Certificat Avancé
Cybersécurité Défensive

tech université technologique

tech université technologique

Certificat Avancé
Cybersécurité Défensive

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

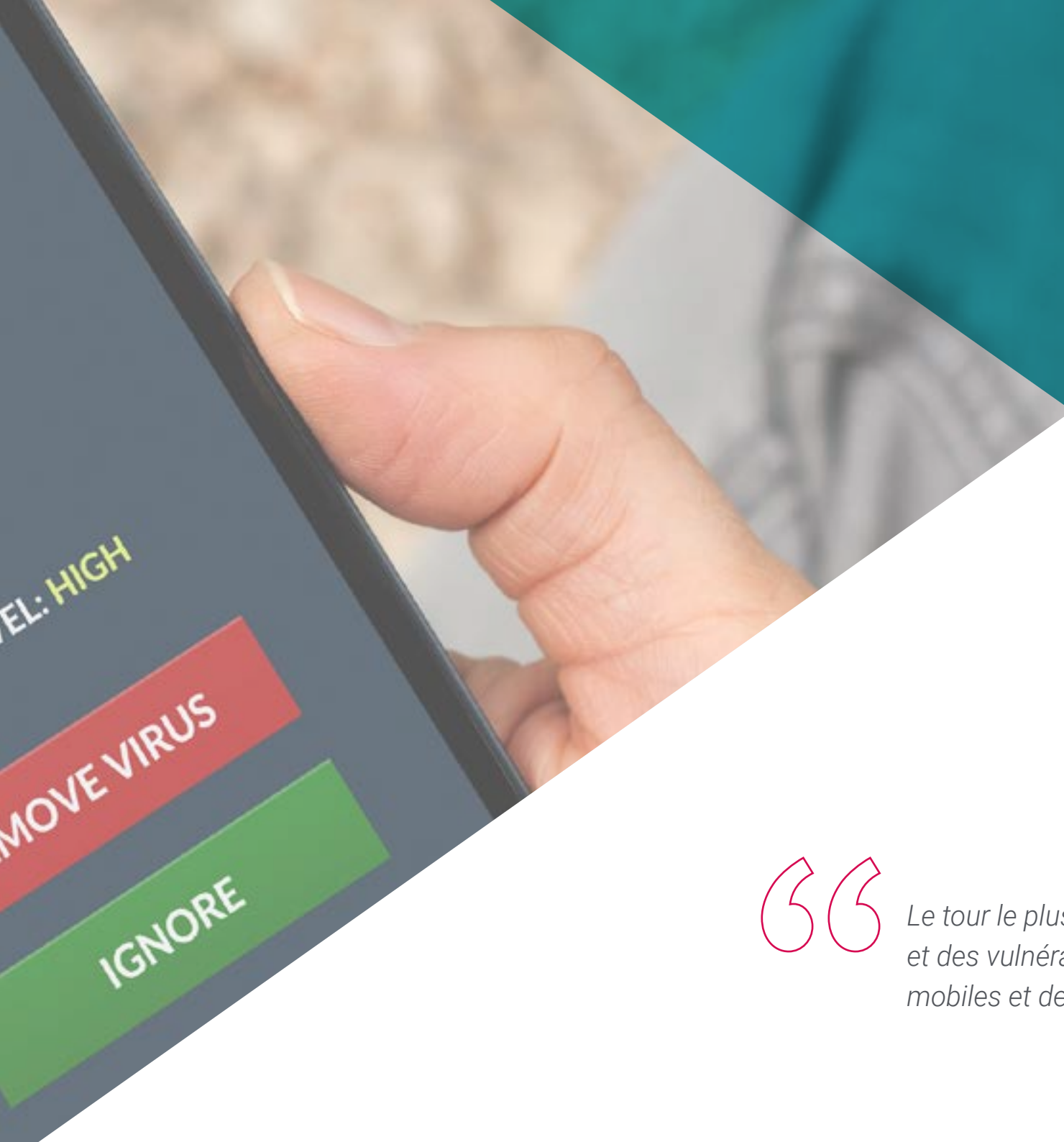
Accès au site web: www.techtitute.com/fr/informatique/diplome-universite/diplome-universite-cybersecurite-defensive

