Certificat Avancé
Cybersécurité Red Team

tech université technologique

tech université technologique

Certificat Avancé
Cybersécurité Red Team

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

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

Sommaire

01

Présentation

La Cybersécurité est devenue un pilier fondamental de l'ère numérique, tandis que l'interconnexion croissante des systèmes a intensifié la menace des cyberattaques. La demande de professionnels hautement qualifiés dans ce domaine est plus évidente que jamais, surtout si l'on considère l'augmentation exponentielle de la cybercriminalité et des attaques sophistiquées. Dans ce contexte, ce programme est présenté comme une réponse stratégique visant à doter les professionnels des compétences nécessaires pour faire face aux cybermenaces. Tout au long du programme, les étudiants seront immergés dans la simulation de menaces avancées. La méthodologie du programme d'études, 100% en ligne, offre flexibilité et accessibilité, avec une grande variété de contenus multimédias et l'application de la méthode *Relearning*.

Vous contribuerez à l'amélioration de la Cybersécurité et à la prévention des crimes numériques majeurs. Ne manquez pas cette occasion et inscrivez-vous dès maintenant!"

Dans le paysage complexe de la Cybersécurité, disposer d'un expert dans ce domaine se présente comme un besoin impératif pour les organisations qui cherchent à renforcer leurs défenses contre des menaces en constante évolution. Cette approche proactive, fondamentale pour l'amélioration continue de la posture de sécurité, met en évidence le besoin critique d'experts.

La mise en œuvre de mesures proactives est essentielle et la formation spécialisée de Red Team donne aux professionnels la capacité d'anticiper, d'identifier et d'atténuer activement les vulnérabilités des systèmes et des réseaux. Dans ce Certificat Avancé, l'étudiant acquerra des compétences en matière de tests de pénétration et de simulations, en abordant l'identification et l'exploitation des vulnérabilités. En ce sens, ils développeront non seulement des compétences techniques avancées, mais favoriseront également une collaboration efficace avec les équipes de sécurité, en intégrant des stratégies de lutte contre les menaces liées aux *malwares*.

En outre, les diplômés acquerront une solide compréhension des principes fondamentaux de l'investigation médico-légale numérique (DFIR), applicables à la résolution des cyberincidents. En outre, cette approche holistique du programme d'études permettra aux professionnels d'acquérir des compétences de pointe dans le domaine de la Cybersécurité.

Ce parcours académique se distingue non seulement par son contenu, mais aussi par sa méthodologie avancée. Il sera accessible aux étudiants entièrement en ligne, ce qui leur donnera la flexibilité nécessaire pour faire progresser leur carrière sans compromettre leurs responsabilités professionnelles.

En outre, l'application du *Relearning*, qui consiste à répéter des concepts clés, est utilisée pour ancrer les connaissances et faciliter un apprentissage efficace. Cette combinaison d'accessibilité et d'approche pédagogique solide fait de ce Certificat Avancé non seulement une option éducative avancée, mais aussi un moteur important pour ceux qui cherchent à exceller dans le domaine de la Cybersécurité.

Ce **Certificat Avancé en Cybersécurité Red Team** contient le programme le plus complet et le plus actualisé du marché. Ses caractéristiques sont les suivantes:

- Le développement d'études de cas présentées par des experts en Cybersécurité Red Team
- Le contenu graphique, schématique et éminemment pratique de l'ouvrage fournit des informations actualisées et pratiques sur les disciplines essentielles à la pratique professionnelle.
- Exercices pratiques permettant de réaliser le processus d'auto-évaluation afin d'améliorer l'apprentissage
- Il met l'accent sur les méthodologies innovantes
- Cours théoriques, questions à l'expert, forums de discussion sur des sujets controversés et travail de réflexion individuel
- La possibilité d'accéder aux contenus depuis n'importe quel appareil fixe ou portable doté d'une connexion internet

Vous vous distinguerez dans un secteur à forte projection grâce à ce programme universitaire exclusif de TECH"

Vous vous plongerez dans les détails d'un rapport médico-légal dans l'université la mieux notée au monde par ses étudiants, selon la plateforme Trustpilot (4.9/5)"

