Mastère Spécialisé
Pentesting et Red Team

tech global university

tech global university

Mastère Spécialisé
Pentesting et Red Team

- Modalité: **en ligne**
- Durée: **12 mois**
- Qualification: **TECH Global University**
- Accréditation: **60 ECTS**
- Horaire: **à votre rythme**
- Examens: **en ligne**

Accès au site web: www.techtitute.com/fr/informatique/master/master-pentesting-red-team

Sommaire

01

Présentation

Le nombre et la sophistication des cyberattaques ont atteint des proportions alarmantes. Avec l'augmentation exponentielle des menaces, des attaques par *ransomware* aux intrusions avancées, le besoin de professionnels de la cybersécurité hautement qualifiés est crucial. C'est dans ce contexte que s'inscrit ce programme, qui offrira non seulement une immersion complète dans les techniques de sécurité avancées, mais abordera également la réalité d'un environnement numérique en constante évolution. Ainsi, les étudiants approfondiront leur compréhension des techniques d'attaque et de défense, en faisant face aux défis les plus sophistiqués en matière de sécurité. Motivé par la nécessité de renforcer les cyberdéfenses, ce programme d'études se distingue par sa méthodologie 100 % en ligne et l'utilisation efficace de la méthode *Relearning* pour optimiser l'apprentissage.

Vous concevrez des protocoles de sécurité imprenables grâce à ce programme pionnier, avec la garantie de TECH"

Il est essentiel de rester à jour pour préserver l'efficacité de la défense contre les menaces actuelles et émergentes. À cet égard, l'évolution rapide de la technologie et des tactiques cybernétiques a fait de la mise à jour constante un impératif. La prolifération des menaces souligne l'urgence de disposer de professionnels hautement qualifiés.

Dans ce contexte, ce programme universitaire s'avère être une réponse essentielle, car il permettra non seulement d'acquérir une compréhension approfondie des techniques les plus avancées en matière de cybersécurité, mais aussi de s'assurer que les professionnels sont à la pointe des dernières tendances et technologies.

Dans le programme de ce Mastère Spécialisé en Pentesting et Red Team, le diplômé abordera de manière exhaustive les demandes dans le domaine de la cybersécurité. Il mettra en œuvre des mesures de sécurité réseau efficaces, notamment des pare-feu, des systèmes de détection d'intrusion (IDS) et une segmentation du réseau. À cette fin, les spécialistes appliqueront des méthodes de recherche en criminalistique numérique pour résoudre les cas, de l'identification à la documentation des résultats.

En outre, ils développeront des compétences en matière de simulation de menaces avancées, en reproduisant les tactiques, techniques et procédures les plus couramment utilisées par les acteurs malveillants. En outre, l'approche innovante de TECH garantira l'acquisition de compétences applicables et utiles dans l'environnement professionnel de la cybersécurité.

La méthodologie du parcours académique renforce son caractère innovant, puisqu'il offrira un environnement éducatif 100 % en ligne. Ce programme sera adapté aux besoins des professionnels occupés qui cherchent à faire progresser leur carrière. En outre, il utilisera la méthodologie *Relearning*, basée sur la répétition de concepts clés pour fixer les connaissances et faciliter l'apprentissage. Ainsi, la combinaison de la flexibilité et de l'approche pédagogique robuste rendra le programme non seulement accessible, mais aussi très efficace pour préparer les informaticiens aux défis dynamiques de la cybersécurité.

Ce **Mastère Spécialisé en Pentesting et 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 Pentesting et 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.
- Les exercices pratiques où effectuer le processus d'auto-évaluation 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

En seulement 12 mois, vous donnerez à votre carrière l'élan dont elle a besoin. Inscrivez-vous dès maintenant et faites des progrès immédiats!"

Vous voulez faire un bond qualitatif dans votre carrière? Avec TECH, vous serez formé à la mise en œuvre de stratégies pour l'exécution efficace de projets de cybersécurité"

Vous apprendrez en profondeur l'identification et l'évaluation des vulnérabilités dans les applications web, grâce à la meilleure université numérique au monde selon Forbes.

Vous maîtriserez les techniques forensiques dans des environnements de Pentesting. Positionnez-vous comme l'expert en cybersécurité que toutes les entreprises recherchent!

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.

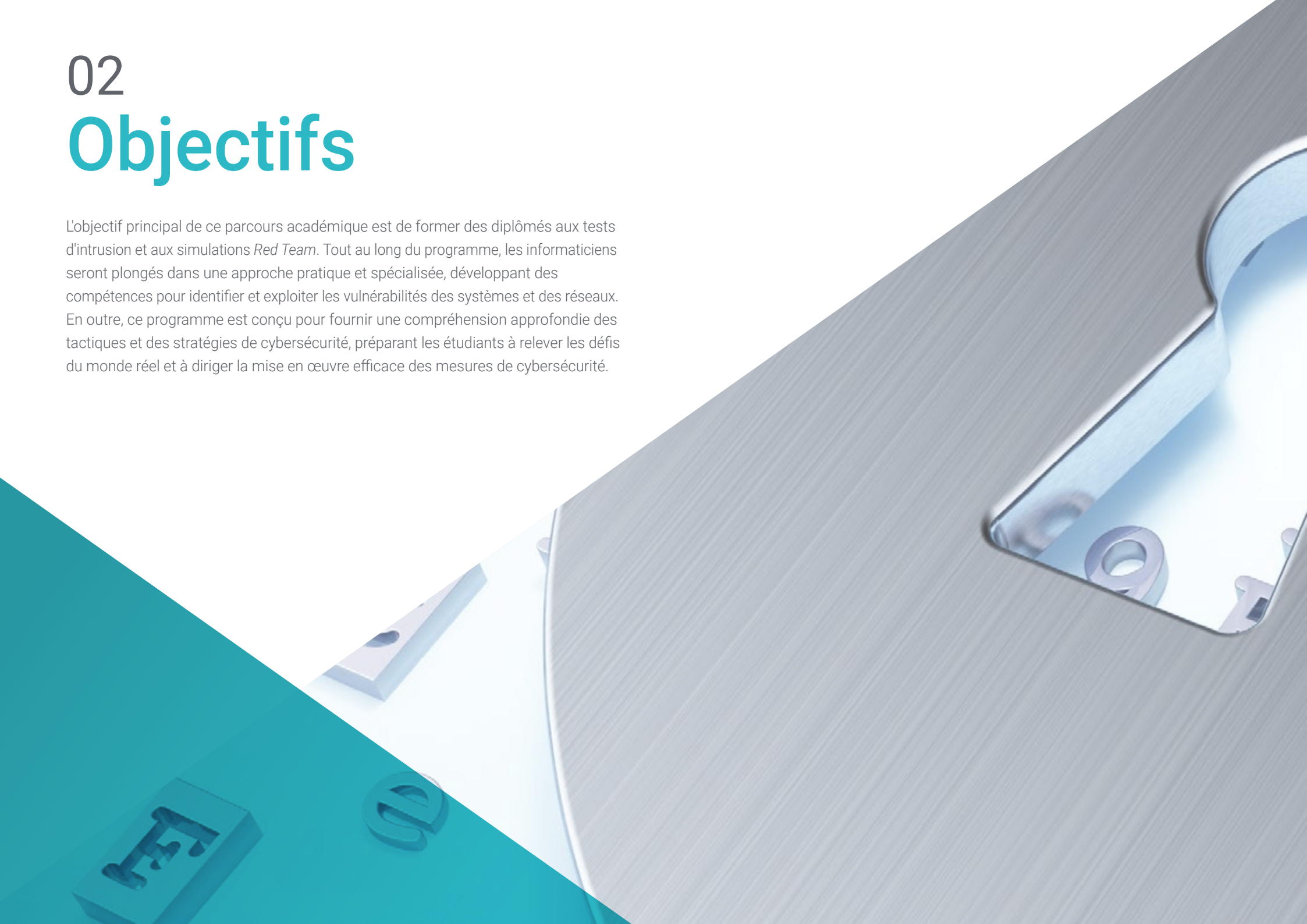
Grâce à son contenu multimédia développé avec les dernières technologies éducatives, les spécialistes bénéficieront d'un apprentissage situé et contextuel, ainsi, ils se formeront dans un environnement simulé qui leur permettra d'apprendre en immersion et de s'entrainer dans des situations réelles.

