Certificat Avancé

Cybersécurité Préventive

tech université technologique

tech université technologique

Certificat Avancé
Cybersécurité Préventive

- 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-cybersecurite-preventive

Sommaire

01

Présentation

L'utilisation des appareils mobiles implique un grand nombre de données dont les programmes ont besoin pour remplir leurs fonctions. Ce type de confiance que les utilisateurs accordent à leur technologie quotidienne signifie qu'ils assument un risque élevé que ces informations soient violées par des cyberattaques. Le développement constant de nouveaux moyens d'obtenir ces données signifie que le développement des systèmes de prévention doit être constant, aller de l'avant et fournir des réponses rapides et efficaces à chaque nouvelle menace. Le spécialiste travaillant dans ce domaine est donc obligé d'actualiser constamment ses connaissances pour qu'elles soient parfaitement à jour, une tâche complexe en raison de la rapidité des changements dans le secteur. Ce programme est la réponse la plus immédiate et la plus qualitative aux besoins de formation en cybersécurité préventive sur le marché de l'enseignement en ligne.

Améliorez vos compétences dans le domaine de la cybersécurité préventive grâce au programme le plus complet et le plus récent dans ce domaine"

Aujourd'hui, aucune entreprise n'est à l'abri d'une cyber-attaque et, par conséquent, des différentes conséquences qu'elle entraîne. Quelle que soit la taille de l'entreprise, elle est exposée au vol d'informations, au chantage, au sabotage, etc. Il est nécessaire de procéder à une évaluation de la vulnérabilité et de déterminer la surface d'attaque. C'est pourquoi des évaluations régulières de la vulnérabilité et des risques sont de plus en plus souvent effectuées. Chaque entreprise devra vérifier si elle respecte les normes et la législation du pays où elle se trouve et être consciente des dommages causés, qu'ils soient monétaires ou non, par exemple à sa réputation.

Ce programme comprend une étude de l'état actuel de l'art en matière de cyberintelligence et de cybersécurité. 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, OSSTM, PTES) et les réglementations actuelles en matière de cybersécurité. Il examine également les organisations internationales les plus pertinentes dans le domaine de la cybersécurité, en expliquant leur champ d'action et leur position sur les différents problèmes.

Tous les développeurs sont confrontés au défi de créer un code d'application de qualité et sécurisé, étant donné que dans l'écosystème d'application actuel, toute vulnérabilité du code ou du système entraînera la perte, l'exposition et le vol de données, ainsi que d'autres problèmes causés par les cyber-attaques. Le développeur a l'obligation de se familiariser avec les différents environnements et phases par lesquels son code passera et de s'assurer qu'il fonctionne, dans chacun d'eux, de la manière la plus efficace et la plus sûre. En outre, ils doivent connaître le les besoins et les dépendances de leur application pour fonctionner et essayer de minimiser l'utilisation de modules et de fonctions, afin de réduire la surface d'attaque. La compréhension des méthodologies et du type de tests à effectuer permettra donc de réduire le temps nécessaire à la résolution des problèmes et à la vérification du code.

Ce **Certificat Avancé en Cybersécurité Préventive** contient le programme académique le plus complet et le plus actuel du marché. Les principales caractéristiques sont les suivantes:

- Le développement de cas pratiques présentés par des experts
- 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 pratiques 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
- La possibilité d'accéder au contenu à partir de n'importe quel appareil fixe ou portable doté d'une connexion internet

Un programme qui vous apprendra à travailler sur la réduction des risques d'attaque et l'optimisation de la résolution des incidents"

Grâce à une approche totalement pratique, ce Certificat Avancé vous permettra d'améliorer vos compétences pour atteindre le niveau d'un spécialiste"