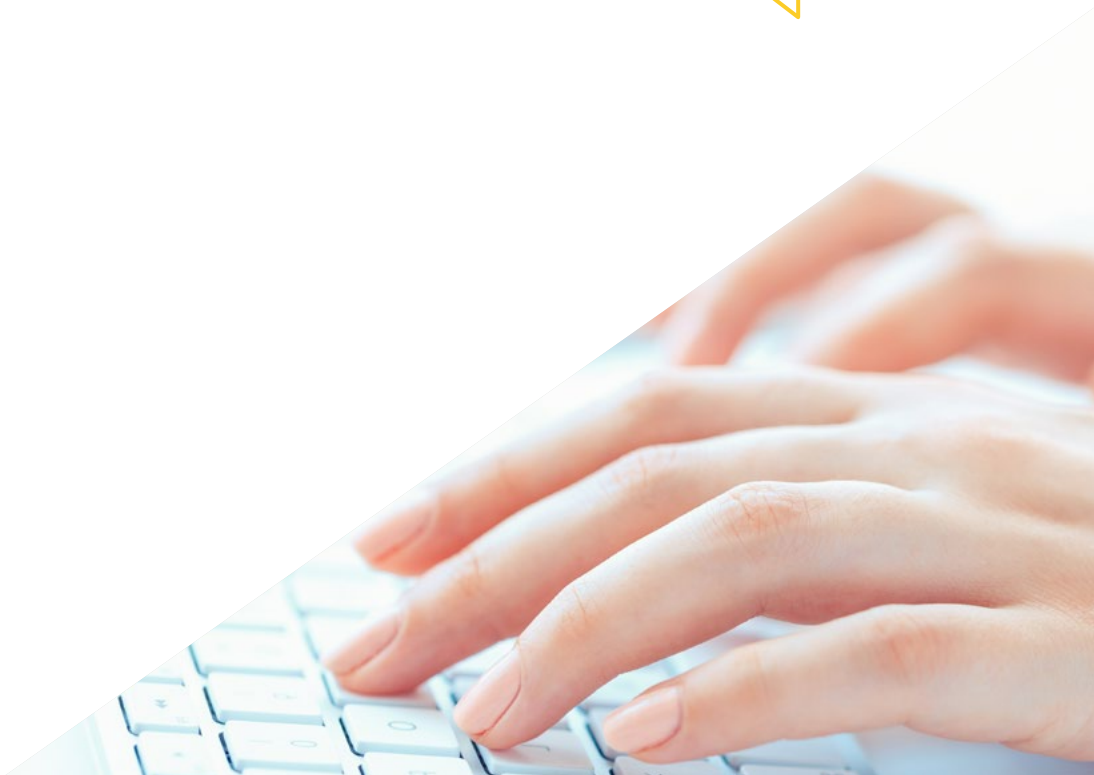
Vous développerez des compétences pour évaluer et sélectionner des outils de sécurité anti-malware.

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

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 la pratique professionnelle qui se présentent tout au long du programme académique. Pour ce faire, l'étudiant sera assisté d'un innovant système de vidéos interactives, créé par des experts reconnus.



02

Objectifs

Le Certificat Avancé en Cybersécurité *Red Team* a pour objectif principal de former les étudiants au développement de compétences dans le domaine de la simulation de menaces avancées. Tout au long du programme, les diplômés seront immergés dans la reproduction des tactiques, techniques et procédures (TTP) utilisées par les acteurs malveillants. Dans ce contexte, l'approche spécialisée ne renforcera pas seulement les compétences techniques des professionnels, mais leur permettra également de faire face aux défis du monde réel dans ce domaine. En outre, l'utilisation de la méthodologie *Relearning* facilitera l'apprentissage, en fixant les concepts clés avec peu d'efforts.

Vous identifierez les faiblesses et les vulnérabilités des infrastructures cybernétiques des entreprises. Atteignez vos objectifs avec TECH!"

Objectifs généraux

- Acquérir des compétences avancées en matière de tests de pénétration et de simulations *Red Team*, afin d'identifier et d'exploiter les vulnérabilités des systèmes et des réseaux
- Développer des compétences en leadership pour coordonner des équipes spécialisées dans la Cybersécurité offensive, en optimisant l'exécution des projets *Pentesting* et *Red Team*
- Développer des compétences dans l'analyse et le développement de *malware*, en comprenant leur fonctionnalité et en appliquant des stratégies défensives et éducatives
- Améliorer les compétences en matière de communication en produisant des rapports techniques et exécutifs détaillés, en présentant les résultats de manière efficace à des auditoires techniques et exécutifs
- Promouvoir une pratique éthique et responsable dans le domaine de la Cybersécurité, en tenant compte des principes éthiques et juridiques dans toutes les activités
- Tenir les étudiants au courant des tendances et des technologies émergentes dans le domaine de la Cybersécurité

Objectifs spécifiques

Module 1. Analyse et Développement de Malware

- Acquérir une connaissance approfondie de la nature, de la fonctionnalité et du comportement du *malware*, en comprenant leurs différentes formes et leurs objectifs.
- Développer des compétences en analyse légale appliquée aux *malware*, permettant l'identification d'indicateurs de compromission (IoC) et de schémas d'attaque
- Apprendre des stratégies de détection et de prévention efficaces des *malware*, y compris le déploiement de solutions de sécurité avancées
- Familiariser l'apprenant avec le développement de *malware* à des fins éducatives et défensives, permettant une compréhension approfondie des tactiques utilisées par les attaquants
- Promouvoir des pratiques éthiques et juridiques dans l'analyse et le développement des logiciels *malveillants*, en garantissant l'intégrité et la responsabilité dans toutes les activités
- Appliquer les connaissances théoriques dans des environnements simulés, participer à des exercices pratiques pour comprendre et contrer les attaques malveillantes
- Développer des compétences pour évaluer et sélectionner des outils de sécurité*anti-malware*, en tenant compte de leur efficacité et de leur adaptabilité à des environnements spécifiques
- Apprendre à mettre en œuvre des mesures d'atténuation efficaces contre les menaces malveillantes, en réduisant l'impact et la propagation des malware sur les systèmes et les réseaux
- Favoriser une collaboration efficace avec les équipes de sécurité, en intégrant les stratégies et les efforts de protection contre les menaces des *malware*
- Maintenir le diplômé au courant des dernières tendances et techniques utilisées dans l'analyse et le développement des logiciels *malware*, en garantissant la pertinence et l'efficacité continues des compétences acquises

