Certificat Avancé

Cybersécurité Corrective et Expertise Forensique

tech université technologique

tech université technologique

Certificat Avancé
Cybersécurité Corrective et Expertise Forensique

- 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-corrective-expertise-forensique

Sommaire

01

Présentation

Dans un monde qui change et évolue chaque jour, avec des technologies qui apparaissent et sont adoptées rapidement sans être mûres, nous devons être prêts à relever de nombreux défis et à prévoir l'impact qu'ils auront sur la société. Ce programme forme des ingénieurs informaticiens à enquêter sur un incident de cybersécurité une fois qu'il s'est produit, en leur fournissant les connaissances et les mécanismes nécessaires pour obtenir, analyser et rendre compte de toutes leurs découvertes. À partir du moment où un médecin légiste découvre un scénario et décide, de manière non destructive, d'acquérir les preuves, il a besoin de directives pour mettre en relation les données obtenues de différentes sources et parvenir à des conclusions irréfutables.

Acquérir la capacité de donner les clés d'un incident de cybersécurité grâce aux connaissances les plus récentes en matière d'expertise judiciaire dans ce domaine"

Dans l'environnement informatique, il existe différentes motivations qui conduisent à l'application de différentes techniques d'ingénierie inverse afin de comprendre et de connaître suffisamment un software, un protocole de communication ou un algorithme.

L'une des applications les plus connues de la rétro-ingénierie est l'analyse de *malware* qui, par le biais de différentes techniques telles que le *sandboxing*, permet de comprendre et de connaître le logiciel malveillant étudié et, par conséquent, de développer des logiciels capables de le détecter et de le contrer, comme dans le cas des logiciels antivirus qui fonctionnent par signatures.

Parfois, la vulnérabilité ne se trouve pas dans le code source, mais est introduite par le compilateur qui génère le code machine. La connaissance de la rétro-ingénierie et, par conséquent, de la façon dont nous obtenons le code machine nous permettra de détecter ces vulnérabilités.

Il est nécessaire de connaître les différents scénarios, de comprendre les différentes technologies et d'être capable de les expliquer dans différentes langues en fonction du public cible du rapport en question. Le nombre de crimes différents qu'un expert médico-légal aura à traiter signifie qu'il doit faire preuve d'expertise, de perspicacité et de sérénité pour entreprendre cette tâche extrêmement importante, car le verdict d'un procès peut dépendre de sa bonne exécution.

Les professionnels de ce secteur doivent avoir une vision large et périphérique afin de détecter non seulement les avantages de ces technologies, mais aussi les dommages qu'elles peuvent causer. Ce programme prépare les étudiants à comprendre ce qui est à venir, comment cela peut affecter les professions actuelles, la façon dont elles sont pratiquées et ce qui peut arriver dans un avenir parfois incertain.

Ce **Certificat Avancé en Cybersécurité Corrective et Expertise Forensique** 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 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 aux contenus depuis n'importe quel appareil fixe ou portable doté d'une connexion internet

Comprenez les principes fondamentaux et le mode opératoire du malware comme base pour créer des voies d'adaptation très efficaces"

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

Un apprentissage qui vous permettra de travailler en tant qu'expert judiciaire en cybersécurité, dans le domaine juridique.

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

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.

