Certificat Avancé

Mesures de Défense de Sécurité Informatiques

tech université technologique

tech université technologique

Certificat Avancé

Mesures de Défense de Sécurité Informatiques

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

Accès au site web: www.techtitute.com/fr/informatique/diplome-universite/diplome-universite-mesures-defense-securite-informatiques

Sommaire

01

Présentation

Les secteurs de la finance, des affaires et du tourisme ont subi une augmentation des attaques d'ingénierie sociale qui compromettent les informations sensibles et précieuses des organisations et de leurs clients. Les cyberattaques continuent d'être un fléau pour les entreprises, c'est pourquoi le nombre d'emplois créés pour garantir la sécurité informatique a augmenté ces dernières années. En réponse à ce besoin, ce programme offre aux professionnels de l'informatique une spécialisation dans l'adoption de mesures de défense informatique face à toute attaque. Un corps enseignant expert dans le domaine enseigne ce Certificat 100% en ligne, ce qui vous permet d'acquérir un apprentissage actuel et complet grâce à son vaste contenu multimédia.

Répondez au mieux en matière de sécurité informatique et évitez aux entreprises de tomber dans le piège de l'ingénierie sociale grâce à ce Certificat Avancé"

L'implémentation des Politiques de Sécurité Informatiques est coûteuse pour les entreprises, mais celles-ci sont prêtes à payer pour ce service, en raison des pertes importantes lorsque leurs systèmes sont piratés, ce qui compromet leur bon fonctionnement et la fourniture de services à leurs clients. Les professionnels de l'informatique jouent un rôle clé dans ce domaine.

Ce Certificat Avancé offre aux étudiants une formation approfondie sur les mesures de défense en matière de sécurité informatique, qui commencent par une analyse des menaces et les classent correctement afin de déterminer où une entreprise est plus ou moins vulnérable. De plus, l'équipe d'enseignants spécialisés dans cette matière fournira les outils essentiels pour effectuer une analyse criminalistique des ordinateurs. Ainsi, la détection des incidents par les systèmes IDS/IPS et leur traitement dans le SIEM jusqu'au processus de notification et d'escalade seront abordés dans ce programme.

Pour être à la pointe de la défense de la sécurité, les professionnels développeront des techniques pour atténuer les dénis de service, le *Session Hacking* et les attaques sur les applications web. Tout cela, dans une modalité d'enseignement 100% en ligne, qui permet aux étudiants de combiner leur travail professionnel avec un programme qui offre un contenu multimédia innovant. Tout ce qu'il leur faut, c'est un appareil doté d'une connexion Internet pour accéder à un programme d'études à suivre à leur propre rythme.

Ce **Certificat Avancé en Mesures de Défense de Sécurité Informatiques** contient le programme académique 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 Sécurité Informatique
- Les contenus graphiques, schématiques et éminemment pratiques avec lesquels il est conçu, fournissent des informations pratiques sur les disciplines essentielles à la pratique professionnelle
- Les exercices pratiques d'auto-évaluation pour améliorer l'apprentissage
- 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
- La possibilité d'accéder au contenu à partir de n'importe quel dispositif fixe ou portable ou d'un ordinateur doté d'une connexion internet

Appliquez efficacement des politiques de sécurité contre le Hijacking, Hacking Web Servers o Mobile Platforms grâce à ce Certificat Avancé"

Contrôlez la norme ISO 27035 et répondez aux exigences d'une bonne gestion des incidents. Inscrivez-vous à ce Certificat Avancé"

Développez votre carrière professionnelle grâce à un programme qui vous permettra d'approfondir l'analyse et le contrôle des menaces informatiques.

Vous êtes à un clic de vous inscrire à ce Certificat Avancé qui vous ouvrira de nouvelles perspectives de carrière.

Le programme comprend un corps enseignant, formé de professionnels du domaine, qui apportent à cette formation l'expérience de leur travail, ainsi que des spécialistes reconnus de grandes sociétés et d'universités prestigieuses.

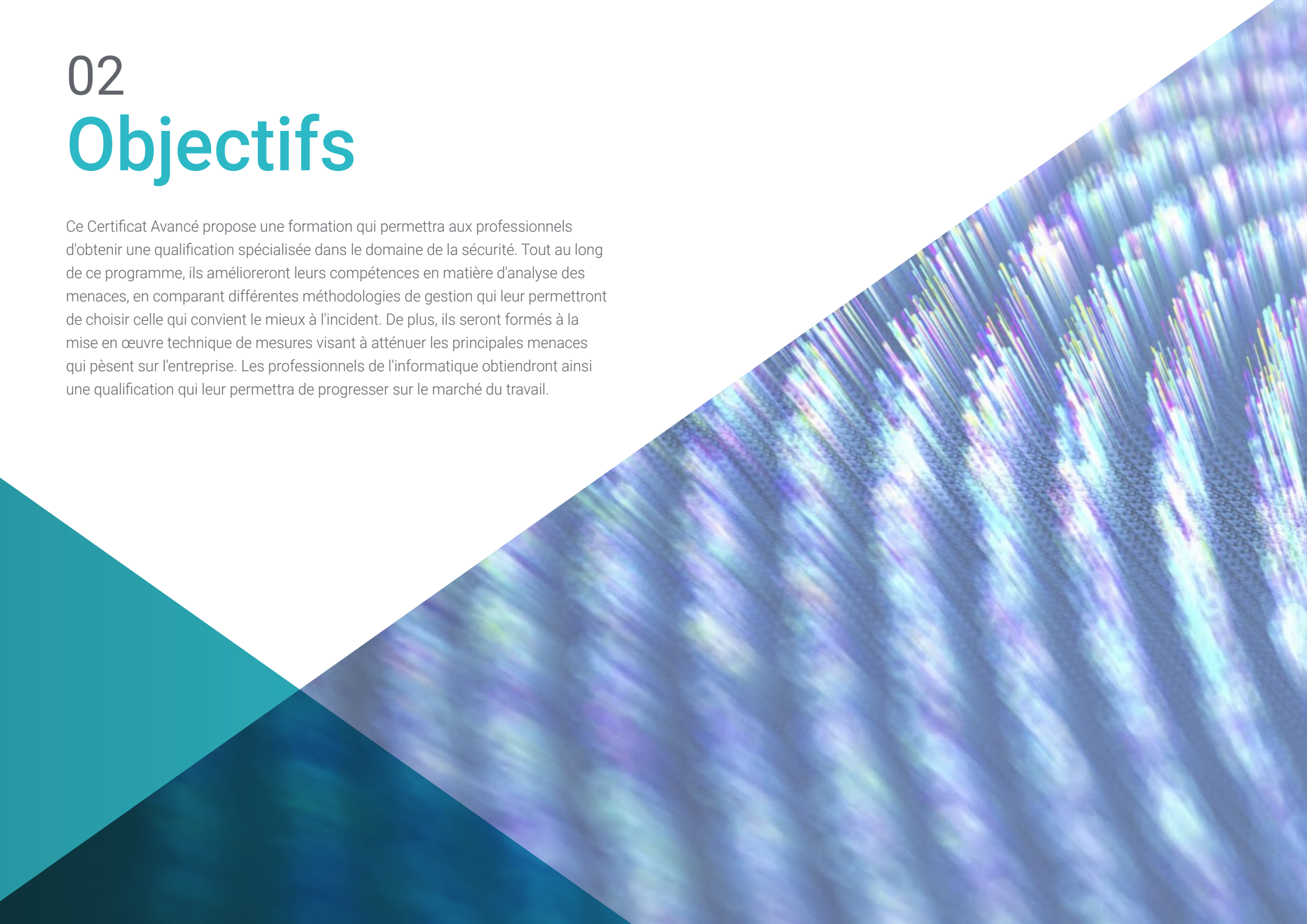
Grâce à son contenu multimédia développé avec les dernières technologies éducatives, les spécialistes bénéficieront d'un apprentissage situé et contextuel. Ainsi, ils se formeront dans un environnement simulé qui leur permettra d'apprendre en immersion et de s'entrainer dans des situations réelles.

