

# Certificat

## Analyse et Développement de Malware



## Certificat

### Analyse et Développement de Malware

- » Modalité: en ligne
- » Durée: 6 semaines
- » Qualification: TECH Université Technologique
- » Horaire: à votre rythme
- » Examens: en ligne

Accès au site web: [www.techtitute.com/fr/informatique/cours/analyse-developpement-malware](http://www.techtitute.com/fr/informatique/cours/analyse-developpement-malware)

# Sommaire

01

Présentation

---

*page 4*

02

Objectifs

---

*page 8*

03

Direction de la formation

---

*page 12*

04

Structure et contenu

---

*page 16*

05

Méthodologie

---

*page 20*

06

Diplôme

---

*page 28*

# 01

# Présentation

Dans un environnement numérique où les actifs des entreprises dépendent de manière critique de la cybersécurité, la menace constante des logiciels malveillants représente un défi de taille. À cet égard, la prolifération des attaques malveillantes souligne l'urgence de disposer de professionnels hautement qualifiés dans ce domaine. En ce sens, le programme d'études répond au besoin impératif d'experts qui non seulement comprennent la complexité des menaces numériques, mais peuvent également concevoir des stratégies proactives pour leur détection et leur atténuation. Les diplômés apprendront les outils essentiels pour sauvegarder l'intégrité des systèmes dans un environnement commercial de plus en plus numérisé. Grâce à la flexibilité du mode 100% en ligne, ce cours garantit l'accessibilité et la mise à jour continue nécessaires pour faire face aux défis changeants du cyberspace.



“

*Devenez un expert en Malware avec des techniques d'analyse dynamique innovantes grâce à ce programme unique 100% en ligne"*

Dans le paysage actuel de la cybersécurité, la sophistication des cybermenaces a atteint des niveaux sans précédent, générant une demande croissante de professionnels spécialisés dans l'Analyse et Développement de Malware. L'évolution constante des tactiques malveillantes exige une réponse tout aussi dynamique de la part des experts en cybersécurité. Dans ce contexte, ce programme universitaire TECH apparaît comme une solution complète pour répondre à ces besoins. Conçu pour fournir aux étudiants des connaissances avancées, le programme va d'une compréhension approfondie de la nature des logiciels malveillants à l'évaluation des outils anti-malware. Cette approche globale prépare les professionnels à faire face aux menaces actuelles et futures.

Le programme d'analyse et de développement des logiciels malveillants de TECH constitue un solide recueil de connaissances couvrant les différentes dimensions du monde du malware. Les diplômés exploreront en profondeur les différentes formes et cibles des malwares, en acquérant des connaissances avancées sur leur nature, leur fonctionnalité et leur comportement. Le programme se penche sur l'analyse médico-légale appliquée aux logiciels malveillants, fournissant aux étudiants les compétences nécessaires pour identifier les indicateurs de compromission (IoC) et les modèles d'attaque, cruciaux pour la détection précoce et la réponse efficace aux incidents de sécurité. En outre, ce parcours met l'accent sur le développement de compétences spécifiques pour évaluer et sélectionner les outils de sécurité anti-malware. Les étudiants apprendront à discerner l'efficacité de ces outils et leur adaptabilité à des environnements particuliers, ce qui est essentiel pour mettre en œuvre des stratégies de défense efficaces.

Avec une approche innovante et adaptable, ce programme universitaire est une proposition de formation unique. Le mode 100% en ligne et la méthodologie *Relearning* garantissent une expérience éducative flexible et efficace, permettant aux professionnels de faire progresser leur carrière sans interruption et de s'adapter en permanence aux exigences changeantes du domaine de la cybersécurité.