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

L'objectif principal de ce parcours académique est de former des diplômés aux tests d'intrusion et aux simulations *Red Team*. Tout au long du programme, les informaticiens seront plongés dans une approche pratique et spécialisée, développant des compétences pour identifier et exploiter les vulnérabilités des systèmes et des réseaux. En outre, ce programme est conçu pour fournir une compréhension approfondie des tactiques et des stratégies de cybersécurité, préparant les étudiants à relever les défis du monde réel et à diriger la mise en œuvre efficace des mesures de cybersécurité.



Vous approfondirez l'analyse et le développement de logiciels malveillants afin de vous positionner en tant que professionnel de premier plan. 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 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

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

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. Gestion des Équipes de Cybersécurité

- Développer des compétences de leadership spécifiques aux équipes de cybersécurité, y compris la capacité à motiver, inspirer et coordonner les efforts pour atteindre des objectifs communs
- Apprendre à allouer efficacement les ressources au sein d'une équipe de cybersécurité, en tenant compte des compétences individuelles et en maximisant la productivité des projets

- Améliorer les compétences de communication spécifiques aux environnements techniques, en facilitant la compréhension et la coordination entre les membres de l'équipe
- Apprendre des stratégies pour identifier et gérer les conflits au sein de l'équipe de cybersécurité, afin de promouvoir un environnement de travail collaboratif et efficace
- Apprendre à mettre en place des mesures et des systèmes d'évaluation pour mesurer les performances des équipes de cybersécurité et procéder aux ajustements nécessaires
- Promouvoir l'intégration de pratiques éthiques dans la gestion des équipes de cybersécurité, en veillant à ce que toutes les activités soient menées dans le respect de l'éthique et de la loi
- Développer des compétences pour la préparation et la gestion efficace des incidents de cybersécurité, en garantissant une réponse rapide et efficace aux menaces

Module 3. Gestion des Projets de Sécurité

- Développer des compétences pour planifier des projets de cybersécurité, en définissant les objectifs, la portée, les ressources et les délais de mise en œuvre
- Apprendre des stratégies pour l'exécution efficace des projets de sécurité, en assurant la mise en œuvre réussie des mesures planifiées
- Développer des compétences pour une gestion efficace des budgets et de l'allocation des ressources dans les projets de sécurité, en maximisant l'efficacité et en minimisant les coûts
- Améliorer l'efficacité de la communication avec *stakeholders*, en présentant des rapports et des mises à jour de manière claire et compréhensible
- Apprendre les techniques de suivi et de contrôle des projets, en identifiant les écarts et en prenant les mesures correctives nécessaires
- Familiariser les apprenants avec les méthodologies agiles de *Pentesting*
- Développer des compétences en matière de documentation et de rapports détaillés, afin de fournir une vision claire de l'avancement du projet et des résultats obtenus
- Favoriser une collaboration efficace entre les différentes équipes et disciplines au sein des projets de sécurité, afin de garantir une approche intégrée et coordonnée
- Apprendre des stratégies pour évaluer et mesurer l'efficacité des mesures mises en œuvre, afin d'assurer une amélioration continue de la posture de sécurité de l'organisation

Module 4. 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 5. *Hacking* Web Avancé

- Développer des compétences pour identifier et évaluer les vulnérabilités des applications web, y compris les injections SQL, le *Cross-Site Scripting* (XSS) et d'autres vecteurs d'attaque courants
- Apprendre à effectuer des tests de sécurité sur des applications web modernes
- Acquérir des compétences dans les techniques avancées de piratage web, en explorant des stratégies pour contourner les mesures de sécurité et exploiter des vulnérabilités sophistiquées
- Familiariser le diplômé avec l'évaluation de la sécurité des API et des services web, en identifiant les points de vulnérabilité possibles et en renforçant la sécurité des interfaces de programmation
- Développer des compétences pour mettre en œuvre des mesures d'atténuation efficaces dans les applications web, en réduisant l'exposition aux attaques et en renforçant la sécurité
- Participer à des simulations pratiques pour évaluer la sécurité dans des environnements web complexes, en appliquant les connaissances à des scénarios du monde réel
- Développer des compétences dans la formulation de stratégies de défense efficaces pour protéger les applications web contre les cyber-menaces
- Apprendre à aligner les pratiques avancées de *hacking web* sur les réglementations et les normes de sécurité pertinentes, en veillant au respect des cadres juridiques et éthiques
- Favoriser une collaboration efficace entre les équipes de développement et de sécurité

Module 6. Architecture et Sécurité des Réseaux

- Acquérir une connaissance avancée de l'architecture des réseaux, y compris les topologies, les protocoles et les composants clés
- Développer des compétences pour identifier et évaluer les vulnérabilités spécifiques des infrastructures de réseau, en tenant compte des menaces potentielles
- Apprendre à mettre en œuvre des mesures de sécurité réseau efficaces, notamment des *firewalls*, des systèmes de détection d'intrusion (IDS) et la segmentation du réseau
- Familiariser l'étudiant avec les technologies de réseau émergentes, telles que les réseaux définis par logiciel (SDN), et comprendre leur impact sur la sécurité
- Développer des compétences en matière de sécurisation des communications réseau, y compris la protection contre les menaces telles que le *sniffing* et les attaques intermédiaires
- Apprendre à évaluer et à améliorer les configurations de sécurité dans les environnements de réseaux d'entreprise, afin de garantir une protection adéquate
- Développer des compétences pour mettre en œuvre des mesures d'atténuation efficaces contre les menaces sur les réseaux d'entreprise, qu'il s'agisse d'attaques internes ou de menaces externes
- Favoriser une collaboration efficace avec les équipes de sécurité, en intégrant les stratégies et les efforts visant à protéger l'infrastructure du réseau
- Promouvoir des pratiques éthiques et juridiques dans la mise en œuvre des mesures de sécurité des réseaux, en veillant au respect des principes éthiques dans toutes les activités

Module 7. 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 8. 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 9. 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