Sommaire

01

Présentation

À l'heure actuelle, où la vie quotidienne est directement liée à l'utilisation des appareils mobiles, connaître les formes possibles de vulnérabilité qui accompagnent leur utilisation est un besoin impératif pour les professionnels des branches technologiques. La sophistication des modèles a permis d'atteindre une capacité de travail inhabituelle, qui les a transformés en outils hautement sophistiqués pouvant même accéder à des données personnelles et professionnelles sensibles. Ce Certificat Avancé en Cybersécurité Défensive étudiera en profondeur tous les aspects dans lesquels les cyber-attaques peuvent se produire, en développant les stratégies défensives de cybersécurité les plus innovantes et efficaces du moment. Un cours hautement qualifié qui vous permettra d'agir en tant que spécialiste dans ce domaine.



Le tour le plus complet des dangers et des vulnérabilités des appareils mobiles et de leur cyberprotection"

La sécurité des habitations et des entreprises doit être structurée en couches, comme une chaîne dont la solidité dépend du maillon le plus faible. Ce Certificat Avancé présente les principales menaces qui pèsent sur les ordinateurs et les serveurs des utilisateurs afin que nous puissions prendre les mesures appropriées et être attentifs à toute situation.

Plus il y a de nouvelles fonctionnalités et plus nous communiquons les uns avec les autres, plus notre surface d'attaque augmente. En d'autres termes, les possibilités et les moyens dont disposent les cybercriminels pour atteindre leurs objectifs sont de plus en plus nombreux. C'est pourquoi les systèmes de surveillance et de défense de la sécurité doivent eux aussi évoluer. Car dans un monde où le télétravail et les services en *Cloud* sont de plus en plus répandus, un *firewall* traditionnel ne suffit pas. Comprendre l'importance de concevoir une défense à plusieurs niveaux, également connue sous le nom de "*Defense in Depth*", couvrant tous les aspects d'un réseau d'entreprise où certains des concepts et systèmes qui seront discutés peuvent également être utilisés et appliqués dans un environnement domestique.

La sécurité à 100 % n'existe pas, mais si vous connaissez les types d'attaques auxquelles vous êtes confronté, les risques auxquels vous êtes exposé et si vous disposez des informations nécessaires pour y faire face, vous avez franchi une étape importante et ajouté une couche supplémentaire de sécurité à vos informations.

Ce **Certificat Avancé en Cybersécurité Défensive** 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
- Il est possible d'accéder aux contenus depuis tout appareil fixe ou portable doté d'une connexion à internet

Commencer à agir avec la connaissance la plus large des types de risques existant actuellement et des moyens de défense applicables dans chaque cas"

Un tour complet qui vous permettra de savoir quelles sont les cybermenaces actuelles et comment elles fonctionnent comme base pour développer des stratégies défensives"

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

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 programme universitaire. Pour ce faire, l'étudiant sera assisté d'un innovant système de vidéos interactives, créé par des experts reconnus.

02

Objectifs

La prise en charge de ce Certificat Avancé permet un progrès exponentiel de 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.

Une mise à jour complète de tous les aspects de la cybersécurité défensive qui se sont développés ces derniers temps"

