Certificat Avancé
Cybersécurité Offensive

tech université technologique

tech université technologique

Certificat Avancé
Cybersécurité Offensive

- 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-offensive

Sommaire

01

Présentation

La cybersécurité est essentielle pour les institutions afin de protéger leurs actifs numériques, de maintenir leur réputation sociale et de se prémunir contre l'espionnage par des concurrents. Par conséquent, de plus en plus d'entreprises demandent à des experts en informatique de rejoindre leur organisation afin d'éviter des conséquences qui pourraient même affecter leurs capacités financières. Dans ce contexte, ces spécialistes doivent constamment mettre à jour leurs connaissances et leurs compétences afin de rester au fait des techniques de cybercriminalité. C'est pourquoi TECH a mis au point un Certificat Avancé innovant, dans le cadre duquel les menaces seront identifiées et atténuées. Il convient de noter que l'ensemble du programme sera enseigné en mode 100 % en ligne, afin de garantir aux étudiants une plus grande commodité et une plus grande flexibilité.

Vous en apprendrez plus sur le protocole Kerberos et sur la protection des informations dans les environnements réseau"

Chaque jour, les médias rapportent des cas de pirates informatiques qui portent atteinte à des institutions en accédant à leurs bases de données. Les conséquences de ces attaques sont graves, car elles perturbent les opérations et empêchent les entreprises de fonctionner efficacement. En fait, elles peuvent avoir un impact direct sur leur économie en entraînant des amendes pour non-respect des réglementations et une baisse des revenus.

À cet égard, TECH a créé un diplôme de pointe pour détecter les techniques d'intrusion les plus couramment utilisées, ainsi que les stratégies les plus optimales pour y faire face. Sous la direction d'un corps enseignant expérimenté dans le domaine, le programme d'études posera les bases essentielles pour comprendre le mode de pensée les hackers. Il fournira également une gamme de solutions visant à fournir des infrastructures sécurisées pour la gestion des certificats numériques sur un réseau d'entreprise.

Les professionnels apprendront également à préparer de manière optimale les environnements virtuels, grâce à la configuration de machines virtuelles ou de snapshots. En outre, les logiciels malveillants seront analysés, en examinant les appels avec API Monitor et en observant les requêtes réseau avec TCPView. Les diplômés apprendront des concepts théoriques dans des environnements simulés, ce qui les préparera à relever les défis du monde réel dans le domaine de la Cybersécurité Offensive. Enfin, l'accent sera mis sur l'éthique et la responsabilité sociale qui doivent caractériser les experts dans ce domaine.

Pour consolider la maîtrise de tous ces contenus, le Certificat Avancé applique le système innovant Relearning. TECH est un pionnier dans l'utilisation de ce modèle d'enseignement, qui favorise l'assimilation de concepts complexes par leur réitération naturelle et progressive. Le programme utilise également du matériel sous différents formats, tels que des vidéos explicatives, des résumés interactifs et des infographies. Tout cela dans un mode pratique 100% en ligne, qui permet à chacun d'adapter son emploi du temps à ses responsabilités et à sa disponibilité.

Ce **Certificat Avancé en Cybersécurité Offensive** 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 Offensive
- Le contenu graphique, schématique et éminemment pratique de l'ouvrage fournit des informations complètes et pratiques sur les disciplines essentielles à la pratique professionnelle
- Des exercices pratiques où le processus d'auto-évaluation peut être utilisé pour 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
- Il est possible d'accéder aux contenus depuis tout appareil fixe ou portable doté d'une connexion à internet

Développez vos compétences en tant qu'auditeur offensif et lancez-vous dans un nouveau défi professionnel au sein des entreprises numériques les plus prestigieuses"

Vous atteindrez vos objectifs grâce aux outils didactiques de TECH, notamment des vidéos explicatives et des résumés interactifs"

Voulez-vous devenir un Big Bounty Hunter? Vous attraperez n'importe quelle vulnérabilité sur Internet grâce à ce programme.

En seulement 6 mois, vous maîtriserez la gestion des identités dans Azure AD. Inscrivez-vous maintenant!