Module 2. Principes Fondamentaux de la Criminalistique et DFIR

- Acquérir une solide compréhension des principes fondamentaux de l'Investigation Numérique (DFIR) et de leur application dans la résolution des cyberincidents
- Développer des compétences dans l'acquisition sécurisée et légale de preuves numériques, en assurant la préservation de la chaîne de possession
- Apprendre à effectuer une analyse criminalistique des systèmes de fichiers
- Familiariser l'étudiant avec les techniques avancées d'analyse des enregistrements et des journaux, permettant de reconstituer les événements dans les environnements numériques
- Apprendre à appliquer les méthodologies d'investigation numérique légale dans la résolution des cas, de l'identification à la documentation des résultats
- Familiariser les étudiants avec l'analyse des preuves numériques et l'application des techniques de police scientifique dans les environnements de *Pentesting*
- Développer des compétences dans la production de rapports criminalistiques détaillés et clairs, présentant les résultats et les conclusions d'une manière compréhensible
- Favoriser une collaboration efficace avec les équipes de réponse aux incidents (RI), en optimisant la coordination dans l'enquête et l'atténuation des menaces
- Promouvoir des pratiques éthiques et juridiques dans le domaine de la criminalistique numérique, en veillant au respect des réglementations et des normes de conduite en matière de Cybersécurité

Module 3. Exercices Avancés du Red Team

- Développer des compétences dans la simulation de menaces avancées, en reproduisant les tactiques, techniques et procédures (TTP) utilisées par des acteurs malveillants attrayants
- Apprendre à identifier les faiblesses et les vulnérabilités de l'infrastructure par le biais d'exercices *Red Team*réalistes, renforçant ainsi le dispositif de sécurité.

- Familiariser le diplômé avec des techniques avancées d'évasion de sécurité, permettant d'évaluer la résilience de l'infrastructure contre des attaques souhaitables
- Développer des compétences de coordination et de collaboration efficaces entre les membres de l'équipe *Red Team*, en optimisant l'exécution des tactiques et des stratégies afin d'évaluer de manière exhaustive la sécurité de l'organisation
- Apprendre à simuler des scénarios de menace actuels, tels que des attaques de *ransomware* ou des campagnes de *phishing* avancées, afin d'évaluer les capacités de réaction de l'organisation
- Familiariser l'étudiant avec les techniques d'analyse post-exercice, l'évaluation des performances de *Red Team* et l'extraction des enseignements tirés en vue d'une amélioration continue
- Développer des compétences dans l'évaluation de la résilience organisationnelle à des attaques simulées, en identifiant les domaines d'amélioration des politiques et des procédures
- Apprendre à produire des rapports détaillés documentant les résultats, les méthodologies utilisées et les recommandations issues des exercices *Red Team* avancés
- Promouvoir des pratiques éthiques et juridiques dans la conduite des exercices *Red Team*, en veillant au respect des réglementations en matière de Cybersécurité et des normes éthiques

Vous atteindrez vos objectifs grâce aux outils didactiques de TECH, y compris les vidéos explicatives et les résumés interactifs"

03

Direction de la formation

Pour ce programme universitaire, TECH a réuni un corps enseignant distingué, composé des meilleurs spécialistes du domaine. En ce sens, chaque membre du corps enseignant dispose d'une expérience professionnelle étendue et reconnue, forgée dans des entreprises de premier plan du secteur de la Cybersécurité. Sélectionnés avec soin pour leur expérience et leur expertise, ces professionnels ne garantiront pas seulement la qualité académique du programme d'études, mais apporteront également une perspective pratique et actualisée, enrichissant la formation des participants avec des idées précieuses tirées de leur expérience réelle dans l'environnement de Red Team.

Soyez au courant des dernières techniques de cryptage Shellcode (XQR) grâce à des experts en Cybersécurité. Lancez votre carrière professionnelle avec TECH!"

Direction

M. Gómez Pintado, Carlos

- Directeur de l'Équipe de Cybersécurité et de Réseau Cipherbit dans le Grupo Oesía
- Directeur, *Conseiller et Investisseur* chez Wesson App
- Diplôme en Ingénierie Logicielle et Technologies de la Société de l'Information, Université Politécnique de Madrid
- Il collabore avec des établissements d'enseignement pour la préparation de **Cycles de Formation de Niveau Supérieur** en cybersécurité

04

Structure et contenu

Ce programme offrira aux étudiants une immersion spécialisée dans l'analyse médico-légale appliquée aux *malwares*, en mettant l'accent sur le développement de compétences clés pour l'identification des indicateurs de compromission (IoC) et des schémas d'attaque. Tout au long du programme, les diplômés seront immergés dans des méthodologies avancées, ce qui leur fournira les outils et les connaissances nécessaires pour faire face aux cybermenaces sophistiquées. En outre, ce programme rigoureusement structuré garantira une formation complète dans le domaine du *Red Team*, préparant les professionnels à analyser et à contrer les stratégies complexes utilisées par les acteurs malveillants.