Objectifs généraux

- Évaluer la sécurité des ordinateurs et des serveurs des utilisateurs
- Examiner les menaces potentielles en fonction de l'environnement d'utilisation
- Analyser les solutions pour chaque menace
- Développer des politiques d'utilisation appropriées
- Analyser le cadre général, l'importance des systèmes de défense et de surveillance à plusieurs niveaux
- Examiner les systèmes de détection et de prévention des principales menaces
- Développement de solutions *firewall* en *Host Linux* et les fournisseurs de *Cloud*
- Évaluer les nouveaux systèmes de détection des menaces ainsi que leur évolution par rapport aux solutions plus traditionnelles
- Générer des solutions intelligentes complètes pour automatiser les comportements en cas d'incident
- Analyser les principales plates-formes mobiles actuelles, leurs caractéristiques et leur utilisation
- Examiner les vulnérabilités et les menaces existantes, ainsi que les principaux vecteurs d'attaque
- Évaluer les risques associés aux vulnérabilités à l'extérieur et à l'intérieur de l'entreprise
- Identifier les outils et les meilleures pratiques pour sécuriser les appareils mobiles
- Analyser l'IdO dans différents domaines aujourd'hui
- Examiner l'évolution et l'impact de IoT
- Déterminer les éléments d'un projet IoT
- Identifier, analyser et évaluer les risques de sécurité des parties du projet IoT

Objectifs spécifiques

Module 1. Sécurité de l'hôte

- Préciser les politiques de *Backup* des données personnelles et professionnelles
- Évaluer les différents outils permettant d'apporter des solutions à des problèmes de sécurité spécifiques
- Établir des mécanismes pour maintenir le système à jour
- Analyser l'équipement pour détecter les intrus
- Déterminer les règles d'accès au système
- Examiner et classer les courriers pour éviter les fraudes
- Générer des listes de *logiciels* autorisés

Module 2. Sécurité des réseaux (périmètre)

- Analyser les architectures de réseau actuelles pour identifier le périmètre à protéger
- Développer des configurations concrètes de *firewall* et de *Linux* pour atténuer les attaques les plus courantes
- Compiler les solutions les plus couramment utilisées telles que *Snort* et *Suricata* ainsi que leur configuration
- Examiner les différentes couches supplémentaires fournies par les *firewalls* de nouvelle génération et les fonctionnalités réseau dans les environnements en *Cloud*
- Déterminer les outils de protection des réseaux et démontrer pourquoi ils sont fondamentaux pour une défense à plusieurs niveaux

Module 3. Sécurité des *smartphones*

- Examiner les différents vecteurs d'attaque pour éviter de devenir une cible facile
- Déterminer les principales attaques et les principaux types de *Malware* auxquels les utilisateurs d'appareils mobiles sont exposés
- Analyser les dispositifs les plus courants pour établir une configuration plus sûre
- Préciser les principales étapes pour effectuer un test de pénétration sur les plateformes iOS et Android
- Développer des connaissances spécialisées sur les différents outils de protection et de sécurité
- Établir les meilleures pratiques en matière de programmation orientée vers les dispositifs mobiles

Module 4. Sécurité IoT

- Analyser les principales architectures IoT
- Examiner les technologies de connectivité
- Développer les principaux protocoles d'application
- Identifier les différents types de dispositifs existants
- Évaluer les niveaux de risque et les vulnérabilités connues
- Développer des politiques d'utilisation sécurisée
- Établir des conditions d'utilisation appropriées pour ces dispositifs

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.

La vision directe d'une profession en perpétuel mouvement, à travers des professionnels experts qui 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

Professeurs

M. Catala Barba, José Francisco

- L'encadrement intermédiaire au MINISDEF. Différentes tâches et responsabilités au sein du GOE III, telles que l'administration et la gestion des incidents du réseau interne, le développement de programmes personnalisés pour différents domaines, les cours de formation pour les utilisateurs du réseau et le personnel du groupe en général
- Technicien électronique dans l'usine Ford située à Almusafes, Valence, programmation de robots, automates, réparation et maintenance
- Technicien en Électronique
- Développeur d'applications pour les appareils mobiles

M. Jiménez Ramos, Alvaro

- Analyste principal de la sécurité à The Workshop
- Analyste en cybersécurité L1 chez Axians
- Analyste en cybersécurité L2 chez Axians
- Analyste en cybersécurité chez SACYR S.A.
- Diplôme d'ingénieur en Télématique de l'Université Polytechnique de Madrid
- Master en Cybersécurité et Hacking Éthique par CICE
- Cours Supérieur en Cybersécurité par Deusto Formation