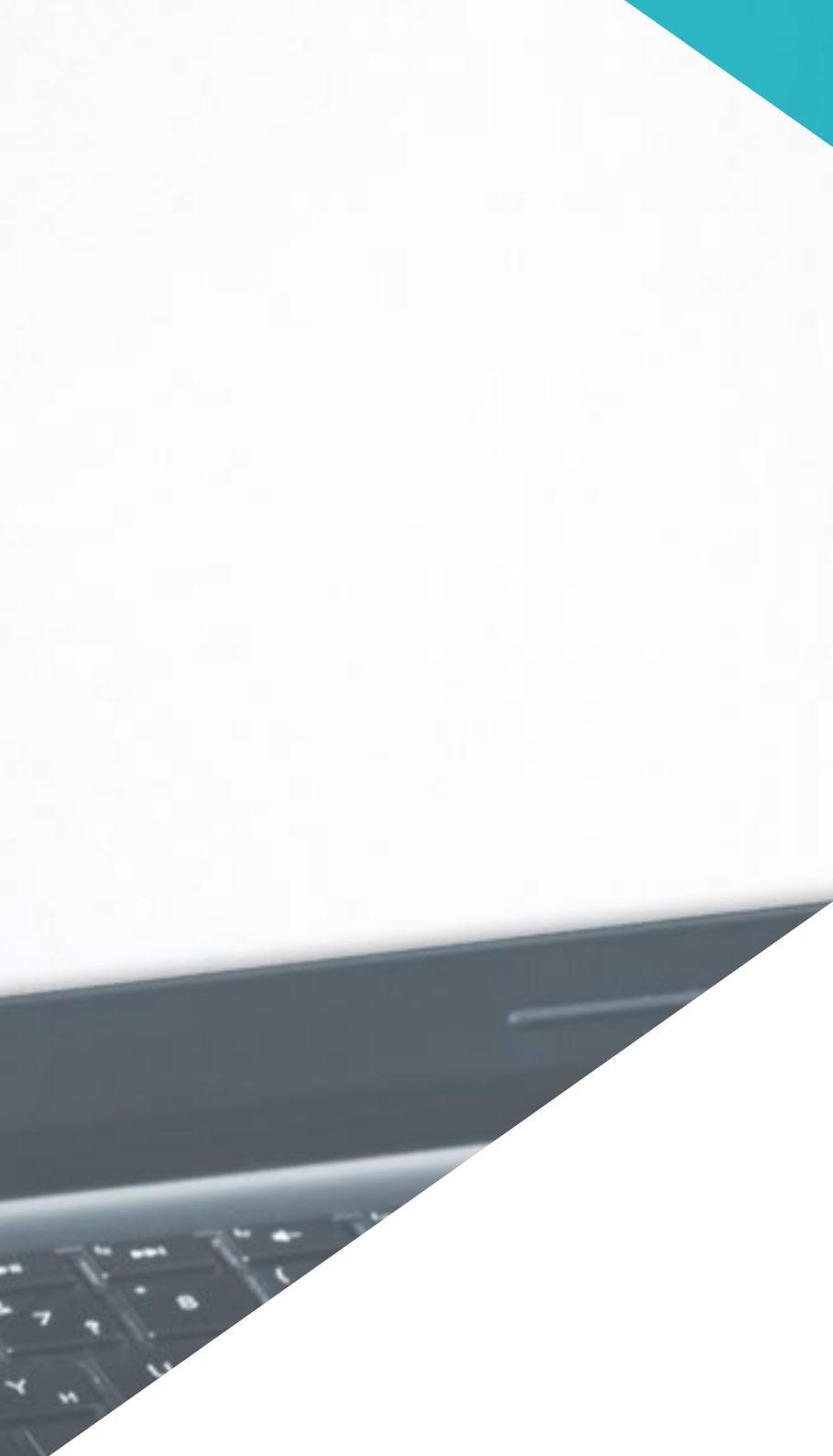
Grâce à son contenu multimédia développé avec les dernières technologies éducatives, les spécialistes bénéficieront d'un apprentissage situé et contextuel. Ainsi, ils se formeront dans un environnement simulé qui leur permettra d'apprendre en immersion et de s'entrainer dans des situations réelles.

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, l'étudiant sera assisté d'un innovant système de vidéos interactives, créé par des experts reconnus.

02

Objectifs

Ce Certificat Avancé renforce la capacité des étudiants à intervenir dans ce domaine, rapidement et facilement. 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.