Le corps enseignant du programme comprend des professionnels du secteur qui apportent à cette formation leur expérience professionnelle dans cette formation, ainsi que des spécialistes reconnus de sociétés et d'organismes de premier plan de sociétés de référence 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 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

La conception de ce programme offre une expérience éducative unique, qui se distingue par son approche pratique et innovante de la Cybersécurité. Ainsi, les étudiants aborderont tous les aspects de la question, de l'analyse des vulnérabilités aux techniques d'intrusion avancées. Dans cette optique, les mesures optimales pour évaluer et renforcer les différents systèmes cybernétiques seront proposées. En outre, l'accent sera mis sur les responsabilités juridiques et éthiques que les experts dans ce domaine devraient adopter.

Réduire les menaces des logiciels malveillants avec la meilleure université numérique du monde, selon Forbes"

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 logiciels malveillants, 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. Sécurité Offensive

- Familiariser le diplômé avec les méthodologies de test de pénétration, y compris les phases clés telles que la collecte d'informations, l'analyse de la vulnérabilité, l'exploitation et la documentation
- Développer des compétences pratiques dans l'utilisation d'outils de *Pentesting* spécialisés pour identifier et évaluer les vulnérabilités des systèmes et des réseaux
- Étudier et comprendre les tactiques, les techniques et les procédures utilisées par les acteurs malveillants, ce qui permet d'identifier et de simuler les menaces
- Appliquer les connaissances théoriques dans des scénarios pratiques et des simulations, en faisant face à des défis réels pour renforcer les compétences de *Pentesting*
- Développer des compétences efficaces en matière de documentation, en créant des rapports détaillés reflétant les résultats, les méthodologies utilisées et les recommandations pour l'amélioration de la sécurité
- Pratiquer une collaboration efficace au sein des équipes de sécurité offensive, en optimisant la coordination et l'exécution des activités de *Pentesting*

Module 2. Attaques des Réseaux et des Systèmes Windows

- Développer des compétences pour identifier et évaluer les vulnérabilités spécifiques des systèmes d'exploitation Windows
- Apprendre les tactiques avancées utilisées par les attaquants pour s'infiltrer et persister dans les réseaux basés sur les environnements Windows
- Acquérir des compétences en matière de stratégies et d'outils permettant d'atténuer les menaces spécifiques ciblant les systèmes d'exploitation Windows
- Familiariser le diplômé avec les techniques d'analyse médico-légale appliquées aux systèmes Windows, afin de faciliter l'identification et la réponse aux incidents

- Appliquer les connaissances théoriques dans des environnements simulés, en participant à des exercices pratiques pour comprendre et contrer des attaques spécifiques contre les systèmes Windows
- Apprendre des stratégies spécifiques pour sécuriser les environnements d'entreprise utilisant des systèmes d'exploitation Windows, en tenant compte de la complexité des infrastructures d'entreprise
- Développer des compétences pour évaluer et améliorer les configurations de sécurité dans les systèmes Windows, en assurant la mise en œuvre de mesures efficaces
- Promouvoir des pratiques éthiques et légales dans l'exécution d'attaques et de tests sur les systèmes Windows, en tenant compte des principes éthiques de la cybersécurité
- Maintenir l'étudiant au courant des dernières tendances et menaces en matière d'attaques sur les systèmes Windows, en garantissant la pertinence et l'efficacité continues des compétences acquises

Module 3. 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

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

03

Direction de la formation

Dans son engagement à offrir une éducation d'excellence, TECH dispose d'un corps enseignant prestigieux. Il convient de noter que ces spécialistes possèdent une vaste expérience professionnelle, ayant fait partie d'entreprises renommées dédiées à la Cybersécurité Offensive. C'est pourquoi le parcours académique comprendra les ressources et les technologies les plus avancées dans ce domaine. En outre, une approche globale sera proposée pour répondre aux attentes des diplômés qui souhaitent se spécialiser dans un domaine qui leur offrira de nombreuses opportunités.

