Mastère Spécialisé

Direction de la Cybersécurité (CISO, Chief Information Security Officer)

tech université technologique

tech université technologique

Mastère Spécialisé

Direction de la Cybersécurité (CISO, Chief Information Security Officer)

- Modalité: **en ligne**
- Durée: **12 mois**
- Qualification: **TECH Université Technologique**
- Intensité: **16h/semaine**
- Horaire: **à votre rythme**
- Examens: **en ligne**

Accès web: **www.techtitute.com/fr/informatique/master/master-direction-cybersecurite-ciso-chief-information-security-officer**

Sommaire

01

Présentation

La technologie progresse, tout comme les menaces, qui perfectionnent leurs techniques d'attaque. En d'autres termes, les possibilités et les moyens dont disposent les cybercriminels pour atteindre leurs objectifs sont de plus en plus nombreux. C'est dans ce contexte que TECH présente un diplôme avec lequel les professionnels peuvent se mettre à jour, apprenant de manière exhaustive à protéger et sécuriser les différents environnements numériques. Tout cela, par le biais d'une méthodologie révolutionnaire, le réapprentissage, et dans un format pratique et totalement en ligne, qui permettra au diplômé d'acquérir des compétences et des capacités sans un timing préétabli. Ainsi, à l'issue de ce diplôme, le professionnel obtiendra les aptitudes et les compétences nécessaires pour exercer efficacement la fonction de responsable de la sécurité des informations, un poste de direction très prestigieux offrant de grandes perspectives de croissance et d'expansion.

À mesure que la technologie et la connectivité progressent, le nombre et la forme des menaces potentielles augmentent. C'est pourquoi il est crucial que les futurs Chief Information Security Officers mettent à jour leurs connaissances pour offrir des solutions plus adaptées aux particularités de l'entreprise"

Ce n'est un secret pour personne que nous sommes en pleine ère de l'information et de la communication, car nous sommes tous connectés, tant à la maison que dans les entreprises. Ainsi, nous avons accès à une multitude d'informations en un seul clic, en une seule recherche sur l'un des moteurs à notre disposition, que ce soit depuis un smartphone, un ordinateur personnel ou professionnel. Dans ce contexte, "le temps, c'est de l'argent", mais l'information aussi.

À mesure que la technologie progresse pour le citoyen et l'employé moyens, les menaces et les techniques d'attaque évoluent également. Plus il y a de nouvelles fonctionnalités et plus nous communiquons, plus la surface d'attaque augmente. En d'autres termes, les possibilités et les moyens dont disposent les cybercriminels pour atteindre leurs objectifs sont de plus en plus nombreux.

Compte tenu de ce contexte préoccupant, TECH lance ce programme de gestion de la cybersécurité (CISO, Chief Information Security Officer), qui a été développé par une équipe aux profils professionnels différents, spécialisée dans différents secteurs, qui combine une expérience professionnelle internationale dans le secteur privé en I+D+i et une vaste expérience de l'enseignement. Par conséquent, non seulement ils sont à jour sur chacune des technologies, mais ils ont également une perspective sur les besoins futurs du secteur et les présentent de manière didactique.

Le programme englobe les différentes matières de base dans le domaine de la cybersécurité, soigneusement sélectionnées pour couvrir rigoureusement un large éventail de technologies applicables à différents domaines de travail. Mais il couvrira également une autre branche de sujets qui sont habituellement rares dans le catalogue académique d'autres institutions et qui nourriront profondément le curriculum du professionnel. De cette manière, et grâce aux connaissances transversales offertes par TECH avec ce programme, le diplômé acquerra les compétences pour travailler en tant que manager dans le domaine de la cybersécurité (Chief Information Security Officer), augmentant ainsi ses perspectives de développement personnel et professionnel.

Ce **Mastère Spécialisé en Direction de la Cybersécurité (CISO, Chief Information Security Officer)** contient le programme le plus complet et le plus actuel du marché. Les principales caractéristiques sont les suivantes:

- El desarrollo de casos prácticos presentados por expertos en ciberseguridad
- Les contenus graphiques, schématiques et éminemment pratiques avec lesquels ils sont conçus fournissent des informations scientifiques et sanitaires essentielles à la pratique professionnelle
- Des exercices où le processus d'auto-évaluation peut être réalisé pour améliorer l'apprentissage.
- Il met l'accent sur les méthodologies innovantes
- Des cours théoriques, des questions à l'expert, des forums de discussion sur des sujets controversés et un travail de réflexion individuel
- La possibilité d'accéder aux contenus depuis n'importe quel appareil fixe ou portable doté d'une connexion internet

Préparez-vous à devenir un Chief Information Security Officer, un profil clé dans l'entreprise en raison de son rôle de protecteur et de garant de la sécurité informatique".

Démarquez-vous dans un secteur en plein essor et devenez un expert en cybersécurité avec ce programme TECH. C'est le plus complet du marché"

Les moyens par lesquels les gens échangent des informations évoluent rapidement. Cela nécessite de nouvelles formes de cyberprotection pour les professionnels.

Un programme 100% en ligne avec une approche éminemment pratique qui jettera les bases de votre développement professionnel.

Le programme comprend, dans son corps enseignant, des professionnels du secteur qui apportent à cette formation l'expérience de leur travail, ainsi que des spécialistes reconnus de grandes sociétés et d'universités prestigieuses.

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

La conception de ce programme est basée sur l'Apprentissage par Problèmes. Ainsi l'étudiant devra essayer de résoudre les différentes situations de pratique professionnelle qui se présentent à lui tout au long du Mastère Spécialisé. Pour ce faire, l'étudiant sera assisté d'un innovant système de vidéos interactives créé par des experts reconnus.

02

Objectifs

Conscient de l'importance de la cybersécurité pour les entreprises, TECH a développé ce Mastère Spécialisé qui vise à nourrir et à mettre à jour les connaissances des professionnels en matière de détection, de protection et de prévention de la cybercriminalité. De cette façon, le futur diplômé deviendra un acteur clé dans la protection des données et des informations, réduisant ainsi la possibilité pour les criminels de profiter des éventuelles failles de sécurité existantes. Une compétence professionnelle qu'à TECH, en seulement 12 mois, le professionnel pourra acquérir.

C'est une occasion unique de réaliser vos rêves et vos objectifs et de devenir un expert en cybersécurité"

Objectifs généraux

- Analyser le rôle de l'analyste en cybersécurité.
- Approfondir l'ingénierie sociale et ses méthodes
- Examiner les méthodologies OSINT, HUMINT, OWASP, OSSTM.. OSSTM, OWISAM
- Effectuer une analyse des risques et comprendre les mesures de risques
- Déterminer l'utilisation appropriée de l'anonymisation et l'utilisation de réseaux tels que TOR, I2P et Freenet
- Compiler les réglementations actuelles en matière de cyber-sécurité
- Générer des connaissances spécialisées pour la réalisation d'un audit de sécurité
- Développer des politiques d'utilisation appropriées
- Examiner les systèmes de détection et de prévention des menaces les plus importantes
- Évaluation des nouveaux systèmes de détection des menaces et de leur évolution par rapport aux solutions plus traditionnelles
- Analyser les principales plateformes mobiles actuelles, leurs caractéristiques et leur utilisation.
- Identifier, analyser et évaluer les risques de sécurité des parties du projet IoT.
- Évaluer les informations obtenues et développer des mécanismes de prévention et *Hacking*
- Appliquer l'ingénierie inverse à l'environnement de la cyber-sécurité
- Spécifier les tests à effectuer sur le software développé
- Rassembler toutes les preuves et données existantes pour réaliser un rapport médico-légal.
- Présenter correctement le rapport médico-légal
- Analyser l'état actuel et futur de la sécurité informatique
- Examiner les risques des nouvelles technologies émergentes
- Compiler les différentes technologies en relation avec la sécurité informatique

Objectifs spécifiques

Module 1. Cyberintelligence et cybersécurité

- Développer les méthodologies utilisées en matière de cybersécurité
- Examiner le cycle du renseignement et établir son application au cyber renseignement
- Déterminer le rôle de l'analyste du renseignement et les obstacles aux activités d'évacuation.
- analyser les méthodologies OSINT, OWISAM, OSSTM, PTES, OWASP
- Établir les outils les plus courants pour la production de renseignements
- Effectuer une analyse des risques et comprendre les mesures utilisées
- Spécifier les options pour l'anonymat et l'utilisation de réseaux tels que TOR, I2P, FreeNet
- Détailler les réglementations actuelles en matière de cyber-sécurité

Module 2. Sécurité de l'hôte

- Précisez les politiques de *Backup* des données personnelles et professionnelles.
- Évaluer les différents outils permettant d'apporter des solutions à des problèmes de sécurité spécifiques.
- Établir des mécanismes pour maintenir le système à jour
- Analyser les équipements pour détecter les intrus
- Déterminer les règles d'accès au système
- Examiner et classer le courrier pour prévenir la fraude
- Générer des listes de software autorisés

Module 3. Sécurité des réseaux (périmètre)

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

Module 4. La sécurité sur les smartphones

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

Module 5. Sécurité IoT

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

Module 6. Piratage éthique

- Examiner les méthodes de l'OSINT
- Rassembler les informations disponibles dans les médias publics
- Rechercher activement des informations sur les réseaux
- Développer des laboratoires d'essai
- Analyser les performances des outils de *Pentesting*
- Cataloguer et évaluer les différentes vulnérabilités des systèmes
- Préciser les différentes méthodologies de *Hacking*

Module 7. Ingénierie inverse

- Analyser les phases d'un compilateur
- Examinez l'architecture des processeurs x86 et l'architecture des processeurs ARM.
- Déterminer les différents types d'analyse
- Appliquer *Sandboxing* dans différents environnements
- Développer les différentes techniques d'analyse des logiciels *Malware*
- Développer les différentes techniques d'analyse des *Malware*

Module 8. Développement sûr

- Établir les exigences nécessaires au bon fonctionnement d'une application de manière sécurisée.
- Examiner les fichiers *journaux* pour comprendre les messages d'erreur
- Analyser les différents événements et décider de ce qui doit être montré à l'utilisateur et de ce qui doit être conservé dans les *logs*.
- Générer un code de qualité, aseptisé et facilement vérifiable.
- Évaluer la documentation appropriée pour chaque phase de développement
- Concrétiser le comportement du serveur pour optimiser le sys
- Développement d'un code modulaire, réutilisable et maintenable