Une formation intensive en Cybersécurité Corrective et Forensique qui vous permettra d'élargir votre champ d'action dans un domaine riche en possibilités d'emploi"

Objectifs généraux

- Analyser l'ingénierie inverse et les différentes techniques
- Examiner les différentes architectures et leur incidence sur la rétroconception
- Déterminer dans quelles conditions utiliser les différentes techniques de rétro-ingénierie
- Appliquer l'ingénierie inverse à l'environnement de cybersécurité
- Rassembler toutes les preuves et données existantes pour réaliser un rapport médico-légal
- Analyser les données et les corréler de manière appropriée
- Préservation les preuves pour réaliser un rapport médico-légal
- Présenter correctement le rapport médico-légal
- Analyser l'état actuel et futur de la sécurité informatique
- Examiner les risques des nouvelles technologies émergentes
- Compiler les différentes technologies en relation avec la sécurité informatique

Objectifs spécifiques

Module 1. Ingénierie inverse

- Analyser les phases d'un compilateur
- Examiner l'architecture des processeurs x86 et l'architecture des processeurs ARM
- Déterminer les différents types d'analyse
- Appliquer le *Sandboxing* dans différents environnements
- Développer différentes techniques d'analyse des *Malware*
- Mettre en place des outils orientés vers l'analyse des *Malware*

Module 2. Analyse médico-légale

- Identifier les différents éléments de preuve d'un crime
- Générer des connaissances spécialisées pour obtenir des données de différents supports avant qu'elles ne soient perdues
- Récupération de données qui ont été intentionnellement supprimées
- Analyser les registres et les Logs du système
- Déterminer comment les données sont dupliquées afin de ne pas altérer les originaux
- Les preuves à l'appui doivent être cohérentes
- Générer un rapport robuste et homogène
- Présenter les résultats de manière cohérente
- Déterminer comment défendre le rapport auprès de l'autorité compétente
- Définir des stratégies pour rendre le télétravail sûr et sécurisé

Module 3. Défis actuels et futurs en matière de sécurité de l'information

- Examiner l'utilisation des crypto-monnaies, leur impact sur l'économie et la sécurité
- Analyser la situation des utilisateurs et le degré d'illettrisme numérique
- Déterminer le champ d'utilisation de la *blockchain*
- Présentation des alternatives à l'IPv4 dans l'adressage des réseaux
- Développer des stratégies pour éduquer la population sur l'utilisation correcte des technologies
- Générer des connaissances spécialisées pour relever les nouveaux défis en matière de sécurité et prévenir l'usurpation d'identité
- Définir des stratégies pour rendre le télétravail sûr et sécurisé

Acquiert la compétence pour préparer et soumettre un rapport complet et de qualité à l'autorité compétente"

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 experts en 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 des 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

Professeurs

M. Redondo, Jesus Serrano

- Développeur FrontEnd junior et technicien junior en cybersécurité
- Développeur FrontEnd chez Telefónica, Madrid
- Développeur FrontEnd. Best Pro Consulting SL, Madrid
- Installateur d'équipements et de services de télécommunications Groupe Zener, Castilla et Leon
- Installateur d'équipements et de services de télécommunications Licence en Comunication SL, Castilla et Leon
- Certificat en Sécurité Informatique. CFTIC Getafe, Madrid
- Technicien Supérieur: Systèmes de Télécommunications et d'Informatique. IES Trinidad Arroyo, Palence
- Technicien Supérieur: Installations Électrotechniques MT et BT. IES Trinidad Arroyo, Palence
- Formation en Ingénierie Inverse, sténographie, cryptage. Académie Hacker Incibe (Talents Incibe)

Un parcours de développement professionnel stimulant, conçu pour maintenir votre intérêt et votre motivation tout au long de la formation"

04

Structure et contenu

Ce Certificat Avancé est une analyse complète de chacun des domaines de connaissances que le professionnel de la cybersécurité doit connaître dans le domaine de la cybersécurité corrective et de l'expertise judiciaire. 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.

Tous les concepts de l'assainissement de la cybersécurité et de l'expertise judiciaire sont développés de manière structurée dans une approche d'étude axée sur l'efficacité"

Module 1. Ingénierie inverse

1.1. Compilateurs
- 1.1.1. Types de codes
- 1.1.2. Phases du compilateur
- 1.1.3. Table des symboles
- 1.1.4. Gestionnaire d'erreurs
- 1.1.5. Compilateur GCC