Vous bénéficierez du soutien d'un corps enseignant composé d'éminents professionnels de la Cybersécurité Offensive"

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

Professeurs

M. González Parrilla, Yuba

- Coordinateur de la Ligne de Sécurité Offensive et Red Team
- Spécialiste en Gestion *Prédictive* de Projet à l'Institut de Gestion de Projet
- Spécialiste de *SmartDefense*
- Expert en *Web Application Penetration Tester* chez eLearnSecurity
- *Junior Penetration Tester* chez eLearnSecurity
- Diplômé en Ingénierie Informatique à l'Université Polytechnique de Madrid

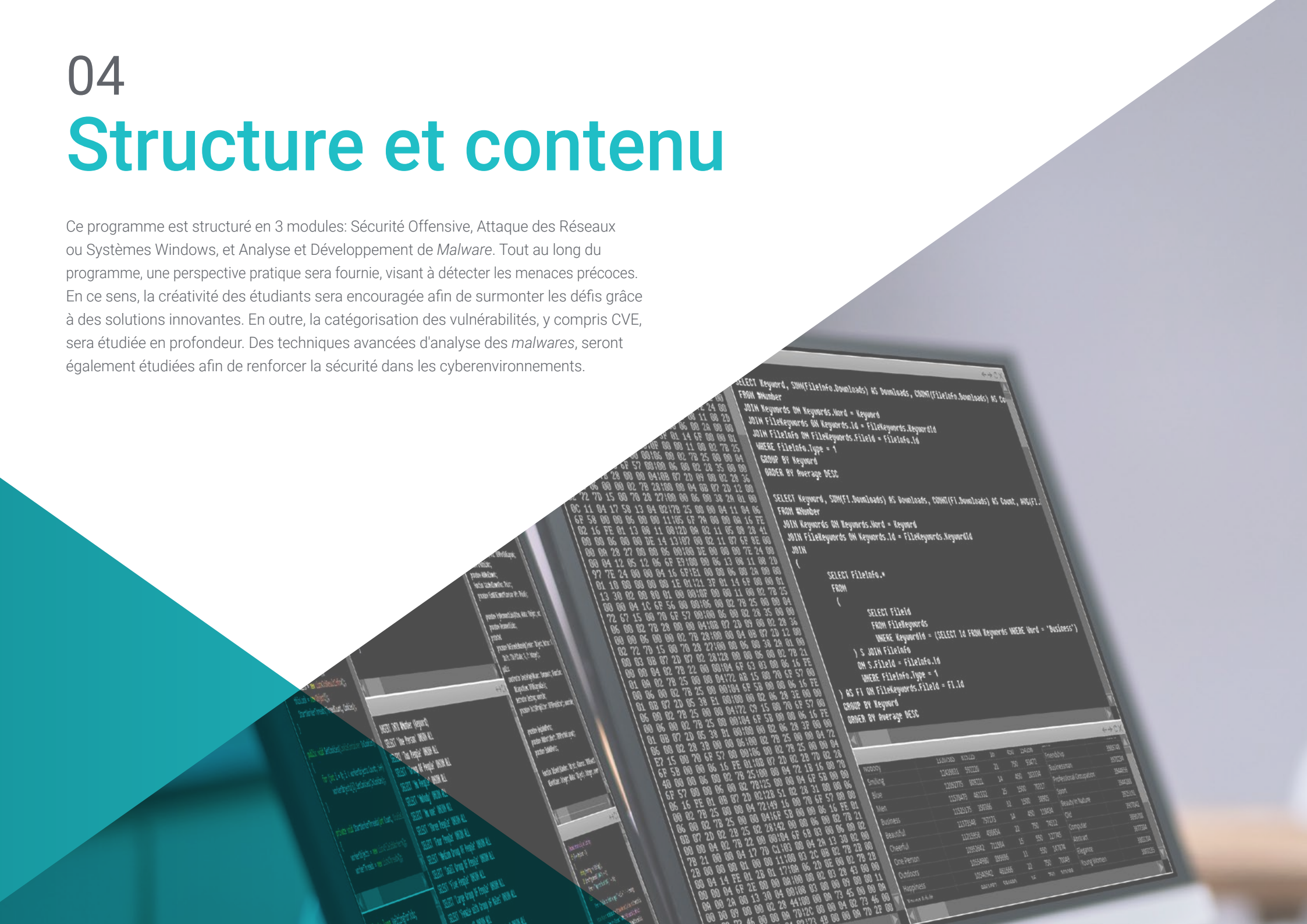
M. Gallego Sánchez, Alejandro

- Pentester chez Groupe Oesía
- Consultant en Cybersécurité à Integration Technologique Empresarial, S.L.
- Technicien Audiovisuel chez Ingénierie Audiovisuelle S.A.
- Diplômé en Ingénierie de la Cybersécurité de l'Université Rey Juan Carlos

04

Structure et contenu

Ce programme est structuré en 3 modules: Sécurité Offensive, Attaque des Réseaux ou Systèmes Windows, et Analyse et Développement de *Malware*. Tout au long du programme, une perspective pratique sera fournie, visant à détecter les menaces précoces. En ce sens, la créativité des étudiants sera encouragée afin de surmonter les défis grâce à des solutions innovantes. En outre, la catégorisation des vulnérabilités, y compris CVE, sera étudiée en profondeur. Des techniques avancées d'analyse des *malwares*, seront également étudiées afin de renforcer la sécurité dans les cyberenvironnements.