Vous approfondirez les techniques avancées de post-exploitation et vous vous positionnerez comme un Red Teamer hors pair"

Module 1. Analyse et Développement de *Malware*

1.1. Analyse et développement de *malware*
- 1.1.1. Histoire et évolution des *malware*
- 1.1.2. Classification et types de *malware*
- 1.1.3. Analyse des *malware*
- 1.1.4. Développement de *malware*

1.2. Préparation de l'environnement
- 1.2.1. Configuration de la Machine Virtuelle et *Snapshots*
- 1.2.2. Outils d'analyse des *malware*
- 1.2.3. Outils de développement de *malware*

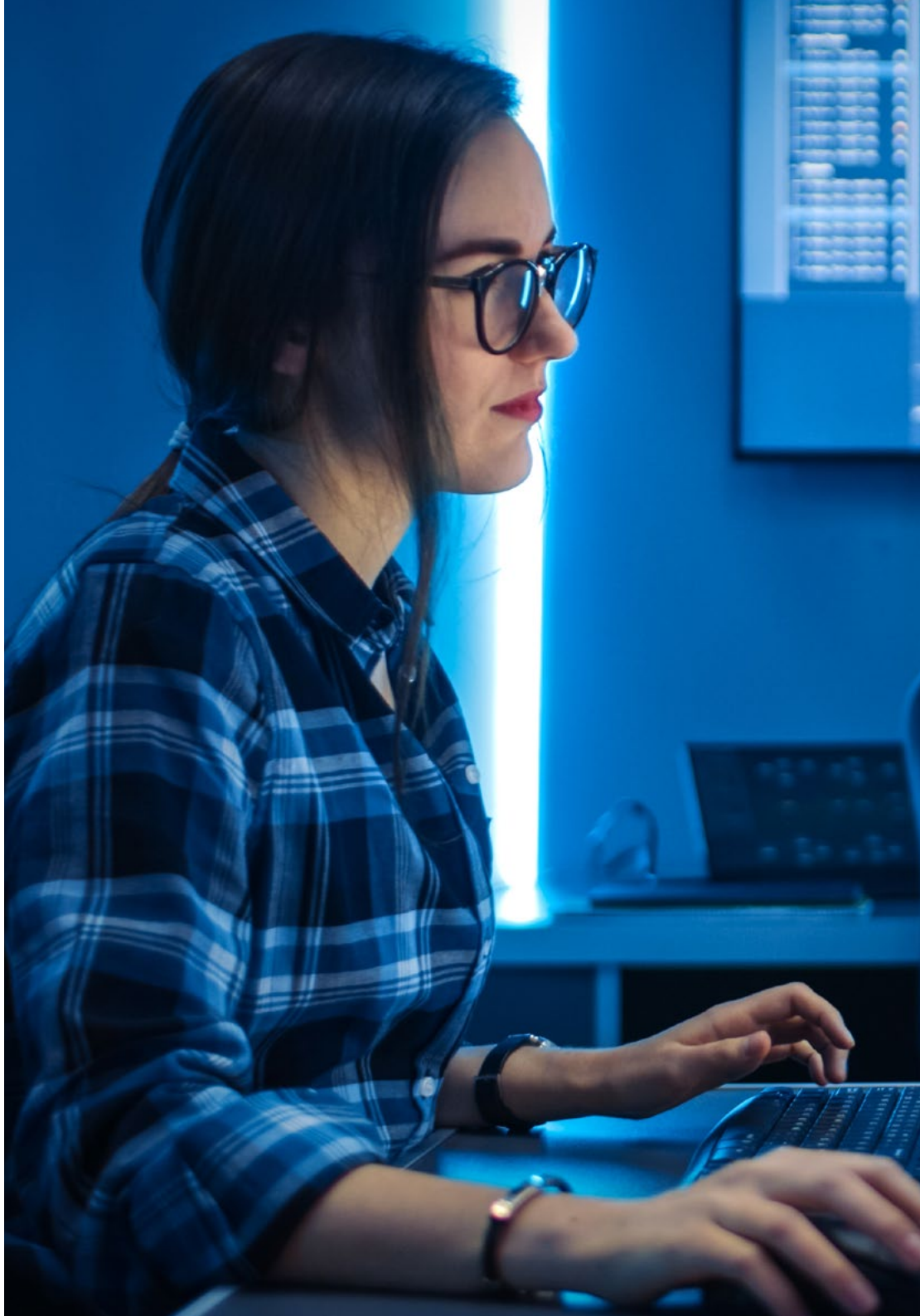
1.3. Principes de base de Windows
- 1.3.1. Format de fichier PE (*Portable Executable*)
- 1.3.2. Processus et *Threads*
- 1.3.3. Système de fichiers et registre
- 1.3.4. *Windows Defender*