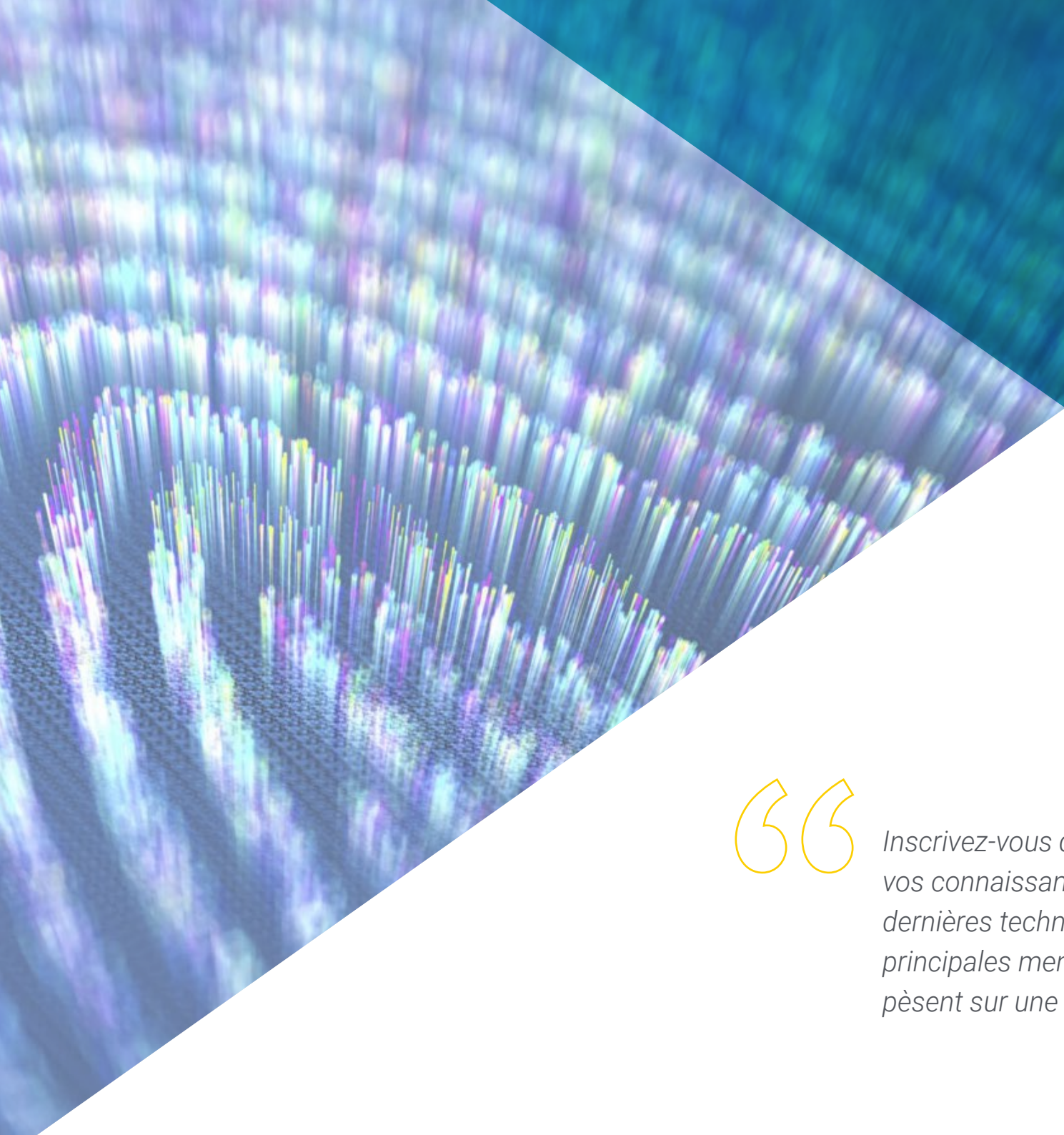
La conception de ce programme est axée sur l'Apprentissage Par les Problèmes, grâce auquel le professionnel doit essayer de résoudre les différentes situations de pratique professionnelle qui se présentent tout au long du programme universitaire. Pour ce faire, il sera assisté d'un système vidéo interactif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

02

Objectifs

Ce Certificat Avancé propose une formation qui permettra aux professionnels d'obtenir une qualification spécialisée dans le domaine de la sécurité. Tout au long de ce programme, ils amélioreront leurs compétences en matière d'analyse des menaces, en comparant différentes méthodologies de gestion qui leur permettront de choisir celle qui convient le mieux à l'incident. De plus, ils seront formés à la mise en œuvre technique de mesures visant à atténuer les principales menaces qui pèsent sur l'entreprise. Les professionnels de l'informatique obtiendront ainsi une qualification qui leur permettra de progresser sur le marché du travail.