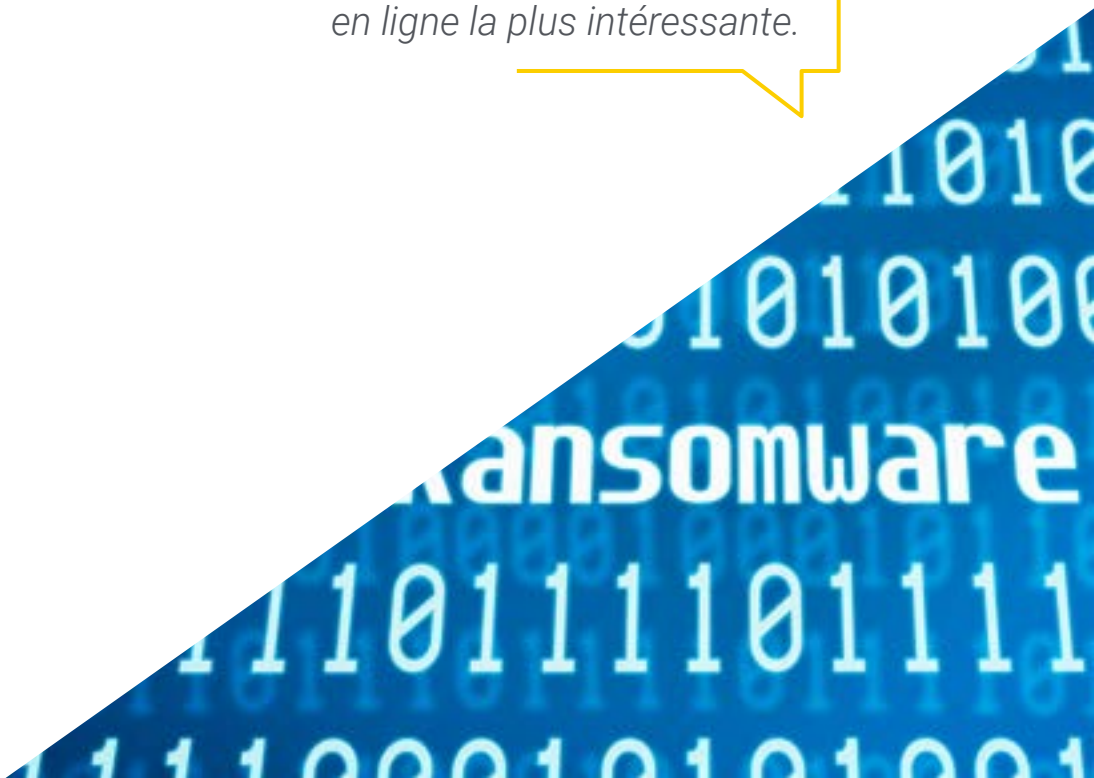
Apprenez à développer un code d'application sécurisé en élaborant des stratégies pour réduire la vulnérabilité.

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

Le programme comprend, dans son corps enseignant, des professionnels du secteur 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 cours académique. Pour ce faire, l'étudiant sera assisté d'un innovant système de vidéos interactives, créé par des experts reconnus.



02

Objectifs

Ce Certificat Avancé renforcera considérablement la capacité d'intervention dans ce domaine. Avec des objectifs réalistes et très intéressants, ce processus d'étude a été configuré pour conduire progressivement les étudiants à l'acquisition des connaissances théoriques et pratiques nécessaires pour intervenir avec qualité, en développant également des compétences transversales qui leur permettront d'affronter des situations complexes en élaborant des réponses ajustées et précises.

Apprenez et appliquez les méthodologies les plus intéressantes en matière de Cybersécurité Préventive et commencez à développer des applications avec les systèmes de prévention les plus efficaces du moment"

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 OSSTM, 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
- Générer des connaissances spécialisées pour l'analyse des SécuritéGénérer des connaissances spécialisées pour réaliser un audit de sécurité
- Analyser les différents systèmes existant
- Évaluer les informations obtenues et développer des mécanismes de prévention et de *Hacking*
- Établir des priorités dans l'étude et la résolution des vulnérabilités
- Démontrer qu'un système est vulnérable, l'attaquer de manière proactive et résoudre ces problèmes
- Déterminer les lignes directrices qu'un bon développeur doit suivre pour répondre aux exigences de sécurité nécessaires
- Établir une méthodologie appropriée pour le développeur et pour l'environnement de production
- Spécifier les tests à effectuer sur le logiciel développé