Ce **Certificat en Analyse et Développement de Malware** contient le programme éducatif le plus complet et le plus actualisé du marché. Ses caractéristiques sont les suivantes:

- ♦ Le développement d'études de cas présentées par des experts en Analyse et Développement de Malware
- ♦ Le contenu graphique, schématique et éminemment pratique de l'ouvrage fournit des informations actualisées et pratiques sur les disciplines essentielles à la pratique professionnelle
- ♦ Exercices pratiques permettant de réaliser le processus d'auto-évaluation afin d'améliorer l'apprentissage
- ♦ Il met l'accent sur les méthodologies innovantes
- ♦ Cours théoriques, questions à l'expert, forums de discussion sur des sujets controversés et travail de réflexion individuel
- ♦ Il est possible d'accéder aux contenus depuis tout appareil fixe ou portable doté d'une connexion à internet



*Vous maîtriserez l'analyse des appels avec les API monkeys en seulement 6 semaines de la meilleure formation en ligne"*

“

*Vous apprendrez à générer du Shellcode dans l'université la mieux notée au monde par ses étudiants selon la plateforme Trustpilot (4.9/5)"*

Le corps enseignant du programme englobe des spécialistes réputés dans le domaine et qui apportent à ce programme l'expérience de leur travail, ainsi que des spécialistes reconnus dans de grandes sociétés et des universités prestigieuses.

Grâce à son contenu multimédia développé avec les dernières technologies éducatives, les spécialistes bénéficieront d'un apprentissage situé et contextuel, ainsi, ils se formeront dans un environnement simulé qui leur permettra d'apprendre en immersion et de s'entraîner dans des situations réelles.

La conception de ce programme est axée sur l'Apprentissage par les Problèmes, grâce auquel le professionnel doit essayer de résoudre les différentes situations de la pratique professionnelle qui se présentent tout au long du programme académique. Pour ce faire, l'étudiant sera assisté d'un innovant système de vidéos interactives, créé par des experts reconnus.

*Vous accéderez à un système d'apprentissage basé sur la répétition, avec un enseignement naturel et progressif tout au long du cursus.*

*Vous approfondirez vos connaissances sur l'obscurcissement des Strings. Donnez à votre carrière le coup de pouce dont elle a besoin!*



# 02 Objectifs

L'objectif principal de ce programme est de permettre aux diplômés de maîtriser des connaissances avancées sur la nature, la fonctionnalité et le comportement des malwares. Tout au long du programme, les étudiants étudieront les différentes formes et cibles des logiciels malveillants, ce qui leur permettra d'analyser et de développer des stratégies défensives efficaces dans le domaine de la cybersécurité. De même, cette approche globale vise à former des professionnels capables de relever les défis émergents en matière de détection, d'analyse et d'atténuation des menaces liées aux logiciels malveillants dans des environnements numériques complexes. En outre, l'utilisation d'une méthodologie 100 % en ligne rend l'apprentissage plus flexible, offrant la possibilité d'y accéder à tout moment et en tout lieu.



“

*Vous atteindrez vos objectifs grâce aux outils didactiques de TECH, y compris les vidéos explicatives et les résumés interactifs”*



## Objectifs généraux

---

- ◆ Acquérir des compétences avancées en matière de tests de pénétration et de simulations Red Team, afin d'identifier et d'exploiter les vulnérabilités des systèmes et des réseaux
- ◆ Développer des compétences en leadership pour coordonner des équipes spécialisées dans la cybersécurité offensive, en optimisant l'exécution des projets Pentesting et Red Team
- ◆ Développer des compétences dans l'analyse et le développement de logiciels malveillants, en comprenant leur fonctionnalité et en appliquant des stratégies défensives et éducatives
- ◆ Améliorer les compétences en matière de communication en produisant des rapports techniques et exécutifs détaillés, en présentant les résultats de manière efficace à des auditoires techniques et exécutifs
- ◆ Promouvoir une pratique éthique et responsable dans le domaine de la cybersécurité, en tenant compte des principes éthiques et juridiques dans toutes les activités

“

*Vous voulez faire un saut de qualité dans votre carrière ? Avec TECH, vous acquérez des compétences en matière d'analyse médico-légale appliquée aux malwares”*