Vous accéderez à un système d'apprentissage basé sur la répétition, avec un enseignement naturel et progressif tout au long du programme"

Module 1. Sécurité Offensive

1.1. Définition et contexte
- 1.1.1. Concepts fondamentaux de la sécurité offensive
- 1.1.2. Importance de la cybersécurité aujourd'hui
- 1.1.3. Défis et opportunités en matière de sécurité offensive

1.2. Bases de la cybersécurité
- 1.2.1. Les premiers défis et l'évolution des menaces
- 1.2.2. Les étapes technologiques et leur impact sur la cybersécurité
- 1.2.3. La cybersécurité à l'ère moderne

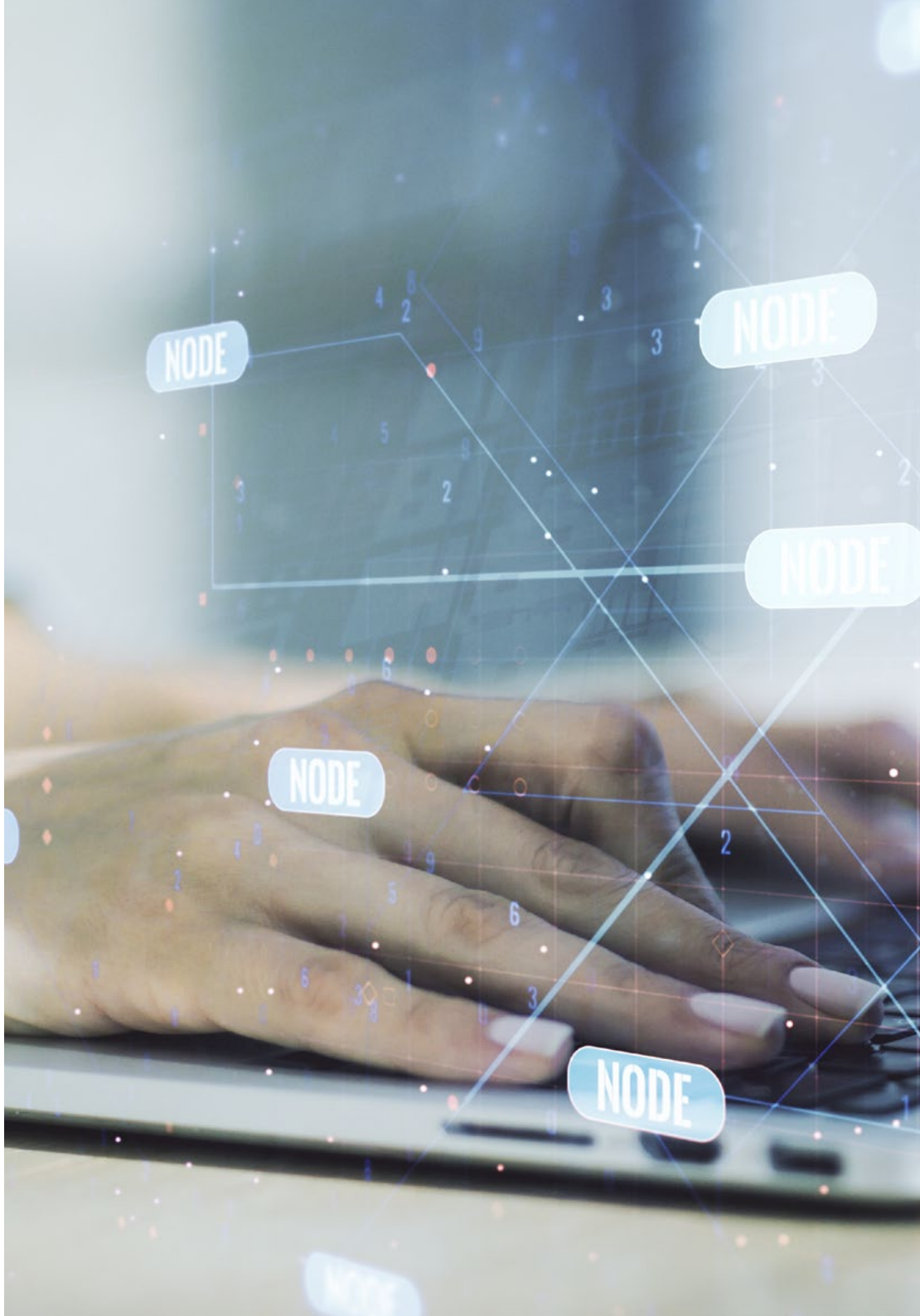
1.3. Bases de la sécurité offensive
- 1.3.1. Concepts clés et terminologie
- 1.3.2. *Think Outside the Box*
- 1.3.3. Différences entre hacking offensif et hacking défensif

