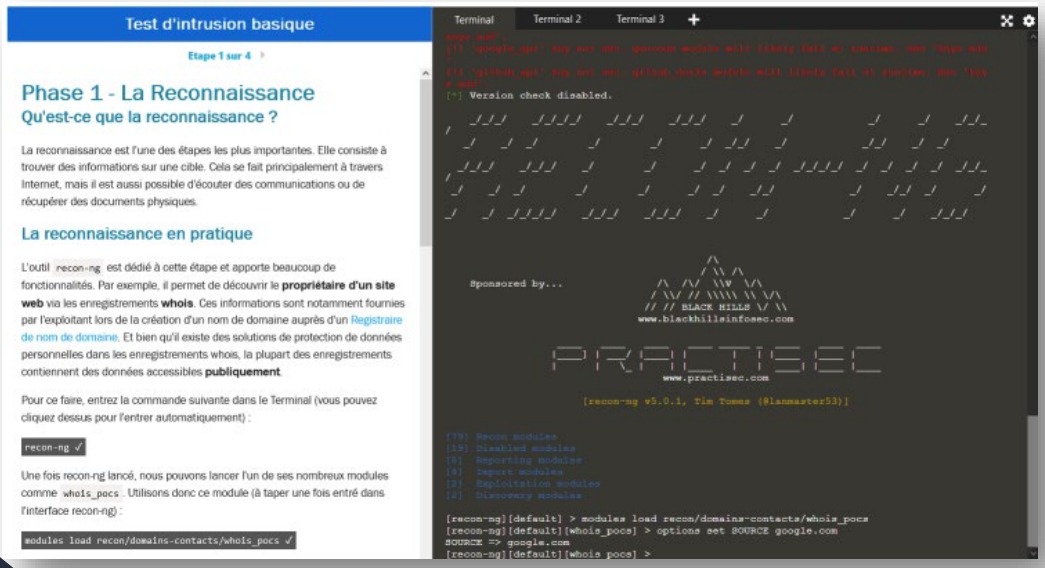
- Retrouvez de **nombreuses autres ressources et outils à télécharger + 70h de vidéos supplémentaires.**
- Apprenez grâce à un **environnement virtuel dédié** aux stagiaires en formation !
- **Accédez à vie** à tout le contenu + les mises à jour sans frais supplémentaires !

Programmation Python pour le Hacking

Malwares, Failles Web & Réseau

Ingénierie sociale, Linux, Anonymat, et bien d'autres...

Pratiquez sans rien installer ni risquer avec l'environnement virtuel !



CRITÈRES QUALITÉ

Cyberini© dispose d'une charte qualité avec **4 engagements** :

1. L'adaptation de la formation au stagiaire
2. L'application des compétences dans le monde réel
3. La satisfaction du client
4. L'amélioration continue

Cyberini© est un centre de formation spécialisé en Cybersécurité permettant à chacun d'apprendre et de monter en compétences à son rythme.

Cyberini est également **labellisé SecNum*edu*-FC** par **l'ANSSI**.

SecNumedu
Formation continue
ANSSI

TOSA® Centre Agréé

CYBERINI© SASU | 128 rue La Boétie, 75008 Paris
SIRET: 948 183 264 00019
Cyberini© est un organisme de formation enregistré sous le numéro 11756654075 auprès du préfet de région d'Ile-de-France
Avis et interviews d'anciens candidats.

DÉROULEMENT DE VOTRE FORMATION

1. Après son inscription, le stagiaire devra rejoindre la formation **en ligne obligatoirement le 1er jour** (au moins 15 secondes) pour signaler son entrée en formation. **Il suffit de se connecter à son compte Cyberini pour cela**.

2. Il peut ensuite **suivre la formation à son rythme tant qu'il passe au moins 20h pendant la période choisie**. Ces conditions sont administratives pour valider le dossier. Le stagiaire bénéficiant ensuite d'un accès **illimité** à la formation. Il pourra donc y revenir à souhait.

3. Durant la formation, le stagiaire sera amené à télécharger des ressources complémentaires, à passer des QCM en cours de formation, ainsi qu'une évaluation finale de formation pour mesurer son acquisition de compétences.

4. La fin de la formation donne un droit de passage à l'examen de certification « **TOSA Cybercitizen** ». Elle donne également un accès à **+70h de cours vidéo supplémentaires sur le Hacking éthique** dont les objectifs sont les suivants :

- Apprendre toutes les bases de la cybersécurité (sécurité offensive).
- Amorcer une carrière informatique ou une reconversion professionnelle.
- Savoir comment se passent les piratages et comment les éviter (web, système et réseau).
- Acquérir des compétences rares et prisées par les entreprises.
- Mettre en place des laboratoires de test personnels pour pratiquer sans risque.
- Maîtriser les bases de Kali Linux

Notez la date

Il faudra suivre la formation pendant les dates choisies. Notez-les dans votre calendrier !

QUODAGIS Digital Security

SPIE

acelys Services Numériques

Des entreprises recrutent les stagiaires formés.
*Et si c'était **votre** tour ?*

100% : C'est le taux de réussite aux examens de certification visé après la formation Cyberini. Ce parcours de formation vous permet de démontrer officiellement de solides compétences sur votre CV !

Cyberini

CONTACT

Cyberini© SASU
128 rue la Boétie, 75008 Paris
SIRET : 948 183 264 00019

+33 6 98 67 93 92

support@cyberini.com
https://cyberini.com/contact/

Cyberini© est un organisme de formation enregistré sous le numéro 11756654075 auprès du préfet de région d'Ile-de-France. Cet enregistrement ne vaut pas agrément de l'État.