1.4. Techniques de *malware* de base
- 1.4.1. Génération de *shellcode*
- 1.4.2. Exécution du *shellcode* sur le disque
- 1.4.3. Disque vs mémoire
- 1.4.4. Exécution du *shellcode* en mémoire

1.5. Techniques de *malware* intermédiaires
- 1.5.1. Persistance sur Windows
- 1.5.2. Dossier d'accueil
- 1.5.3. Clés de registre
- 1.5.4. Économiseur d'écran

1.6. Techniques des *malwares* avancés
- 1.6.1. Cryptage du *shellcode* (XOR)
- 1.6.2. Cryptage du *shellcode* (RSA)
- 1.6.3. Obfuscation de *strings*
- 1.6.4. Injection de processus

1.7. Analyse statique du *malware*
- 1.7.1. Analyse des *packers* avec DIE (*Detect It Easy*)
- 1.7.2. Analyse des sections avec PE-Bear
- 1.7.3. Décompilation avec Ghidra



1.8. Analyse dynamique du *malware*
- 1.8.1. Observation du comportement avec Process Hacker
- 1.8.2. Analyse des appels avec API Monitor
- 1.8.3. Analyser les modifications du registre avec Regshot
- 1.8.4. Observer les requêtes réseau avec TCPView

1.9. Analyse en .NET
- 1.9.1. Introduction à .NET
- 1.9.2. Décompilation avec dnSpy
- 1.9.3. Débogage avec dnSpy

1.10. Analyser de vrais *malware*
- 1.10.1. Préparation de l'environnement
- 1.10.2. Analyse statique du *malware*
- 1.10.3. Analyse dynamique du *malware*
- 1.10.4. Création de règles YARA

Module 2. Principes Fondamentaux de la Criminalistique et DFIR

2.1. La criminalistique numérique
- 2.1.1. Histoire et évolution de la criminalistique informatique
- 2.1.2. Importance de l'informatique légale dans la cybersécurité
- 2.1.3. Histoire et évolution de la criminalistique informatique

2.2. Principes fondamentaux de l'Informatique légale
- 2.2.1. La chaîne de contrôle et son application
- 2.2.2. Types de preuves numériques
- 2.2.3. Processus d'acquisition des preuves

2.3. Systèmes de fichiers et structure des données
- 2.3.1. Principaux systèmes de fichiers
- 2.3.2. Méthodes de dissimulation des données
- 2.3.3. Analyse des métadonnées et des attributs des fichiers

2.4. Analyse des Systèmes d'Exploitation
- 2.4.1. Analyse criminalistique des systèmes Windows
- 2.4.2. Analyse légale des systèmes Linux
- 2.4.3. Analyse légale des systèmes macOS

2.5. Récupération de données et analyse de disques
- 2.5.1. Récupération de données à partir de supports endommagés
- 2.5.2. Outils d'analyse de disque
- 2.5.3. Interprétation des tables d'allocation de fichiers

2.6. Analyse du réseau et du trafic
- 2.6.1. Capture et analyse des paquets réseau
- 2.6.2. Analyse du journal du *firewall*
- 2.6.3. Détection des intrusions sur le réseau

2.7. *Malware* et analyse des codes malveillants
- 2.7.1. Classification des *malwares* et de leurs caractéristiques
- 2.7.2. Analyse statique et dynamique des *malwares*
- 2.7.3. Techniques de désassemblage et de débogage

2.8. Analyse des journaux et des événements
- 2.8.1. Types de journaux dans les systèmes et les applications
- 2.8.2. Interprétation des événements pertinents
- 2.8.3. Outils d'analyse des journaux

2.9. Réaction aux incidents de sécurité
- 2.9.1. Processus de réponse aux incidents
- 2.9.2. Création d'un plan de réponse aux incidents
- 2.9.3. Coordination avec les équipes de sécurité

2.10. Présentation des preuves et aspects juridiques
- 2.10.1. Règles de la preuve numérique dans le domaine juridique
- 2.10.2. Préparation des rapports médico-légaux
- 2.10.3. Comparaître au procès en tant que témoin expert

Module 3. Exercices Avancés du *Red Team*

3.1. Techniques avancées de reconnaissance
- 3.1.1. Énumération avancée des sous-domaines
- 3.1.2. *Google Dorking* avancé
- 3.1.3. Les Réseaux Sociaux et theHarvester

3.2. Campagnes de *phishing* avancées
- 3.2.1. Qu'est-ce que le *Reverse-Proxy Phishing*
- 3.2.2. *2FA Bypass* avec Evilginx
- 3.2.3. Exfiltration de données

3.3. Techniques avancées de persistance
- 3.3.1. *Golden Tickets*
- 3.3.2. *Silver Tickets*
- 3.3.3. Technique *DCShadow*

3.4. Techniques d'évasion avancées
- 3.4.1. *Bypass* de l'AMSI
- 3.4.2. Modification des outils existants
- 3.4.3. Obfuscation de *Powershell*