## Objectifs spécifiques

---

- ◆ Acquérir une connaissance approfondie de la nature, de la fonctionnalité et du comportement du malware, en comprenant leurs différentes formes et leurs objectifs
- ◆ Développer des compétences en analyse légale appliquée aux malware, permettant l'identification d'indicateurs de compromission (IoC) et de schémas d'attaque
- ◆ Apprendre des stratégies de détection et de prévention efficaces des malware, y compris le déploiement de solutions de sécurité avancées
- ◆ Familiariser l'apprenant avec le développement de malware à des fins éducatives et défensives, permettant une compréhension approfondie des tactiques utilisées par les attaquants
- ◆ Promouvoir des pratiques éthiques et juridiques dans l'analyse et le développement des logiciels malveillants, en garantissant l'intégrité et la responsabilité dans toutes les activités
- ◆ Appliquer les connaissances théoriques dans des environnements simulés, participer à des exercices pratiques pour comprendre et contrer les attaques malveillantes
- ◆ Développer des compétences pour évaluer et sélectionner des outils de sécurité anti-malware, en tenant compte de leur efficacité et de leur adaptabilité à des environnements spécifiques
- ◆ Apprendre à mettre en œuvre des mesures d'atténuation efficaces contre les menaces malveillantes, en réduisant l'impact et la propagation des malware sur les systèmes et les réseaux
- ◆ Favoriser une collaboration efficace avec les équipes de sécurité, en intégrant les stratégies et les efforts de protection contre les menaces des malwares

# 03

## Direction de la formation

Le programme d'Analyse et Développement de Malware dispose d'un corps professoral exceptionnellement qualifié. Pour ce faire, TECH a sélectionné des experts possédant une vaste expérience et un prestige reconnu dans des entreprises de premier plan du secteur de la cybersécurité. Ce corps professoral, composé de professionnels de premier plan, apporte non seulement son expérience pratique dans l'analyse et le développement de malware, mais aussi son engagement dans la formation de futurs spécialistes, garantissant un enseignement actualisé et aligné sur les exigences et les défis actuels du domaine de la cybersécurité.





“

*Les meilleurs experts en la matière vous mettront à jour sur la configuration des machines virtuelles et des snapshots. Lancez votre carrière professionnelle avec TECH!”*

## Direction



### M. Gómez Pintado, Carlos

- Directeur de l'Équipe de Cybersécurité et de Réseau CIPHERBIT dans le Grupo Oesía
- Directeur, *Conseiller* et *Investisseur* chez Wesson App
- Diplôme en Ingénierie Logicielle et Technologies de la Société de l'Information, Université Politécnica de Madrid
- Il collabore avec des établissements d'enseignement pour la préparation de Cycles de Formation de Niveau Supérieur en cybersécurité



# 04

## Structure et contenu

Ce programme universitaire permettra aux étudiants de plonger dans le monde des logiciels malveillants, en se concentrant sur leur développement à des fins éducatives et défensives. Tout au long du cursus, les diplômés aborderont les complexités des malwares, ce qui leur permettra de comprendre en détail les tactiques employées par les attaquants. À cet égard, l'approche équilibrée du programme favorise non seulement l'acquisition de connaissances avancées dans l'analyse des logiciels malveillants, mais permet également aux étudiants de développer des stratégies défensives essentielles dans le domaine de la cybersécurité.