1.4. Méthodologies de sécurité offensives
- 1.4.1. PTES (*Penetration Testing Execution Standard*)
- 1.4.2. OWASP (*Open Web Application Security Project*)
- 1.4.3. *Cyber Security Kill Chain*

1.5. Rôles et responsabilités en matière de sécurité offensive
- 1.5.1. Profils principaux
- 1.5.2. *Bug Bounty Hunters*
- 1.5.3. *Researching:* L'art de la recherche

1.6. L'arsenal offensif de l'auditeur
- 1.6.1. Systèmes d'exploitation pour hacking
- 1.6.2. Introduction au C2
- 1.6.3. *Metasploit:* Principes de base et Utilisation
- 1.6.4. Ressources utiles

1.7. OSINT: Renseignement de Sources Ouvertes
- 1.7.1. Les bases de la OSINT
- 1.7.2. Techniques et outils OSINT
- 1.7.3. Applications OSINT en matière de sécurité offensive



1.8. Scripting: Introduction à l'automatisation
- 1.8.1. Principes de base de scripting
- 1.8.2. *Scripting* en Bash
- 1.8.3. *Scripting* en Python

1.9. Catégorisation des vulnérabilités
- 1.9.1. CVE (*Common Vulnerabilities and Exposure*)
- 1.9.2. CWE (*Common Weakness Enumeration*)
- 1.9.3. CAPEC (*Common Attack Pattern Enumeration and Classification*)
- 1.9.4. CVSS (*Common Vulnerability Scoring System*)
- 1.9.5. MITRE ATT & CK

1.10. Éthique et *hacking*
- 1.10.1. Principes de l'éthique du *hacker*
- 1.10.2. La frontière entre le *hacking* éthique et le hacking malveillant
- 1.10.3. Implications et conséquences juridiques
- 1.10.4. Étude de cas: Situations éthiques en cybersécurité

Module 2. Attaques des Réseaux et des Systèmes Windows

2.1. Windows et Active Directory
- 2.1.1. Histoire et évolution de Windows
- 2.1.2. Principes de base d'Active Directory
- 2.1.3. Fonctions et services d'Active Directory
- 2.1.4. Architecture générale d'Active Directory

2.2. Réseaux dans les environnements Active Directory
- 2.2.1. Protocoles de réseau dans Windows
- 2.2.2. DNS et son fonctionnement dans Active Directory
- 2.2.3. Outils de diagnostic réseau
- 2.2.4. Mise en œuvre du réseau dans Active Directory

2.3. Authentification et autorisation dans Active Directory
- 2.3.1. Processus et flux d'authentification
- 2.3.2. Types de certificats
- 2.3.3. Stockage et gestion des certificats
- 2.3.4. Sécurité de l'authentification

2.4. Permissions et stratégies dans Active Directory
- 2.4.1. GPOs
- 2.4.2. Application et gestion des GPO
- 2.4.3. Gestion des autorisations dans Active Directory
- 2.4.4. Vulnérabilités en matière de permissions et mesures d'atténuation

2.5. Principes de base de Kerberos
- 2.5.1. Qu'est-ce que Kerberos?
- 2.5.2. Composants et fonctionnement
- 2.5.3. Tickets dans Kerberos
- 2.5.4. Kerberos dans le contexte d'Active Directory