Mme Marcos Sbarbaro, Victoria Alicia

- Développeur d'applications mobiles Android natives chez B60. UK
- Analyste-programmeur pour la gestion, la coordination et la documentation d'un environnement d'alarme de sécurité virtualisé chez un client
- Analyste programmeur d'applications Java pour les guichets automatiques pour le client
- Professionnel du développement de logiciels pour une application de validation de signature et de gestion de documents chez le client
- Technicien système pour la migration des équipements et pour la gestion, la maintenance et la formation des appareils mobiles PDA sur le site du client
- Ingénierie Technique des Systèmes Informatiques. Université Oberta de Catalunya
- Master en sécurité informatique et Ethical Hacking officiel EC-Council et CompTIA par l'Ecole Professionnelle des Nouvelles Technologies CICE

M. Peralta Alonso, Jon

- Avocat / DPO Altia Consultores S.A
- Chargé de cours pour le Mastère en protection des données personnelles, cybersécurité et droit des TIC. et le droit des TIC. Université publique du Pays basque (UPV-EHU)
- Avocat / Conseiller juridique Arriaga Associés Conseillers Juridiques et Economiques, S.L.
- Conseiller juridique / Stagiaire. Bureau professionnel: Oscar Padura
- Diplôme en Droit. Université Public du Pays Basque
- Master en protection des données Délégué; EIS Innovative School
- Master en Droit. Université Public du Pays Basque
- Master Spécialisé dans la Pratique du Contentieux Civil. Université Internationale Isabel I de Castilla

04

Structure et contenu

Le plan d'études de ce programme couvre tous les domaines de connaissances que le professionnel de la cybersécurité doit connaître dans le domaine de la défense. 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 aspects que l'analyse et l'intervention en matière de cybersécurité défensive requièrent, développés de manière structurée dans une approche d'étude axée sur l'efficacité"

Module 1. Sécurité de l' *hôte*

1.1. Copies de sécurité
- 1.1.1. Stratégies de copies de sauvegarde
- 1.1.2. Outils pour Windows
- 1.1.3. Outils pour Linux
- 1.1.4. Outils pour MacOS

1.2. Antivirus de l'utilisateur
- 1.2.1. Types d'anti-virus
- 1.2.2. Antivirus pour Windows
- 1.2.3. Antivirus pour Linux
- 1.2.4. Antivirus pour MacOS
- 1.2.5. Antivirus pour smartphones

1.3. Détecteurs d'intrusion - HIDS
- 1.3.1. Méthodes de détection d'intrusion
- 1.3.2. Sagan
- 1.3.3. Aide
- 1.3.4. *Rkhunter*

1.4. *Pare-feu* local
- 1.4.1. *Pare-feu* pour Windows
- 1.4.2. *Pare-feu* pour Linux
- 1.4.3. *Pare-feu* pour MacOS

1.5. Gestionnaires de mots de passe
- 1.5.1. Mot de passe
- 1.5.2. *LastPass*
- 1.5.3. *KeePass*
- 1.5.4. *Sticky password*
- 1.5.5. RoboForm

1.6. Détecteurs de *phishing*
- 1.6.1. Détection de *phishing* manuelle
- 1.6.2. Outils *antiphishing*

1.7. *Spyware*
- 1.7.1. Mécanismes d'évitement
- 1.7.2. Outils *antispyware*

1.8. Trackers
- 1.8.1. Mesures de protection du système
- 1.8.2. Outils anti-traceurs

1.9. *EDR- Détection et réponse du point final*
- 1.9.1. Comportement du système EDR
- 1.9.2. Différences entre EDR et anti-virus
- 1.9.3. L'avenir des systèmes de CED

