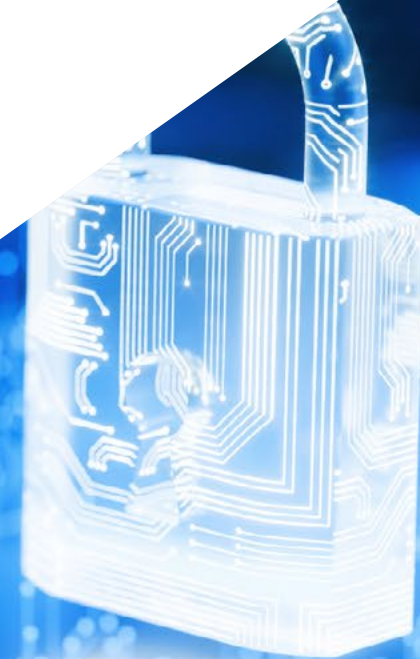


Certificat

Sécurité Offensive





Certificat Sécurité Offensive

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

Accès au site web: www.techtitute.com/fr/informatique/cours/securite-offensive

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 le monde rapide de la cybersécurité, l'évolution constante des cybermenaces exige une préparation permanente pour garder une longueur d'avance sur les acteurs malveillants. Dans ce contexte, rester à jour devient un atout inestimable pour assurer la sécurité des organisations et la protection contre des cyber-attaques de plus en plus élaborées. En ce sens, ce programme propose une plongée en profondeur dans les tactiques de sécurité offensives, permettant aux participants d'anticiper et de répondre efficacement à des menaces complexes. Avec un format 100 % en ligne, le programme d'études offre la flexibilité nécessaire pour s'adapter à l'emploi du temps des professionnels occupés, en proposant une grande variété de contenus multimédias et en appliquant la méthodologie *Relearning* afin d'optimiser la rétention des connaissances.



“

Vous vous attaquez à des défis du monde réel grâce à des simulations avancées de cybermenaces dans le cadre de ce programme universitaire unique 100 % en ligne"

Dans le paysage actuel de la cybersécurité, où les menaces évoluent constamment, une gestion efficace du travail d'équipe est devenue essentielle. Ainsi, une collaboration efficace entre les équipes de sécurité n'est pas seulement une nécessité, mais un impératif pour anticiper et atténuer les cybermenaces complexes. C'est là qu'apparaît le besoin critique de ce programme qui non seulement reconnaît, mais aussi aborde l'importance d'une bonne gestion d'équipe dans l'identification et la protection contre les menaces de malware. Ce plan d'études fournit les outils et les stratégies nécessaires pour intégrer les équipes de sécurité, répartir efficacement les rôles et optimiser la coordination en réponse aux menaces numériques.

Tout au long du parcours académique de ce Certificat en Sécurité Offensive, le diplômé approfondira sa compréhension des méthodologies de test de pénétration, en fournissant une compréhension complète des phases clés telles que la collecte d'informations, l'analyse des vulnérabilités, l'exploitation et la documentation. Les étudiants n'acquièrent pas seulement des connaissances théoriques, mais développent également des compétences pratiques grâce à l'utilisation d'outils de Pentesting spécialisés. Cette immersion pratique permet d'identifier et d'évaluer efficacement les vulnérabilités des systèmes et des réseaux. En outre, un accent particulier est mis sur la pratique d'une collaboration efficace au sein d'équipes de sécurité offensives, optimisant l'attribution des rôles, la coordination et l'exécution des activités de Pentesting. Cette orientation pratique garantit que les participants ne se contentent pas de comprendre les concepts théoriques, mais qu'ils sont également préparés à les appliquer efficacement dans des situations réelles.

Ce programme se distingue par sa méthodologie innovante. 100% en ligne, il offre la flexibilité nécessaire pour s'adapter à l'emploi du temps des professionnels, en éliminant les barrières géographiques et temporelles. En outre, l'application du *Relearning*, basée sur la répétition de concepts clés, est mise en œuvre pour renforcer la rétention des connaissances et faciliter un apprentissage efficace.