2.6. Techniques avancées de Kerberos
- 2.6.1. Attaques courantes contre Kerberos
- 2.6.2. Atténuations et protections
- 2.6.3. Surveillance du trafic Kerberos
- 2.6.4. Attaques avancées contre Kerberos

2.7. *Active Directory Certificate Services* (ADCS)
- 2.7.1. Les bases du PKI
- 2.7.2. Rôles et composants ADCS
- 2.7.3. Configuration et déploiement de l'ADCS
- 2.7.4. Sécurité ADCS

2.8. Attaques et défenses des *Active Directory Certificate Services* (ADCS)
- 2.8.1. Vulnérabilités courantes dans ADCS
- 2.8.2. Attaques et techniques d'exploitation
- 2.8.3. Défenses et atténuations
- 2.8.4. Surveillance et audit des ADCS

2.9. Audit de l'Active Directory
- 2.9.1. Importance de l'audit de l'Active Directory
- 2.9.2. Outils d'audit
- 2.9.3. Détection des anomalies et des comportements suspects
- 2.9.4. Réponse aux incidents et récupération

2.10. Azure AD
- 2.10.1. Principes de base d'Azure AD
- 2.10.2. Synchronisation avec l'Active Directory local
- 2.10.3. Gestion des identités dans Azure AD
- 2.10.4. Intégration avec les applications et les services

Module 3. Analyse et Développement de *Malware*

3.1. Analyse et développement de *malware*
- 3.1.1. Histoire et évolution des *malware*
- 3.1.2. Classification et types de *malware*
- 3.1.3. Analyse des *malware*
- 3.1.4. Développement de *malware*

3.2. Préparation de l'environnement
- 3.2.1. Configuration de la Machine Virtuelle et *Snapshots*
- 3.2.2. Outils d'analyse des malware
- 3.2.3. Outils de développement de malware

3.3. Principes de base de Windows
- 3.3.1. Format de fichier PE (*Portable Executable*)
- 3.3.2. Processus et *Threads*
- 3.3.3. Système de fichiers et registre
- 3.3.4. *Windows Defender*

3.4. Techniques de *malware* de base
- 3.4.1. Génération de *shellcode*
- 3.4.2. Exécution du *shellcode* sur le disque
- 3.4.3. Disque vs mémoire
- 3.4.4. Exécution du *shellcode* en mémoire

3.5. Techniques de *malware* intermédiaires
- 3.5.1. Persistance sur Windows
- 3.5.2. Dossier d'accueil
- 3.5.3. Clés de registre
- 3.5.4. Économiseur d'écran

3.6. Techniques des *malwares* avancés
- 3.6.1. Cryptage du *shellcode* (XOR)
- 3.6.2. Cryptage du *shellcode* (RSA)
- 3.6.3. Obfuscation de *strings*
- 3.6.4. Injection de processus

3.7. Analyse statique du *malware*
- 3.7.1. Analyse des *packers* avec DIE (*Detect It Easy*)
- 3.7.2. Analyse des sections avec PE-Bear
- 3.7.3. Décompilation avec Ghidra

3.8. Analyse dynamique du *malware*
- 3.8.1. Observation du comportement avec Process Hacker
- 3.8.2. Analyse des appels avec API Monitor
- 3.8.3. Analyser les modifications du registre avec Regshot
- 3.8.4. Observer les requêtes réseau avec TCPView

3.9. Analyse en .NET
- 3.9.1. Introduction à .NET
- 3.9.2. Décompilation avec dnSpy
- 3.9.3. Débogage avec dnSpy
- 3.10. Analyser de vrais malware

3.10.1. Préparation de l'environnement
- 3.10.2. Analyse statique du *malware*
- 3.10.3. Analyse dynamique du *malware*
- 3.10.4. Création de règles YARA

Pas d'horaires préétablis ni de programmes d'évaluation. Voilà ce qu'est cette formation TECH!"