Module 9. Analyse médico-légale

- Identifier les différents éléments de preuve d'un crime
- Générer connaissances spécialisées pour obtenir des données sur différents supports avant qu'elles ne soient perdues.
- Récupération de données qui ont été intentionnellement supprimées
- Analyser les journaux et *logs* des systèmes
- Déterminer comment les données sont dupliquées afin de ne pas altérer les originaux.
- étayer les preuves afin qu'elles soient cohérentes
- Générer un rapport robuste et homogène
- Présenter les résultats de manière cohérente
- Établir comment défendre le rapport devant l'autorité compétente
- Identifier des stratégies pour rendre le télétravail sûr et sécurisé

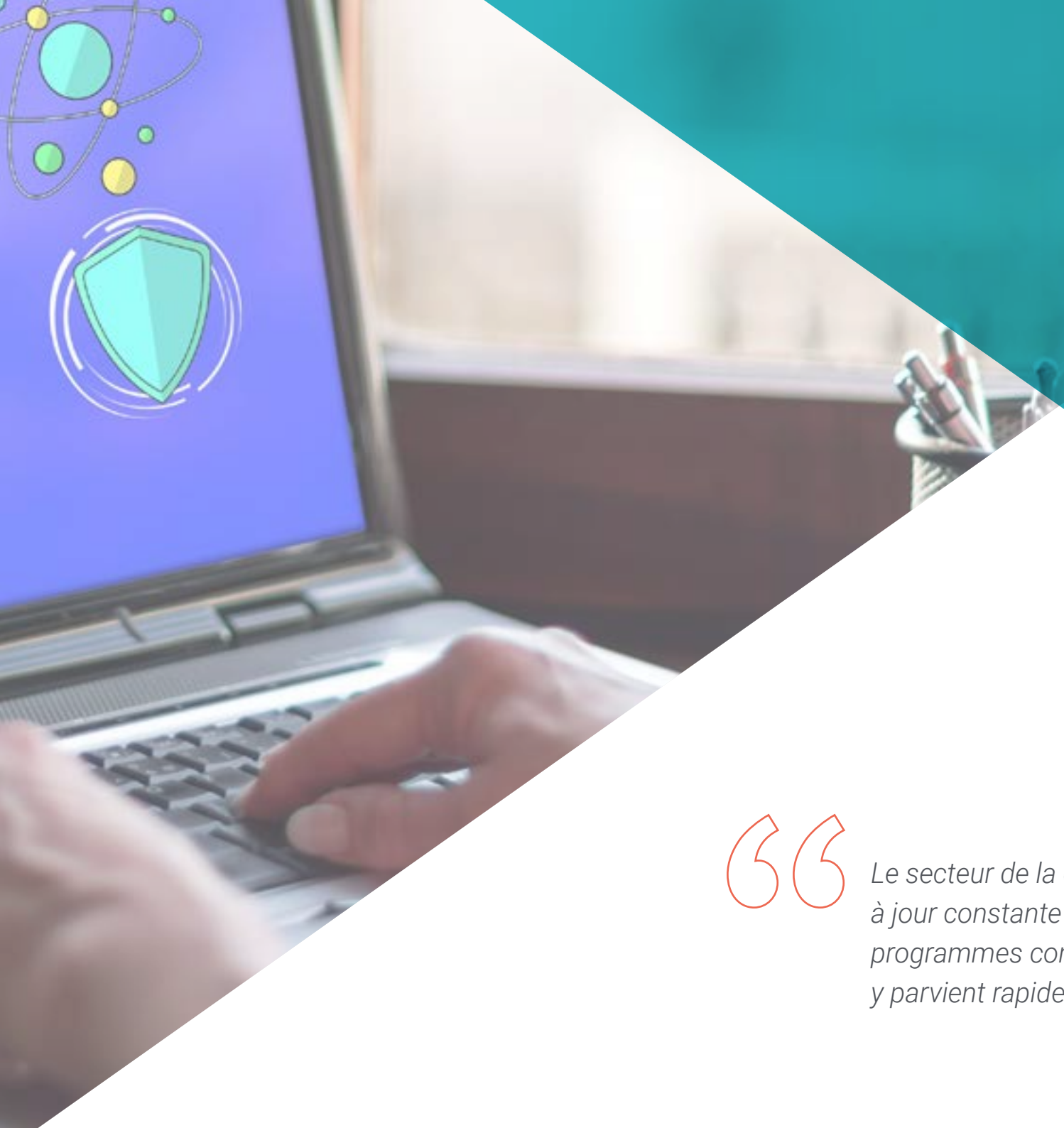
Module 10. Défis actuels et futurs en matière de sécurité informatique

- Examen de l'utilisation des crypto-monnaies, de leur impact sur l'économie et de la sécurité.
- Analyser la situation des utilisateurs et le degré d'illettrisme numérique
- Déterminer le champ d'utilisation de *Blockchain*
- Présenter les alternatives à l'IPv4 dans l'adressage des réseaux.
- Développer des stratégies pour former la population à l'utilisation correcte des technologies.
- Générer de l'expertise pour relever les nouveaux défis en matière de sécurité et prévenir le vol d'identité.
- Identifier des stratégies pour rendre le télétravail sûr et sécurisé

03

Compétences

Au terme du processus d'évaluation de ce Mastère Spécialisé, le professionnel aura acquis une série de connaissances, d'outils et de compétences qui lui permettront de travailler dans ce secteur avec de plus grandes garanties de succès. De cette manière, l'étudiant deviendra non seulement un expert en cybersécurité, mais il contribuera également de manière positive à la réduction de la cybercriminalité en forgeant un réseau plus sûr et plus sécurisé pour tous. Accéder à des postes de direction tels que celui de responsable de la sécurité de l'information.

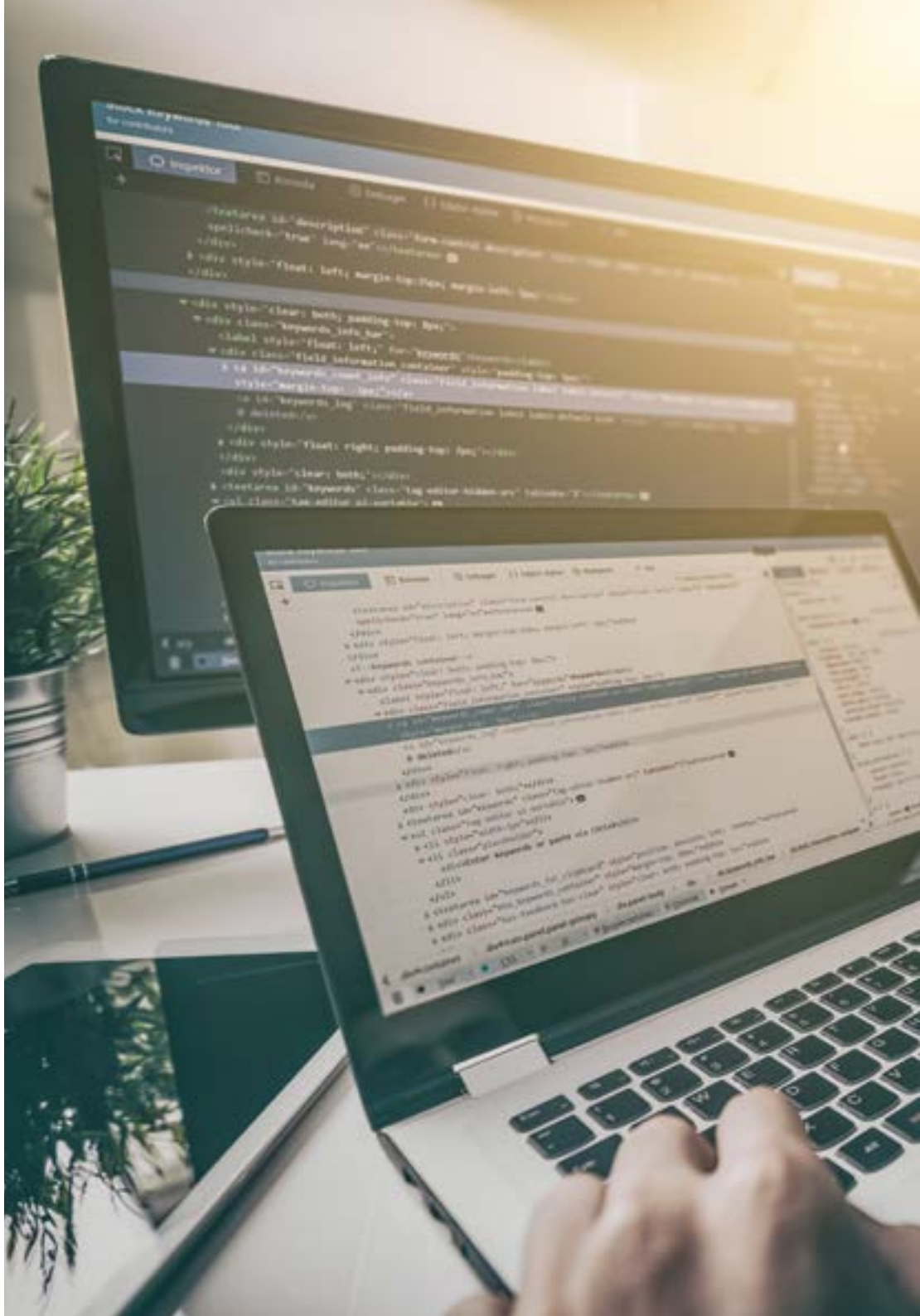


Le secteur de la cybersécurité exige une mise à jour constante des connaissances. Avec des programmes comme celui-ci, le professionnel y parvient rapidement et efficacement"

Compétences générales

- Connaître les méthodologies utilisées en matière de cyber-sécurité
- Savoir évaluer chaque type de menace afin d'offrir une solution optimale dans chaque cas.
- Être capable de générer des solutions intelligentes complètes pour automatiser le comportement en cas d'incidents.
- Savoir évaluer les risques liés aux vulnérabilités à l'intérieur et à l'extérieur de l'entreprise.
- Comprendre l'évolution et l'impact de l'IdO au fil du temps
- Être capable de démontrer qu'un système est vulnérable, de l'attaquer de manière proactive et de résoudre ces problèmes.
- Savoir comment appliquer le *sandboxing* dans différents environnements
- Connaître les directives qu'un bon développeur doit suivre afin de répondre aux exigences de sécurité nécessaires