Objectifs spécifiques

Module 1. Cyber intelligence et cybersécurité

- 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, OSSTM, 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

Module 2. Hacking éthique

- Examiner les méthodes IOSINT
- Rassembler les informations disponibles dans les médias publics
- Analyse des réseaux pour trouver des informations sur le mode actif
- Développer des laboratoires d'essai
- Analyser les performances des outils de *Pentesting*
- Cataloguer et évaluer les différentes vulnérabilités des systèmes
- Concrétiser les différentes méthodologies de *Hacking*

Module 3. Développement sécurisé

- Établir les exigences nécessaires au bon fonctionnement d'une application de manière sécurisée
- Examinez les fichiers de Logs pour comprendre les messages d'erreur
- Analyser les différents événements et décider ce qui doit être montré à l'utilisateur et ce qui doit être conservé dans les *Logs*
- Générer un code de qualité, aseptisé et facilement vérifiable
- Évaluer la documentation appropriée pour chaque phase de développement
- Concrétiser le comportement du serveur pour optimiser le système
- Développer un code modulaire, réutilisable et facile à maintenir

Vous apprendrez à optimiser les systèmes en appliquant des exigences qui permettront d'améliorer la sécurité et la convivialité des applications"

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 cours 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.

Mettez votre apprentissage entre les mains de professionnels experts qui vous guideront à travers 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 Techonologies. E-Council. Madrid


SHARE
HTML
JUST MAKE THE BEST THINGS!
CREATIVE
LAYOUT
CONTENT

04

Structure et contenu

Ce programme vous permettra d'étudier chacun des domaines de connaissances que le professionnel de la cybersécurité doit connaître dans le domaine de l'action préventive. À cette fin, il a été structuré en vue de l'acquisition efficace de connaissances sommatives, qui faciliteront la pénétration de l'apprentissage et consolideront ce qui a été étudié, en donnant aux étudiants la capacité d'intervenir le plus rapidement possible. Un cours de haute intensité et de haute qualité créé pour former les meilleurs du secteur.

L'analyse et l'intervention préventives en matière de cybersécurité développées de manière structurée dans une démarche d'étude axée sur l'efficacité"

Module 1. Cyber intelligence et cybersécurité

1.1. Cyber intelligence
- 1.1.1. Cyber intelligence
- 1.1.2. Intelligence
  - 1.1.2.1. Cycle du renseignement
  - 1.1.2.2. Cyber intelligence
  - 1.1.2.3. Cyber intelligence et cybersécurité
- 1.1.3. L'analyste d' Intelligence
  - 1.1.3.1. Le rôle de l'analyste du renseignement
  - 1.1.3.2. 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

Module 2. Hacking Étique

2.1. Environnement de travail
  2.1.1. Distributions de Linux
    2.1.1.1. Kali Linux - Sécurité offensive
    2.1.1.2. Parrot OS
    2.1.1.3. Ubuntu
  2.1.2. Systèmes de virtualisation
  2.1.3. Sandbox
  2.1.4. Déploiement des laboratoires
2.2. Méthodologies
  2.2.1. OSSTMM
  2.2.2. OWASP
  2.2.3. NIST
  2.2.4. PTES
  2.2.5. ISSAF
2.3. Footprinting
  2.3.1. Renseignement de source ouverte (OSINT)
  2.3.2. Recherche de violations de données et de vulnérabilités
  2.3.3. Utilisation d'outils passifs
2.4. Analyse du réseau
  2.4.1. Outils d'analyse
    2.4.1.1. Nmap
    2.4.1.2. Hping3
    2.4.1.3. Autres outils d'analyse
  2.4.2. Techniques de balayage
  2.4.3. Techniques de contournement des *firewalls* et des IDS
  2.4.4. Banner*grabbing*
  2.4.5. Diagrammes de réseau
2.5. Énumération
  2.5.1. Énumération SMTP
  2.5.2. Énumération DNS
  2.5.3. Énumération NetBIOS et Samba
  2.5.4. Énumération LDAP
  2.5.5. Énumération SNMP
  2.5.6. Autres techniques d' Énumération
2.6. Analyse de vulnérabilité
  2.6.1. Solutions d'analyse de vulnérabilité
    2.6.1.1. Qualys
    2.6.1.2. Nessus
    2.6.1.3. CFI LanGuard
  2.6.2. Systèmes d'évaluation des vulnérabilités
    2.6.2.1. CVSS
    2.6.2.2. CVE
    2.6.2.3. NVD