Module 10. Rapports Techniques et Exécutifs

- Développer des compétences pour produire des rapports techniques détaillés, présentant les résultats, les méthodologies et les recommandations d'une manière claire et complète
- Apprendre à communiquer efficacement avec des publics techniques, en utilisant un langage précis et approprié pour transmettre des informations techniques complexes
- Développer des compétences pour formuler des recommandations pratiques et réalisables visant à atténuer les vulnérabilités et à améliorer le niveau de sécurité
- Apprendre à évaluer l'impact potentiel des vulnérabilités identifiées, en tenant compte des aspects techniques, opérationnels et stratégiques
- Familiariser l'apprenant avec les meilleures pratiques en matière de rapports exécutifs, en adaptant des informations techniques à des publics non techniques
- Développer des compétences pour aligner les résultats et les recommandations sur les objectifs stratégiques et opérationnels de l'organisation
- Apprendre à utiliser des outils de visualisation des données pour représenter graphiquement les informations contenues dans les rapports, afin d'en faciliter la compréhension
- Promouvoir l'inclusion d'informations pertinentes sur le respect des réglementations et des normes dans les rapports, afin de garantir le respect des exigences légales
- Favoriser une collaboration efficace entre les équipes techniques et exécutives, afin de garantir la compréhension et le soutien des mesures d'amélioration proposées dans le rapport

03

Compétences

Grâce à ce programme, les diplômés seront formés avec des compétences spécialisées pour mettre en œuvre des mesures de défense active, renforçant la sécurité des systèmes et des réseaux sur la base des meilleures pratiques en matière de cybersécurité. En outre, les étudiants acquerront des compétences avancées en matière de tests de pénétration et de simulations *Red Team*, excellant dans l'identification proactive et l'atténuation des vulnérabilités. En ce sens, les professionnels maîtriseront les compétences techniques nécessaires pour faire face aux menaces du monde réel, ce qui les préparera à mener des stratégies efficaces d'évaluation et de renforcement de la sécurité dans des environnements cybernétiques dynamiques. En outre, l'approche 100% en ligne rend l'apprentissage flexible.

Devenez un expert en cybersécurité grâce à 1 500 heures du meilleur contenu multimédia, avec le label de qualité TECH"

Compétences générales

- Acquérir des compétences en matière de planification, d'exécution et de gestion de projets de cybersécurité, en garantissant des résultats efficaces et le respect des objectifs
- Acquérir des connaissances avancées en matière d'architecture de réseau et de ses aspects liés à la sécurité, en évaluant les vulnérabilités et en appliquant des stratégies pour renforcer l'infrastructure
- Développer des compétences en matière de criminalistique numérique et de réponse aux incidents, de la collecte de preuves à l'atténuation des menaces et au rétablissement opérationnel
- Appliquer des tactiques avancées dans la planification et l'exécution d'exercices *Red Team*, en simulant des scénarios réels pour évaluer la résilience de l'infrastructure, détecter les faiblesses et améliorer la préparation aux cybermenaces

Améliorer vos compétences dans le processus d'identification, d'évaluation et d'atténuation des risques spécifiques aux projets de cybersécurité. Misez sur TECH!"

Compétences spécifiques

- Acquérir des compétences en matière de coaching pour le développement professionnel des membres de l'équipe, en favorisant la croissance et l'amélioration
- Développer des compétences en matière de prise de décision stratégique dans des situations de cybersécurité, en tenant compte de l'impact à court et à long terme sur la sécurité de l'organisation
- Acquérir des compétences dans l'identification, l'évaluation et l'atténuation des risques spécifiques des projets de cybersécurité
- Développer des compétences pour mettre en œuvre des mesures de défense active, en renforçant la sécurité des systèmes et des réseaux
- Apprendre les techniques d'analyse du trafic web afin d'identifier les modèles et les comportements anormaux, facilitant ainsi la détection d'éventuelles menaces
- Acquérir des compétences en matière d'analyse criminalistique appliquée aux environnements de réseau, permettant une identification et une réponse efficaces aux cyberincidents
- Apprendre des stratégies de détection et de prévention efficaces des malware, y compris le déploiement de solutions de sécurité avancées
- Développer des compétences dans l'identification d'indicateurs de compromission (IoC) au cours d'une enquête médico-légale, afin de faciliter la détection et la réponse aux incidents
- Acquérir des compétences en matière de planification stratégique des exercices du *Red Team*, en tenant compte des objectifs, de la portée, des ressources et des scénarios réalistes
- Acquérir des compétences en matière d'identification et de hiérarchisation des vulnérabilités, en mettant en évidence celles qui présentent le plus grand risque pour la sécurité

04

Direction de la formation

Pour la création du corps enseignant du Mastère Spécialisé en Pentesting et Red Team, TECH a réuni les meilleurs spécialistes, qui ont une expérience professionnelle étendue et reconnue dans des entreprises leaders du secteur. En ce sens, chaque membre du corps enseignant apportera son expérience pratique et son expertise, garantissant ainsi que les étudiants bénéficieront de l'enseignement de professionnels hautement qualifiés. En outre, la sélection minutieuse de ces experts garantira non seulement la qualité académique, mais aussi la pertinence immédiate et l'applicabilité du contenu à l'environnement dynamique de la cybersécurité.

Les géants de l'industrie de la cybersécurité vous catapulteront vers le succès en seulement 12 mois grâce à ce programme universitaire unique de 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