L'amélioration de vos compétences dans un service pour tous donnera un coup de fouet à votre carrière professionnelle et personnelle"



Compétences spécifiques

- Savoir réaliser des opérations de sécurité défensive
- Avoir une perception approfondie et spécialisée de la sécurité informatique
- Posséder des connaissances spécialisées dans le domaine de la cybersécurité et de la cyberintelligence.
- Avoir une connaissance approfondie des aspects fondamentaux tels que le cycle du renseignement, les sources de renseignement, l'ingénierie sociale, la méthodologie OSINT, le HUMINT, l'anonymisation, l'analyse des risques, les méthodologies existantes (OWASP, OWISAM, OSSTM, PTES) et la réglementation actuelle en matière de cybersécurité.
- Comprendre l'importance de concevoir une défense à plusieurs niveaux, également connue sous le nom de "*Defense in Depth*", couvrant tous les aspects d'un réseau d'entreprise où certains des concepts et systèmes qui seront discutés peuvent également être utilisés et appliqués dans un environnement domestique.
- Savoir appliquer les processus de sécurité pour les smartphones et les appareils portables.
- Connaître les moyens de réaliser un *Hacking* dit éthique et protéger une entreprise d'une cyberattaque. d'une cyber-attaque
- Être capable d'enquêter sur un incident de cybersécurité.
- Connaître les différentes techniques d'attaque et de défense disponibles
- Analyse du rôle de l'analyste en cybersécurité
- Comprendre le fonctionnement de l'ingénierie sociale et ses méthodes.

04

Direction de la formation

Le Mastère Spécialisé en Direction de la Cybersécurité (CISO, Chief Information Security Officer) a été développé par une équipe de personnes aux profils professionnels différents, spécialisées dans différents secteurs, qui combinent une expérience professionnelle internationale dans le secteur privé en I+D+i et une vaste expérience de l'enseignement. Par conséquent, non seulement ils sont à jour sur chacune des technologies, mais ils ont également une perspective sur les besoins futurs du secteur et les présentent de manière didactique. De cette manière, le professionnel est assuré d'apprendre auprès des meilleurs du secteur, avec la garantie de disposer des connaissances les plus récentes.

Pendant le programme, vous serez accompagné par un certain nombre d'experts professionnels qui rendront votre expérience éducative unique"

Directeur invité international

Le Docteur Frédéric Lemieux est internationalement reconnu comme un expert innovant et un leader inspirant dans les domaines du **Renseignement, de la Sécurité Nationale, de la Sécurité Intérieure, de la Cybersécurité et des Technologies de Rupture.** Son dévouement constant et ses contributions pertinentes à la recherche et à l'éducation font de lui une figure clé de la promotion de la sécurité et de la compréhension des technologies émergentes d'aujourd'hui. Au cours de sa carrière professionnelle, il a conceptualisé et dirigé des programmes académiques de pointe dans plusieurs institutions renommées, telles que **l'Université de Montréal, l'Université George Washington et l'Université de Georgetown**.

Tout au long de sa carrière, il a publié de nombreux ouvrages importants, tous liés au **renseignement criminel, à la police, aux cybermenaces et à la sécurité internationale.** Il a également contribué de manière significative au domaine de la cybersécurité en publiant de nombreux articles dans des revues universitaires sur la lutte contre la criminalité lors de catastrophes majeures, la lutte contre le terrorisme, les agences de renseignement et la coopération policière. En outre, il a participé en tant que panéliste et orateur principal à diverses conférences nationales et internationales, s'imposant ainsi comme un universitaire et un praticien de premier plan.

Le Docteur Lemieux a occupé des fonctions éditoriales et d'évaluation dans diverses organisations universitaires, privées et gouvernementales, ce qui témoigne de son influence et de son engagement en faveur de l'excellence dans son domaine d'expertise. Sa prestigieuse carrière universitaire l'a amené à occuper le poste de professeur de pratique et de directeur des programmes MPS **en Intelligence appliquée, Gestion des Risques de Cybersécurité, Gestion de la Technologie et Gestion des Technologies de l'Information à l'Université de Georgetown.**

Dr. Lemieux, Frederic

- Chercheur en Intelligence, Cybersécurité et Technologies de Rupture à l'Université de Georgetown
- Directeur du Master en Information Technology Management à l'Université de Georgetown
- Directeur du Master en Technology Management à l'Université de Georgetown
- Directeur du Master en Cybersecurity Risk Management de l'Université de Georgetown
- Directeur du Master en Applied Intelligence à l'Université de Georgetown
- Professeur de Stage à l'Université de Georgetown
- Licence en Sociologie, Mineure en Psychologie, Université Laval
- Doctorat en Criminologie de l'École de Criminologie de l'Université de Montréal.
  Membre de:
  New Program Roundtable Committee, de l'Université de Georgetown

Grâce à TECH, vous pourrez apprendre avec les meilleurs professionnels du monde"

Direction

Mme Fernández Sapena, Sonia

- Formateur en sécurité informatique et Ethical Hacking au Centre National de Référence pour l'informatique et les télécommunications.
- Instructeur certifié E-Council
- Formateur dans les certifications suivantes : EXIN Ethical Hacking Foundation y EXIN Cyber & IT Security Foundation. Madrid
- Formateur expert accrédité par le CAM pour les certificats de professionnalisme suivants : Sécurité informatique (IFCT0190), Gestion des réseaux voix et données (IFCM0310), Administration des réseaux départementaux (IFCT0410), Gestion des alarmes dans les réseaux de télécommunications (IFCM0410), Opérateur de réseaux voix et données (IFCM0110), et Administration des services Internet (IFCT0509).
- Collaborateur externe CSO/SSA (Chief Security Officer/Senior Security Architect) à l'Université des Baléares.
- Diplôme d'ingénieur en informatique de l'université d'Alcalá de Henares à Madrid.
- Master en DevOps : Docker et Kubernetes. Cas-Training
- Technologies de sécurité Microsoft Azure. E-Council

Professeurs

M. Redondo, Jesús Serrano

- Développeur web et technicien en cybersécurité
- Développeur Web. Roams, Palencia
- Développeur FrontEnd chez Telefónica, Madrid
- Développeur FrontEnd. Best Pro Consulting SL, Madrid
- Installateur d'équipements et de services de télécommunications. Groupe Zener, Castilla y León
- Installateur d'équipements et de services de télécommunications. Lican Comunicaciones SL, Castilla y León
- Certificat en sécurité informatique. CFTIC Getafe, Madrid
- Technicien supérieur : Télécommunications et systèmes informatiques. IES Trinidad Arroyo, Palencia
- Technicien supérieur : Installations électrotechniques MT et BT. IES Trinidad Arroyo, Palencia
- Formation en reverse engineering, sténographie, cryptage. Incibe Hacker Academy (Talents d'Incibe)

M. Jiménez Ramos, Álvaro

- Analyste en cybersécurité
- Analyste principal de la sécurité à The Workshop
- Analyste en cybersécurité L1 chez Axians
- Analyste en cybersécurité L2 chez Axians
- Analyste en cybersécurité chez SACYR S.A.
- Diplôme d'ingénieur en télématique de l'université polytechnique de Madrid.
- Master en cybersécurité et Hacking éthique par le CICE
- Cours avancé en cybersécurité par Deusto Formación

Mme Marcos Sbarbaro, Victoria Alicia

- Développeur d'applications mobiles natives Android chez B60. UK
- Analyste-programmeur pour la gestion, la coordination et la documentation d'un environnement d'alarme de sécurité virtualisé.
- Analyste-programmeur d'applications Java pour les guichets automatiques bancaires (GAB)
- Professionnel du développement de Software pour une application de validation de signature et de gestion de documents
- Technicien système pour la migration des équipements et pour la gestion, la maintenance et la formation des PDA mobiles
- Ingénierie technique en systèmes informatiques par l'Université ouverte de Catalogne
- Master en sécurité informatique et piratage éthique Officielle EC- Council et CompTIA par l'Escuela Profesional de Nuevas Tecnologías CICE

M. Peralta Alonso, Jon

- Consultant senior - Protection des données et cybersécurité. Altia
- Avocat / Conseiller juridique. Arriaga Asociados Asesoramiento Jurídico y Económico, S.L. Conseiller juridique / Stagiaire. Bureau professionnel : Oscar Padura
- Diplôme en droit. Université publique du Pays basque
- Master en protection des données Délégué. EIS Innovative School
- Maîtrise en droit. Université publique du Pays basque
- Maîtrise spécialisée en pratique du contentieux civil. Université internationale Isabel I de Castille
- Chargé de cours pour le Master en protection des données personnelles, cybersécurité et droit des TIC

M. Catalá Barba, José Francisco

- Technicien en électronique expert en cybersécurité
- Développeur d'applications pour les appareils mobiles
- Technicien en électronique L'encadrement intermédiaire au sein du ministère espagnol de la défense.
- Technicien en électronique à l'usine Ford d'Almusafes, à Valence.

Une expérience éducative unique, clé et décisive pour stimuler votre développement professionnel et sauter le pas”

05

Structure et contenu

Pour s'assurer que les étudiants acquièrent les connaissances les plus rigoureuses et les plus pointues dans le domaine de la cybersécurité, TECH a conçu une série de matériels qui rassemblent les dernières mises à jour de la profession. Ces contenus ont été conçus par un groupe d'experts en la matière, ils sont donc adaptés aux besoins actuels des postes offerts dans le secteur. Une opportunité unique et éminemment professionnelle qui catapultera les étudiants vers le succès dans leur développement professionnel.

Un programme de haut niveau, conçu par et pour des professionnels de haut niveau, allez-vous manquer cette opportunité ?"