1.2. Types d'analyse de compilateur
- 1.2.1. Analyse lexicale
  - 1.2.1.1. Terminologie
  - 1.2.1.2. Composants lexicaux
  - 1.2.1.3. LEX analyseur lexical
- 1.2.2. Analyse syntaxique
  - 1.2.2.1. Grammaires sans contexte
  - 1.2.2.2. Types d'analyse syntaxique
    - 1.2.2.2.1. Analyse syntaxique descendante
    - 1.2.2.2.2. Analyse ascendante
  - 1.2.2.3. Arbres syntaxiques et dérivations
  - 1.2.2.4. Types d'analyseurs syntaxiques
    - 1.2.2.4.1. Analyseurs LR (*Left to Right*)
    - 1.2.2.4.2. Analyseurs LALR
- 1.2.3. Analyse sémantique
  - 1.2.3.1. Grammaires d'attributs
  - 1.2.3.2. Attributs S
  - 1.2.3.3. L-attributs

1.3. Structures de données de l'assemblage
- 1.3.1. Variables
- 1.3.2. Arrays
- 1.3.3. Pointeurs
- 1.3.4. Structures
- 1.3.5. Objets

1.4. Structures du code d'assemblage
- 1.4.1. Structures de sélection
  - 1.4.1.1. If, else if, Else
  - 1.4.1.2. *Switch*
- 1.4.2. Structures d'itération
  - 1.4.2.1. *For*
  - 1.4.2.2. *While*
  - 1.4.2.3. Utilisation du *break*
- 1.4.3. Fonctions

1.5. Architecture Hardware x86
- 1.5.1. Architecture des processeurs x86
- 1.5.2. Structures de données x86
- 1.5.3. Structures de code x86

1.6. Architecture Hardware ARM
- 1.6.1. Architecture des processeurs ARM
- 1.6.2. Structures de données ARM
- 1.6.3. Structures de code ARM

1.7. Analyse du code statique
- 1.7.1. Démonteurs
- 1.7.2. IDA
- 1.7.3. Reconstructeurs de codes

1.8. Analyse dynamique du code
- 1.8.1. Analyse comportementale
  - 1.8.1.1. Communications
  - 1.8.1.2. Suivi
- 1.8.2. Débogueurs de code Linux
- 1.8.3. Débogueurs de code Windows

1.9. *Sandbox*
- 1.9.1. Architecture de type *Sandbox*
- 1.9.2. Évasion de type *Sandbox*
- 1.9.3. Techniques de détection
- 1.9.4. Techniques d'évasion
- 1.9.5. Contre-mesures
- 1.9.6. *Sandbox* en Linux
- 1.9.7. *Sandbox* en Windows
- 1.9.8. *Sandbox* en MacOS
- 1.9.9. *Sandbox* en android

1.10. Analyse du *Malware*
- 1.10.1. Méthodes d'analyse du *Malware*
- 1.10.2. Techniques d'obscurcissement du *Malware*
  - 1.10.2.1. Obfuscation des exécutables
  - 1.10.2.2. Restriction des environnements d'exécution
- 1.10.3. Outils d'analyse du *Malware*

Module 2. Analyse médico-légale

2.1. Acquisition et réplication des données
- 2.1.1. Acquisition de données volatiles
  - 2.1.1.1. Informations sur le système
  - 2.1.1.2. Informations sur le réseau
  - 2.1.1.3. Ordre de volatilité
- 2.1.2. Acquisition de données statiques
  - 2.1.2.1. Création d'une image dupliquée
  - 2.1.2.2. Préparation d'un document pour la chaîne de contrôle
- 2.1.3. Méthodes de validation des données acquises
  - 2.1.3.1. Méthodes pour Linux
  - 2.1.3.2. Méthodes pour Windows

2.2. Évaluation et défaite des techniques anti-forensic
- 2.2.1. Objectifs des techniques anti-forensic
- 2.2.2. Effacement des données
  - 2.2.2.1. Effacement des données et des fichiers
  - 2.2.2.2. Récupération de fichiers
  - 2.2.2.3. Récupération de partitions supprimées
- 2.2.3. Protection du mot de passe
- 2.2.4. Stéganographie
- 2.2.5. Suppression sécurisée des dispositifs
- 2.2.6. Cryptage