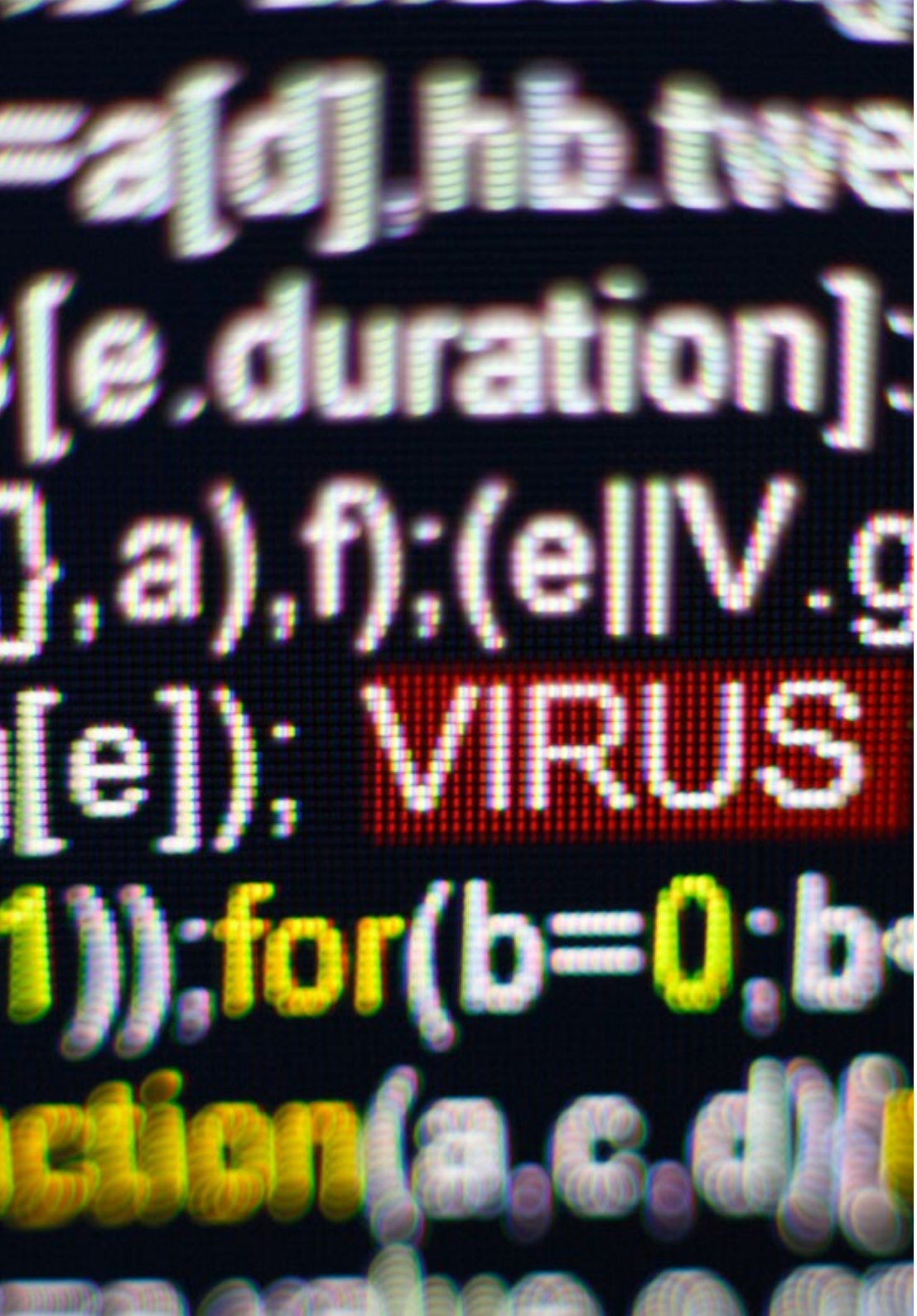
Professeurs

M. Siles Rubia, Marcelino

- Cibersecurity Engineer
- Ingénieur en Cybersécurité à l'Université Rey Juan Carlos
- Connaissances: Programmation Compétitive, *Hacking Web, Active Directory et Malware Development*
- Gagnant du Concours AdaByron

M. Redondo Castro, Pablo

- Pentester chez Groupe Oesía
- Ingénieur en Cybersécurité de l'Université Rey Juan Carlos
- Vaste expérience en tant que *Cibersecurity Evaluator Traineev*
- Il accumule de l'expérience dans l'enseignement, en donnant des formations liées aux tournois "Capture The Flag"



M. Gallego Sánchez, Alejandro

- 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

M. González Sanz, Marcos

- Cybersecurity Consultant-Red Teamer Cipherbit chez Groupe Oesía
- Ingénieur en Logiciel de l'Université Polytechnique de Madrid
- Spécialiste en Cybersécurité Tutor et Core Dumped

M. Mora Navas, Sergio

- Consultant en Cybersécurité chez Groupe Oesía
- Ingénieur en Cybersécurité de l'Université Rey Juan Carlos
  Ingénieur en Informatique de l'Université de Burgos

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

05

Structure et contenu

Ce programme universitaire offre une immersion complète dans les disciplines cruciales que sont les tests de pénétration et les simulations *Red Team*. Tout au long du cursus, les diplômés développeront des compétences avancées pour identifier et exploiter les vulnérabilités des systèmes et des réseaux, en utilisant des techniques et des outils modernes. Conçu dans une optique pratique, cette formation permettra aux professionnels de la cybersécurité de relever les défis du monde réel. Ainsi, les étudiants bénéficieront d'une combinaison unique de théorie et de pratique, guidée par des experts de l'industrie, pour renforcer leur compréhension et appliquer efficacement des stratégies d'évaluation de la sécurité dans les cyberenvironnements.

Vous découvrirez les différents rôles et responsabilités de l'équipe de cybersécurité. Inscrivez-vous maintenant!"

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. Gestion des Équipes de Cybersécurité

2.1. Gestion des équipes
- 2.1.1. Qui est qui
- 2.1.2. Le manager
- 2.1.3. Conclusions

2.2. Rôles et responsabilités
- 2.2.1. Identification des rôles
- 2.2.2. Délégation effective
- 2.2.3. Gestion des attentes

2.3. Formation et développement des équipes
- 2.3.1. Étapes de la formation des équipes
- 2.3.2. Dynamique de groupe
- 2.3.3. Évaluation et retour d'information

2.4. Gestion des talents
- 2.4.1. Identification des talents
- 2.4.2. Développement des capacités
- 2.4.3. Fidélisation des talents

2.5. Direction et motivation de l'équipe
- 2.5.1. Styles de leadership
- 2.5.2. Théories de la motivation
- 2.5.3. Reconnaissance des résultats

2.6. Communication et coordination
- 2.6.1. Outil de communication
- 2.6.2. Obstacles à la communication
- 2.6.3. Stratégies de coordination

2.7. Planification stratégique pour le développement du personnel
- 2.7.1. Identification des besoins de formation
- 2.7.2. Plans de développement individuel
- 2.7.3. Suivi et évaluation

2.8. Résolution des conflits
- 2.8.1. Identification des conflits
- 2.8.2. Méthodes de mesure
- 2.8.3. Prévention des conflits

2.9. Gestion de la qualité et amélioration continue
- 2.9.1. Principes de qualité
- 2.9.2. Techniques d'amélioration continue
- 2.9.3. *Feedback* et retour d'information

2.10. Outils et technologies
- 2.10.1. Plateformes de collaboration
- 2.10.2. Gestion de projets
- 2.10.3. Conclusions

Module 3. Gestion des Projets de Sécurité

3.1. Gestion des projets de sécurité
- 3.1.1. Définition et objectif de la gestion de projet de cybersécurité
- 3.1.2. Principaux défis
- 3.1.3. Considérations

3.2. Cycle de vie d'un projet de sécurité
- 3.2.1. Étapes initiales et définition des objectifs
- 3.2.2. Mise en œuvre et exécution
- 3.2.3. Évaluation et révision

3.3. Planification et estimation des ressources
- 3.3.1. Concepts de base de la gestion économique
- 3.3.2. Détermination des ressources humaines et techniques
- 3.3.3. Budgétisation et coûts associés

3.4. Mise en œuvre et contrôle du projet
- 3.4.1. Contrôle et suivi
- 3.4.2. Adaptation et modifications du projet
- 3.4.3. Évaluation à mi-parcours et révisions

3.5. Communication et rapports sur le projet
- 3.5.1. Stratégies de communication efficaces
- 3.5.2. Préparation de rapports et de présentations
- 3.5.3. Communication avec le client et la direction

3.6. Outils et technologies
- 3.6.1. Outils de planification et d'organisation
- 3.6.2. Outils de collaboration et de communication
- 3.6.3. Outils de documentation et de stockage

3.7. Documentation et protocoles
- 3.7.1. Structuration et création de la documentation
- 3.7.2. Protocoles d'action
- 3.7.3. Guide

3.8. Réglementation et conformité dans les projets de cybersécurité
- 3.8.1. Lois et réglementations internationales
- 3.8.2. Conformité
- 3.8.3. Audits

3.9. Gestion des risques dans les projets de sécurité
- 3.9.1. Identification et analyse des risques
- 3.9.2. Stratégies d'atténuation
- 3.9.3. Surveillance et examen des risques