Module 1 Cyberintelligence et cybersécurité

1.1. Cyber intelligence
- 1.1.1. Cyber intelligence
  - 1.1.1.1. Intelligence
    - 1.1.1.1.1. Cycle de l'intelligence
  - 1.1.1.2. Cyber intelligence
  - 1.1.1.3. Cyber intelligence et cybersécurité
- 1.1.2. L'analyste de l'intelligence
  - 1.1.2.1. Le rôle de l'analyste du renseignement
  - 1.1.2.2. Biais de l'analyste du renseignement dans l'activité d'évaluation

1.2. Cybersécurité
- 1.2.1. Couches de sécurité
- 1.2.2. Identification des cybermenaces
  - 1.2.2.1. Menaces extérieures
  - 1.2.2.2. Menaces internes
- 1.2.3. Actions défavorables
  - 1.2.3.1. Ingénierie sociale
  - 1.2.3.2. Méthodes de communément utilisées

1.3. Techniques et outils des intelligences
- 1.3.1. OSINT
- 1.3.2. SOCMINT
- 1.3.3. HUMIT
- 1.3.4. Distributions et outils Linux
- 1.3.5. OWISAM
- 1.3.6. OWASP
- 1.3.7. PTES
- 1.3.8. OSSTMM

1.4. Méthodologie d'évaluation
- 1.4.1. L'analyse de Intelligence
- 1.4.2. Techniques d'organisation des informations acquises
- 1.4.3. Fiabilité et crédibilité des sources d'information
- 1.4.4. Méthodologie d'analyse
- 1.4.5. Présentation les résultats de l'Intelligence

1.5. Audits et documentation
- 1.5.1. Audit de la sécurité informatique
- 1.5.2. Documentation et autorisations pour l'audit
- 1.5.3. Types d'audits
- 1.5.4. Produits livrables
  - 1.5.4.1. Rapport technique
  - 1.5.4.2. rapport exécutif

1.6. Détection sur le web
- 1.6.1. Utilisation de l'anonymat
- 1.6.2. Techniques d'anonymat (Proxy, VPN)
- 1.6.3. Réseaux TOR, Freenet et IP2

1.7. Menaces et types de sécurité
- 1.7.1. Types de menaces
- 1.7.2. Sécurité physique
- 1.7.3. Sécurité des réseaux
- 1.7.4. Sécurité logique
- 1.7.5. Sécurité sur les applications web
- 1.7.6. Sécurité des appareils mobiles

1.8. Réglementation et *Compliance*
- 1.8.1. Le RGPD
- 1.8.2. La stratégie nationale de cybersécurité de 2019
- 1.8.3. Famille ISO 27000
- 1.8.4. Cadre de cybersécurité du NIST
- 1.8.5. PIC
- 1.8.6. ISO 27032
- 1.8.7. Réglementation *du Cloud*
- 1.8.8. SOX
- 1.8.9. PCI

1.9. Analyse et mesure des risques
- 1.9.1. Portée des risques
- 1.9.2. Les actifs
- 1.9.3. Menaces
- 1.9.4. Vulnérabilités
- 1.9.5. Évaluation des risques
- 1.9.6. Traitement des risques

1.10. Organismes importants en matière de cybersécurité
- 1.10.1. NIST
- 1.10.2. ENISA
- 1.10.3. INCIBE
- 1.10.4. OEA
- 1.10.5. UNASUR-PROSUR

Module 2. Sécurité de l'hôte

2.1. Copies de sauvegarde
- 2.1.1. Stratégies de sauvegarde
- 2.1.2. Outils pour Windows
- 2.1.3. Outils pour Linux
- 2.1.4. Outils pour MacOS

2.2. Antivirus utilisateur
- 2.2.1. Types d'antivirus
- 2.2.2. Antivirus pour Windows
- 2.2.3. Antivirus pour Linux
- 2.2.4. Antivirus pour MacOS
- 2.2.5. Antivirus pour smartphones

2.3. Détecteurs d'intrusionHIDS
- 2.3.1. Méthodes de détection des intrusions
- 2.3.2. Sagan
- 2.3.3. Aide
- 2.3.4. *Rkhunter*

2.4. *Firewall* local
- 2.4.1. *Firewalls* pour Windows
- 2.4.2. *Firewalls* pour Linux
- 2.4.3. *Firewalls* pour MacOS

2.5. Gestionnaires de mots de passe
- 2.5.1. Mot de passe
- 2.5.2. *LastPass*
- 2.5.3. *KeePass*
- 2.5.4. *Sticky password*
- 2.5.5. RoboForm

2.6. Détecteurs pour *phishing*
- 2.6.1. Détection manuelle du *Phishing* .
- 2.6.2. Outils *antiphishing*

2.7. *Spyware*
- 2.7.1. Mécanismes d'évitement
- 2.7.2. Outils *antispyware*

2.8. Trackers
- 2.8.1. Mesures de protection du système
- 2.8.2. Outils anti-pistage

2.9. *EDR- End point Detection and Response*
- 2.9.1. Comportement du système EDR
- 2.9.2. Différences entre EDR et Antivirus
- 2.9.3. L'avenir des systèmes EDR

2.10. Contrôle de l'installation des software
- 2.10.1. Dépôts et magasins de logiciels
- 2.10.2. Listes des logiciels autorisés ou interdits
- 2.10.3. Critères de mise à jour
- 2.10.4. Privilèges d'installation des logiciels

Module 3. Sécurité des réseaux (périmètre)

3.1. Systèmes de détection et de prévention des menaces
- 3.1.1. Cadre général des incidents de sécurité
- 3.1.2. Les systèmes de défense actuels : *defense in depth* et SOC
- 3.1.3. Architectures de réseau actuelles
- 3.1.4. Types d'outils de détection et de prévention des incidents
  - 3.1.4.1. Systèmes en réseau
  - 3.1.4.2. Systèmes basés sur *Host*
  - 3.1.4.3. Systèmes centralisés
- 3.1.5. Communication et découverte d'instances/*hosts*, conteneurs et *Serverless*

3.2. *Firewall*
- 3.2.1. Types de *firewalls*
- 3.2.2. Attaques et atténuation

3.2.3. *Firewalls* courants en *Kernel* Linux
3.2.3.1. UFW
3.2.3.2. *Nftables* et *iptables*
3.2.3.3. *Firewalls*
3.2.4. Systèmes de détection basés sur les *logs* du système
3.2.4.1. TCP *wrappers*
3.2.4.2. *BlockHosts* et *DenyHosts*
3.2.4.3. Fail2Ban
3.3. Systèmes de détection et de prévention des Intrusion: (IDS/IPS)
3.3.1. Attaques contre les IDS/IPS
3.3.2. Systèmes IDS/IPS
3.3.2.1. *Snort*
3.3.2.2. Suricata
3.4. *Firewalls* de nouvelle génération (NGFW)
3.4.1. Différences entre les NGFW et les *Firewall* traditionnels
3.4.2. Principales capacités
3.4.3. Solutions commerciales
3.4.4. *Firewalls* pour les services en *cloud*
3.4.4.1. Architecture *Cloud* VPC
3.4.4.2. *Cloud* ACLs
3.4.4.3. *Security group*
3.5. *Proxy*
3.5.1. Types de *Proxy*
3.5.2. Utilisation du *Proxy*. Avantages et inconvénients
3.6. Moteurs antivirus
3.6.1. Contexte général des *malwares* et des IOCs
3.6.2. Problèmes de moteur antivirus
3.7. Systèmes de protection du courrier
3.7.1. Antispam
3.7.1.1. Liste blanche et liste noire
3.7.1.2. Filtres bayésiens
3.7.2. *Mail Gateway* (MGW)
3.8. SIEM
3.8.1. Composants et architecture
3.8.2. Règles de corrélation et cas d'utilisation
3.8.3. Les défis actuels des systèmes SIEM
3.9. SOAR
3.9.1. SOAR et SIEM : ennemis ou alliés
3.9.2. L'avenir des systèmes SOAR
3.10. Autres systèmes en réseau
3.10.1. WAF
3.10.2. NAC
3.10.3. *HoneyPots* y *HoneyNets*
3.10.4. CASB

Module 4. La sécurité sur les smartphones

4.1. Le monde de l'appareil mobile
4.1.1. Types de plateformes mobiles
4.1.2. Dispositifs Ios
4.1.3. Dispositifs Android
4.2. Gestion de la sécurité mobile
4.2.1. Projet de sécurité mobile de l'OWASP
4.2.1.1. Les 10 principales vulnérabilités
4.2.2. Communications, réseaux et modes de connexion
4.3. Le dispositif mobile dans l'environnement professionnel
4.3.1. Risques
4.3.2. Politiques de sécurité
4.3.3. Surveillance des dispositifs
4.3.4. Gestion des dispositifs mobiles (MDM)
4.4. Vie privée des utilisateurs et sécurité des données
4.4.1. États d'information
4.4.2. Protection des données et confidentialité
4.4.2.1. Permissions
4.4.2.2. Cryptage

4.4.3. Stockage sécurisé des données
4.4.3.1. Stockage sécurisé sur iOS
4.4.3.2. Stockage sécurisé sur Android
4.4.4. Bonnes pratiques en matière de développement d'applications
4.5. Vulnérabilités et vecteurs d'attaque
4.5.1. Vulnérabilités
4.5.2. Vecteurs d'attaque
4.5.2.1. *Malware*
4.5.2.2. Exfiltration de données
4.5.2.3. Manipulation des données
4.6. Principales menaces
4.6.1. Utilisateur non formé
4.6.2. Malware
4.6.2.1. Types de malware
4.6.3. Ingénierie sociale
4.6.4. Fuite de données
4.6.5. Vol d'informations
4.6.6. Réseaux Wi-Fi non sécurisés
4.6.7. Software obsolètes
4.6.8. Applications malveillantes
4.6.9. Mots de passe non sécurisés
4.6.10. Paramètres de sécurité faibles ou inexistants
4.6.11. Accès physique
4.6.12. Perte ou vol de l'appareil
4.6.13. Vol d'identité (intégrité)
4.6.14. Cryptographie faible ou brisée
4.6.15. Déni de service (DoS)
4.7. Attaques majeures
4.7.1. Attaques de Phishing
4.7.2. Attaques liées aux modes de communication
4.7.3. Attaques de *Smishing*
4.7.4. Attaques de *Criptojacking*
4.7.5. *Man in the Middle*
4.8. *Hacking*
4.8.1. *Rooting* et *Jailbreaking*
4.8.2. Anatomie d'une attaque mobile
4.8.2.1. Propagation de la menace
4.8.2.2. Installation d'un *malware* sur l'appareil
4.8.2.3. Persistance
4.8.2.4. Exécution du *payload* et extraction de l'information
4.8.3. *Hacking* des appareils iOS : mécanismes et outils
4.8.4. *Hacking* des appareils Android : mécanismes et outils
4.9. Tests de pénétration
4.9.1. iOS *pentesting*
4.9.2. Android *pentesting*
4.9.3. Outils
4.10. Sûreté et sécurité
4.10.1. Paramètres de sécurité
4.10.1.1. Sur les appareils iOS
4.10.1.2. Sur les appareils androïdes
4.10.2. Mesures de sécurité
4.10.3. Outils de protection