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

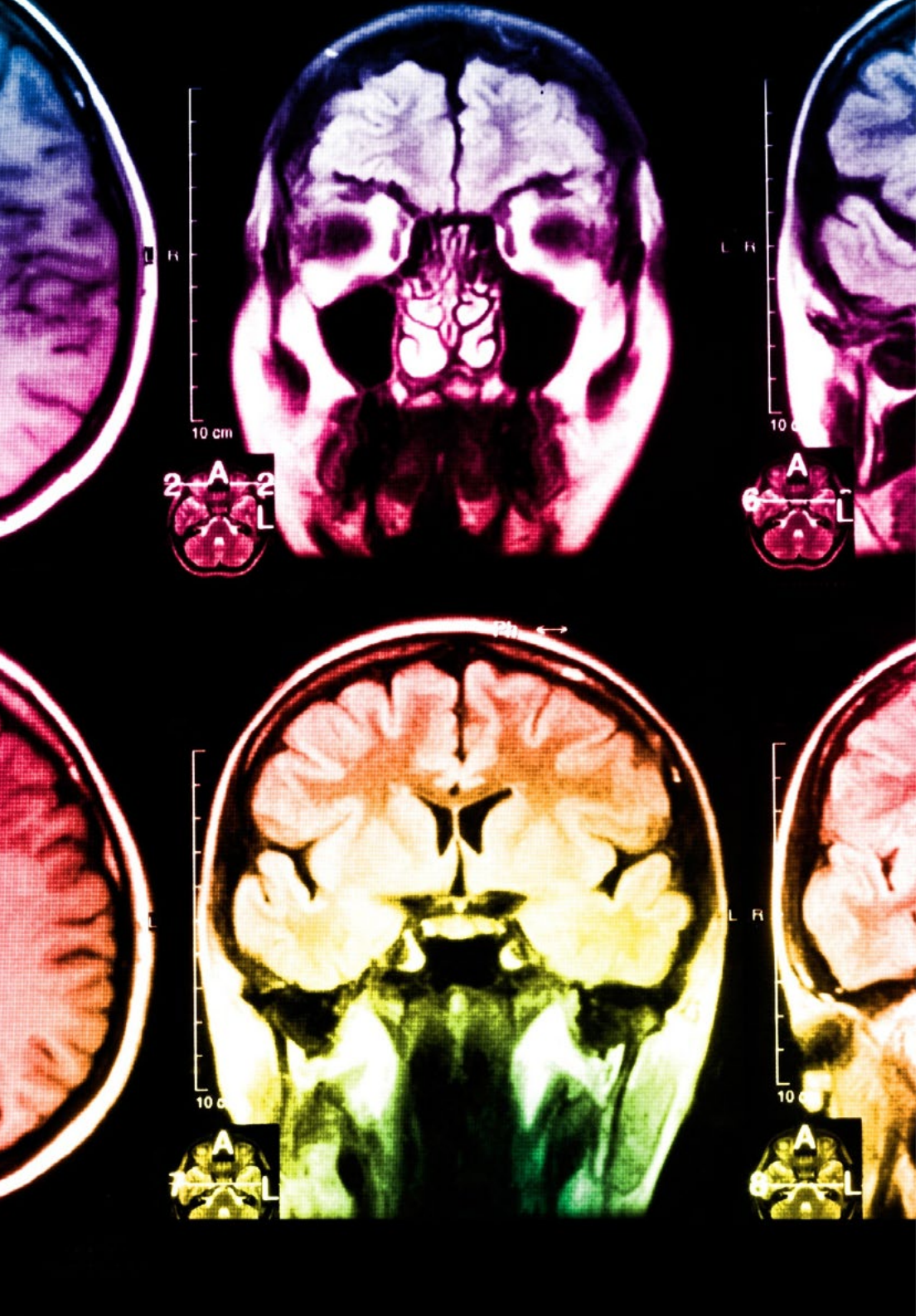
TECH combine efficacement la méthodologie des Études de Cas avec un système d'apprentissage 100% en ligne basé sur la répétition, qui associe différents éléments didactiques dans chaque leçon.

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.