1.10. Contrôle de l'installation des logiciels
- 1.10.1. Dépôts et magasins de logiciels
- 1.10.2. Listes des logiciels autorisés ou interdits
- 1.10.3. Critères de mise à jour
- 1.10.4. Privilèges d'installation des logiciels

Module 2. Sécurité des réseaux (périmètre)

2.1. Systèmes de détection et de prévention des menaces
- 2.1.1. Cadre général des incidents de sécurité
- 2.1.2. Systèmes de défense actuelles: *defense in depth* et SOC
- 2.1.3. Architectures de réseau actuelles
- 2.1.4. Types d'outils de détection et de prévention des incidents
  - 2.1.4.1. Systèmes basés sur réseau
  - 2.1.4.2. Systèmes basés sur *l'Hôte*
  - 2.1.4.3. Systèmes centralisés
- 2.1.5. Communication et détection des instances/*Hosts*, conteneurs et *serverless*

2.2. *Firewall*
- 2.2.1. Types de *pare-feu*
- 2.2.2. Attaques et atténuation
- 2.2.3. *Firewalls* comunes en *Kernel* Linux
  - 2.2.3.1. UFW
  - 2.2.3.2. Nftables e iptables
  - 2.2.3.3. *Firewalld*
- 2.2.4. Systèmes de détection basés sur les *logs* du système
  - 2.2.4.1. TCP *wrappers*
  - 2.2.4.2. *BlockHosts* et *DenyHosts*
  - 2.2.4.3. Fail2Ban

2.3. Systèmes de détection et de prévention des intrusions (IDS/IPS)
- 2.3.1. Attaques contre les IDS/IPS
- 2.3.2. Systèmes IDS/IPS
  - 2.3.2.1. *Snort*
  - 2.3.2.2. Suricate

2.4. *Firewalls* la sécurité alimentaire de la prochaine génération (SNG)
- 2.4.1. Différences entre les NGFW et les *Firewall* traditionnels
- 2.4.2. Capacités principales
- 2.4.3. Solutions commerciales
- 2.4.4. *Firewalls* pour les services *Cloud*
  - 2.4.4.1. Architecture Cloud VPC
  - 2.4.4.2. *Cloud* ACLs
  - 2.4.4.3. *Security Group*

2.5. *Proxy*
- 2.5.1. Types de *Proxy*
- 2.5.2. Utilisation de *Proxy*. Avantages et inconvénients

2.6. Moteurs antivirus
- 2.6.1. Contexte général des *Malware* et des IOCs
- 2.6.2. Problèmes avec les moteurs anti-virus

2.7. Systèmes de protection du courrier
- 2.7.1. Antispam
  - 2.7.1.1. Liste blanche et liste noire
  - 2.7.1.2. Filtres bayésiens
- 2.7.2. *Mail Gateway* (MGW)

2.8. SIEM
- 2.8.1. Composants et architecture
- 2.8.2. Règles de corrélation et cas d'utilisation
- 2.8.3. Les défis actuels des systèmes SIEM

2.9. SOAR
- 2.9.1. SOAR et SIEM: Ennemis ou alliés?
- 2.9.2. L'avenir des systèmes SOAR

2.10. Autres systèmes en réseau
- 2.10.1. WAF
- 2.10.2. NAC
- 2.10.3. *HoneyPots* et les *HoneyNets*
- 2.10.4 CASB

Module 3. Sécurité des Smartphones

3.1. Le monde de l'appareil mobile
- 3.1.1. Types de plateformes mobiles
- 3.1.2. Dispositifs IOS
- 3.1.3. Dispositifs Android

3.2. Gestion de la sécurité mobile
- 3.2.1. Projet de sécurité mobile de l'OWASP
  - 3.2.1.1. Top 10 des vulnérabilités
- 3.2.2. Communications, réseaux et modes de connexion

3.3. Le dispositif mobile dans l'environnement de l'entreprise
- 3.3.1. Risques
- 3.3.2. Politique de sécurité
- 3.3.3. Surveillance des dispositifs
- 3.3.4. Gestion des dispositifs mobiles (MDM)