Ce **Certificat en Sécurité Offensive** 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 Sécurité Offensive
- 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 vous plongerez dans les systèmes d'exploitation les plus innovants pour le Hacking sans horaires rigides et sans programmes d'évaluation : c'est ce que ce programme TECH est en train de faire"

“

Découvrez les dernières méthodologies en matière de Sécurité Offensive dans la meilleure université numérique au monde selon Forbes"

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.

Oubliez la mémorisation! Avec le système du Relearning, vous intégrerez les concepts de manière naturelle et progressive.

Vous maîtriserez les bases de la sécurité offensive et stimulerez votre carrière grâce à ce programme innovant.



02 Objectifs

L'objectif principal de ce programme universitaire est d'étudier et de comprendre les tactiques, les techniques et les procédures employées par les acteurs malveillants dans le domaine de la cybersécurité. Tout au long du programme, les diplômés se plongeront dans une analyse détaillée de ces pratiques, ce qui leur permettra non seulement d'identifier mais aussi de simuler des menaces de manière efficace. En ce sens, cette approche spécialisée garantit que les étudiants acquièrent des connaissances avancées et des compétences applicables pour relever les défis du monde réel dans le domaine de la sécurité offensive, les préparant ainsi à jouer un rôle de premier plan dans la protection contre les cybermenaces.



“

Vous plongerez dans l'arsenal de l'auditeur offensif. Tirez le meilleur parti de vos armes et atteignez vos objectifs avec TECH!"



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

“

En seulement 6 semaines, vous donnerez un coup de pouce à votre carrière grâce à ce programme universitaire portant le label de qualité TECH”





Objectifs spécifiques

- ♦ Familiariser le diplômé avec les méthodologies de test de pénétration, y compris les phases clés telles que la collecte d'informations, l'analyse de la vulnérabilité, l'exploitation et la documentation
- ♦ Développer des compétences pratiques dans l'utilisation d'outils de Pentesting spécialisés pour identifier et évaluer les vulnérabilités des systèmes et des réseaux
- ♦ Étudier et comprendre les tactiques, les techniques et les procédures utilisées par les acteurs malveillants, ce qui permet d'identifier et de simuler les menaces
- ♦ Appliquer les connaissances théoriques dans des scénarios pratiques et des simulations, en faisant face à des défis réels pour renforcer les compétences de Pentesting
- ♦ Développer des compétences efficaces en matière de documentation, en créant des rapports détaillés reflétant les résultats, les méthodologies utilisées et les recommandations pour l'amélioration de la sécurité
- ♦ Pratiquer une collaboration efficace au sein des équipes de sécurité offensive, en optimisant la coordination et l'exécution des activités de Pentesting

03

Direction de la formation

TECH a soigneusement sélectionné les meilleurs spécialistes du domaine pour constituer le corps enseignant de ce parcours académique. En ce sens, chaque membre de cette faculté apporte une vaste expérience professionnelle, forgée dans des entreprises de premier plan dans le secteur de la cybersécurité. De même, cette sélection minutieuse garantit que les diplômés bénéficient de l'expérience directe et actualisée de professionnels qui ont affronté et résolu des défis en matière de sécurité offensive. En outre, l'application de la méthode *Relearning* facilite l'apprentissage et ancre les connaissances grâce à la répétition de concepts clés tout au long du programme.



“

Vous serez soutenu par un corps enseignant composé d'éminents gourous de la Sécurité Offensive. Qu'attendez-vous pour faire avancer votre carrière ?”