2.7. Attaques contre les réseaux sans fil
- 2.7.1. Méthodologie de *hacking* dans les réseaux sans fil
  - 2.7.1.1. WiFi *discovery*
  - 2.7.1.2. Analyse du trafic
  - 2.7.1.3. Attaques d'*aircrack*
    - 2.7.1.3.1. Attaques WEP
    - 2.7.1.3.2. Attaques WPA/WPA2
  - 2.7.1.4. Attaques de Evil Twin
  - 2.7.1.5. Attaques a WPS
  - 2.7.1.6. *Jamming*
- 2.7.2. Outils pour la sécurité sans fil

2.8. Hacking de serveurs web
- 2.8.1. *Cross site Scripting*
- 2.8.2. CSRF
- 2.8.3. *Session Hijacking*
- 2.8.4. SQL *injection*

2.9. Exploitation des vulnérabilités
- 2.9.1. Utilisation d'*Exploits*connus
- 2.9.2. Utilisation des*metasploit*
- 2.9.3. Utilisation de *malware*
  - 2.9.3.1. Définition et portée
  - 2.9.3.2. Génération de *malware*
  - 2.9.3.3. Bypass des solutions anti-virus

2.10. Persistance
- 2.10.1. Installation de*Rootkits*
- 2.10.2. Utilisation de Ncat
- 2.10.3. Utilisation des tâches planifiées pour les*Backdoors*
- 2.10.4. Création d'utilisateurs
- 2.10.5. Détection des HIDS

Module 3. Développement sécurisé

3.1. Développement sécurisé
- 3.1.1. Qualité, fonctionnalité et sécurité
- 3.1.2. Confidentialité, intégrité et disponibilité
- 3.1.3. Cycle de vie du développement du software

3.2. Phase des exigences
- 3.2.1. Contrôle de l'authentification
- 3.2.2. Contrôle des rôles et des privilèges
- 3.2.3. Exigences axées sur le risque
- 3.2.4. Approbation des privilèges

3.3. Phases d'analyse et de conception
- 3.3.1. Accès aux composants et administration du système
- 3.3.2. Pistes de contrôle
- 3.3.3. Gestion des sessions
- 3.3.4. Données historiques
- 3.3.5. Traitement approprié des erreurs
- 3.3.6. Séparation des fonctions

3.4. Phase de mise en œuvre et de codage
- 3.4.1. Sécuriser l'environnement de développement
- 3.4.2. Élaboration de la documentation technique
- 3.4.3. Codage sécurisé
- 3.4.4. Communications sécurisées

3.5. Bonnes pratiques de codage sécurisé
- 3.5.1. Validation des données d'entrée
- 3.5.2. Codage des données de sortie
- 3.5.3. Style de programmation
- 3.5.4. Traitement du journal des modifications
- 3.5.5. Pratiques cryptographiques
- 3.5.6. Gestion des erreurs et des journaux
- 3.5.7. Gestion des fichiers
- 3.5.8. Gestion de la mémoire
- 3.5.9. Standardisation et réutilisation des fonctions de sécurité

3.6. Préparation du serveur et*hardening*
- 3.6.1. Gestion des utilisateurs, des groupes et des rôles sur le serveur
- 3.6.2. Installation du software
- 3.6.3. *Hardening*du serveur
- 3.6.4. Configuration robuste de l'environnement de l'application

3.7. Préparation de la BBDD et*hardening*
- 3.7.1. Optimisation du moteur BBDD
- 3.7.2. Création d'un utilisateur propre pour l'application
- 3.7.3. Attribuer les privilèges nécessaires à l'utilisateur
- 3.7.4. *Hardening*de la BBDD