Inscrivez-vous dès maintenant. Actualisez vos connaissances et découvrez les dernières techniques pour prévenir les principales menaces informatiques qui pèsent sur une entreprise"

Objectifs généraux

- Approfondir la compréhension des concepts clés de la sécurité de l'information
- Développer les mesures nécessaires pour assurer de bonnes pratiques en matière de sécurité de l'information
- Développer les différentes méthodologies pour effectuer une analyse exhaustive des menaces
- Installer et apprendre les différents outils utilisés dans le traitement et la prévention des incidents

Accédez à un programme universitaire qui vous fournira les stratégies les plus récentes et les plus efficaces pour gérer n'importe quelle attaque informatique"

Objectifs spécifiques

Module 1. Politiques de Sécurité pour l'Analyse de la Menace des Systèmes Informatiques

- Analyser la signification des menaces
- Déterminer les phases de la gestion préventive des menaces
- Comparer différentes méthodologies de gestion des menaces

Module 2. Politiques de Gestion des Incidents de Sécurité

- Développer des connaissances spécialisées sur la manière de gérer les incidents causés par des événements liés à la sécurité informatique
- Déterminer le fonctionnement d'une équipe de traitement des incidents de sécurité
- Analyser les différentes phases de la gestion des événements de sécurité informatique
- Examiner les protocoles standardisés pour le traitement des incidents de sécurité

Module 3. Implémentation des Politiques de Sécurité de Software face aux Attaques

- Déterminer les différentes attaques réelles contre le système d'information
- Évaluer les différentes politiques de sécurité pour atténuer les attaques
- Mettre en œuvre techniquement des mesures pour atténuer les principales menaces

03

Direction de la formation

TECH sélectionne avec soin l'ensemble du personnel enseignant qui dispense les diplômes. Ce Certificat Avancé dispose d'un professionnel hautement qualifié dans le domaine de la sécurité informatique. Grâce à son expérience en tant que Responsable de la Sécurité auprès de structures publiques et privées, il garantit aux étudiants une connaissance approfondie qui constitue une richesse, pour le professionnel qui perfectionner les principales mesures adoptées dans ce domaine face aux principales menaces Ainsi, les cas pratiques présentés sont similaires aux situations réelles auxquelles les étudiants sont confrontés dans leur environnement de travail, et les aideront donc à se développer professionnellement.

Une équipe d'experts en Sécurité Informatique met à votre disposition toutes ses connaissances pour développer votre carrière"

Direction

Mme Fernández Sapena, Sonia

- Formatrice en Sécurité Informatique et Piratage Ethique au Centre National de Référence pour l'Informatique et les Télécommunications à Getafe, Madrid
- Formatrice Agréée E-Council
- Formatrice en: EXIN Ethical Hacking Foundation et EXIN Cyber & IT Security Foundation Madrid
- Formatrice Spécialisée accréditée par le CAM pour les Certificats Professionnels suivants: Sécurité Informatique (IFCT0190), Gestion des Réseaux de Voix et de Données (IFCM0310), Administration des Réseaux Départementaux (IFCT0410), Gestion des Alarmes de Réseaux de Télécommunications (IFCM0410), Opérateur de Réseaux de Voix et Données (IFCM0110), et Administration des Services Internet (IFCT0509)
- Collaboratrice Externe CSO/SSA (Chief Security Officer/Senior Security Architect) à l'Université des Iles Baléares
- Ingénierie Informatique, Université d'Alcalá de Henares de Madrid
- Master en DevOps: Docker and Kubernetes Cas-Training
- Microsoft Azure Security Techonologies E-Council

Professeurs

Mme López García, Rosa María

- Spécialiste en information de Gestion
- Professeur à l'Institut Professionnel Linux
- Collaboratrice à l'Incibe Hacker Academy
- Capitaine des Talents de la Cybersécurité à Teamciberhack
- Responsable Administratif, Comptable et Financier à Integra2Transportes
- Assistante Administrative en Ressources des Achats au Centre d'Education Cardinal Marcelo Espínola
- Technicienne Supérieure en Cybersécurité et Piratage Ethique
- Membre de Ciberpatrol