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 Politéchnique de Madrid
- ♦ Il collabore avec des établissements d'enseignement pour la préparation de **Cycles de Formation de Niveau Supérieur** en cybersécurité

Professeurs

M. González Parrilla, Yuba

- ♦ Coordinateur de la Ligne de Sécurité Offensive et Red Team
- ♦ Spécialiste en Gestion *Prédictive* de Projet à l'Institut de Gestion de Projet
- ♦ Spécialiste de *SmartDefense*
- ♦ Expert en *Web Application Penetration Tester* chez eLearnSecurity
- ♦ *Junior Penetration Tester* chez eLearnSecurity
- ♦ Diplômé en Ingénierie Informatique à l'Université Polytechnique de Madrid



04

Structure et contenu

Ce programme d'études plonge les diplômés dans le développement de compétences pratiques grâce à l'utilisation d'outils de Pentesting spécialisés. Tout au long du programme, l'accent est mis sur le développement de compétences techniques avancées, permettant aux étudiants d'identifier et d'évaluer les vulnérabilités des systèmes et des réseaux. En outre, cette approche pratique, soutenue par un programme d'études structuré, garantit que les professionnels acquièrent des compétences fondamentales en matière de sécurité offensive. En mettant l'accent sur l'application directe des connaissances, ce programme constitue une plate-forme essentielle pour ceux qui cherchent à exceller dans le domaine dynamique de la cybersécurité.