3.10. La clôture des projets
- 3.10.1. Examen et évaluation
- 3.10.2. Documentation finale
- 3.10.3. Feedback

Module 4. Attaques des Réseaux et des Systèmes Windows

4.1. Windows et Active Directory
- 4.1.1. Histoire et évolution de Windows
- 4.1.2. Principes de base d'Active Directory
- 4.1.3. Fonctions et services d'Active Directory
- 4.1.4. Architecture générale d'Active Directory

4.2. Réseaux dans les environnements Active Directory
- 4.2.1. Protocoles de réseau dans Windows
- 4.2.2. DNS et son fonctionnement dans Active Directory
- 4.2.3. Outils de diagnostic réseau
- 4.2.4. Mise en œuvre du réseau dans Active Directory

4.3. Authentification et autorisation dans Active Directory
- 4.3.1. Processus et flux d'authentification
- 4.3.2. Types de certificats
- 4.3.3. Stockage et gestion des certificats
- 4.3.4. Sécurité de l'authentification

4.4. Permissions et stratégies dans Active Directory
- 4.4.1. GPOs
- 4.4.2. Application et gestion des GPO
- 4.4.3. Gestion des autorisations dans Active Directory
- 4.4.4. Vulnérabilités en matière de permissions et mesures d'atténuation

4.5. Principes de base de Kerberos
- 4.5.1. Qu'est-ce que Kerberos?
- 4.5.2. Composants et fonctionnement
- 4.5.3. Tickets dans Kerberos
- 4.5.4. Kerberos dans le contexte d'Active Directory

4.6. Techniques avancées de Kerberos
- 4.6.1. Attaques courantes contre Kerberos
- 4.6.2. Atténuations et protections
- 4.6.3. Surveillance du trafic Kerberos
- 4.6.4. Attaques avancées contre Kerberos

4.7. *Active Directory Certificate Services* (ADCS)
- 4.7.1. Les bases du PKI
- 4.7.2. Rôles et composants ADCS
- 4.7.3. Configuration et déploiement de l'ADCS
- 4.7.4. Sécurité ADCS

4.8. Attaques et défenses des *Active Directory Certificate Services* (ADCS)
- 4.8.1. Vulnérabilités courantes dans ADCS
- 4.8.2. Attaques et techniques d'exploitation
- 4.8.3. Défenses et atténuations
- 4.8.4. Surveillance et audit des ADCS

4.9. Audit de l'Active Directory
- 4.9.1. Importance de l'audit de l'Active Directory
- 4.9.2. Outils d'audit
- 4.9.3. Détection des anomalies et des comportements suspects
- 4.9.4. Réponse aux incidents et récupération

4.10. Azure AD
- 4.10.1. Principes de base d'Azure AD
- 4.10.2. Synchronisation avec l'Active Directory local
- 4.10.3. Gestion des identités dans Azure AD
- 4.10.4. Intégration avec les applications et les services

Module 5. *Hacking* Web Avancé

5.1. Fonctionnement d'un site web
- 5.1.1. L'URL et ses composantes
- 5.1.2. Les méthodes HTTP
- 5.1.3. Les en-têtes
- 5.1.4. Comment visualiser les requêtes web avec Burp Suite

5.2. Sessions
- 5.2.1. Les *cookies*
- 5.2.2. *Tokens* JWT
- 5.2.3. Attaques par détournement de session
- 5.2.4. Attaques sur le JWT

5.3. *Cross Site Scripting* (XSS)
- 5.3.1. Qu'est-ce que le XSS
- 5.3.2. Types de XSS
- 5.3.3. Exploiter un XSS
- 5.3.4. Introduction à *XSLeaks*

5.4. Injections dans les bases de données
- 5.4.1. Qu'est-ce qu'une *SQL Injection*
- 5.4.2. Exfiltrer des informations avec *SQLi*
- 5.4.3. *SQLi Blind, Time-Based et Error-Based*
- 5.4.4. Injections NoSQLi

5.5. *Path Traversal* et *Local File Inclusion*
- 5.5.1. Qu'est-ce que c'est et quelles sont leurs différences
- 5.5.2. Filtres courants et comment les contourner
- 5.5.3. *Log Poisoning*
- 5.5.4. LFIs en PHP

5.6. *Broken Authentication*
- 5.6.1. *User Enumeration*
- 5.6.2. *Password Bruteforce*
- 5.6.3. *2FA Bypass*
- 5.6.4. *Cookies* contenant des informations sensibles et modifiables

5.7. *Remote Command Execution*
- 5.7.1. *Command Injection*
- 5.7.2. *Blind Command Injection*
- 5.7.3. *Insecure Deserialization PHP*
- 5.7.4. *Insecure Deserialization Java*

5.8. *File Uploads*
- 5.8.1. RCE à travers les *webshells*
- 5.8.2. XSS dans les téléchargements de fichiers
- 5.8.3. XML *External Entity* (XXE) *Injection*
- 5.8.4. *Path traversal* dans les téléchargements de fichiers

5.9. *Broken Acess Control*
- 5.9.1. Accès illimité au panneau
- 5.9.2. *Insecure Direct Object References* (IDOR)
- 5.9.3. Bypass des filtres
- 5.9.4. Méthodes d'autorisation insuffisantes

5.10. Vulnérabilités du DOM et attaques plus avancées
- 5.10.1. *Regex Denial of Service*
- 5.10.2. DOM *Clobbering*
- 5.10.3. *Prototype Pollution*
- 5.10.4. HTTP *Request Smuggling*

Module 6. Architecture et Sécurité des Réseaux

6.1. Réseaux informatiques
- 6.1.1. Concepts de base: Protocoles LAN, WAN, CP, CC
- 6.1.2. Modèle OSI et TCP/IP
- 6.1.3. *Commutation:* Concepts de base
- 6.1.4. *Routing:* Concepts de base

6.2. *Switching*
- 6.2.1. Introduction aux VLAN
- 6.2.2. STP
- 6.2.3. *EtherChannel*
- 6.2.4. Attaques de la couche 2

6.3. VLANs
- 6.3.1. Importance des VLAN
- 6.3.2. Vulnérabilités des VLAN
- 6.3.3. Attaques courantes contre les VLAN
- 6.3.4. Atténuations

6.4. *Routing*
- 6.4.1. Adressage IP - IPv4 et IPv6
- 6.4.2. Routage: Concepts clés
- 6.4.3. Routage Statique
- 6.4.4. Routage Dynamique: Introduction

6.5. Protocoles IGP
- 6.5.1. RIP
- 6.5.2. OSPF
- 6.5.3. RIP vs OSPF
- 6.5.4. Analyse des besoins en matière de topologie

6.6. Protection du périmètre
- 6.6.1. DMZ
- 6.6.2. *Firewalls*
- 6.6.3. Architectures communes
- 6.6.4. *Zero Trust Network Access*

6.7. IDS et IPS
- 6.7.1. Caractéristiques
- 6.7.2. Mise en œuvre
- 6.7.3. SIEM et SIEM CLOUDS
- 6.7.4. Détection basée sur les *HoneyPots*

6.8. TLS y VPN
- 6.8.1. SSL/TLS
- 6.8.2. TLS: Attaques courantes
- 6.8.3. VPN avec TLS
- 6.8.4. VPN avec IPSEC

6.9. Sécurité dans les réseaux sans fil
- 6.9.1. Introduction aux réseaux sans fil
- 6.9.2. Protocoles
- 6.9.3. Éléments clés
- 6.9.4. Attaques courantes