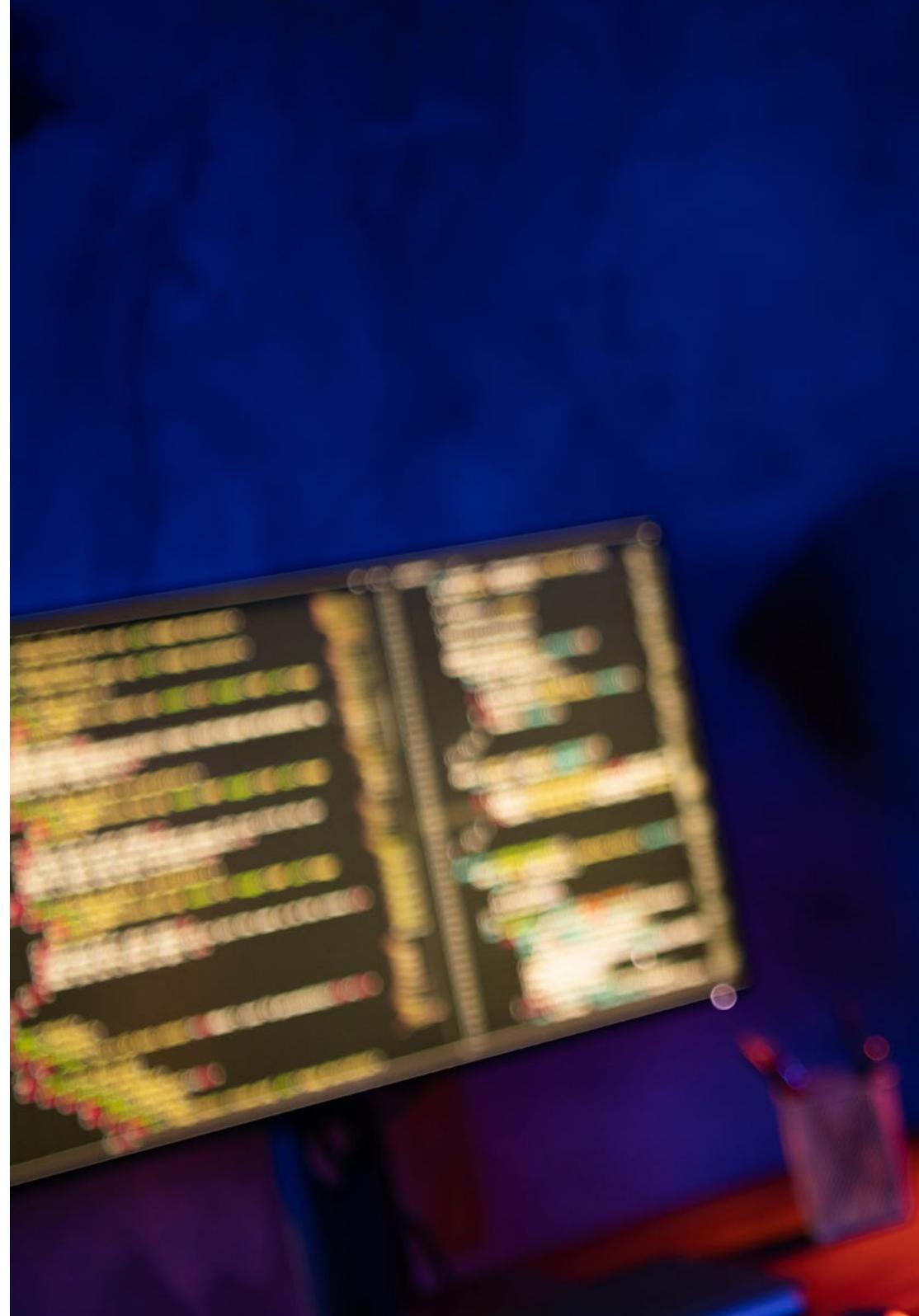


“

*Vous aurez accès à un syllabus conçu par un corps enseignant réputé, ce qui vous garantira un apprentissage réussi”*

## Module 1. Analyse et développement de Malware

- 1.1. Analyse et Développement de Malware
  - 1.1.1. Histoire et Évolution des Malware
  - 1.1.2. Classification et Types de Malware
  - 1.1.3. Analyse de Malware
  - 1.1.4. Développement de Malware
- 1.2. Préparation de l'Environnement
  - 1.2.1. Configuration de la Machine Virtuelle et Snapshots
  - 1.2.2. Outils d'Analyse des Malwares
  - 1.2.3. Outils de Développement des Malwares
- 1.3. Principes de base de Windows
  - 1.3.1. Format de fichier PE (Portable Executable)
  - 1.3.2. Processus et Fils d'exécution
  - 1.3.3. Système de Fichiers et Registre
  - 1.3.4. Windows Defender
- 1.4. Techniques de Malware de Base
  - 1.4.1. Génération de Shellcode
  - 1.4.2. Exécution du Shellcode sur le disque
  - 1.4.3. Disque et Mémoire
  - 1.4.4. Exécution du Shellcode en mémoire
- 1.5. Techniques de Malware intermédiaires
  - 1.5.1. Persistance sur Windows
  - 1.5.2. Dossier d'accueil
  - 1.5.3. Clés de Registre
  - 1.5.4. Économiseur d'écran
- 1.6. Techniques des Malwares Avancés
  - 1.6.1. Cryptage du Shellcode (XOR)
  - 1.6.2. Cryptage du Shellcode (RSA)
  - 1.6.3. Obfuscation de Strings
  - 1.6.4. Injection de Processus