3.5. Techniques avancées de déplacement latéral
- 3.5.1. *Pass-the-Ticket* (PtT)
- 3.5.2. *Overpass-the-Hash (Pass-the-Key)*
- 3.5.3. NTLM Relay

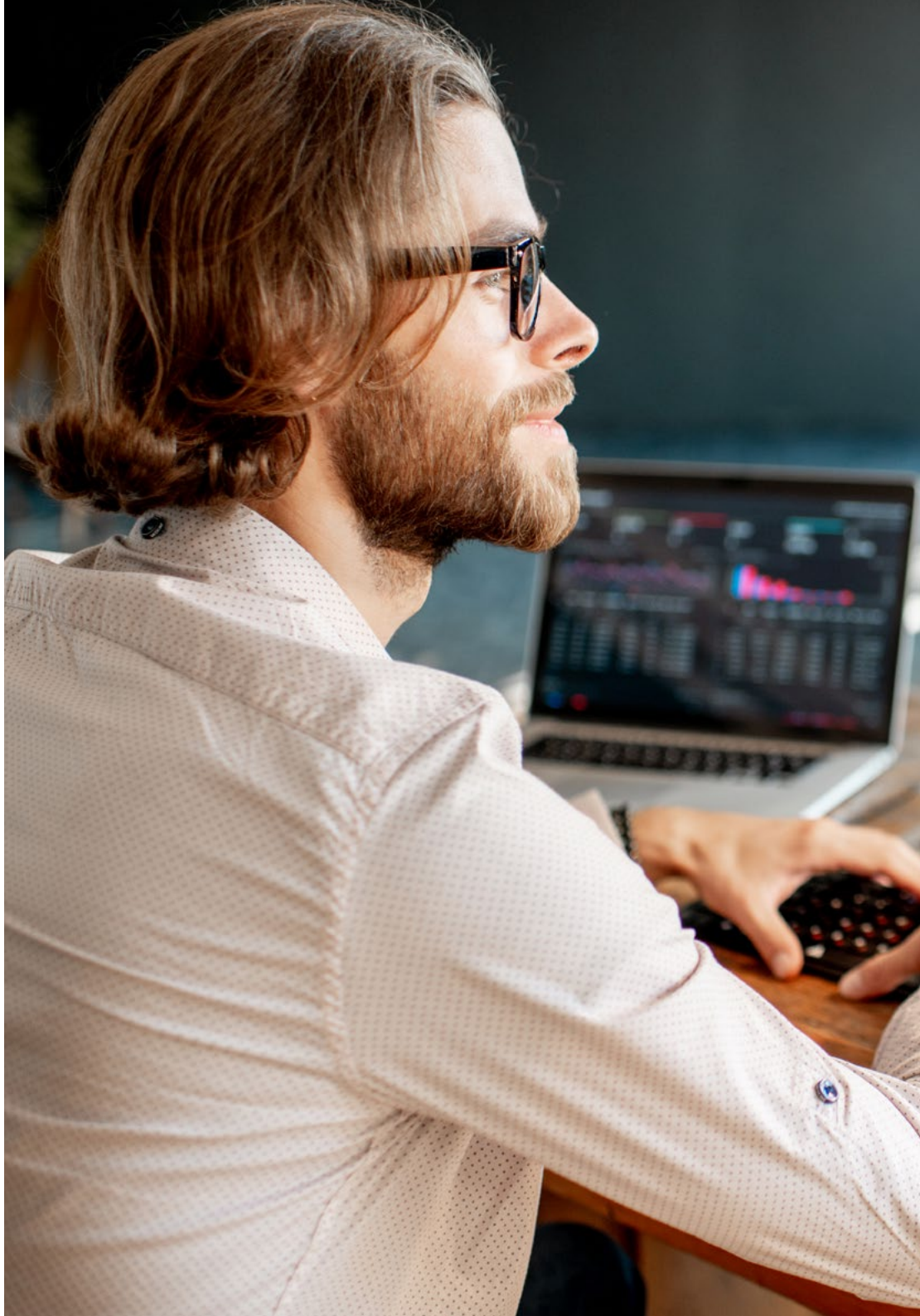
3.6. Techniques avancées de post-exploitation
- 3.6.1. *Dump* de LSASS
- 3.6.2. *Dump* de SAM
- 3.6.3. Attaque *DCSync*

3.7. Techniques avancées de *pivoting*
- 3.7.1. Qu'est-ce que le *pivoting*
- 3.7.2. Tunnel SSH
- 3.7.3. *Pivoting* avec un Ciseau

3.8. Intrusions physiques
- 3.8.1. Surveillance et reconnaissance
- 3.8.2. *Tailgating et Piggybacking*
- 3.8.3. *Lock-Picking*

3.9. Attaques Wi-Fi
- 3.9.1. Attaques WPA/WPA2 PSK
- 3.9.2. Attaques des Rogue AP
- 3.9.3. Attaques WPA2 *Enterprise*

3.10. Attaques RFID
- 3.10.1. Lecture de cartes RFID
- 3.10.2. Manipulation de cartes RFID
- 3.10.3. Création de cartes clonées



Ne manquez pas cette occasion de donner un coup de pouce à votre carrière grâce à ce programme innovant. Devenez un expert en Cybersécurité!"