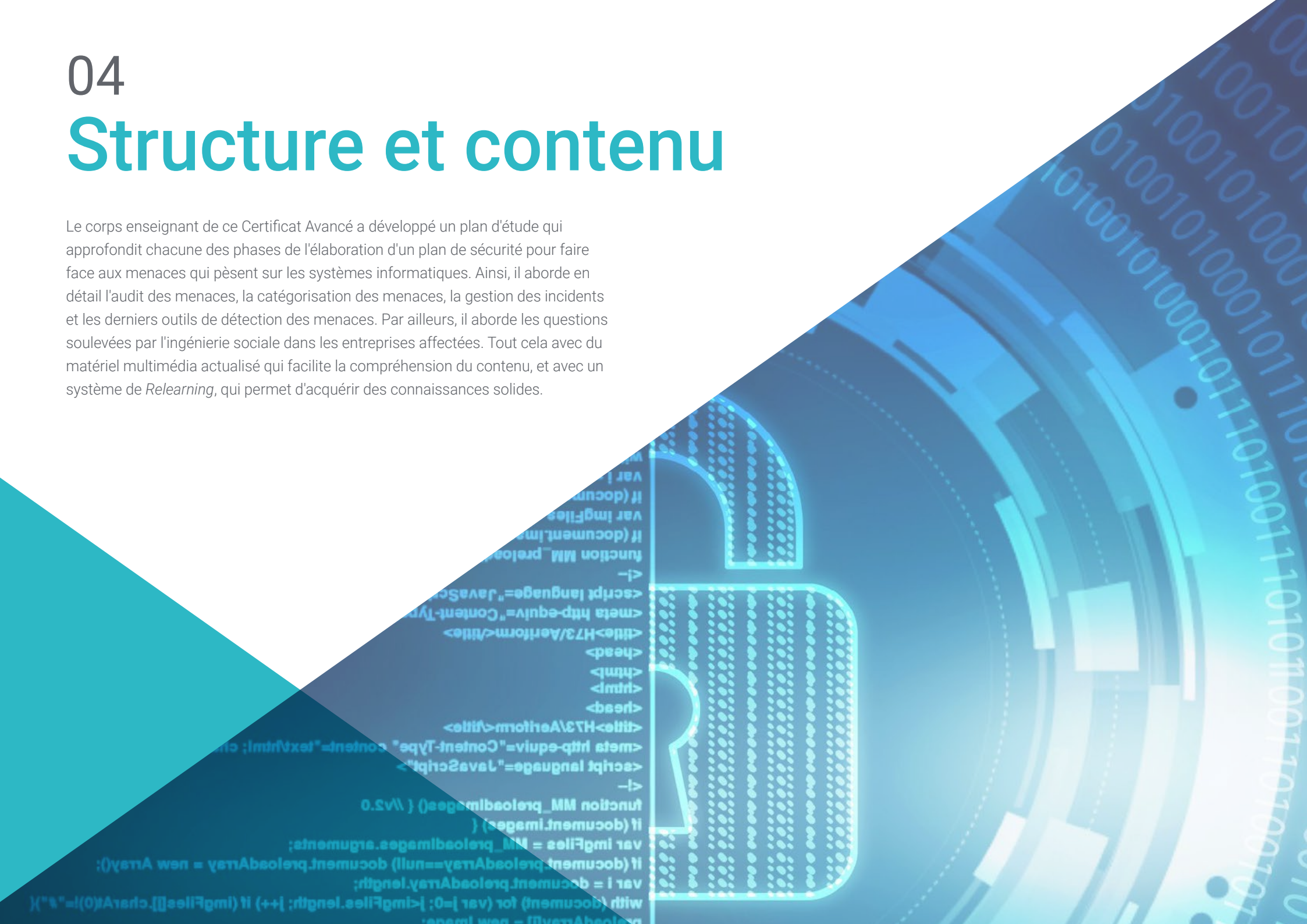
M. Oropesiano Carrizosa, Francisco

- Ingénieur informatique
- Technicien en Micro-informatique, Réseaux et Sécurité à Cas-Training
- Développeur de Services Web, CMS, e-Commerce, UI et UX à Fersa Reparaciones
- Gestionnaire de Services Web, de Contenu, de Courrier et de DNS à Oropesia Web & Network
- Designer Graphique et d'Applications Web à Xarxa Sakai Projectes
- Diplôme en Systèmes Informatiques de l'Université d'Alcalá de Henares
- Master en DevOps: Docker and Kubernetes por Cyber Business Center
- Technicien en Réseau et Sécurité Informatique de l'Université des Iles Baléares
- Certificat en Design Graphique de l'Université Polytechnique de Madrid

04

Structure et contenu

Le corps enseignant de ce Certificat Avancé a développé un plan d'étude qui approfondit chacune des phases de l'élaboration d'un plan de sécurité pour faire face aux menaces qui pèsent sur les systèmes informatiques. Ainsi, il aborde en détail l'audit des menaces, la catégorisation des menaces, la gestion des incidents et les derniers outils de détection des menaces. Par ailleurs, il aborde les questions soulevées par l'ingénierie sociale dans les entreprises affectées. Tout cela avec du matériel multimédia actualisé qui facilite la compréhension du contenu, et avec un système de *Relearning*, qui permet d'acquérir des connaissances solides.



Bénéficiez d'un enseignement 100% en ligne, flexible, qui vous permet d'avancer à votre rythme. Combinez votre vie personnelle avec un enseignement de qualité. Inscrivez-vous dès maintenant"

Module 1. Politiques de Sécurité pour l'Analyse des Menaces des Systèmes Informatiques

1.1. Gestion de Menaces dans les Politique de Sécurité
- 1.1.1. Gestion des risques
- 1.1.2. Risque de sécurité
- 1.1.3. Méthodes de gestion des menaces
- 1.1.4. Implémentation des méthodologies

1.2. Phases de la gestion des menaces
- 1.2.1. Identification
- 1.2.2. Analyses
- 1.2.3. Localisation
- 1.2.4. Mesures de sauvegarde

1.3. Systèmes d'audit pour la localisation des menaces
- 1.3.1. Classification et flux d'informations
- 1.3.2. Analyse des processus vulnérables

1.4. Classification des risques
- 1.4.1. Types de risques
- 1.4.2. Calcul de la probabilité de la menace
- 1.4.3. Risque résiduel

1.5. Traitement du risque
- 1.5.1. Implémentation des mesures de sauvegarde
- 1.5.2. Transfert ou prise en charge

1.6. Maîtrise des risques
- 1.6.1. Processus continu de gestion des risques
- 1.6.2. Implémentation de mesures de sécurité
- 1.6.3. Modèle stratégique de mesures de la sécurité de l'information

1.7. Méthodes pratiques d'analyse et de surveillance des menaces
- 1.7.1. Catalogue des menaces
- 1.7.2. Catalogue des mesures de contrôle
- 1.7.3. Catalogue des mesures de protection

1.8. Norme ISO 27005
- 1.8.1. Identification des risques
- 1.8.2. Analyse des risques
- 1.8.3. Évaluation des risques

1.9. Matrice des risques, incidences et menaces
- 1.9.1. Données, systèmes et personnel
- 1.9.2. Probabilité de la menace
- 1.9.3. Ampleur des dommages

1.10. Phases et processus de conception dans l'analyse des risques
- 1.10.1. Identification des éléments critiques de l'organisation
- 1.10.2. Détermination des menaces et des impacts
- 1.10.3. Analyse des impacts et des risques
- 1.10.4. Méthodologie

Module 2. Politiques de Gestion des Incidents de Sécurité

2.1. Politiques de Gestion des Incidents de Sécurité Informatique et leurs avancées
- 2.1.1. Gestion des incidents
- 2.1.2. Responsabilités et procédures
- 2.1.3. Notification des événements