- 1.7. Analyse Statique des Malwares
  - 1.7.1. Analyse des Packers avec DIE (Detect It Easy)
  - 1.7.2. Analyse des sections avec PE-Bear
  - 1.7.3. Décompilation avec Ghidra
- 1.8. Analyse Dynamique des Malwares
  - 1.8.1. Observation du comportement avec Process Hacker
  - 1.8.2. Analyse des appels avec API Monitor
  - 1.8.3. Analyser les modifications du registre avec Regshot
  - 1.8.4. Observer les requêtes réseau avec TCPView
- 1.9. Analyse en .NET
  - 1.9.1. Introduction à .NET
  - 1.9.2. Décompilation avec dnSpy
  - 1.9.3. Débogage avec dnSpy
- 1.10. Analyser de vrais Malwares
  - 1.10.1. Préparation de l'Environnement
  - 1.10.2. Analyse Statique du Malware
  - 1.10.3. Analyse Dynamique du Malware
  - 1.10.4. Création de règles YARA



*Ne manquez pas l'occasion  
de donner un coup de pouce  
à votre carrière grâce à ce  
programme innovant"*

# 05 Méthodologie

Ce programme de formation offre une manière différente d'apprendre. Notre méthodologie est développée à travers un mode d'apprentissage cyclique: ***le Relearning***.

Ce système d'enseignement est utilisé, par exemple, dans les écoles de médecine les plus prestigieuses du monde et a été considéré comme l'un des plus efficaces par des publications de premier plan telles que le ***New England Journal of Medicine***.



“

*Découvrez Relearning, un système qui renonce à l'apprentissage linéaire conventionnel pour vous emmener à travers des systèmes d'enseignement cycliques: une façon d'apprendre qui s'est avérée extrêmement efficace, en particulier dans les matières qui exigent la mémorisation”*

## Étude de Cas pour mettre en contexte tout le contenu

Notre programme offre une méthode révolutionnaire de développement des compétences et des connaissances. Notre objectif est de renforcer les compétences dans un contexte changeant, compétitif et hautement exigeant.

“

*Avec TECH, vous pouvez expérimenter une manière d'apprendre qui ébranle les fondations des universités traditionnelles du monde entier”*



*Vous bénéficierez d'un système d'apprentissage basé sur la répétition, avec un enseignement naturel et progressif sur l'ensemble du cursus.*



*L'étudiant apprendra, par des activités collaboratives et des cas réels, à résoudre des situations complexes dans des environnements commerciaux réels.*

## Une méthode d'apprentissage innovante et différente

Cette formation TECH est un programme d'enseignement intensif, créé de toutes pièces, qui propose les défis et les décisions les plus exigeants dans ce domaine, tant au niveau national qu'international. Grâce à cette méthodologie, l'épanouissement personnel et professionnel est stimulé, faisant ainsi un pas décisif vers la réussite. La méthode des cas, technique qui constitue la base de ce contenu, permet de suivre la réalité économique, sociale et professionnelle la plus actuelle.

“ Notre programme vous prépare à relever de nouveaux défis dans des environnements incertains et à réussir votre carrière ”

La méthode des cas est le système d'apprentissage le plus largement utilisé dans les meilleures écoles d'informatique du monde depuis qu'elles existent. Développée en 1912 pour que les étudiants en Droit n'apprennent pas seulement le droit sur la base d'un contenu théorique, la méthode des cas consiste à leur présenter des situations réelles complexes afin qu'ils prennent des décisions éclairées et des jugements de valeur sur la manière de les résoudre. En 1924, elle a été établie comme méthode d'enseignement standard à Harvard.

Dans une situation donnée, que doit faire un professionnel? C'est la question à laquelle nous sommes confrontés dans la méthode des cas, une méthode d'apprentissage orientée vers l'action. Tout au long du programme, les étudiants seront confrontés à de multiples cas réels. Ils devront intégrer toutes leurs connaissances, faire des recherches, argumenter et défendre leurs idées et leurs décisions.