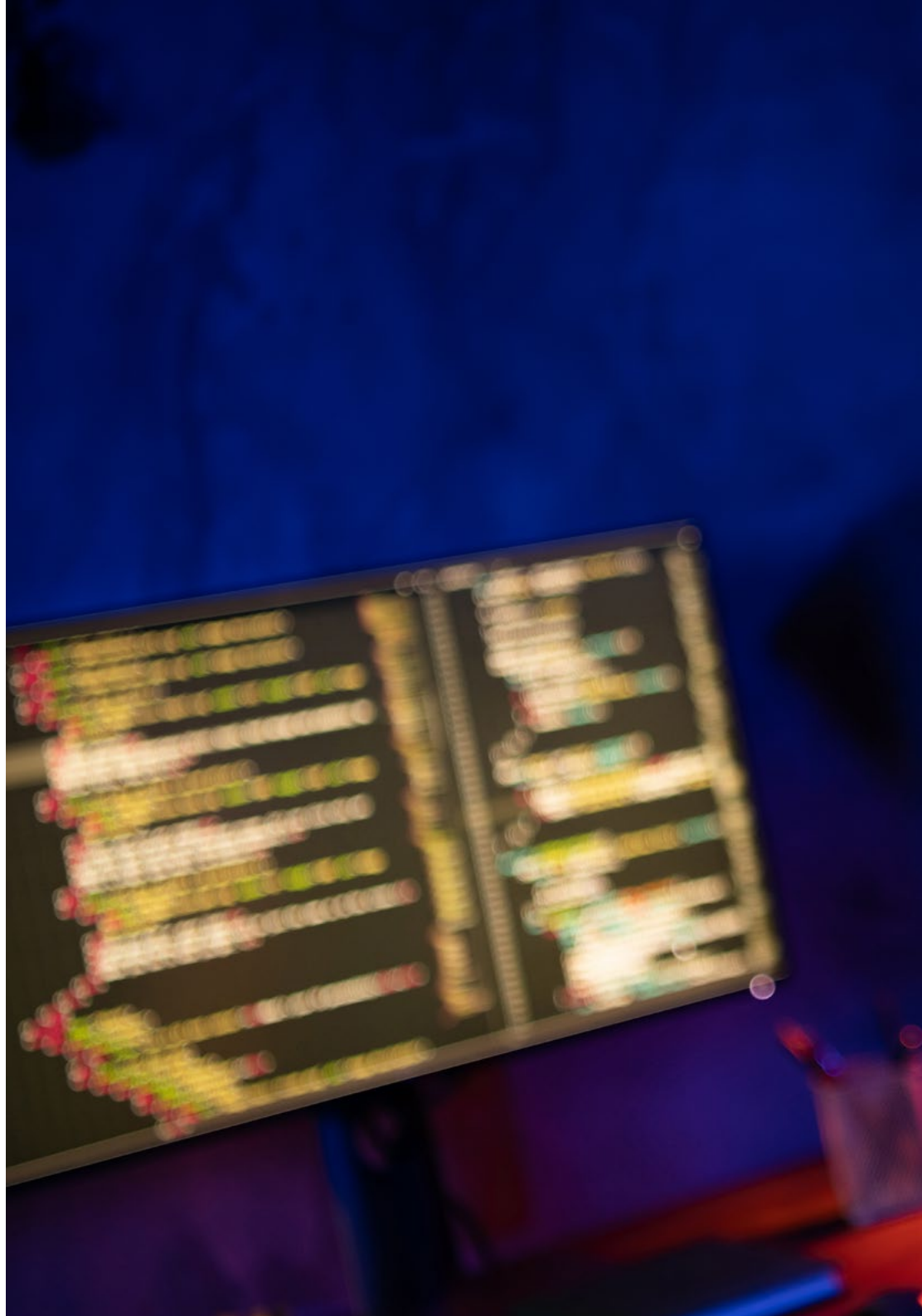


“

Vous serez initié aux Méthodologies de Sécurité Offensives innovantes avec ce Certificat 100% en ligne. Et en seulement 6 mois !

Module 1. Sécurité offensive

- 1.1. Définition et Contexte
 - 1.1.1. Concepts fondamentaux de la sécurité offensive
 - 1.1.2. Importance de la cybersécurité aujourd'hui
 - 1.1.3. Défis et opportunités en matière de Sécurité Offensive
- 1.2. Bases de la cybersécurité
 - 1.2.1. Les premiers défis et l'évolution des menaces
 - 1.2.2. Les étapes technologiques et leur impact sur la cybersécurité
 - 1.2.3. La cybersécurité à l'ère moderne
- 1.3. Bases de la Sécurité Offensive
 - 1.3.1. Concepts clés et terminologie
 - 1.3.2. Think outside the Box
 - 1.3.3. Différences entre Hacking Offensif et Hacking Défensif
- 1.4. Méthodologies de Sécurité Offensives
 - 1.4.1. PTES (Penetration Testing Execution Standard)
 - 1.4.2. OWASP (Open Web Application Security Project)
 - 1.4.3. Cyber Security Kill Chain
- 1.5. Rôles et responsabilités en matière de Sécurité Offensive
 - 1.5.1. Profils principaux
 - 1.5.2. Bug Bounty Hunters
 - 1.5.3. Researching: l'art de la recherche
- 1.6. L'Arsenal Offensif de l'Auditeur
 - 1.6.1. Systèmes d'Exploitation pour Hacking
 - 1.6.2. Introduction au C2
 - 1.6.3. Metasploit: Principes de base et Utilisation
 - 1.6.4. Ressources utiles
- 1.7. OSINT Intelligence de Sources Ouvertes
 - 1.7.1. Les bases de la OSINT
 - 1.7.2. Techniques et Outils OSINT
 - 1.7.3. Applications OSINT en matière de Sécurité Offensive





- 1.8. Scripting: Introduction à l'automatisation
 - 1.8.1. Principes de base de Scripting
 - 1.8.2. Scripting en Bash
 - 1.8.3. Scripting en Python
- 1.9. Catégorisation des Vulnérabilités
 - 1.9.1. CVE (Common Vulnerabilities and Exposure)
 - 1.9.2. CWE (Common Weakness Enumeration)
 - 1.9.3. CAPEC (Common Attack Pattern Enumeration and Classification)
 - 1.9.4. CVSS (Common Vulnerability Scoring System)
 - 1.9.5. MITRE ATT & CK
- 1.10. Éthique et Hacking
 - 1.10.1. Principes de l'éthique du hacker
 - 1.10.2. La frontière entre le hacking éthique et le hacking malveillant
 - 1.10.3. Implications et conséquences juridiques
 - 1.10.4. Étude de cas: Situations éthiques en cybersécurité

“

Ne manquez pas l'occasion de donner un coup de pouce à votre carrière dans le domaine de la cybersécurité 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 Sécurité Offensive 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 Sécurité Offensive** 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 Sécurité Offensive**

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
Sécurité Offensive

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

Certificat

Sécurité Offensive