6.10. Les réseaux d'entreprises et la manière de les gérer
- 6.10.1. Segmentation logique
- 6.10.2. Segmentation physique
- 6.10.3. Contrôle d'accès
- 6.10.4. Autres mesures à prendre en compte

Module 7. Analyse et Développement de *Malware*

7.1. Analyse et développement de *malware*
- 7.1.1. Histoire et évolution des *malware*
- 7.1.2. Classification et types de *malware*
- 7.1.3. Analyse des *malware*
- 7.1.4. Développement de *malware*

7.2. Préparation de l'environnement
- 7.2.1. Configuration de la Machine Virtuelle et *Snapshots*
- 7.2.2. Outils d'analyse des *malware*
- 7.2.3. Outils de développement de *malware*

7.3. Principes de base de Windows
- 7.3.1. Format de fichier PE (*Portable Executable*)
- 7.3.2. Processus et *Threads*
- 7.3.3. Système de fichiers et registre
- 7.3.4. *Windows Defender*

7.4. Techniques de malware de base
- 7.4.1. Génération de *shellcode*
- 7.4.2. Exécution du *shellcode* sur le disque
- 7.4.3. Disque vs mémoire
- 7.4.4. Exécution du shellcode en mémoire

7.5. Techniques de malware intermédiaires
- 7.5.1. Persistance sur Windows
- 7.5.2. Dossier d'accueil
- 7.5.3. Clés de registre
- 7.5.4. Économiseur d'écran

7.6. Techniques des *malwares* avancés
- 7.6.1. Cryptage du *shellcode* (XOR)
- 7.6.2. Cryptage du *shellcode* (RSA)
- 7.6.3. Obfuscation de *strings*
- 7.6.4. Injection de processus

7.7. Analyse statique du *malware*
- 7.7.1. Analyse des *packers* avec DIE (Detect It Easy)
- 7.7.2. Analyse des sections avec PE-Bear
- 7.7.3. Décompilation avec Ghidra

7.8. Analyse dynamique du *malware*
- 7.8.1. Observation du comportement avec Process Hacker
- 7.8.2. Analyse des appels avec API Monitor
- 7.8.3. Analyser les modifications du registre avec Regshot
- 7.8.4. Observer les requêtes réseau avec TCPView

7.9. Analyse en .NET
- 7.9.1. Introduction à .NET
- 7.9.2. Décompilation avec dnSpy
- 7.9.3. Débogage avec dnSpy

7.10. Analyser de vrais *malware*
- 7.10.1. Préparation de l'environnement
- 7.10.2. Analyse statique du *malware*
- 7.10.3 Analyse dynamique du *malware*
- 7.10.4. Création de règles YARA

Module 8. Principes Fondamentaux de la Criminalistique et DFIR

8.1. La criminalistique numérique
- 8.1.1. Histoire et évolution de la criminalistique informatique
- 8.1.2. Importance de l'informatique légale dans la cybersécurité
- 8.1.3. Histoire et évolution de la criminalistique informatique

8.2. Principes fondamentaux de l'Informatique légale
- 8.2.1. La chaîne de contrôle et son application
- 8.2.2. Types de preuves numériques
- 8.2.3. Processus d'acquisition des preuves

8.3. Systèmes de fichiers et structure des données
- 8.3.1. Principaux systèmes de fichiers
- 8.3.2. Méthodes de dissimulation des données
- 8.3.3. Analyse des métadonnées et des attributs des fichiers

8.4. Analyse des Systèmes d'Exploitation
- 8.4.1. Analyse criminalistique des systèmes Windows
- 8.4.2. Analyse légale des systèmes Linux
- 8.4.3. Analyse légale des systèmes macOS

8.5. Récupération de données et analyse de disques
- 8.5.1. Récupération de données à partir de supports endommagés
- 8.5.2. Outils d'analyse de disque
- 8.5.3. Interprétation des tables d'allocation de fichiers

8.6. Analyse du réseau et du trafic
- 8.6.1. Capture et analyse des paquets réseau
- 8.6.2. Analyse du journal du *firewall*
- 8.6.3. Détection des intrusions sur le réseau

8.7. Malware et analyse des codes malveillants
- 8.7.1. Classification des *malwares* et de leurs caractéristiques
- 8.7.2. Analyse statique et dynamique des *malwares*
- 8.7.3. Techniques de désassemblage et de débogage

8.8. Analyse des journaux et des événements
- 8.8.1. Types de journaux dans les systèmes et les applications
- 8.8.2. Interprétation des événements pertinents
- 8.8.3. Outils d'analyse des journaux

8.9. Réaction aux incidents de sécurité
- 8.9.1. Processus de réponse aux incidents
- 8.9.2. Création d'un plan de réponse aux incidents
- 8.9.3. Coordination avec les équipes de sécurité

8.10. Présentation des preuves et aspects juridiques
- 8.10.1. Règles de la preuve numérique dans le domaine juridique
- 8.10.2. Préparation des rapports médico-légaux
- 8.10.3. Comparaître au procès en tant que témoin expert

Module 9. Exercices Avancés du *Red Team*

9.1. Techniques avancées de reconnaissance
- 9.1.1. Énumération avancée des sous-domaines
- 9.1.2. *Google Dorking* avancé
- 9.1.3. Les Réseaux Sociaux et theHarvester

9.2. Campagnes de *phishing* avancées
- 9.2.1. Qu'est-ce que le *Reverse-Proxy Phishing*
- 9.2.2. *2FA Bypass* avec Evilginx
- 9.2.3. Exfiltration de données

9.3. Techniques avancées de persistance
- 9.3.1. *Golden Tickets*
- 9.3.2. *Silver Tickets*
- 9.3.3. Technique *DCShadow*

9.4. Techniques d'évasion avancées
- 9.4.1. Contournement de l'AMSI
- 9.4.2. Modification des outils existants
- 9.4.3. Obfuscation de *Powershell*

9.5. Techniques avancées de déplacement latéral
- 9.5.1. *Pass-the-Ticket* (PtT)
- 9.5.2. *Overpass-the-Hash* (Pass-the-Key)
- 9.5.3. NTLM Relay

9.6. Techniques avancées de post-exploitation
- 9.6.1. *Dump* de LSASS
- 9.6.2. *Dump* de SAM
- 9.6.3. Attaque *DCSync*

9.7. Techniques avancées de *pivoting*
- 9.7.1. Qu'est-ce que le *pivoting*
- 9.7.2. Tunnel SSH
- 9.7.3. Pivoter avec un Ciseau

9.8. Intrusions physiques
- 9.8.1. Surveillance et reconnaissance
- 9.8.2. *Tailgating* et *Piggybacking*
- 9.8.3. *Lock-Picking*

9.9. Attaques Wi-Fi
- 9.9.1. Attaques WPA/WPA2 PSK
- 9.9.2. Attaques des Rogue AP
- 9.9.3. Attaques WPA2 *Enterprise*

9.10. Attaques RFID
- 9.10.1. Lecture de cartes RFID
- 9.10.2. Manipulation de cartes RFID
- 9.10.3. Création de cartes clonées

