

Certificat

Cyber-intelligence et cybersécurité





## Certificat Cyber-intelligence et cybersécurité

- » Modalité: en ligne
- » Durée: 6 semaines
- » Qualification: TECH Université Technologique
- » Intensité: 16h/semaine
- » Horaire: à votre rythme
- » Examens: en ligne

Accès au site web: [www.techtitute.com/fr/informatique/cours/cyber-intelligence-cybersecurite](http://www.techtitute.com/fr/informatique/cours/cyber-intelligence-cybersecurite)

# 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

À mesure que la technologie et la connectivité progressent, le nombre et la forme des menaces potentielles augmentent. Il est donc crucial pour les professionnels d'actualiser leurs connaissances dans ce domaine afin de proposer des solutions plus efficaces et adaptées aux différents contextes. Ce programme complet offre un cours hautement qualifié qui permettra aux étudiants d'acquérir les connaissances d'un spécialiste en cyberintelligence et en cybersécurité, avec la méthode d'étude la plus pratique et la plus efficace du marché de l'éducation.



“

*Mettez-vous sur la voie d'un avenir de compétitivité professionnelle maximale avec ce programme de haute intensité que nous mettons à votre portée avec la qualité TECH"*

Le Certificat en Cyber-intelligence et Cybersécurité est un programme intensif qui compile les connaissances spécialisées dans ce domaine à travers un cursus à fort impact.

Il aborde des aspects fondamentaux tels que le cycle du renseignement, les sources de renseignement, l'ingénierie sociale, la méthodologie OSINT, le HUMINT, l'anonymisation, l'analyse des risques, les méthodologies existantes (OWASP, OWISAM, OSSTMM, PTES) et les réglementations actuelles en matière de cybersécurité. Ces domaines sont enseignés avec la vision la plus actuelle qui inclut tous les derniers développements.

D'autre part, les réglementations jouent un rôle fondamental dans la cybersécurité et la confidentialité des données, nous abordons les réglementations concernant toutes les données, qu'elles soient sanitaires, économiques, fiscales, etc. Ce programme examine également les organismes internationaux les plus pertinents en matière de cybersécurité, en exposant son champ d'action et sa position sur différentes problématiques.

“ Grâce à une approche totalement axée sur la pratique, ce Certificat vous permettra d'atteindre le niveau d'un spécialiste ”

Ce **Certificat en Cyber-intelligence et Cybersécurité** contient le programme éducation le plus complet et le plus actuel du marché. Les principales caractéristiques sont les suivantes:

- ◆ Le développement d'études de cas présentées par des experts en Cybersécurité
- ◆ Les contenus graphiques, schématiques et éminemment pratiques avec lesquels ils sont conçus fournissent des informations scientifiques et sanitaires essentielles à la pratique professionnelle
- ◆ Des exercices où le processus d'auto-évaluation peut être réalisé pour améliorer l'apprentissage
- ◆ Il met l'accent sur les méthodologies innovantes
- ◆ Des cours théoriques, des questions à l'expert, des forums de discussion sur des sujets controversés et un travail de réflexion individuel
- ◆ Il est possible d'accéder aux contenus depuis tout appareil fixe ou portable doté d'une connexion à internet

“*Spécialisez-vous dans un secteur en croissance constante et obtenez l'amélioration professionnelle que vous souhaitez*”

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 pratique professionnelle qui se présentent tout au long du programme universitaire. Pour ce faire, l'étudiant sera assisté d'un innovant système de vidéos interactives, créé par des experts reconnus.

*Un apprentissage rapide et efficace qui vous permettra d'avancer en toute confiance en quelques semaines de travail stimulant.*

*Un processus hautement qualifié créé pour être abordable et flexible, avec la méthodologie d'enseignement en ligne la plus intéressante.*



# 02 Objectifs

Ce Certificat conduira les étudiants, rapidement et facilement, à atteindre leurs objectifs d'apprentissage. Avec des objectifs réalistes et très intéressants, ce processus d'étude a été conçu pour conduire progressivement les étudiants à l'acquisition des connaissances théoriques et pratiques nécessaires pour intervenir avec qualité et pour développer des compétences transversales qui leur permettront de faire face à des situations complexes en élaborant des réponses ajustées et précises.