3.4. Vie privée des utilisateurs et sécurité des données
- 3.4.1. États d'information
- 3.4.2. Protection des données et confidentialité
  - 3.4.2.1. Permissions
  - 3.4.2.2. Cryptage
- 3.4.3. Stockage sécurisé des données
  - 3.4.3.1. Stockage sécurisé sur iOS
  - 3.4.3.2. Stockage sécurisé sur Android
- 3.4.4. Meilleures pratiques en matière de développement d'applications

3.5. Vulnérabilités et vecteurs d'attaque
- 3.5.1. Vulnérabilités
- 3.5.2. Vecteurs d'attaque
  - 3.5.2.1. *Malware*
  - 3.5.2.2. Exfiltration de données
  - 3.5.2.3. Manipulation des données

3.6. Principales menaces
- 3.6.1. Utilisateur non respecté
- 3.6.2. *Malware*
  - 3.6.2.1. Types de *Malware*
- 3.6.3. Ingénierie sociale
- 3.6.4. Fuite de données
- 3.6.5. Vol d'informations
- 3.6.6. Réseaux WiFi non sécurisés
- 3.6.7. Logiciels obsolètes
- 3.6.8. Applications malveillantes
- 3.6.9. Mots de passe non sécurisés
- 3.6.10. Paramètres de sécurité faibles ou inexistants
- 3.6.11. Accès physique
- 3.6.12. Perte ou vol de l'appareil
- 3.6.13. Usurpation d'identité (intégrité)
- 3.6.14. Cryptographie faible ou cassée
- 3.6.15. Déni de service (DoS)

3.7. Principales attaques
- 3.7.1. Attaques de *phishing*
- 3.7.2. Attaques liées aux modes de communication
- 3.7.3. Attaques de *smishing*
- 3.7.4. Attaques de *Criptojacking*
- 3.7.5. *Man in the middle*

3.8. *Hacking*
- 3.8.1. *Rooting* et *jailbreaking*
- 3.8.2. Anatomie d'une attaque mobile
  - 3.8.2.1. Propagation de la menace
  - 3.8.2.2. Installation de *Malware* sur le dispositif
  - 3.8.2.3. Persistance
  - 3.8.2.4. Exécution du *Payload* et extraction de l'information
- 3.8.3. Hacking en des dispositifs IOS: mécanismes et outils
- 3.8.4. Hacking en des dispositifs Android: mécanismes et outils

3.9. Tests de pénétration
- 3.9.1. iOS *pentesting*
- 3.9.2. Android *pentesting*
- 3.9.3. Outils

3.10. Protection et sécurité
- 3.10.1. Paramètres de sécurité
  - 3.10.1.1. Sur les dispositifs iOS
  - 3.10.1.2. Sur les dispositifs androïdes
- 3.10.2 Mesures de sécurité
- 3.10.3 Outils de protection

Module 4. Sécurité en IoT

4.1. Dispositifs
- 4.1.1. Types d'appareils
- 4.1.2. Architectures standardisées
  - 4.1.2.1. OneM2M
  - 4.1.2.2. IoTWF
- 4.1.3. Protocoles d'application
- 4.1.4. Technologies de la connectivité

4.2. Dispositifs IoT Domaines d'application
- 4.2.1. SmartHome
- 4.2.2. SmartCity
- 4.2.3. Transports
- 4.2.4. *Wearables*
- 4.2.5. Secteur de la santé
- 4.2.6. IIoT