Module 5. Sécurité IoT

5.1. Dispositifs
5.1.1. Types de dispositifs
5.1.2. Architectures standardisées
5.1.2.1. OneM2M
5.1.2.2. IoTWF
5.1.3. Protocoles d'application
5.1.4. Technologies de la connectivité
5.2. Dispositifs IoT. Domaines d'application
5.2.1. SmartHome
5.2.2. SmartCity
5.2.3. Transport
5.2.4. *Wearables*
5.2.5. Secteur de la santé
5.2.6. IioT

5.3. Protocoles de communication
- 5.3.1. MQTT
- 5.3.2. LWM2M
- 5.3.3. OMA-DM
- 5.3.4. TR-069

5.4. SmartHome
- 5.4.1. Domotique
- 5.4.2. Réseaux
- 5.4.3. Appareils ménagers
- 5.4.4. Surveillance et sécurité

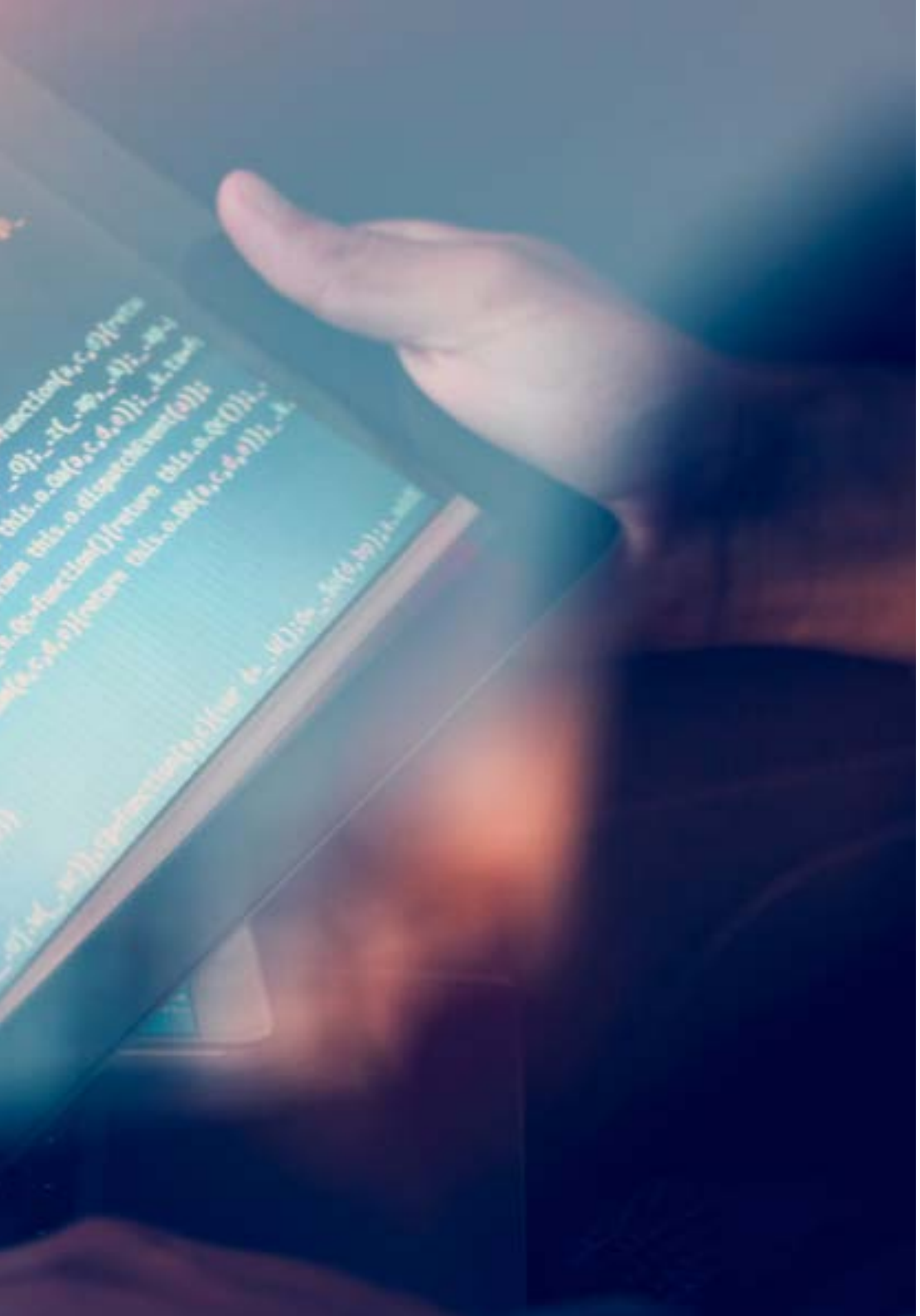
5.5. SmartCity
- 5.5.1. Éclairage
- 5.5.2. Météorologie
- 5.5.3. Sécurité

5.6. Transport
- 5.6.1. Localisation
- 5.6.2. Effectuer des paiements et obtenir des services
- 5.6.3. Connectivité

5.7. *Wearables*
- 5.7.1. Vêtements intelligents
- 5.7.2. Bijoux intelligents
- 5.7.3. Montres intelligentes

5.8. Secteur de la santé
- 5.8.1. Surveillance de l'effort et de la fréquence cardiaque
- 5.8.2. Surveillance des patients et des personnes âgées
- 5.8.3. Implantable
- 5.8.4. Robots chirurgicaux

5.9. Connectivité
- 5.9.1. Wifi
- 5.9.2. Bluetooth
- 5.9.3. Connectivité embarquée



5.10. Titrisation
- 5.10.1. Réseaux dédiés
- 5.10.2. Gestionnaire de mots de passe
- 5.10.3. Utilisation de protocoles cryptés
- 5.10.4. Conseils d'utilisation

Module 6. Piratage éthique

6.1. Environnement de travail
- 6.1.1. Distributions Linux
  - 6.1.1.1. Kali Linux-Offensive Security
  - 6.1.1.2. Parrot OS
  - 6.1.1.3. Ubuntu
- 6.1.2. Systèmes de virtualisation
- 6.1.3. Sandbox
- 6.1.4. Déploiement des laboratoires

6.2. Méthodologies
- 6.2.1. OSSTMM
- 6.2.2. OWASP
- 6.2.3. NIST
- 6.2.4. PTES
- 6.2.5. ISSAF

6.3. Footprinting
- 6.3.1. Renseignement de source ouverte (OSINT)
- 6.3.2. Recherche de violations de données et de vulnérabilité
- 6.3.3. Utilisation d'outils passif

6.4. Analyse du réseau
- 6.4.1. Outils d'analyse
  - 6.4.1.1. Nmap
  - 6.4.1.2. Hping3
  - 6.4.1.3. Autres outils d'analyse
- 6.4.2. Techniques de balayage
- 6.4.3. Techniques de contournement des *Firewall* et IDS
- 6.4.4. Banner *grabbing*
- 6.4.5. Diagrammes de réseau

6.5. Énumération
- 6.5.1. Énumération SMTP
- 6.5.2. Énumération DNS
- 6.5.3. Énumération de NetBIOS et de samba
- 6.5.4. Énumération LDAP
- 6.5.5. Énumération SNMP
- 6.5.6. Autres techniques d'énumération

6.6. Analyse des vulnérabilités
- 6.6.1. Solutions d'analyse des vulnérabilitéss
  - 6.6.1.1. Qualys
  - 6.6.1.2. Nessus
  - 6.6.1.3. Nessus
- 6.6.2. Systèmes d'évaluation des vulnérabilités
  - 6.6.2.1. CVSS
  - 6.6.2.2. CVE
  - 6.6.2.3. NVD

6.7. Attaques contre les réseaux sans fil
- 6.7.1. Méthodologie de *hacking* des réseaux sans fil
  - 6.7.1.1. Wifi Discovery
  - 6.7.1.2. Analyse du trafic
  - 6.7.1.3. Attaques d' *Aircrack*
    - 6.7.1.3.1. Attaques WEP
    - 6.7.1.3.2. Attaques WPA/WPA2
  - 6.7.1.4. Les attaques de *Evil Twin*
  - 6.7.1.5. Attaques sur le WPS
  - 6.7.1.6. *Jamming*
- 6.7.2. Outils pour la sécurité sans fil

6.8. Piratage de serveurs web
- 6.8.1. *Cross site Scripting*
- 6.8.2. CSRF
- 6.8.3. *Session Hijacking*
- 6.8.4. *SQL Injection*

6.9. Exploitation des vulnérabilités
- 6.9.1. Utilisation *Exploits* connus
- 6.9.2. Utilisation des *metasploit*
- 6.9.3. Utilisation des *Malware*
  - 6.9.3.1. Définition et champ d'application
  - 6.9.3.2. Génération de *malware*
  - 6.9.3.3. Bypass des solutions anti-virus

6.10. Persistance
- 6.10.1. Installation de *Rootkits*
- 6.10.2. Utilisation de Ncat
- 6.10.3. Utilisation de tâches planifiées pour les *Backdoors*
- 6.10.4. Création d'utilisateurs
- 6.10.5. Détection HIDS

Module 7. Ingénierie inverse

7.1. Compilateurs
- 7.1.1. Types de code
- 7.1.2. Les phases d'un compilateur
- 7.1.3. Table des symboles
- 7.1.4. Gestionnaire d'erreurs
- 7.1.5. Compilateur GCC