*Un domaine de travail riche en possibilités  
d'emploi qui vous permettra de rivaliser avec  
les professionnels les plus qualifiés du secteur"*



## Objectifs généraux

---

- ◆ Analyser le rôle de l'analyste en cybersécurité
- ◆ Se plonger dans l'ingénierie sociale et ses méthodes
- ◆ Examiner les méthodologies OSINT, HUMINT, OWASP, PTEC OSSTMM, OWISAM
- ◆ Effectuer une analyse des risques et comprendre les mesures de risques
- ◆ Déterminer l'utilisation appropriée de l'anonymat et l'utilisation de réseaux tels que TOR, I2P et Freenet
- ◆ Compiler les réglementations actuelles en matière de cybersécurité

“

*Confort et efficacité dans un programme de haute qualité”*





## Objectifs spécifiques

---

- ◆ Développer les méthodologies utilisées en matière de cybersécurité
- ◆ Examiner le cycle du renseignement et établir son application au cyber renseignement
- ◆ Déterminer le rôle de l'analyste du renseignement et les obstacles à l'activité d'évacuation
- ◆ Analyser les méthodologies OSINT, OWISAM, OSSTMM, PTES et OWASP
- ◆ Établir les outils les plus courants pour la production de renseignements
- ◆ Effectuer une analyse des risques et comprendre les mesures utilisées
- ◆ Spécifier les options pour l'anonymat et l'utilisation de réseaux tels que TOR, I2P, FreeNet
- ◆ Détailler les réglementations actuelles en matière de cybersécurité

# 03

## Direction de la formation

Les enseignants qui dispensent ce programme ont été sélectionnés pour leurs compétences exceptionnelles dans le domaine. Ils associent l'expérience technique et pratique à l'expérience pédagogique, offrant aux étudiants un soutien de premier ordre pour atteindre leurs objectifs. À travers eux, le programme offre la vision la plus directe et immédiate des caractéristiques réelles de l'intervention dans ce domaine, en obtenant une vision contextuelle d'un intérêt maximal.



“

*Des du Certificat en Cyber-intelligence et Cybersécurité , vous accompagneront à chaque phase de l'étude et vous donneront la vision la plus réaliste de ce travail"*

## Directeur invité international

Le Docteur Frédéric Lemieux est internationalement reconnu comme un expert innovant et un leader inspirant dans les domaines du **Renseignement, de la Sécurité Nationale, de la Sécurité Intérieure, de la Cybersécurité et des Technologies de Rupture**. Son dévouement constant et ses contributions pertinentes à la recherche et à l'éducation font de lui une figure clé de la promotion de la sécurité et de la compréhension des technologies émergentes d'aujourd'hui. Au cours de sa carrière professionnelle, il a conceptualisé et dirigé des programmes académiques de pointe dans plusieurs institutions renommées, telles que **l'Université de Montréal, l'Université George Washington et l'Université de Georgetown**.

Tout au long de sa carrière, il a publié de nombreux ouvrages importants, tous liés au **renseignement criminel, à la police, aux cybermenaces et à la sécurité internationale**. Il a également contribué de manière significative au domaine de la cybersécurité en publiant de nombreux articles dans des revues universitaires sur la lutte contre la criminalité lors de catastrophes majeures, la lutte contre le terrorisme, les agences de renseignement et la coopération policière. En outre, il a participé en tant que panéliste et orateur principal à diverses conférences nationales et internationales, s'imposant ainsi comme un universitaire et un praticien de premier plan.

Le Docteur Lemieux a occupé des fonctions éditoriales et d'évaluation dans diverses organisations universitaires, privées et gouvernementales, ce qui témoigne de son influence et de son engagement en faveur de l'excellence dans son domaine d'expertise. Sa prestigieuse carrière universitaire l'a amené à occuper le poste de professeur de pratique et de directeur des programmes MPS en **Intelligence appliquée, Gestion des Risques de Cybersécurité, Gestion de la Technologie et Gestion des Technologies de l'Information à l'Université de Georgetown**.