2.3. Analyse médico-légale du système d'exploitation
- 2.3.1. Analyse légale de Windows
- 2.3.2. Analyse légale de Linux
- 2.3.3. Analyse médico-légale de Mac

2.4. Analyse légale de sur le réseau
- 2.4.1. Analyse des *LOGs*
- 2.4.2. Corrélation des données
- 2.4.3. Recherche sur le réseau
- 2.4.4. Étapes à suivre dans l'analyse criminelle du réseau

2.5. Analyse médico-légale Web
- 2.5.1. Enquête sur les attaques sur Internet
- 2.5.2. Détection des attaques
- 2.5.3. Localisation de l'adresse IP

2.6. Analyse médico-légale de la base de données
- 2.6.1. Analyse médico-légale MSSQL
- 2.6.2. Analyse médico-légale MySql
- 2.6.3. Analyse médico-légale PostgreSQL
- 2.6.4. Analyse médico-légale MongoDB

2.7. Analyse médico-légale en Cloud
- 2.7.1. Types d'infrastructures en Cloud
  - 2.7.1.1. Cloud comme sujet
  - 2.7.1.2. Cloud comme objet
  - 2.7.1.3. Cloud comme outil
- 2.7.2. Défis des analyses forensiques en Cloud
- 2.7.3. Enquête sur les services de stockage en Cloud
- 2.7.4. Outils d'analyse médico-légale pour Cloud

2.8. Enquêtes sur les crimes commis par courrier électronique
- 2.8.1. Systèmes de courrier
  - 2.8.1.1. Clients de messagerie
  - 2.8.1.2. Serveur de messagerie
  - 2.8.1.3. Serveur SMTP
  - 2.8.1.4. Serveur POP3
  - 2.8.1.5. Serveur IMAP4
- 2.8.2. Serveur IMAP4
- 2.8.3. Message de courrier
  - 2.8.3.1. En-têtes standard
  - 2.8.3.2. En-têtes étendus
- 2.8.4. Étapes de l'enquête sur ces crimes
- 2.8.5. Outils d'analyse des e-mails

2.9. Analyse médico-légale des mobiles
- 2.9.1. Réseaux cellulaires
  - 2.9.1.1. Types de réseaux
  - 2.9.1.2. Contenu du CdR
- 2.9.2. *Subscriber Identity Module* (SIM)
- 2.9.3. Acquisition logique
- 2.9.4. Acquisition physique
- 2.9.5. Acquisition du système de fichiers

2.10. Rédaction et soumission de rapports médico-légaux
- 2.10.1. Aspects importants d'un rapport médico-légal
- 2.10.2. Classification et types de rapports
- 2.10.3. Guide pour la rédaction d'un rapport
- 2.10.4. Présentation du rapport
  - 2.10.4.1. Préparation préalable au témoignage
  - 2.10.4.2. Dépôt
  - 2.10.4.3. Traiter avec les médias

Module 3. Défis actuels et futurs en matière de sécurité de l'information

3.1. Technologie *blockchain*
- 3.1.2. Domaines d'application
- 3.1.3. Garantie de confidentialité
- 3.1.4. Garantie de non-répudiation

3.2. La monnaie numérique
- 3.2.1. Bitcoins
- 3.2.2. Cryptocurrencies
- 3.2.3. Extraction de crypto-monnaies
- 3.2.4. Fraudes pyramidales
- 3.2.5. Autres infractions et problèmes potentiels

3.3. *Deepfake*
- 3.3.2. Impact des médias
- 3.3.3. Dangers pour la société
- 3.3.4. Mécanismes de détection

3.4. L'avenir de l'intelligence artificielle
- 3.4.1. Intelligence artificielle et informatique cognitive
- 3.4.2. Utilisations pour simplifier le service à la clientèle

3.5. Vie privée numérique
- 3.5.1. Valeur des données sur le réseau
- 3.5.2. Utilisation des données sur le réseau
- 3.5.3. Vie privée et gestion de l'identité numérique

3.6. Cyberconflits, cybercriminels et cyberattaques
- 3.6.1. Impact de la cybersécurité sur les conflits internationaux
- 3.6.2. Conséquences des cyber-attaques sur la population générale
- 3.6.3. Types de cybercriminels. Mesures de protection