## Relearning Methodology

TECH combine efficacement la méthodologie des Études de Cas avec un système d'apprentissage 100% en ligne basé sur la répétition, qui associe différents éléments didactiques dans chaque leçon.

Nous enrichissons l'Étude de Cas avec la meilleure méthode d'enseignement 100% en ligne: le Relearning.

*En 2019, nous avons obtenu les meilleurs résultats d'apprentissage de toutes les universités en ligne du monde.*

À TECH, vous apprendrez avec une méthodologie de pointe conçue pour former les managers du futur. Cette méthode, à la pointe de la pédagogie mondiale, est appelée Relearning.

Notre université est la seule université autorisée à utiliser cette méthode qui a fait ses preuves. En 2019, nous avons réussi à améliorer les niveaux de satisfaction globale de nos étudiants (qualité de l'enseignement, qualité des supports, structure des cours, objectifs...) par rapport aux indicateurs de la meilleure université en ligne.





Dans notre programme, l'apprentissage n'est pas un processus linéaire, mais se déroule en spirale (apprendre, désapprendre, oublier et réapprendre). Par conséquent, chacun de ces éléments est combiné de manière concentrique. Cette méthodologie a permis de former plus de 650.000 diplômés universitaires avec un succès sans précédent dans des domaines aussi divers que la biochimie, la génétique, la chirurgie, le droit international, les compétences en gestion, les sciences du sport, la philosophie, le droit, l'ingénierie, le journalisme, l'histoire, les marchés financiers et les instruments. Tout cela dans un environnement très exigeant, avec un corps étudiant universitaire au profil socio-économique élevé et dont l'âge moyen est de 43,5 ans.

*Le Relearning vous permettra d'apprendre avec moins d'efforts et plus de performance, en vous impliquant davantage dans votre formation, en développant un esprit critique, en défendant des arguments et en contrastant les opinions: une équation directe vers le succès.*

À partir des dernières preuves scientifiques dans le domaine des neurosciences, non seulement nous savons comment organiser les informations, les idées, les images et les souvenirs, mais nous savons aussi que le lieu et le contexte dans lesquels nous avons appris quelque chose sont fondamentaux pour notre capacité à nous en souvenir et à le stocker dans l'hippocampe, pour le conserver dans notre mémoire à long terme.

De cette manière, et dans ce que l'on appelle Neurocognitive context-dependent e-learning, les différents éléments de notre programme sont reliés au contexte dans lequel le participant développe sa pratique professionnelle.

Ce programme offre le support matériel pédagogique, soigneusement préparé pour les professionnels:



#### Support d'étude

Tous les contenus didactiques sont créés par les spécialistes qui enseigneront le cours, spécifiquement pour le cours, afin que le développement didactique soit vraiment spécifique et concret.

Ces contenus sont ensuite appliqués au format audiovisuel, pour créer la méthode de travail TECH en ligne. Tout cela, avec les dernières techniques qui offrent des pièces de haute qualité dans chacun des matériaux qui sont mis à la disposition de l'étudiant.



#### Cours magistraux

Il existe des preuves scientifiques de l'utilité de l'observation par un tiers expert.

La méthode "Learning from an Expert" renforce les connaissances et la mémoire, et donne confiance dans les futures décisions difficiles.



#### Pratiques en compétences et aptitudes

Les étudiants réaliseront des activités visant à développer des compétences et des aptitudes spécifiques dans chaque domaine. Des activités pratiques et dynamiques pour acquérir et développer les compétences et aptitudes qu'un spécialiste doit développer dans le cadre de la mondialisation dans laquelle nous vivons.



#### Lectures complémentaires

Articles récents, documents de consensus et directives internationales, entre autres. Dans la bibliothèque virtuelle de TECH, l'étudiant aura accès à tout ce dont il a besoin pour compléter sa formation.





**Case studies**

Ils réaliseront une sélection des meilleures études de cas choisies spécifiquement pour ce diplôme. Des cas présentés, analysés et tutorés par les meilleurs spécialistes de la scène internationale.