2.2. Systèmes de détection et prévention des intrusions (IDS/IPS)
- 2.2.1. Données relatives au fonctionnement du système
- 2.2.2. Types de systèmes de détection d'intrusion
- 2.2.3. Critères de localisation des IDS/IPS

2.3. Réponse aux incidents de sécurité
- 2.3.1. Procédure de collecte d'informations
- 2.3.2. Procédure de vérification des intrusions
- 2.3.3. Organismes CERT

2.4. Processus de notification et gestion des tentatives d'intrusion
- 2.4.1. Responsabilité sur le processus de notification
- 2.4.2. Classification des incidents
- 2.4.3. Processus de résolution et de rétablissement

2.5. L'analyse criminalistique en tant que politique de sécurité
- 2.5.1. Preuves volatiles et non volatiles
- 2.5.2. Analyse et collecte de preuves électroniques
  - 2.5.2.1. Analyse des preuves électroniques
  - 2.5.2.2. Collecte de preuves électroniques

2.6. Outils de détection et prévention des intrusions (IDS/IPS)
- 2.6.1. Snort
- 2.6.2. Suricata
- 2.6.3. SolarWinds

2.7. Outils de centralisation des événements
- 2.7.1. SIM
- 2.7.2. SEM
- 2.7.3. SIEM

2.8. Guide de sécurité CCN-STIC 817
- 2.8.1. Gestion des cyberincidents
- 2.8.2. Mesures et indicateurs

2.9. NIST SP800-61
- 2.9.1. Capacité de réponse aux incidents de sécurité Informatique
- 2.9.2. Gestion d'un incident
- 2.9.3. Coordination et partage d'informations

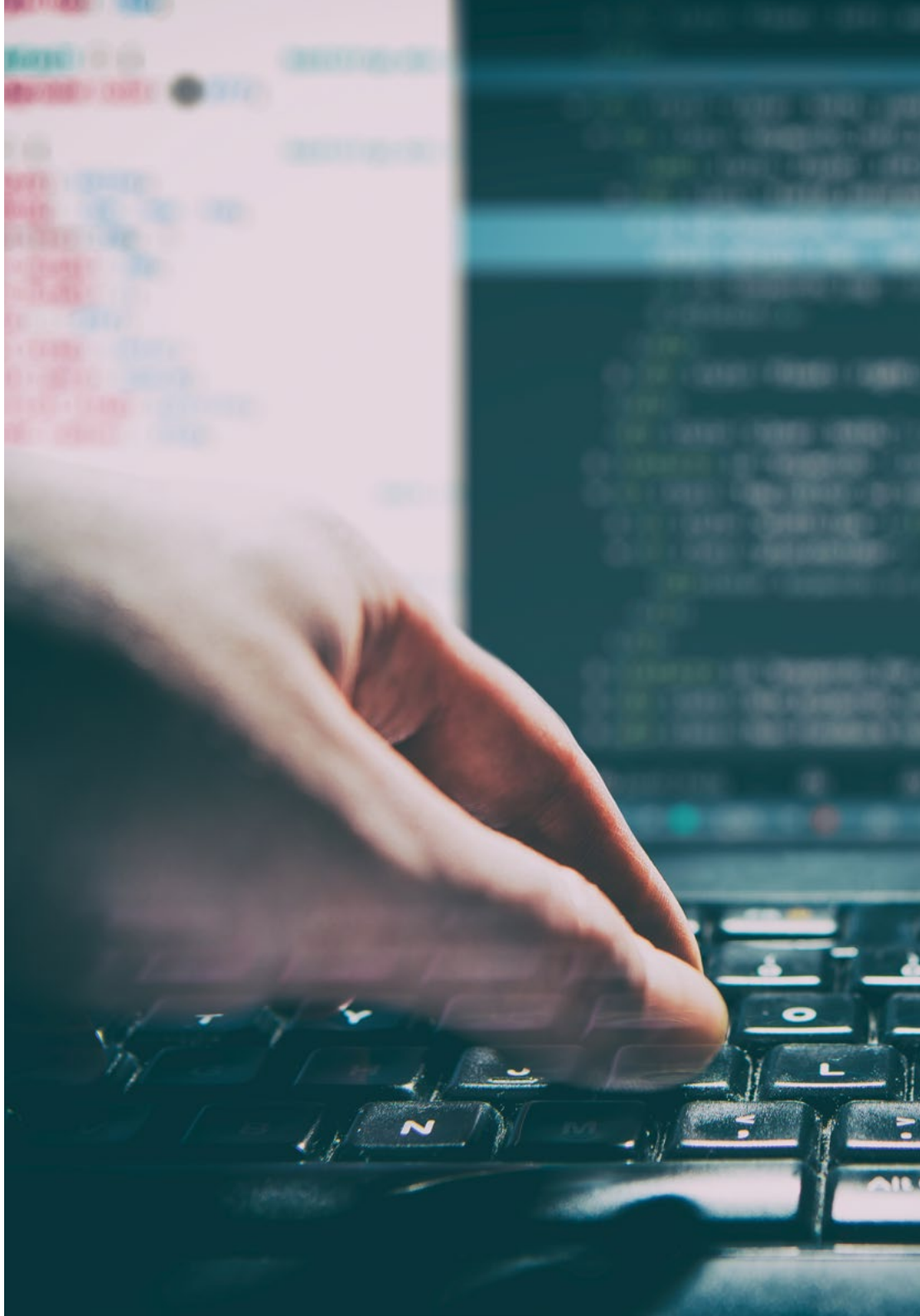
2.10. Norme ISO 27035
- 2.10.1. Norme ISO 27035 Principes de gestion des incidents
- 2.10.2. Lignes directrices pour l'élaboration d'un plan de gestion des incidents
- 2.10.3. Lignes directrices pour une réponse aux incidents