3.8. Phase de test
- 3.8.1. Contrôle de la qualité des contrôles de sécurité
- 3.8.2. Inspection progressive du code
- 3.8.3. Contrôle de la gestion de la configuration
- 3.8.4. Tests en boîte noire

3.9. Préparation de la transition vers la production
- 3.9.1. Effectuer le contrôle des changements
- 3.9.2. Effectuer la procédure de changement de production
- 3.9.3. Effectuer une procédure de*rollback*
- 3.9.4. Essais de pré-production

3.10. Phase de maintenance
- 3.10.1. Sécuriser fondée sur le risque
- 3.10.2. Tests de maintenance de la sécurité en boîte blanche
- 3.10.3. Test de maintenance de la sécurité z boîte noire

Un programme à fort impact sur vos compétences qui vous permettra d'intervenir efficacement en matière de cybersécurité préventive avec des moyens de pointe"

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

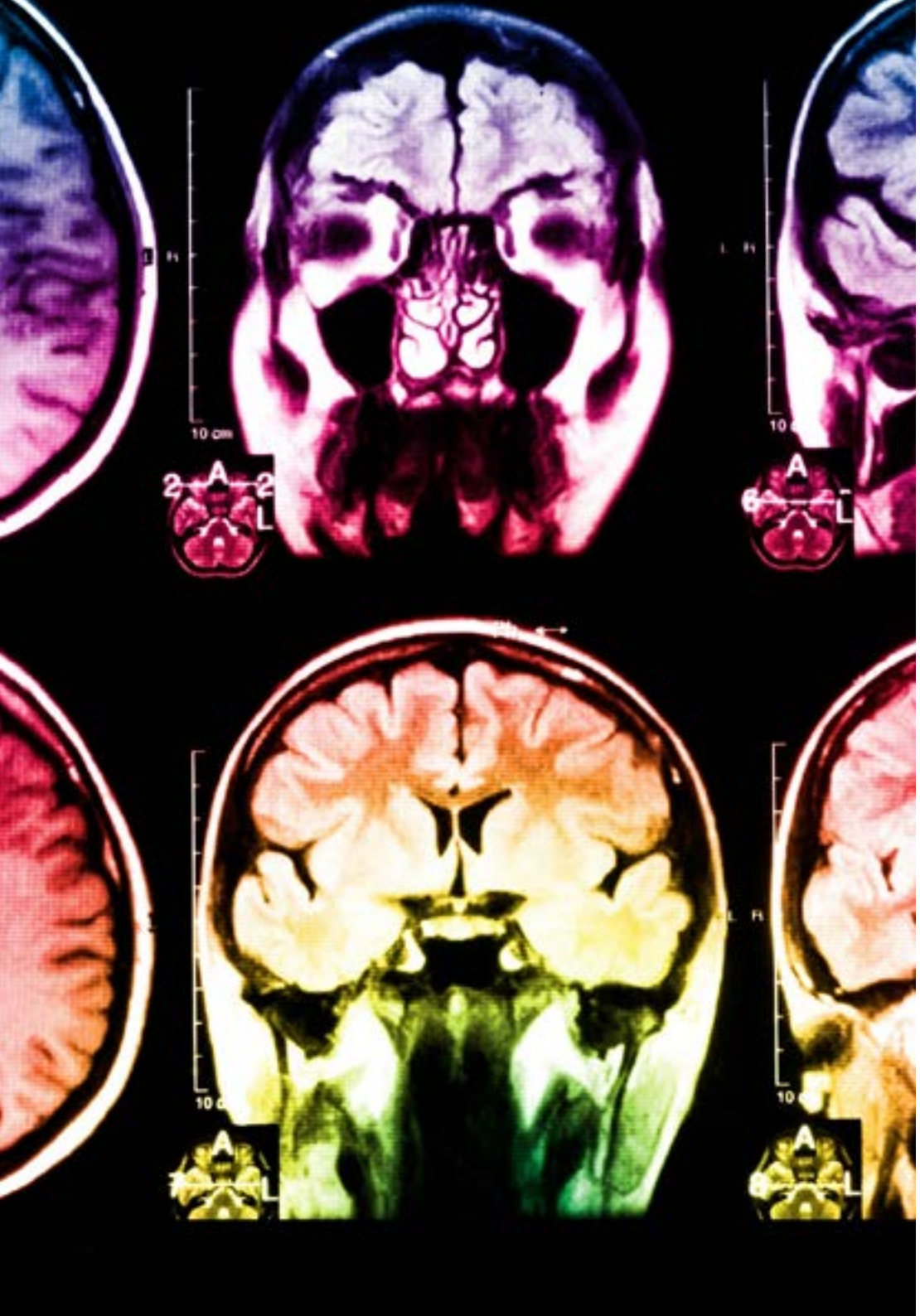
TECH combine efficacement la méthodologie des Études de Cas avec un système d'apprentissage 100% en ligne basé sur la répétition, qui associe différents éléments didactiques dans chaque leçon.