## Dr. Lemieux, Frederic

---

- Chercheur en Intelligence, Cybersécurité et Technologies de Rupture à l'Université de Georgetown
  - Directeur du Master en Information Technology Management à l'Université de Georgetown
  - Directeur du Master en Technology Management à l'Université de Georgetown
  - Directeur du Master en Cybersecurity Risk Management de l'Université de Georgetown
  - Directeur du Master en Applied Intelligence à l'Université de Georgetown
  - Professeur de Stage à l'Université de Georgetown
  - Licence en Sociologie, Mineure en Psychologie, Université Laval
  - Doctorat en Criminologie de l'École de Criminologie de l'Université de Montréal.
- Membre de:  
New Program Roundtable Committee, de l'Université de Georgetown

“

*Grâce à TECH, vous pourrez apprendre avec les meilleurs professionnels du monde”*

## Direction



### Mme Fernandez Sapena, Sonia

- ◆ Formateur en sécurité informatique et en Hacking Éthique Centre national de référence de Getafe pour l'informatique et les Télécommunications Madrid
- ◆ Instructrice certifiée E-Council. Madrid
- ◆ Formatrice dans les certifications suivantes : EXIN Ethical Hacking Foundation et EXIN Cyber & IT Security Foundation. Madrid
- ◆ Formatrice experte accréditée par le CAM pour les certificats de professionnalisme suivants : Sécurité informatique (IFCT0190), Gestion des réseaux voix et données (IFCM0310), Administration des réseaux départementaux (IFCT0410), Gestion des alarmes dans les réseaux de télécommunications (IFCM0410), Opérateur de réseaux voix et données (IFCM0110), et Administration des services Internet (IFCT0509)
- ◆ Collaboratrice externe CSO/SSA (Chief Security Officer/Senior Security Architect) Université des Îles Baléares
- ◆ Ingénieur en Informatique. Université d'Alcalá de Henares. Madrid
- ◆ Master en DevOps: Docker and Kubernetes. Cas-Training. Madrid
- ◆ Microsoft Azure Security Technologies. E-Council. Madrid





# 04

## Structure et contenu

Tout au long de l'étude des différents sujets de ce programme, les étudiants pourront acquérir les derniers développements dans le domaine de la cyber-intelligence et de la cybersécurité. À cette fin, le programme a été structuré en vue de l'acquisition efficace d'apprentissages complémentaires, qui permettront d'intervenir le plus rapidement possible. Un parcours de haute intensité conçu pour les meilleurs du secteur.



“

*Tous les concepts de la Cyber-Intelligence et de la Cybersécurité développés de manière structurée dans une approche d'étude axée sur l'efficacité"*

## Module 1. Cyber-intelligence et Cybersécurité

- 1.1. Cyber intelligence
  - 1.1.1. Cyber intelligence
    - 1.1.1.1. Intelligence
      - 1.1.1.1.1. Cycle du renseignement
    - 1.1.1.2. Cyber intelligence
    - 1.1.1.3. Cyber intelligence et cybersécurité
  - 1.1.2. L'analyste d' Intelligence
    - 1.1.2.1. Le rôle de l'analyste du renseignement
    - 1.1.2.2. Biais de l'analyste du renseignement dans l'activité d'évaluation
- 1.2. Cybersécurité
  - 1.2.1. Les couches de sécurité
  - 1.2.2. Identification des cybermenaces
    - 1.2.2.1. Menaces externes
    - 1.2.2.2. Menaces internes
  - 1.2.3. Actions défavorables
    - 1.2.3.1. Ingénierie sociale
    - 1.2.3.2. Méthodes de communément utilisées
- 1.3. Techniques et Outils de Intelligence.
  - 1.3.1. OSINT:
  - 1.3.2. SOCMINT
  - 1.3.3. Humit
  - 1.3.4. Distributions et outils Linux
  - 1.3.5. OWISAM
  - 1.3.6. OWASP
  - 1.3.7. PTES
  - 1.3.8. OSSTMM
- 1.4. Méthodologie d'évaluation
  - 1.4.1. L'analyse du renseignement
  - 1.4.2. Techniques d'organisation des informations acquises
  - 1.4.3. Fiabilité et crédibilité des sources d'information
  - 1.4.4. Méthodologie d'analyse
  - 1.4.5. Présentation les résultats de la Intelligence.