7.2. Types d'analyse de compilateur
- 7.2.1. Analyse lexicale
  - 7.2.1.1. Terminologie
  - 7.2.1.2. Composante lexicale
  - 7.2.1.3. Analyseur Lexical LEX
- 7.2.2. Analyse syntaxique
  - 7.2.2.1. Grammaires sans contexte
  - 7.2.2.2. Types d'analyse syntaxique
    - 7.2.2.2.1. Analyse syntaxique descendante
    - 7.2.2.2.2. Analyse ascendante
  - 7.2.2.3. Arbres syntaxiques et dérivations
  - 7.2.2.4. Types d'analyseurs syntaxiques
    - 7.2.2.4.1. Analyseurs LR(*Left To Right*)
    - 7.2.2.4.2. Analizadores LALR

7.2.3. Analyse sémantique
7.2.3.1. Grammaires d'attributs
7.2.3.2. S-Attributs
7.2.3.3. L-attributs
7.3. Structures de données de l'assemblage
7.3.1. Variables
7.3.2. Arrays
7.3.3. Pointeurs
7.3.4. Structures
7.3.5. Objets
7.4. Structures du code d'assemblage
7.4.1. Structures de sélection
7.4.1.1. If, else if, Else
7.4.1.2. *Switch*
7.4.2. Structures d'itération
7.4.2.1. *For*
7.4.2.2. *While*
7.4.2.3. Utilisation du *Break*
7.4.3. Fonctions
7.5. Architecture Hardware x86
7.5.1. Architecture de processeur x86
7.5.2. Structures de données x86
7.5.3. Structures de code x86
7.5.4. Structures de code x86
7.6. Architecture Hardware ARM
7.6.1. Architecture du processeur ARM
7.6.2. Structures de données ARM
7.6.3. Structures de code ARM
7.7. Analyse du code statique
7.7.1. Démonteurs
7.7.2. IDA
7.7.3. Reconstructeurs de code
7.8. Analyse dynamique du code
7.8.1. Analyse comportementale
7.8.1.1. Communications
7.8.1.2. Suivi
7.8.2. Débogueurs de code Linux
7.8.3. Débogueurs de code sous Windows
7.9. Sandbox
7.9.1. Architecture du Sandbox
7.9.2. Évasion du Sandbox
7.9.3. Techniques de détection
7.9.4. Techniques d'évasion
7.9.5. Contre-mesures
7.9.6. Sandbox sur Linux
7.9.7. Sandbox sur Windows
7.9.8. *Sandbox* sur MacOS
7.9.9. Sandbox sur Android
7.10. Analyse des *malware*
7.10.1. Méthodes d'analyse des *malware*
7.10.2. Techniques d'obscurcissement des *malware*
7.10.2.1. Obfuscation des exécutables
7.10.2.2. Restriction des environnements d'exécution
7.10.3. Outils d'analyse des *malware*

Module 8. Développement sûr

8.1. Développement sûr
8.1.1. Qualité, fonctionnalité et sécurité
8.1.2. Confidentialité, intégrité et disponibilité
8.1.3. Cycle de vie du développement du Software
8.2. Phase des exigences
8.2.1. Gestion de l'authentification
8.2.2. Contrôle des rôles et des privilèges
8.2.3. Exigences axées sur le risque
8.2.4. Approbation des privilèges

8.3. Phase de Analyse et de conception
- 8.3.1. Accès aux composants et administration du système
- 8.3.2. Pistes d'audit
- 8.3.3. Gestion des sessions
- 8.3.4. Données historiques
- 8.3.5. Traitement approprié des erreurs
- 8.3.6. Séparation des fonctions

8.4. Phase de mise en œuvre et de codification
- 8.4.1. Sécuriser l'environnement de développement
- 8.4.2. Élaboration de la documentation technique
- 8.4.3. Codage sécurisé
- 8.4.4. Communications sécurisées

8.5. Bonnes pratiques de codage sécurisé
- 8.5.1. Validation des données d'entrée
- 8.5.2. Cryptage des données de sortie
- 8.5.3. Style de programmation
- 8.5.4. Traitement du journal des modifications
- 8.5.5. Pratiques cryptographiques
- 8.5.6. Gestion des erreurs et des journaux
- 8.5.7. Gestion des fichiers
- 8.5.8. Gestion de la mémoire
- 8.5.9. Standardisation et réutilisation des fonctions de sécurité

8.6. Préparation du serveur et *hardening*
- 8.6.1. Gestion des utilisateurs, des groupes et des rôles sur le serveur
- 8.6.2. Installation du logiciel
- 8.6.3. *Hardening* du serveur
- 8.6.4. Configuration robuste de l'environnement de l'application

8.7. Préparation et durcissement de la BBDD et *hardening*
- 8.7.1. Optimisation de la BBDD
- 8.7.2. Création d'un utilisateur propre pour l'application
- 8.7.3. Attribution les privilèges nécessaires à l'utilisateur
- 8.7.4. *Hardening* de la BBDD

8.8. Phase de test
- 8.8.1. Contrôle de la qualité des contrôles de sécurité
- 8.8.2. Inspection progressive du code
- 8.8.3. Contrôle de la gestion de la configuration
- 8.8.4. Tests en boîte noire

8.9. Préparer la transition vers la production
- 8.9.1. Effectuer le contrôle des changements
- 8.9.2. Effectuer la procédure de changement de production
- 8.9.3. Exécuter la procédure de *rollback*
- 8.9.4. Essais de pré-production

8.10. Phase de maintenance
- 8.10.1. Assurance basée sur le risque
- 8.10.2. Test de maintenance de la sécurité de la boîte blanche
- 8.10.3. Tests de maintenance de la sécurité en boîte noire

Module 9. Analyse médico-légale

9.1. Acquisition et réplication des données
- 9.1.1. Acquisition de données volatiles
  - 9.1.1.1. Informations sur le système
  - 9.1.1.2. Informations sur le réseau
  - 9.1.1.3. Ordre de volatilité
- 9.1.2. Acquisition de données statiques
  - 9.1.2.1. Création d'une image dupliquée
  - 9.1.2.2. Préparation d'un document de chaîne de contrôle
- 9.1.3. Méthodes de validation des données acquises
  - 9.1.3.1. Méthodes pour Linux
  - 9.1.3.2. Méthodes pour Windows

9.2. Évaluation et défaite des techniques anti-forensic
- 9.2.1. Objectifs des techniques médico-légales
- 9.2.2. Effacement des données
  - 9.2.2.1. Effacement des données et des fichiers
  - 9.2.2.2. Récupération de fichiers
  - 9.2.2.3. Récupération de partitions supprimées

9.2.3. Protection par mot de passe
9.2.4. Stéganographie
9.2.5. Effacement sécurisé des dispositifs
9.2.6. Cryptage
9.3. Analyse judiciaire des systèmes d'exploitation
9.3.1. Analyse légale de Windows
9.3.2. Analyse légale de Linux
9.3.3. Analyse légale de Mac
9.4. Analyse judiciaire des réseaux
9.4.1. Analyse du *Logs*
9.4.2. Corrélation des données
9.4.3. Enquête sur le réseau
9.4.4. Étapes à suivre pour l'analyse criminelle du réseau
9.5. Analyse légale Web
9.5.1. Enquête sur les attaques sur Internet
9.5.2. Détection des attaques
9.5.3. Localisation de l'adresse IP
9.6. Police scientifique des bases de données
9.6.1. Analyse légale de MSSQL
9.6.2. Analyse légale de MySQL
9.6.3. Analyse légale de PostgreSQL
9.6.4. Analyse légale de MongoDB
9.7. Analyse légale en *Cloud*
9.7.1. Types de délits en *Cloud*
9.7.1.1. Le Cloud comme sujet
9.7.1.2. Le cloud comme objet
9.7.1.3. Le cloud comme outil
9.7.2. Les défis Forensics du *Cloud*
9.7.3. Recherche sur les services de stockage en *Cloud*
9.7.4. Outils d'analyse légale pour le *Cloud*
9.8. Enquêtes sur les crimes par courriel
9.8.1. Systèmes de courrier
9.8.1.1. Clients de messagerie
9.8.1.2. Serveur de messagerie
9.8.1.3. Serveur SMTP
9.8.1.4. Serveur POP3
9.8.1.5. Serveur IMAP4
9.8.2. Délits de courrier
9.8.3. Message de courrier
9.8.3.1. En-têtes standard
9.8.3.2. En-têtes étendus
9.8.4. Étapes de l'enquête sur ces crimes
9.8.5. Outils d'analyse des e-mails
9.9. Analyse légale des mobiles
9.9.1. Réseaux cellulaires
9.9.1.1. Types de réseaux
9.9.1.2. Contenu du CDR
9.9.2. *Subscriber Identity Module* (SIM)
9.9.3. Acquisition logique
9.9.4. Acquisition physique
9.9.5. Acquisition du système de fichiers
9.10. Rédaction et soumission de rapports légaux
9.10.1. Aspects importants d'un rapport légal
9.10.2. Classification et types de rapports
9.10.3. Guide pour la rédaction d'un rapport
9.10.4. Présentation du rapport.
9.10.4.1. Préparation préalable au témoignage
9.10.4.2. Dépôt
9.10.4.3. Traiter avec les médias

Module 10. Défis actuels et futurs en matière de sécurité informatique

10.1. Technologie de la blockchain
- 10.1.1. Domaines d'application
- 10.1.2. Garantie de confidentialité
- 10.1.3. Garantie de non-répudiation

10.2. La monnaie numérique
- 10.2.1. Bitcoins
- 10.2.2. Cryptocurrencies
- 10.2.3. Extraction de crypto-monnaies
- 10.2.4. Les systèmes pyramidaux
- 10.2.5. Autres crimes et problèmes potentiels