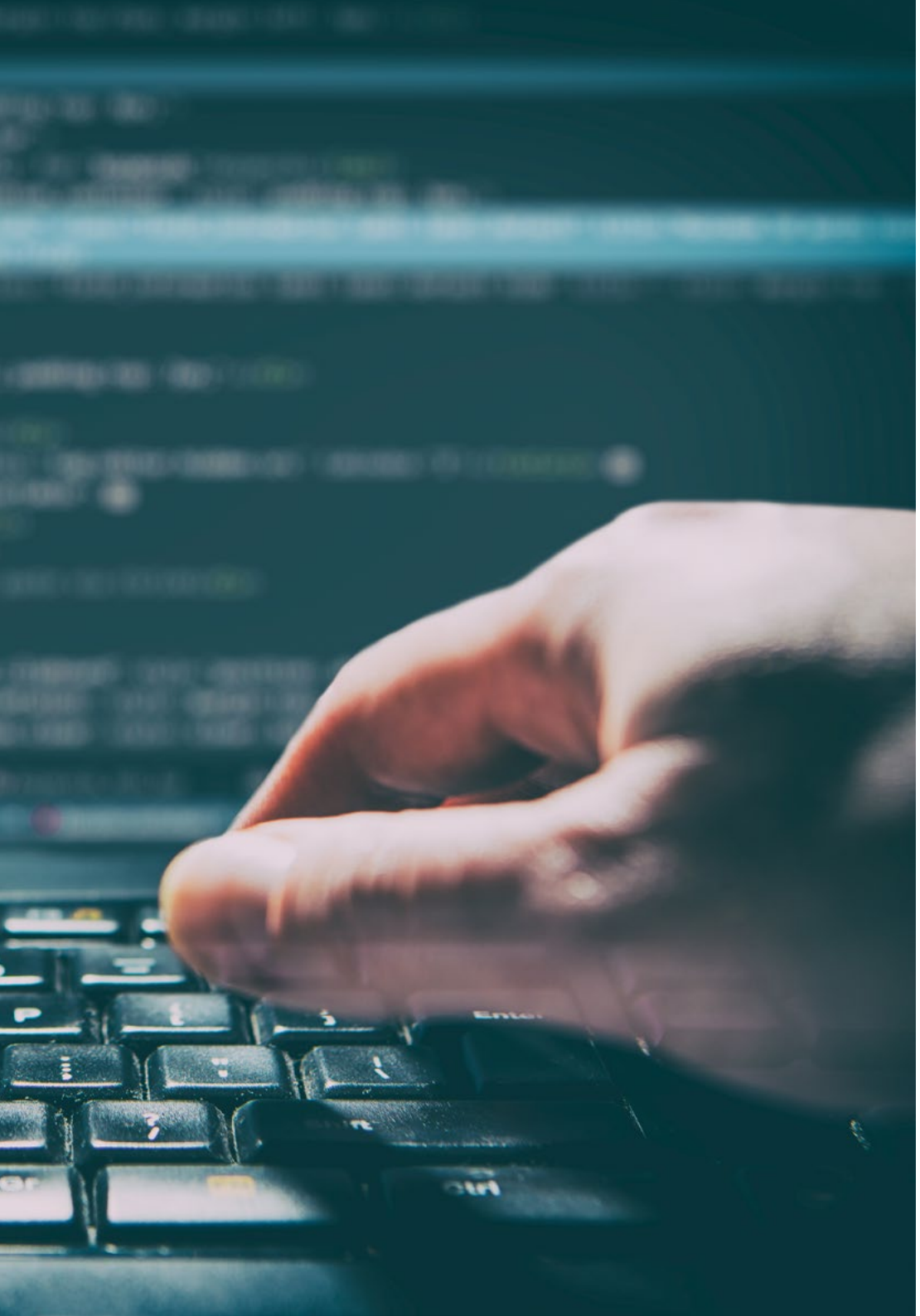
Module 3. Implémentation des Politiques de Sécurité de Software face aux Attaques

3.1. *System Hacking*
- 3.1.1. Risques et vulnérabilités
- 3.1.2. Contre-mesures

3.2. DoS dans les services
- 3.2.1. Risques et vulnérabilités
- 3.2.2. Contre-mesures

3.3. *Session Hijacking*
- 3.3.1. Le processus de *Hijacking*
- 3.3.2. Contre-mesures au *Hijacking*





3.4. Évasion des IDS, *Firewalls and Honeypots*
  3.4.1. Techniques d'évasion
  3.4.2. Implémentation de contre-mesures
3.5. *Hacking Web Servers*
  3.5.1. Attaques contre les serveurs web
  3.5.2. Implémentation de mesures de défense
3.6. *Hacking Web Applications*
  3.6.1. Attaques contre les Application web
  3.6.2. Implémentation de mesures de défense
3.7. *Hacking Wireless Networks*
  3.7.1. Vulnérabilités des réseaux wifi
  3.7.2. Implémentation de mesures de défense
3.8. *Hacking Mobile Platforms*
  3.8.1. Vulnérabilités des plateformes mobiles
  3.8.2. Implémentation de contre-mesures
3.9. *Ramsonware*
  3.9.1. Vulnérabilités à l'origine de *Ramsonware*
  3.9.2. Implémentation de contre-mesures
3.10. Ingénierie sociale
  3.10.1. Types d'ingénierie sociale
  3.10.2. tre-mesures en matière d'ingénierie sociale

Les études de cas et le contenu multimédia sont les outils les plus performants de ce Certificat Avancé. Téléchargez-les dès le premier jour et développez votre carrière professionnelle"

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***.