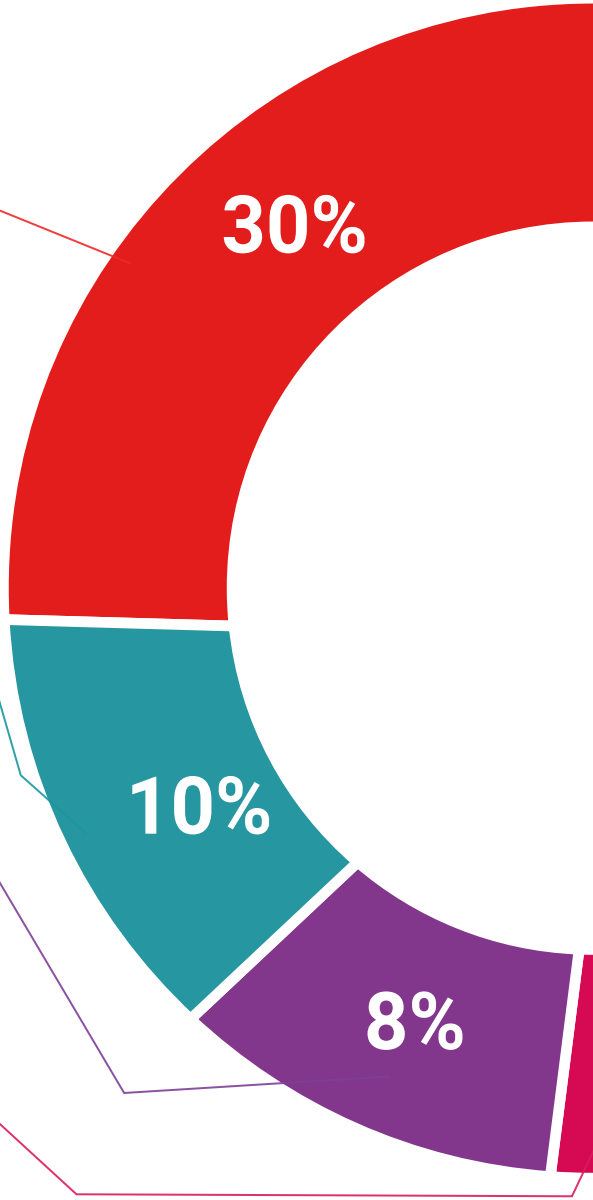
La méthode "Learning from an Expert" renforce les connaissances et la mémoire, et donne confiance dans les futures décisions difficiles.

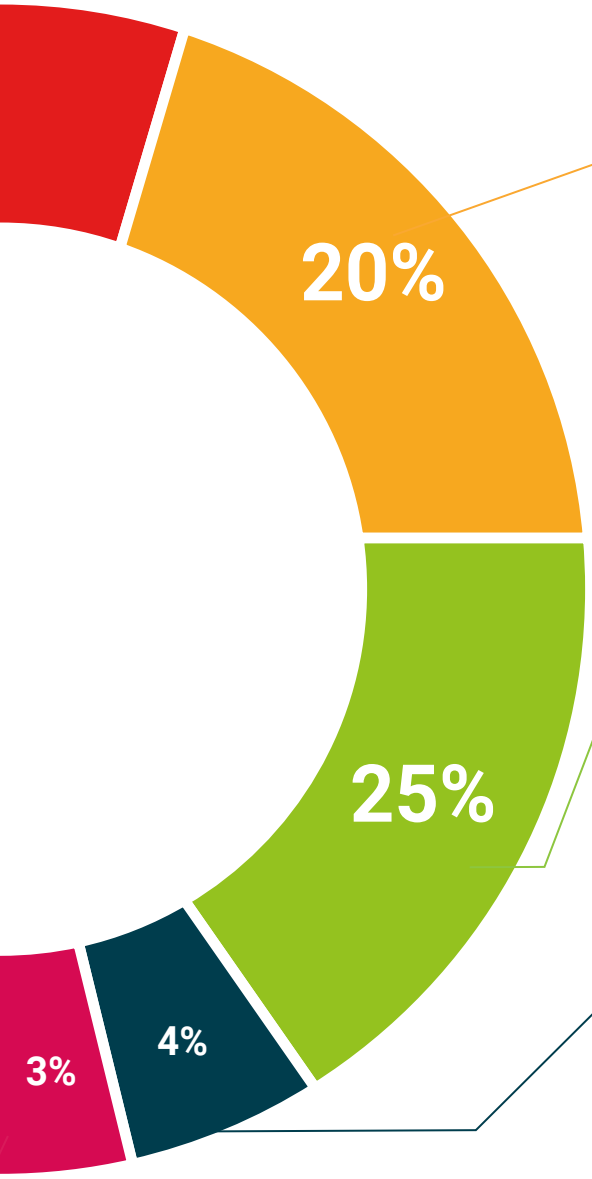
Pratiques en compétences et aptitudes

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 Offensive 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 Offensive** 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 Offensive**

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 Offensive

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 Offensive

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

Certificat Avancé
Cybersécurité Offensive

tech université technologique