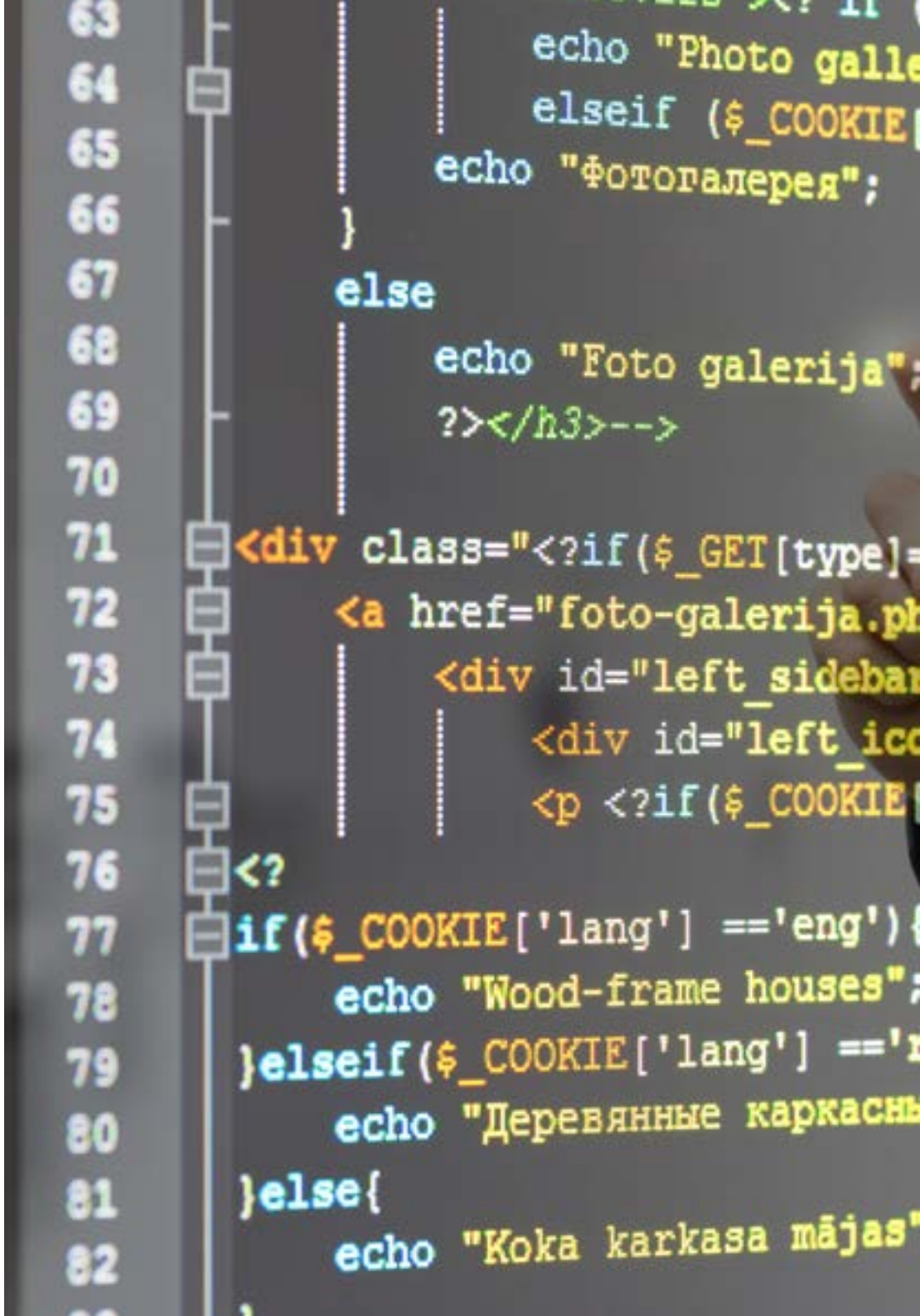
10.3. Deepfake
- 10.3.1. Impact des médias
- 10.3.2. Dangers pour la société
- 10.3.3. Mécanismes de détection

10.4. L'avenir de l'intelligence artificielle
- 10.4.1. Intelligence artificielle et informatique cognitive
- 10.4.2. Utilisations pour simplifier le service à la clientèle

10.5. Vie privée numérique
- 10.5.1. Valeur des données sur le réseau
- 10.5.2. Utilisation des données sur le réseau
- 10.5.3. Vie privée et gestion de l'identité numérique

10.6. Cyberconflits, cybercriminels et cyberattaques
- 10.6.1. Impact de la cybersécurité sur les conflits internationaux
- 10.6.2. Conséquences des cyberattaques sur la population générale
- 10.6.3. Types de cybercriminels. Mesures de protection

10.7. Télétravail
- 10.7.1. La révolution du télétravail pendant et après la COVID-19
- 10.7.2. Goulets d'étranglement dans l'accès
- 10.7.3. Variation de la surface d'attaque
- 10.7.4. Besoins des travailleurs



10.8. Technologies *Wireless* émergentes
- 10.8.1. WPA3
- 10.8.2. 5G
- 10.8.3. Ondes millimétriques
- 10.8.4. Tendance "*Get Smart*"" au lieu de "*Get more*"

10.9. L'adressage futur dans les réseaux
- 10.9.1. Problèmes actuels de l'adressage IP
- 10.9.2. IPv6
- 10.9.3. IPv4+
- 10.9.4. Avantages d'IPv4+ par rapport à IPv4
- 10.9.5. Avantages d'IPv6 par rapport à IPv4

10.10. Le défi de la sensibilisation de la population à l'éducation précoce et continue
- 10.10.1. Stratégies gouvernementales actuelles
- 10.10.2. Résistance de la population à l'apprentissage
- 10.10.3. Des plans de formation à adopter par les entreprises

Votre avenir commence ici. Inscrivez-vous dès aujourd'hui et devenez le directeur de l'information de grandes entreprises"

06

Méthodologie

Cette formation vous propose une manière différente d'apprendre. Notre méthodologie est développée à travers un mode d'apprentissage cyclique: ***Le Relearning***.
Ce système d'enseignement s'utilise, notamment, dans les Écoles de Médecine les plus prestigieuses du monde. De plus il a été considéré comme l'une des Méthodes les plus efficaces par des magazines scientifiques de renom comme par exemple le ***New England Journal of Medicine.***

Découvrez Relearning, un système qui abandonne 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 contextualiser tout le contenu.

Notre programme propose une approche révolutionnaire du développement des compétences et des connaissances. Notre objectif est de renforcer les compétences dans un contexte changeant, compétitif et très exigeant.

Avec TECH, vous ferez l'expérience d'une méthode d'apprentissage qui ébranle les fondements des universités traditionnelles du monde entier"

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

L'étudiant apprendra, par le biais d'activités collaboratives et de cas réels, à résoudre des situations complexes dans des environnements commerciaux réels.

Une méthode d'apprentissage innovante et différente

Ce Mastère Spécialisé de TECH est un programme d'enseignement intensif, créé de toutes pièces, offrir aux managers des défis et des décisions d'affaires au plus haut niveau, que ce soit au niveau national ou international. Grâce à cette méthodologie, l'épanouissement personnel et professionnel est stimulé, faisant ainsi un pas décisif vers la réussite. La méthode des cas, une technique qui jette les bases de ce contenu, garantit que la réalité économique, sociale et professionnelle la plus actuelle est suivie.

> *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 de Sciences informatique du monde et ce depuis leur fondement. Développée en 1912 à Harvard pour que les étudiants en Droit n'apprennent pas uniquement sur la base d'un contenu théorique, la méthode des cas consistait à leur présenter des situations réelles complexes pour que les apprenants s'entraînent à les résoudre et à prendre des décisions. Elle a été établie comme méthode d'enseignement standard à Harvard en 1924.

Face à une situation donnée, que doit faire un professionnel? C'est la question à laquelle nous vous confrontons dans la méthode des cas, une méthode d'apprentissage orientée vers l'action. Tout au long du programme, vous serez confronté à de multiples cas réels. Ils devront intégrer toutes leurs connaissances, faire des recherches, argumenter et défendre leurs idées et leurs décisions.

Relearning Methodology

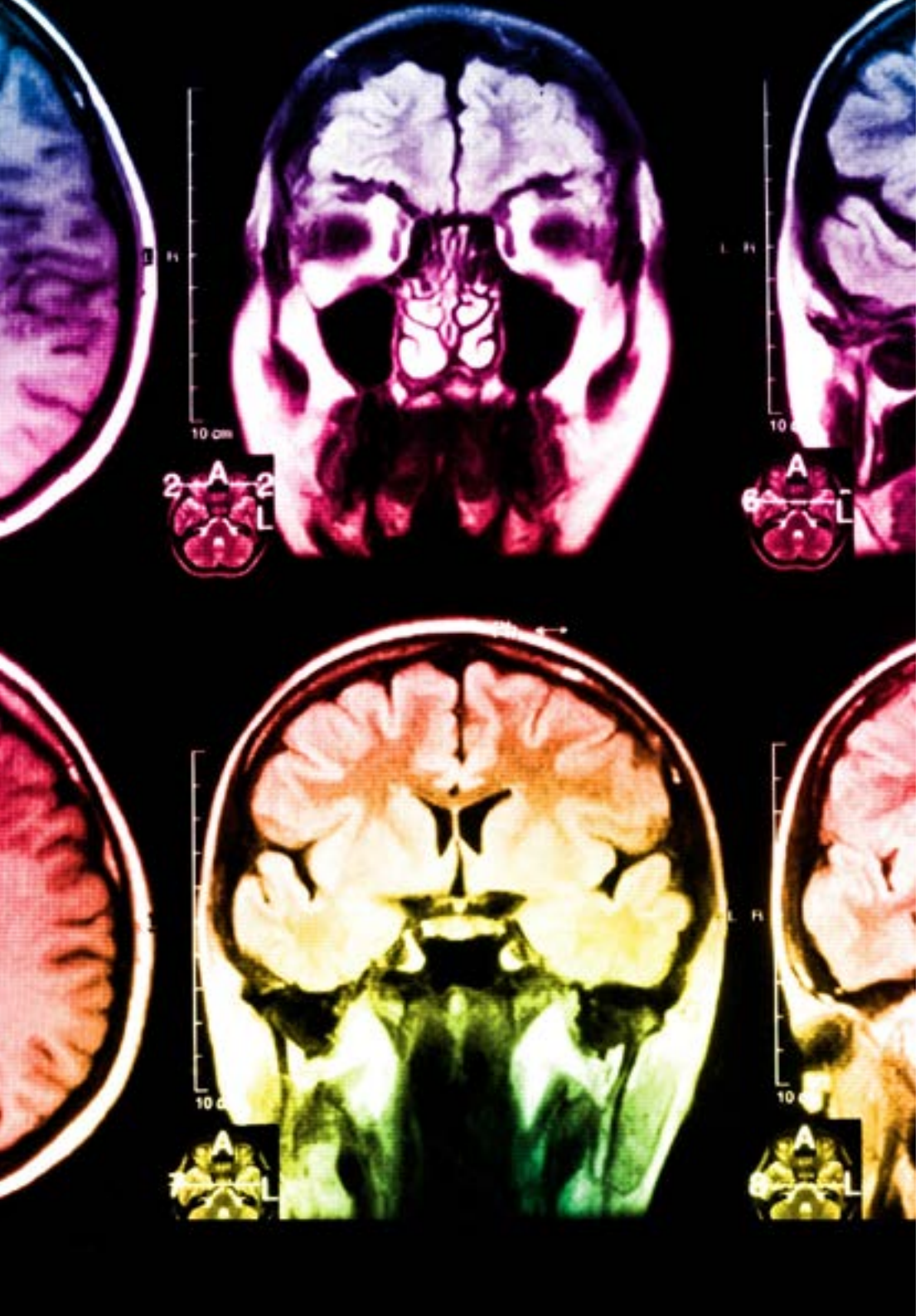
TECH est la première Université au monde à combiner les case studies de Cas avec un système d'apprentissage 100% en ligne basé sur la répétition, qui combine éléments didactiques différents dans chaque leçon.