Module 10. Rapports Techniques et Exécutifs

10.1. Processus de rapport
- 10.1.1. Structure d'un rapport
- 10.1.2. Processus de rapport
- 10.1.3. Concepts clés
- 10.1.4. Exécutif vs. Technique

10.2. Guide
- 10.2.1. Introduction
- 10.2.2. Types de Guides
- 10.2.3. Types de guides
- 10.2.4. Cas d'utilisation

10.3. Méthodologie
- 10.3.1. Évaluation
- 10.3.2. *Pentesting*
- 10.3.3. Revue des méthodologies communes
- 10.3.4. Introduction aux méthodologies nationales

10.4. Approche technique de la phase de rapport
- 10.4.1. Comprendre les limites du *pentester*
- 10.4.2. Utilisation de la langue et indices
- 10.4.3. Présentation de l'information
- 10.4.4. Erreurs courantes

10.5. Approche exécutive de la phase de rapport
- 10.5.1. Adapter le rapport au contexte
- 10.5.2. Utilisation de la langue et indices
- 10.5.3. Normalisation
- 10.5.4. Erreurs courantes

10.6. OSSTMM
- 10.6.1. Comprendre la méthodologie
- 10.6.2. Reconnaissance
- 10.6.3. Documentation
- 10.6.4. Élaboration du rapport

10.7. LINCE
- 10.7.1. Comprendre la méthodologie
- 10.7.2. Reconnaissance
- 10.7.3. Documentation
- 10.7.4. Élaboration du rapport

10.8. Signalement des vulnérabilités
- 10.8.1. Concepts clés
- 10.8.2. Quantifier la portée
- 10.8.3. Vulnérabilités et preuves
- 10.8.4. Erreurs courantes

10.9. Orienter le rapport vers le client
- 10.9.1. Importance des tests de travail
- 10.9.2. Solutions et atténuations
- 10.9.3. Données sensibles et pertinentes
- 10.9.4. Exemples et cas pratiques

10.10. Rapport sur les *retakes*
- 10.10.1. Concepts clés
- 10.10.2. Comprendre les informations héritées du passé
- 10.10.3. Vérification des erreurs
- 10.10.4. Ajout d'informations

06

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

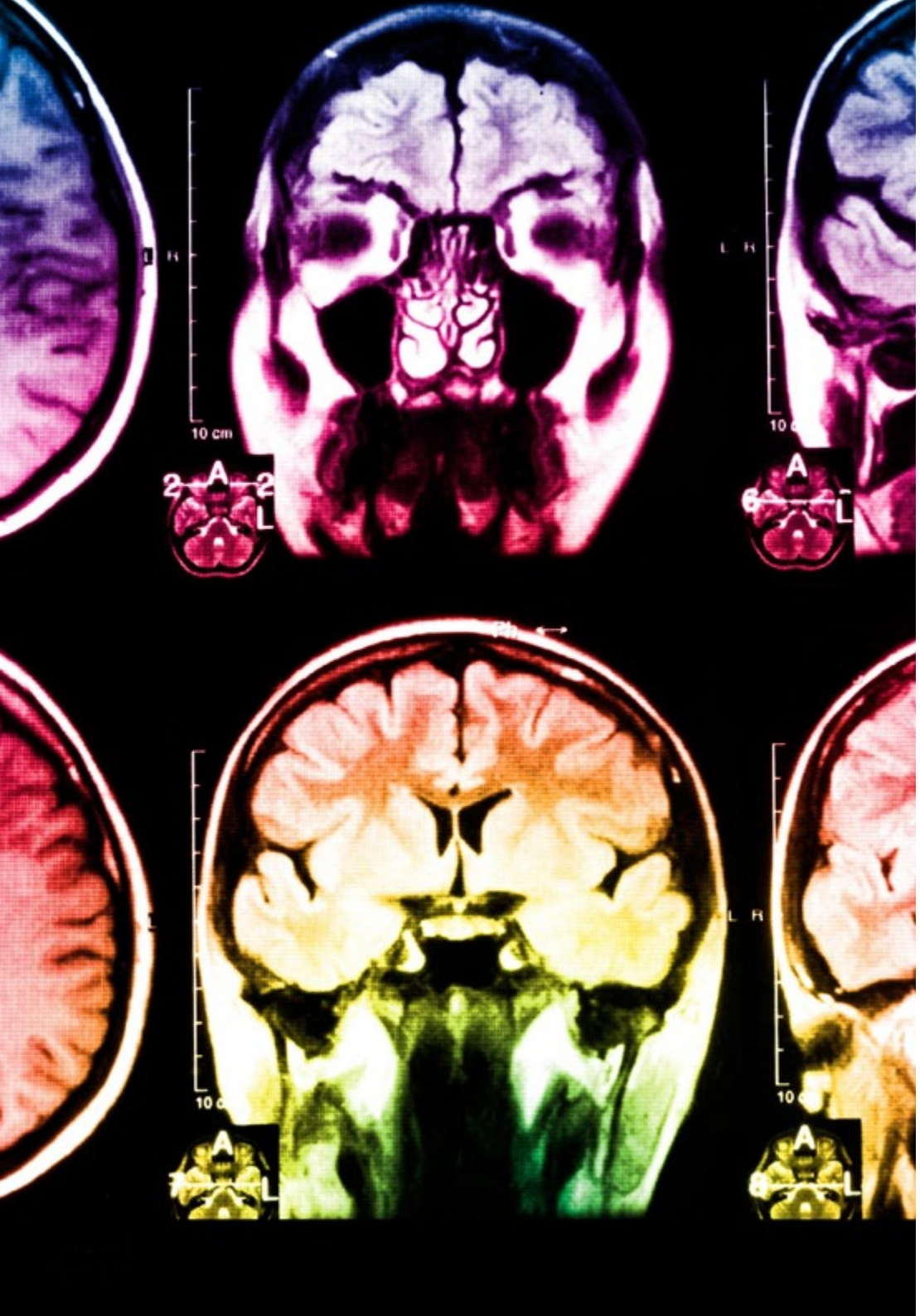
TECH combine efficacement la méthodologie des Études de Cas avec un système d'apprentissage 100% en ligne basé sur la répétition, qui associe différents éléments didactiques dans chaque leçon.

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.