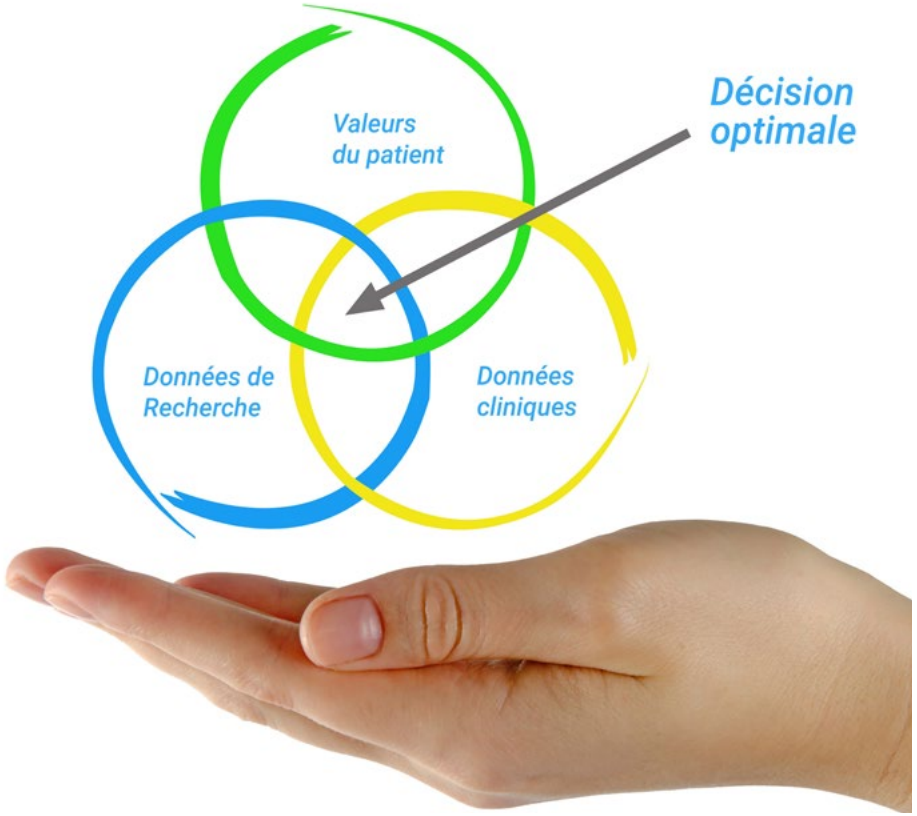
Ce système d'enseignement est utilisé, par exemple, dans les écoles de médecine les plus prestigieuses du monde et a été considéré comme l'un des plus efficaces par des publications de premier plan telles que le ***New England Journal of Medicine.***

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

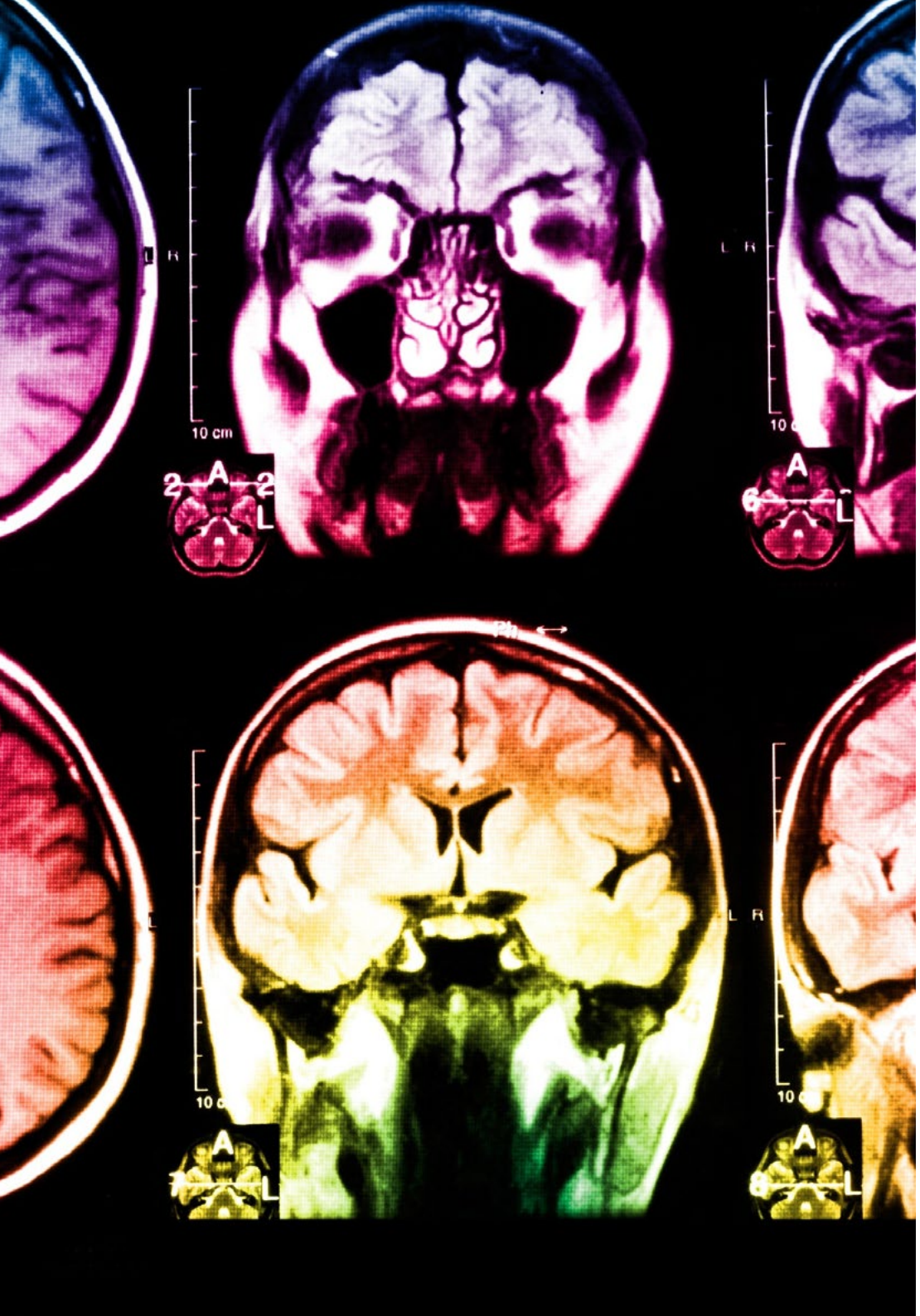
TECH combine efficacement la méthodologie des Études de Cas avec un système d'apprentissage 100% en ligne basé sur la répétition, qui associe différents éléments didactiques dans chaque leçon.

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.