3.7. Télétravail
- 3.7.1. La révolution du télétravail pendant et après COVID-19
- 3.7.2. Goulets d'étranglement dans l'accès
- 3.7.3. Variation de la surface d'attaque
- 3.7.4. Besoins des travailleurs

3.8. Technologies *Wireless* émergentes
- 3.8.1. WPA3
- 3.8.2. 5G
- 3.8.3. Ondes millimétriques
- 3.8.4. Tendencia en "*Get Smart*" au lieu de "*Get more*"

3.9. Adressage futur dans les réseaux
- 3.9.1. Problèmes actuels de l'adressage IP
- 3.9.2. IPv6
- 3.9.2. IPv4+
- 3.9.3. Avantages d'IPv4+ par rapport à IPv4
- 3.9.4. Avantages d'IPv4 par rapport à IPv4

3.10. Le défi de la sensibilisation de la population à l'éducation précoce et continue
- 3.10.1. Stratégies gouvernementales actuelles
- 3.10.2 Résistance de la population à l'apprentissage
- 3.10.3 Plans de formation à adopter par les entreprises

Un plan d'études à fort impact sur vos compétences qui vous permettra d'intervenir efficacement en matière de cybersécurité corrective et de criminalistique avec des ressources 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

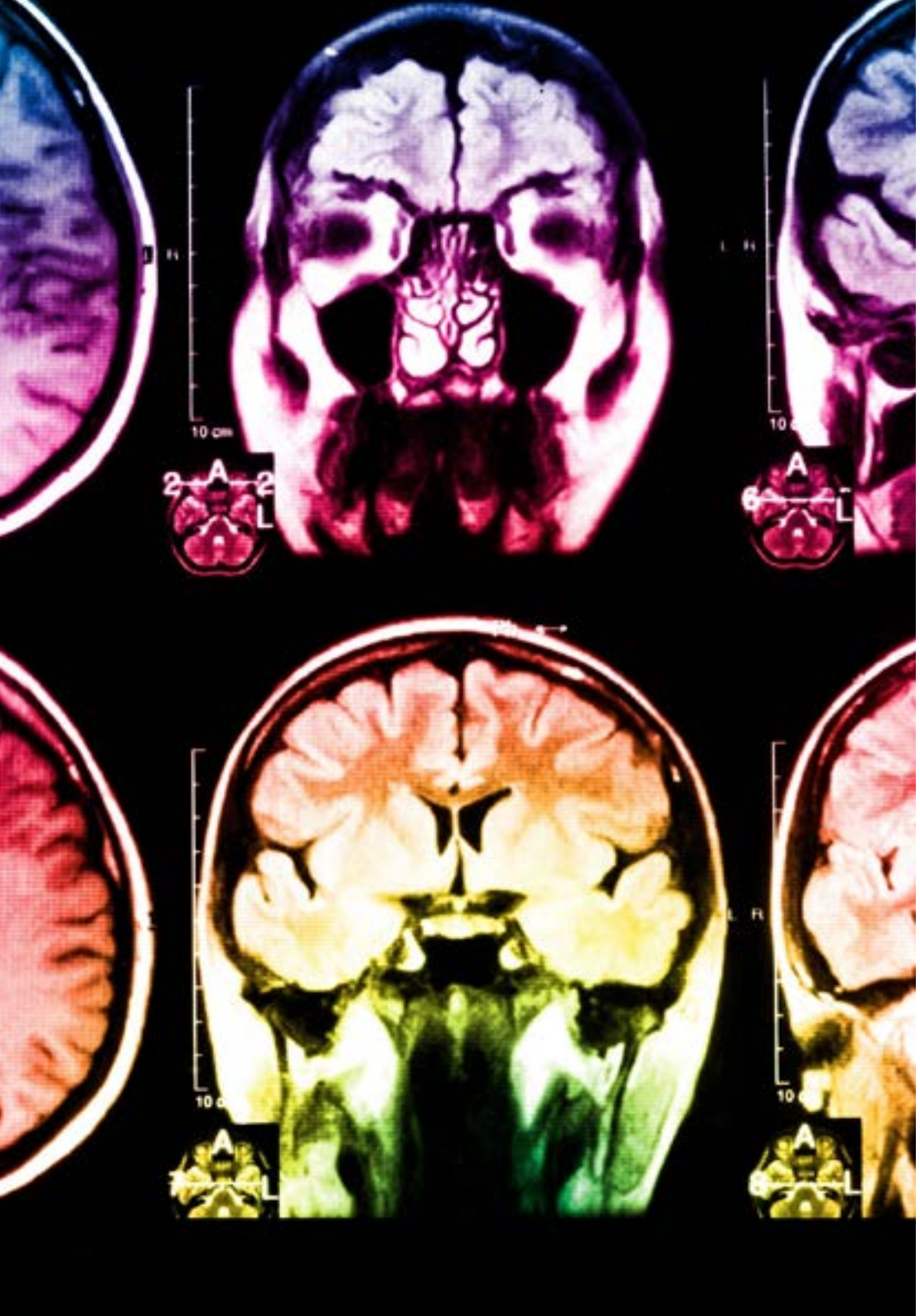
TECH combine efficacement la méthodologie des Études de Cas avec un système d'apprentissage 100% en ligne basé sur la répétition, qui associe différents éléments didactiques dans chaque leçon.