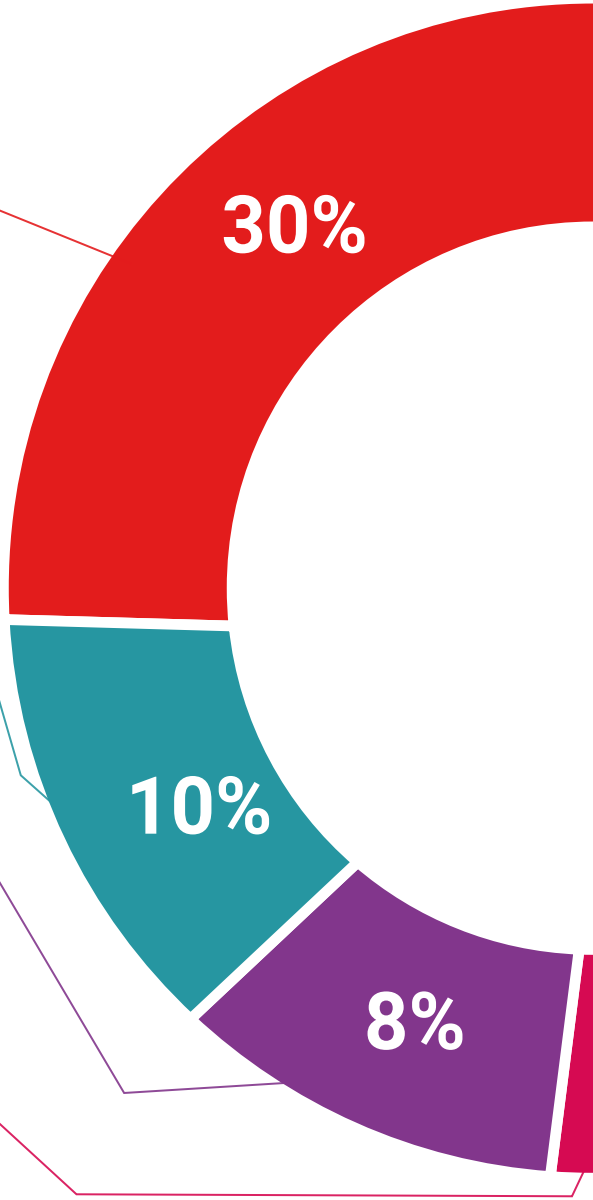
La méthode "Learning from an Expert" renforce les connaissances et la mémoire, et donne confiance dans les futures décisions difficiles.

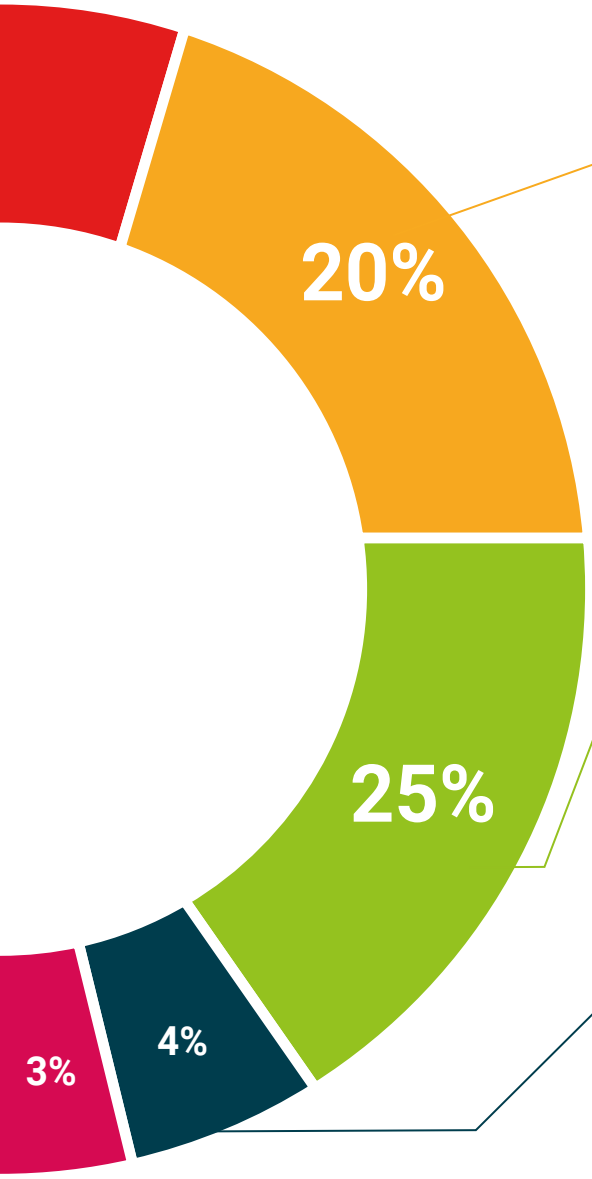
Pratiques en compétences et aptitudes

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.

07

Diplôme

Le Mastère Spécialisé en Pentesting et Red Team garantit, outre la formation la plus rigoureuse et la plus actualisée, l'accès à un diplôme de Mastère Spécialisé délivré par TECH Global University.

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

Ce programme vous permettra d'obtenir votre diplôme de **Mastère Spécialisé en Pentesting et Red Team** approuvé par **TECH Global University**, la plus grande Université numérique du monde.

TECH Global University est une Université Européenne Officielle reconnue publiquement par le Gouvernement d'Andorre ***(journal officiel)***. L'Andorre fait partie de l'Espace Européen de l'Enseignement Supérieur (EEES) depuis 2003. L'EEES est une initiative promue par l'Union européenne qui vise à organiser le cadre international de formation et à harmoniser les systèmes d'enseignement supérieur des pays membres de cet espace. Le projet promeut des valeurs communes, la mise en œuvre d'outils communs et le renforcement de ses mécanismes d'assurance qualité afin d'améliorer la collaboration et la mobilité des étudiants, des chercheurs et des universitaires.

Ce diplôme de Mastère Spécialisé de **TECH Global University** est un programme européen de formation continue et d'actualisation professionnelle qui garantit l'acquisition de compétences dans son domaine de connaissances, conférant une grande valeur curriculaire à l'étudiant qui réussit le programme.

Diplôme: **Mastère Spécialisé en Pentesting et Red Team**

Modalité: **en ligne**

Durée: **12 mois**

Accréditation: **60 ECTS**


tech global university

M./Mme _____, avec document d'identification _____
a passé et obtenu avec succès le diplôme de:

Mastère Spécialisé en Pentesting et Red Team

Il s'agit d'un diplôme de Mastère Spécialisé de 1.500 heures, équivalant à 60 ECTS, dont la date de début est le jj/mm/aaaa et la date de fin le jj/mm/aaaa.

TECH Global University est une université officiellement reconnue par le Gouvernement d'Andorre le 31 janvier 2024, qui appartient à l'Espace Européen de l'Enseignement Supérieur (EEES).

À Andorre-la-Vieille, 28 février 2024

Dr Pedro Navarro Illana
Recteur

Code Unique TECH: AFW0R23S techtitute.com/diplômes


Mastère Spécialisé en Pentesting et Red Team

Types de matière | Crédits ECTS
Obligatoire (OB) 60
Optionnelle (OP) 0
Stages Externes (ST) 0
Mémoire du Mastère (MDM) 0
Total 60

Distribution Générale du Programme d'Études

Cours	Matière	ECTS	Type
1°	Sécurité Offensive	6	OB
1°	Gestion des Équipes de Cybersécurité	6	OB
1°	Gestion des Projets de Sécurité	6	OB
1°	Attaques des Réseaux et des Systèmes Windows	6	OB
1°	Hacking Web Avancé	6	OB
1°	Architecture et Sécurité des Réseaux	6	OB
1°	Analyse et Développement de Malware	6	OB
1°	Principes Fondamentaux de la Criminalistique et DFIR	6	OB
1°	Exercices Avancés du Red Team	6	OB
1°	Rapports Techniques et Exécutifs	6	OB

Dr Pedro Navarro Illana
Recteur

tech global university

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

tech global university

Mastère Spécialisé
Pentesting et Red Team

- Modalité: **en ligne**
- Durée: **12 mois**
- Qualification: **TECH Global University**
- Accréditation: **60 ECTS**
- Horaire: **à votre rythme**
- Examens: **en ligne**

Mastère Spécialisé
Pentesting et Red Team

tech global university