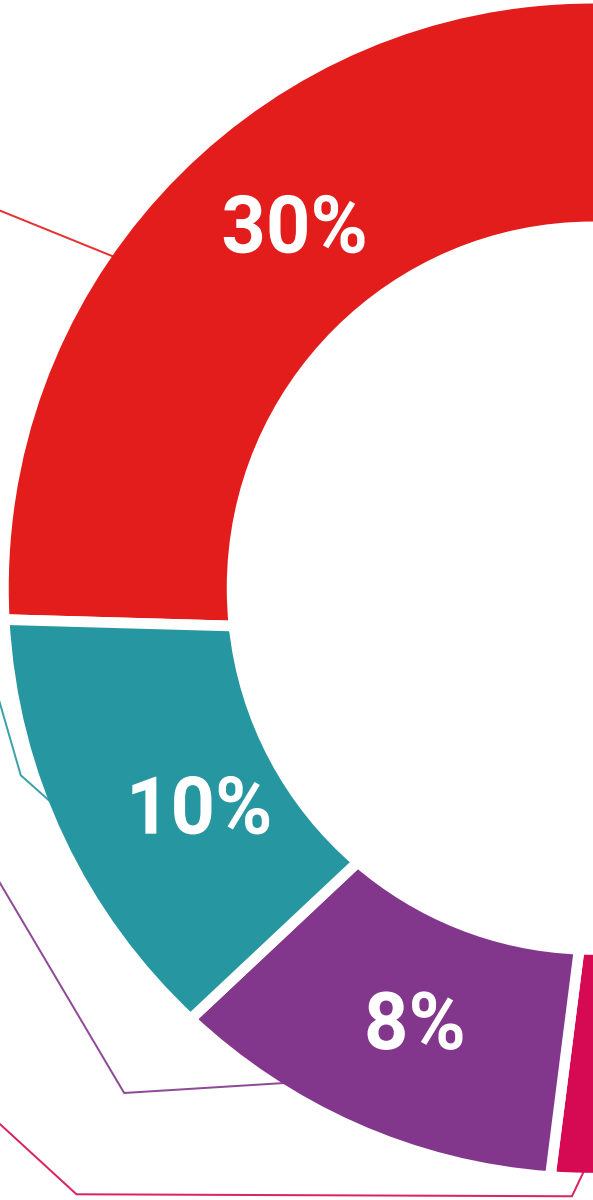
La méthode "Learning from an Expert" renforce les connaissances et la mémoire, et donne confiance dans les futures décisions difficiles.

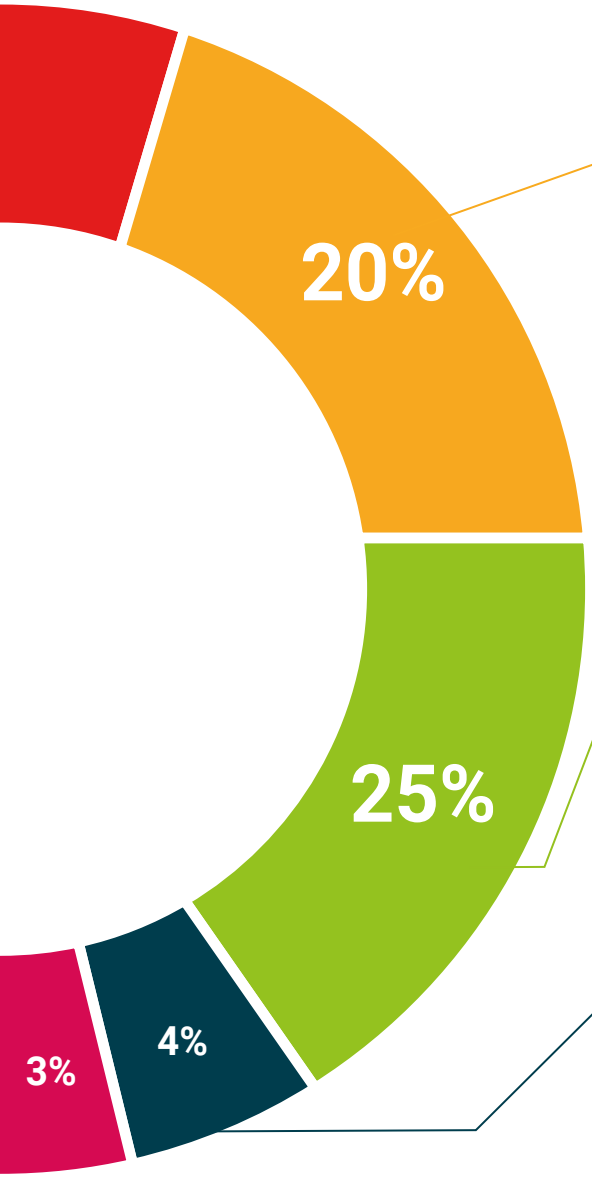
Pratiques en compétences et aptitudes

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 Avancé en Mesures de Défense de Sécurité Informatiques vous garantit, en plus de la formation la plus rigoureuse et la plus actuelle, l'accès à un diplôme universitaire de Certificat Avancé délivré par TECH Université Technologique.

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

Ce **Certificat Avancé en Mesures de Défense de Sécurité Informatiques** contient le programme le plus complet et le plus à jour du marché.

Après avoir réussi l'évaluation, l'étudiant recevra par courrier postal* avec accusé de réception son correspondant diplôme de **Certificat Avancé** délivré par **TECH Université Technologique.**

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

Diplôme: **Certificat Avancé en Mesures de Défense de Sécurité Informatiques**
N.º heures officielles: **450 h.**


tech université technologique

Délivre le présent

DIPLÔME

à

Mme/M. _____, avec nº d'identification _____

Pour avoir finalisé et accrédité avec succès le programme de

CERTIFICAT AVANCÉ

en

Mesures de Défense de Sécurité Informatiques

Il s'agit d'un diplôme spécialisé octroyé par cette Université d'une durée de 450 heures, débutant le dd/mm/aaaa et finalisant le dd/mm/aaaa.

TECH est une Institution Privée d'Enseignement Supérieur reconnue par le Ministère de l'Enseignement Public depuis le 28 juin 2018.

Fait le 17 juin 2020

Pre Tere Guevara Navarro
Rectrice

Code Unique TECH: AFWOR23S techtitute.com/diplômes

*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.

tech université technologique

Certificat Avancé
Mesures de Défense de Sécurité Informatiques

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

Certificat Avancé

Mesures de Défense de Sécurité Informatiques

tech université technologique