- 1.5. Contrôles et documentation
  - 1.5.1. Le contrôle de la sécurité informatique
  - 1.5.2. Documentation et autorisations de contrôle
  - 1.5.3. Types de contrôles
  - 1.5.4. Produits livrables
    - 1.5.4.1. Rapport technique
    - 1.5.4.2. Rapport exécutif
- 1.6. L'anonymat sur le réseau
  - 1.6.1. Utilisation des L'anonymat
  - 1.6.2. Techniques d'anonymisation (Proxy, VPN)
  - 1.6.3. Réseaux TOR, Freenet et IP2
- 1.7. Menaces et types de sécurité
  - 1.7.1. Types de menaces
  - 1.7.2. Sécurité physique
  - 1.7.3. Sécurité des réseaux
  - 1.7.4. Sécurité logique
  - 1.7.5. Sécurité des applications en Web
  - 1.7.6. Sécurité des appareils mobiles
- 1.8. Réglementation et *Compliance*
  - 1.8.1. RGPD
  - 1.8.2. La stratégie nationale de cybersécurité 2019
  - 1.8.3. Famille IEC 27000
  - 1.8.4. Cadre de cybersécurité du NIST
  - 1.8.5. PIC
  - 1.8.6. ISO 27032
  - 1.8.7. Réglementations Cloud
  - 1.8.8. SOX
  - 1.8.9. PCI
- 1.9. Analyse et Prévention des Risques
  - 1.9.1. Portée des risques
  - 1.9.2. Les actifs
  - 1.9.3. Les menaces
  - 1.9.4. Les vulnérabilités
  - 1.9.5. Évaluation des risques
  - 1.9.6. Traitement du risque
- 1.10. Organismes importants en matière de cybersécurité
  - 1.10.1. NIST
  - 1.10.2. ENISA
  - 1.10.3. INCIBE
  - 1.10.4. OEA
  - 1.10.5. UNASUR PROSUR



*Un plan de travail actuel qui comprend chacun des aspects qu'un spécialiste de ce domaine doit maîtriser"*

# 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 Cyber-intelligence et Cybersécurité vous garantit, en plus de la formation la plus rigoureuse et la plus actuelle, l'accès à un diplôme universitaire de Certificat délivré par TECH Université Technologique.



“

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

Ce **Certificat en Cyber-intelligence et Cybersécurité** contient le programme le plus complet et le plus actuel du marché.

Après avoir réussi l'évaluation, l'étudiant recevra par courrier postal\* avec accusé de réception son correspondant diplôme de **Certificat** délivré 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 Cyber-intelligence et Cybersécurité**

N.º d'heures Officielles: **150 h.**



\*Si l'étudiant souhaite que son diplôme version papier possède l'Apostille de La Haye, TECH EDUCATION fera les démarches nécessaires pour son obtention moyennant un coût supplémentaire.



future

santé confiance personnes

éducation information tuteurs

garantie accréditation enseignement

institutions technologie apprentissage

communauté engagement

service personnalisé innovation

connaissance présent qualité

en ligne formation

développement institutions

classe virtuelle langues

**tech** université  
technologique

**Certificat**  
Cyber-intelligence et  
cybersécurité

- » Modalité: en ligne
- » Durée: 6 semaines
- » Qualification: TECH Université Technologique
- » Intensité: 16h/semaine
- » Horaire: à votre rythme
- » Examens: en ligne

# Certificat

## Cyber-intelligence et Cybersécurité