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

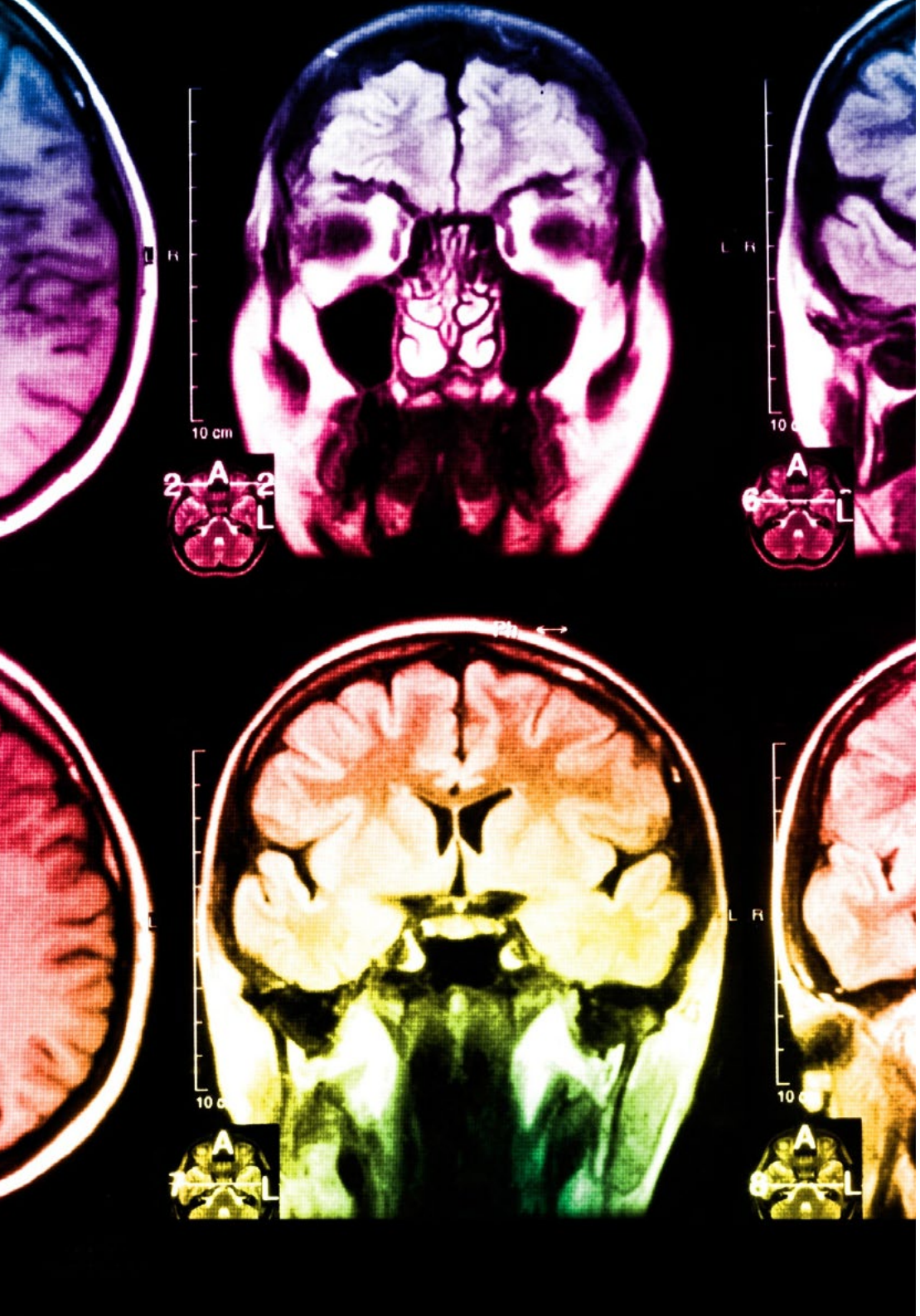
TECH combine efficacement la méthodologie des Études de Cas avec un système d'apprentissage 100% en ligne basé sur la répétition, qui associe différents éléments didactiques dans chaque leçon.

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.