4.3. Protocoles de communication
- 4.3.1. MQTT
- 4.3.2. LWM2M
- 4.3.3. OMA-DM
- 4.3.4. TR-069

4.4. SmartHome
- 4.4.1. Domotique
- 4.4.2. Réseaux
- 4.4.3. Appareils ménagers
- 4.4.4. Surveillance et sécurité

4.5. SmartCity
- 4.5.1. Éclairage
- 4.5.2. Météorologie
- 4.5.3. Sécurité

4.6. Transports
- 4.6.1. Localisation
- 4.6.2. Réalisation de paiements et obtention de services
- 4.6.3. Connectivité

4.7. Wearables
- 4.7.1. Vêtements intelligents
- 4.7.2. Bijoux intelligents
- 4.7.3. Montres intelligentes

4.8. Secteur de la santé
- 4.8.1. Surveillance de l'effort et de la fréquence cardiaque
- 4.8.2. Suivi des patients et des personnes âgées
- 4.8.3. Implantables
- 4.8.4. Robots chirurgicaux

4.9. Connectivité
- 4.9.1. WiFi
- 4.9.2. Bluetooth
- 4.9.3. Connectivité embarquée

4.10. Securitisation
- 4.10.1 Réseaux dédiés
- 4.10.2. Gestionnaires de mots de passe
- 4.10.3. Utilisation de protocoles cryptés
- 4.10.4. Conseils d'utilisation

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

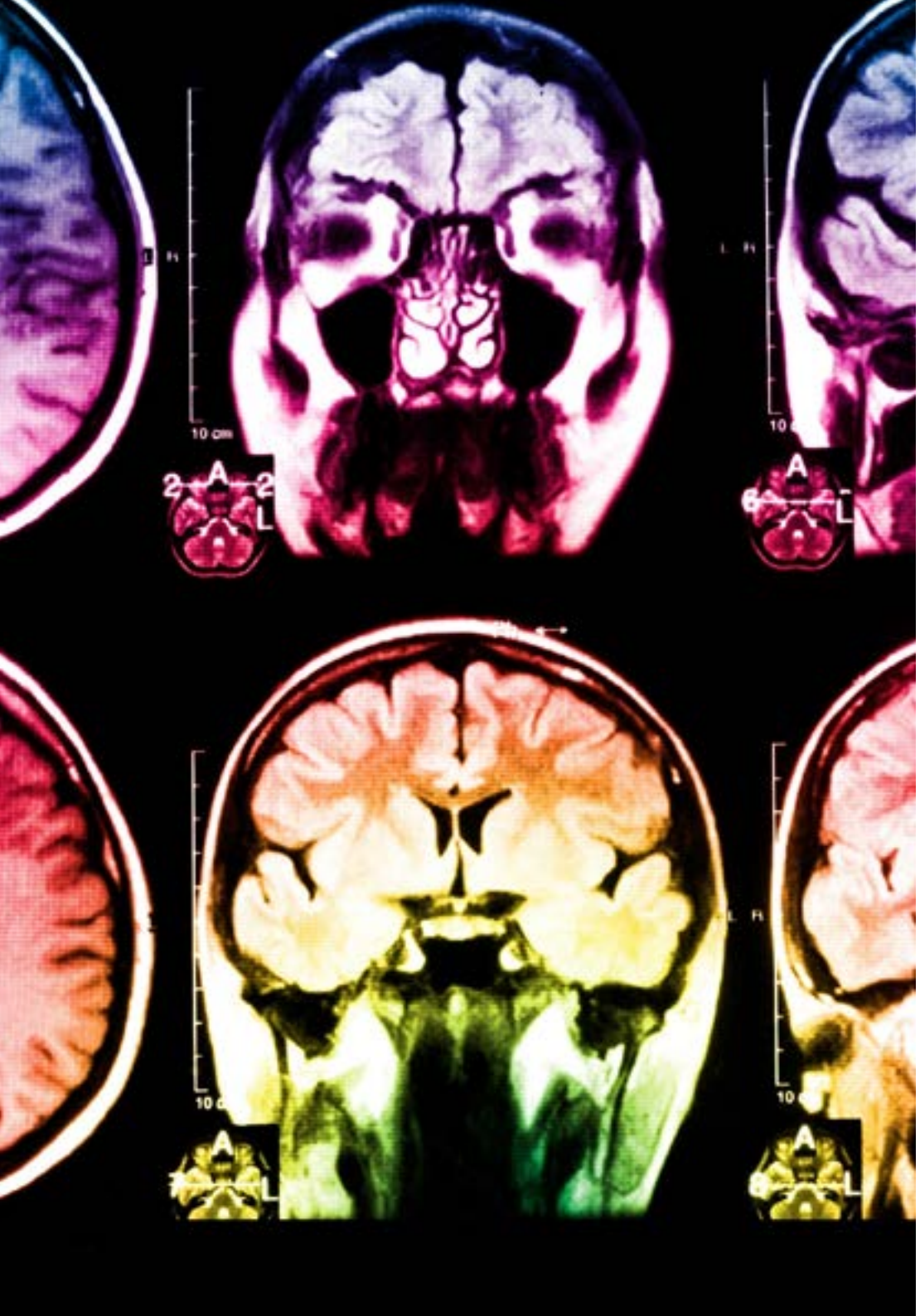
TECH combine efficacement la méthodologie des Études de Cas avec un système d'apprentissage 100% en ligne basé sur la répétition, qui associe différents éléments didactiques dans chaque leçon.