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 serez formé 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 efficace. 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 Mastère Spécialisé, 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. Grâce à cette méthodologie, nous avons formé 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 matière de gestion, les sciences du sport, la philosophie, le droit, l'ingénierie, le journalisme, l'histoire ou les marchés et instruments financiers. Le tout 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 plus facilement et de manière plus productive tout en développant un esprit critique, en défendant des arguments et en contrastant des opinions : une équation directe vers le succès.

D'après les dernières données 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 façon, et dans ce que l'on appelle Neurocognitive context-dependent elearning les différents éléments de notre programme sont liés au contexte dans lequel le participant développe sa pratique professionnelle.

Ce programme offre les meilleurs matériels éducatifs, préparés à l'intention des professionnels :

Support d'étude

Tous les contenus didactiques sont créés par les spécialistes qui enseignent les cours. Ils ont été conçus en exclusivité pour le programme 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 online. Ils sont élaborés à l'aide des dernières techniques ce qui nous permet de vous offrir une grande qualité dans chacun des supports que nous partageons avec vous.

Cours magistraux

Il existe de nombreux faits scientifiques prouvant l'utilité de l'observation par un tiers expert.

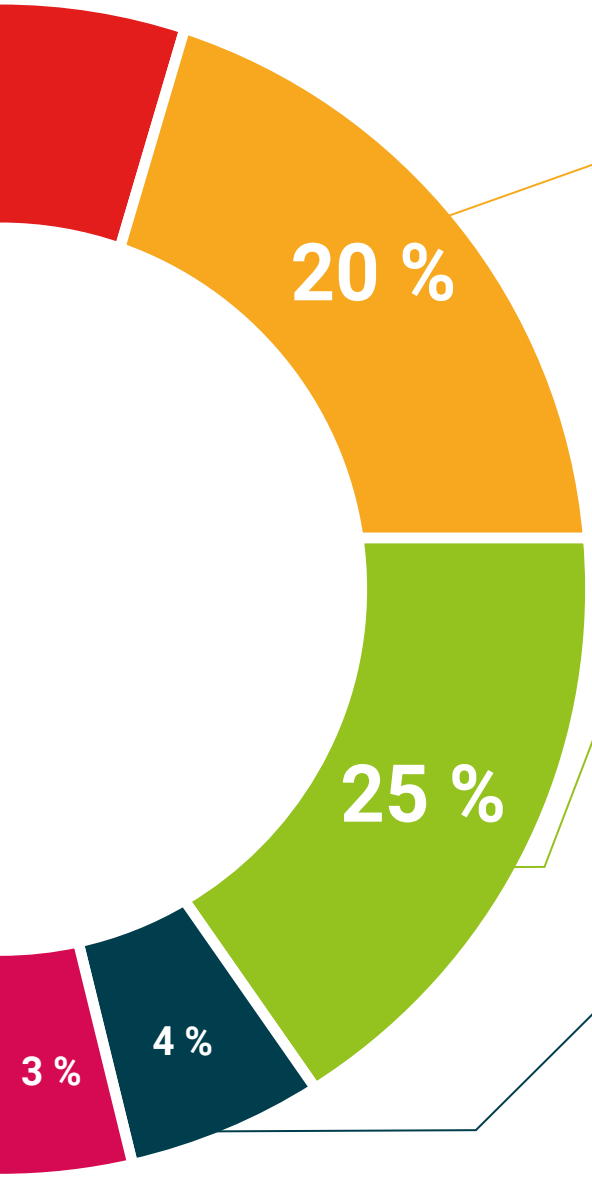
Apprendre d'un expert renforce les connaissances et la mémoire, et génère de la confiance dans les futures décisions difficiles.

Pratique des aptitudes et des compétences

Ils réaliseront des activités visant à développer des compétences et des aptitudes spécifiques dans chaque domaine. Pratiques et dynamiques pour acquérir et développer les compétences et les capacités 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 notre bibliothèque virtuelle TECH, vous aurez accès à tout ce dont vous avez besoin pour compléter votre 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

Nous présentons les contenus de manière attrayante et dynamique dans des dossiers multimédias comprenant des fichiers audios, des vidéos, des images, des diagrammes et des cartes conceptuelles afin de consolider les connaissances.

Ce système unique de formation à 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 Direction de la Cybersécurité (CISO, Chief Information Security Officer) garantit, outre la formation la plus rigoureuse et la plus actualisée, le respect des normes de sécurité, accès à un diplôme délivré par la TECH Université technologique.

Réussissez ce programme et recevez votre Mastère Spécialisé sans déplacements ni formalités administratives"

Ce **Mastère Spécialisé en Direction de la Cybersécurité (CISO, Chief Information Security Officer)** contient le programme le plus complet et le plus actuel du marché.

Après avoir réussi les évaluations, l'étudiant recevra par courrier postal avec accusé de réception le diplôme de **Mastère Spécialisé** délivré par **TECH Université Technologique.**

Le diplôme délivré par **TECH Université Technologique** indiquera la qualification obtenue lors du Mastère Spécialisé, et répond aux exigences communément demandées par les bourses d'emploi, les concours et les commissions d'évaluation des carrières professionnelles.

Diplôme : **Mastère Spécialisé en Direction de la Cybersécurité (CISO, Chief Information Security Officer)**

N.º d'Heures Officielles : **1.500 h.**

tech université technologique

Délivre le présent

DIPLÔME

a

Mme/M. _____, avec nº d'identification _____

Pour avoir finalisé et accrédité avec succès le programme de

MASTÈRE HYBRIDE

en

Direction de la Cybersécurité (CISO, Chief Information Security Officer)

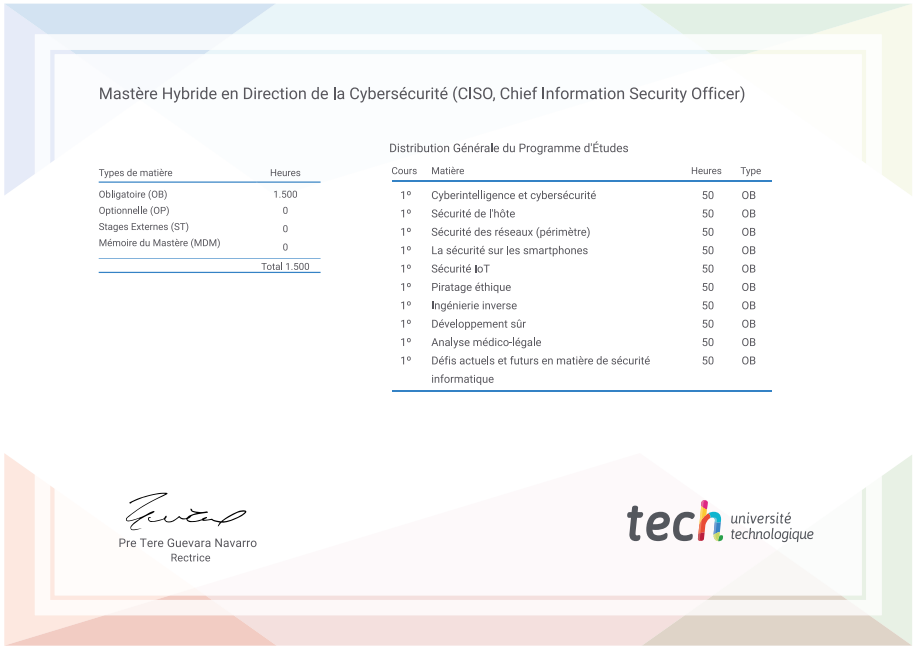
Il s'agit d'un diplôme spécialisé octroyé par cette Université d'une durée de 1.620 heures, débutant le dd/mm/aaaa et finalisant le dd/mm/aaaa.

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



Mastère Hybride en Direction de la Cybersécurité (CISO, Chief Information Security Officer)

Types de matière	Heures
Obligatoire (OB)	1.500
Optionnelle (OP)	0
Stages Externes (ST)	0
Mémoire du Mastère (MDM)	0
	Total 1.500

Distribution Générale du Programme d'Études

Cours	Matière	Heures	Type
1º	Cyberintelligence et cybersécurité	50	OB
1º	Sécurité de l'hôte	50	OB
1º	Sécurité des réseaux (périmètre)	50	OB
1º	La sécurité sur les smartphones	50	OB
1º	Sécurité IoT	50	OB
1º	Piratage éthique	50	OB
1º	Ingénierie inverse	50	OB
1º	Développement sûr	50	OB
1º	Analyse médico-légale	50	OB
1º	Défis actuels et futurs en matière de sécurité informatique	50	OB

Pre Tere Guevara Navarro
Rectrice

tech université technologique

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

tech université technologique

Mastère Spécialisé

Direction de la Cybersécurité (CISO, Chief Information Security Officer)

- Modalité: **en ligne**
- Durée: **12 mois**
- Qualification: **TECH Université Technologique**
- Intensité: **16h/semaine**
- Horaire: **à votre rythme**
- Examens: **en ligne**

Mastère Spécialisé

Direction de la Cybersécurité (CISO, Chief Information Security Officer)

tech université technologique