**Résumés interactifs**

L'équipe TECH présente les contenus de manière attrayante et dynamique dans des pilules multimédia comprenant des audios, des vidéos, des images, des diagrammes et des cartes conceptuelles afin de renforcer les connaissances. Ce système éducatif unique pour la présentation de contenu multimédia a été récompensé par Microsoft en tant que "European Success Story".



**Testing & Retesting**

Les connaissances de l'étudiant sont périodiquement évaluées et réévaluées tout au long du programme, par le biais d'activités et d'exercices d'évaluation et d'auto-évaluation, afin que l'étudiant puisse vérifier comment il atteint ses objectifs.



# 06 Diplôme

Le Certificat en Analyse et Développement de Malware garantit, outre la formation la plus rigoureuse et la plus actualisée, l'accès à un diplôme de Certificat délivré par TECH Université Technologique.



“

*Terminez ce programme avec succès  
et recevez votre diplôme sans avoir  
à vous soucier des déplacements ou  
des formalités administratives”*

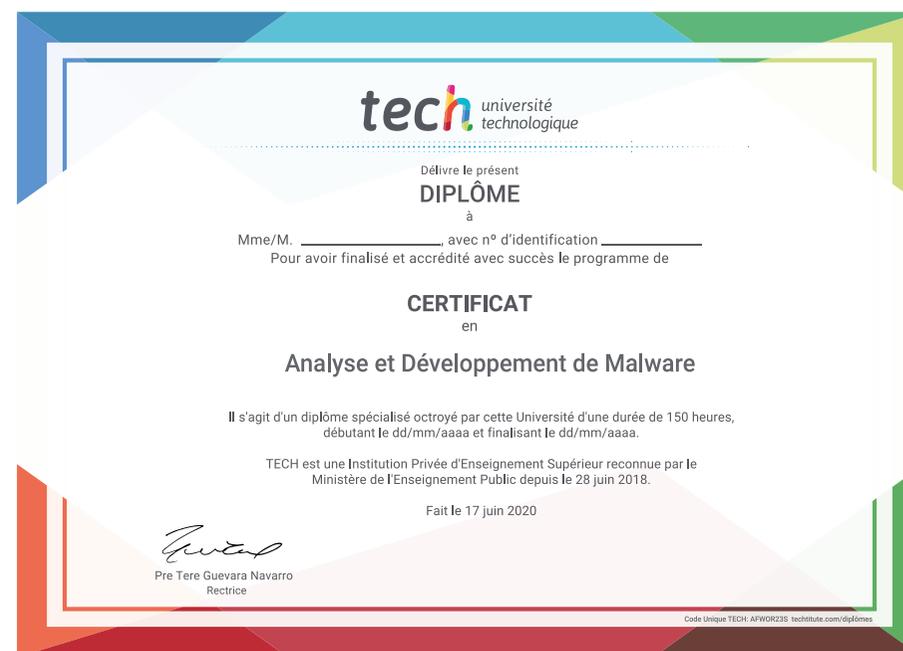
Ce **Certificat en Analyse et Développement de Malware** contient le programme le plus complet et actualisé du marché.

Après avoir passé l'évaluation, l'étudiant recevra par courrier\* avec accusé de réception son diplôme de **Certificat** délivrée par **TECH Université Technologique**

Le diplôme délivré par **TECH Université Technologique** indiquera la note obtenue lors du **Certificat**, et répond aux exigences communément demandées par les bourses d'emploi, les concours et les commissions d'évaluation des carrières professionnelles.

Diplôme : **Certificat en Analyse et Développement de Malware**

Heures Officielles: **150 h.**



future  
santé confiance personnes  
éducation information tuteurs  
garantie accréditation enseignement  
institutions technologie apprentissage  
communauté engagement  
service personnalisé innovation  
connaissance présent qualité  
en ligne formations  
développement institutions  
classe virtuelle langues

**tech** université  
technologique

**Certificat**  
Analyse et Développement  
de Malware

- » Modalité : en ligne
- » Durée : 6 semaines
- » Diplôme : TECH Université Technologique
- » Horaire: à votre rythme
- » Examens: en ligne

# Certificat

## Analyse et Développement de Malware