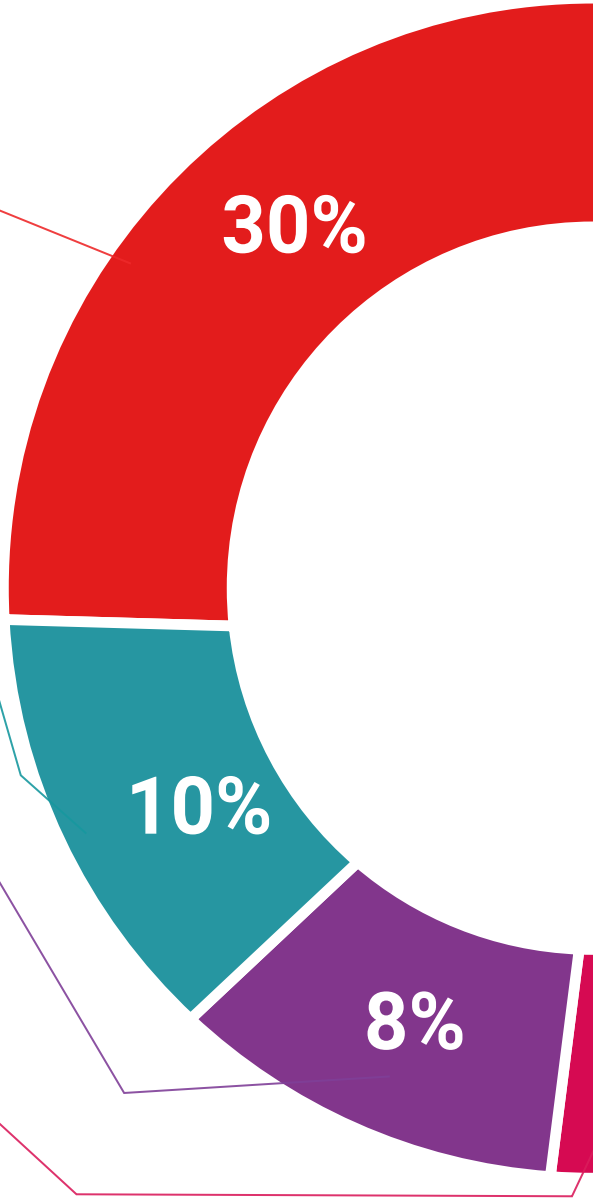
La méthode "Learning from an Expert" renforce les connaissances et la mémoire, et donne confiance dans les futures décisions difficiles.

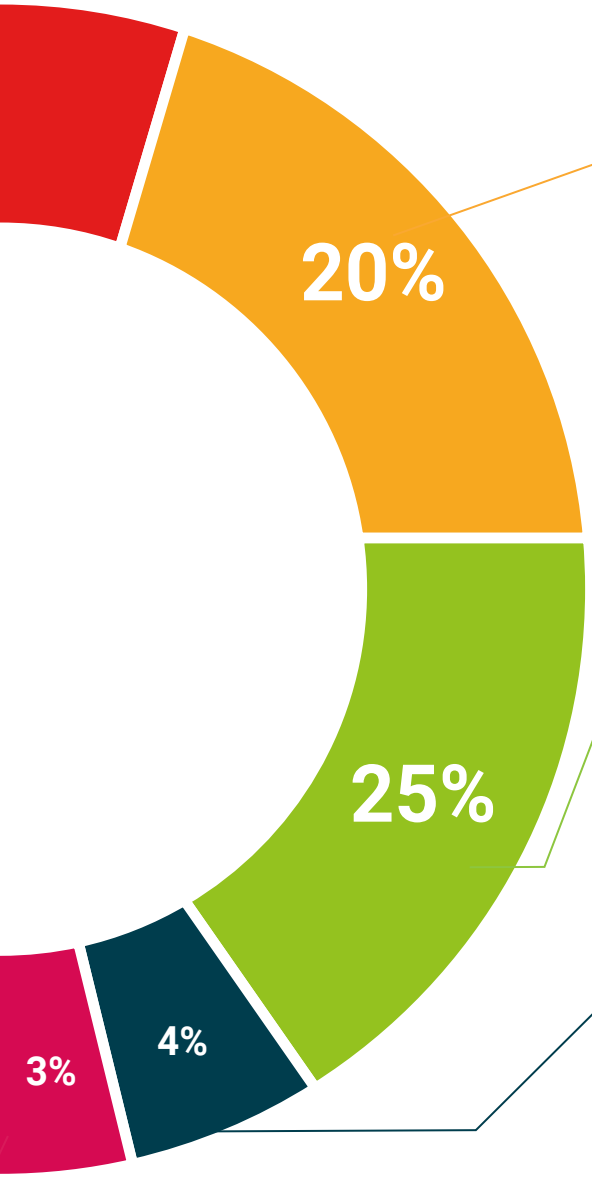
Pratiques en compétences et aptitudes

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 Red Team garantit, outre la formation la plus rigoureuse et la plus actualisée, l'accès à un diplôme de Certificat Avancé délivré par TECH Université Technologique.

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

Ce **Certificat Avancé en Cybersécurité Red Team** contient le programme le plus complet et actualisé du marché.

Après avoir passé l'évaluation, l'étudiant recevra par courrier* avec accusé de réception son diplôme de **Certificat Avancé** délivrée 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 Red Team**

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 Red Team

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

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

Fait le 17 juin 2020

Pre Tere Guevara Navarro
Rectrice

Code Unique TECH: AFWOR23S techtitute.com/diplômes

*Si l'étudiant souhaite que son diplôme version papier possède l'Apostille de La Haye, TECH EDUCATION fera les démarches nécessaires pour son obtention moyennant un coût supplémentaire.

tech université technologique

Certificat Avancé
Cybersécurité Red Team

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

Certificat Avancé
Cybersécurité Red Team

tech université technologique