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.

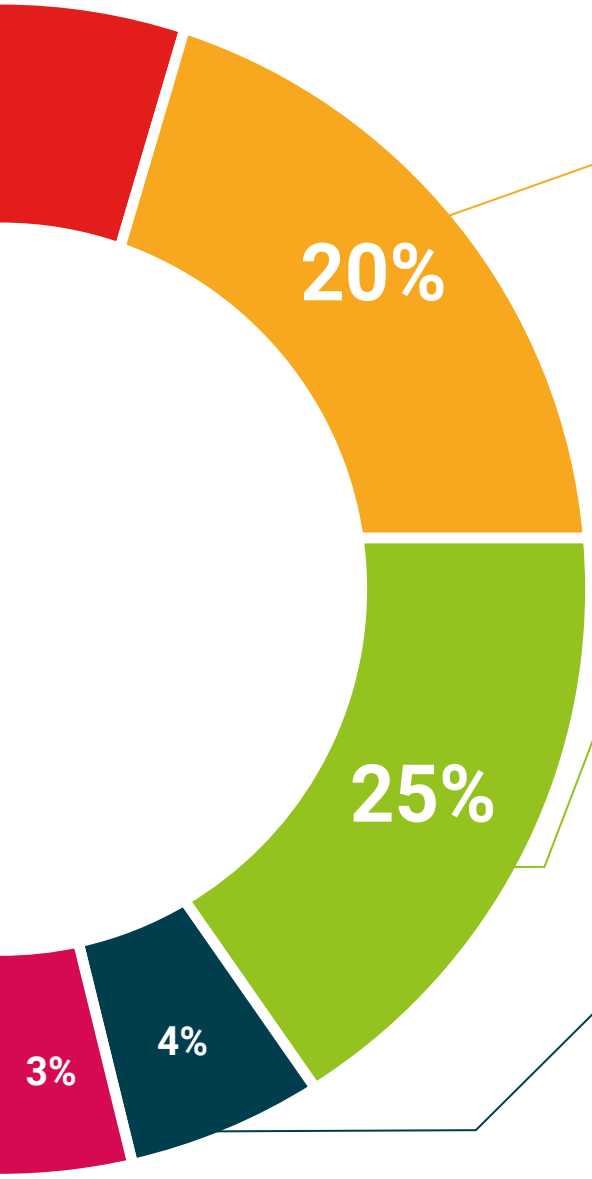
La méthode "Learning from an Expert" renforce les connaissances et la mémoire, et donne confiance dans les futures décisions difficiles.

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 Cybersécurité Préventive 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 sans avoir à vous soucier des contraintes de déplacements ou des formalités administratives”

Ce **Certificat Avancé en Cybersécurité Préventive** 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 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 Cybersécurité Préventive**

N.º d'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

Cybersécurité Préventive

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

Ce diplôme doit impérativement être accompagné d'un diplôme universitaire reconnu par les autorités compétentes afin d'exercer la profession dans chaque pays.

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
Cybersécurité Préventive

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

Certificat Avancé

Cybersécurité Préventive

tech université technologique