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.

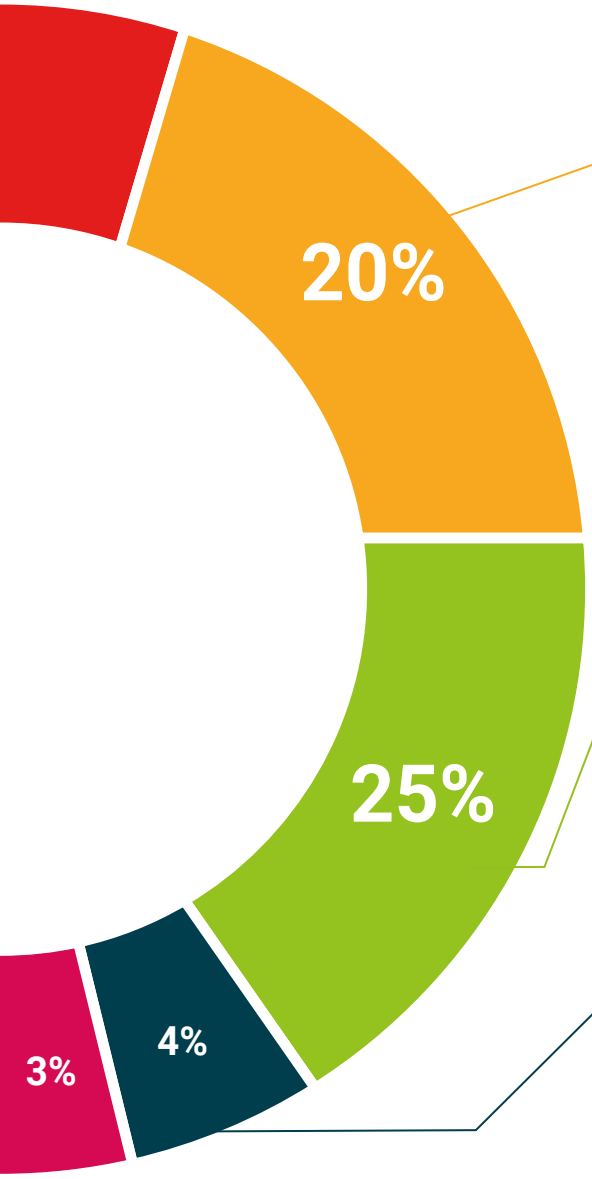
La méthode "Learning from an Expert" renforce les connaissances et la mémoire, et donne confiance dans les futures décisions difficiles.

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 Défensive 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 Défensive** 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 Cybersécurité Défensive**

N.º d'heures Officielles: **600 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 Défensive

Il s'agit d'un diplôme spécialisé octroyé par cette Université d'une durée de 600 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
Cybersécurité Défensive

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

Certificat Avancé
Cybersécurité Défensive

tech université technologique