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.

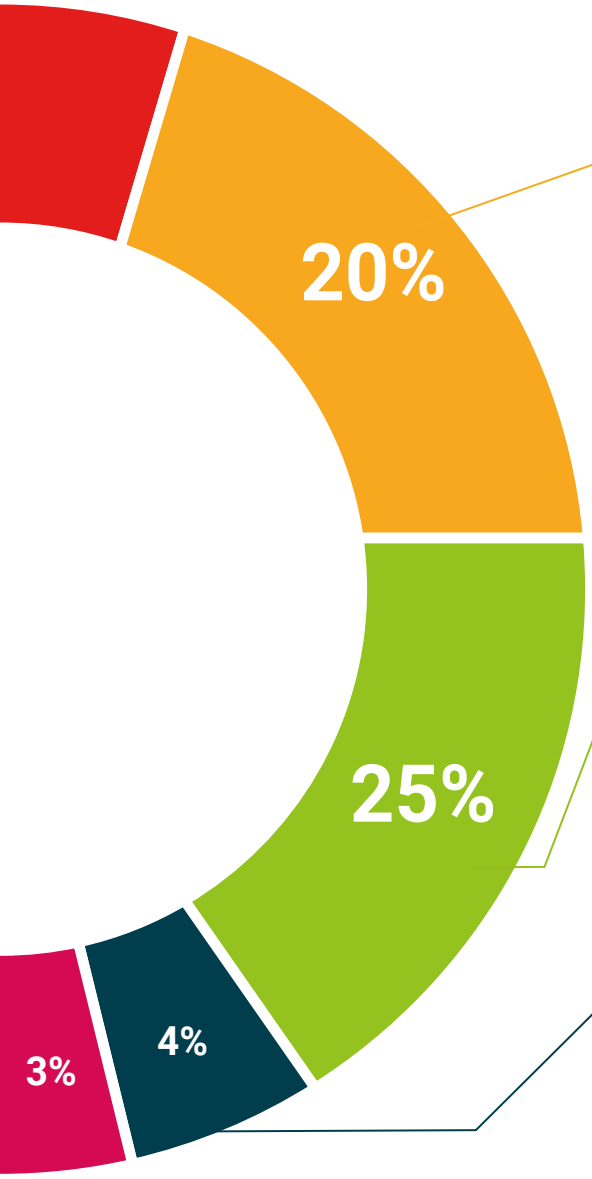
La méthode "Learning from an Expert" renforce les connaissances et la mémoire, et donne confiance dans les futures décisions difficiles.

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 Corrective et Expertise Forensique 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 Corrective et Expertise Forensique** 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 Corrective et Expertise Forensique**

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 Corrective et Expertise Forensique

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 Corrective et Expertise Forensique

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

Certificat Avancé

Cybersécurité Corrective et Expertise Forensique

tech université technologique