Mastère Avancé

Haute Direction en Cybersécurité

tech université technologique

tech université technologique

Mastère Avancé
Haute Direction en Cybersécurité

- Modalité: **en ligne**
- Durée: **2 ans**
- Quali ication: **TECH Université Technologique**
- Horaire: **à votre rythme**
- Examens: **en ligne**

Accès au site web: www.techtitute.com/fr/informatique/mastere-avance/mastere-avance-haute-direction-cybersecurite

Accueil

01

Présentation

Dans le monde d'aujourd'hui, la cybersécurité est un élément fondamental pour les individus et les entreprises, qui sont plus exposés que jamais aux attaques. Cela est dû au développement continu des nouvelles technologies et au processus de numérisation, qui a entraîné des transformations dans tous les types d'entreprises, rationalisant de nombreuses activités mais entraînant également l'apparition de nouvelles vulnérabilités. C'est pourquoi l'un des profils les plus recherchés aujourd'hui est celui du responsable de la cybersécurité, une figure en pleine expansion qui offre de nombreuses opportunités professionnelles. Ce programme explore cette figure en profondeur et prépare l'informaticien à faire face de manière efficace et complète à tous les défis actuels dans ce domaine, où des compétences en gestion et une perspective commerciale sont également requises. En outre, la formation est développée dans un format 100% en ligne, ce qui la rend idéale pour la combiner avec le travail, permettant au professionnel d'étudier quand il le souhaite.

Ce programme vous préparera à relever tous les défis actuels et futurs dans le domaine de la cybersécurité, en vous permettant de vous spécialiser dans la gestion de cet important secteur des technologies de l'information"

Processus bancaires, achats en ligne, communications internes dans différentes organisations, procédures administratives... Aujourd'hui, la numérisation a transformé la manière dont les individus et les entreprises fonctionnent au quotidien. Elle a rationalisé de nombreuses activités, rendu inutiles certains déplacements, amélioré la qualité de vie de la population et permis aux entreprises de réaliser des économies. Toutefois, ces avantages ont entraîné d'autres inconvénients en termes de cybersécurité.

Un grand nombre de technologies et d'outils numériques actuellement utilisés sont en développement continu et sont donc susceptibles d'être attaqués. L'utilisation d'applications et de dispositifs numériques s'étant généralisée, une défaillance de ceux-ci est critique, car elle peut affecter le développement de l'organisation, non seulement en termes de marketing et de ventes, mais aussi dans son propre fonctionnement interne, qui dépend également de ces utilitaires.

C'est pourquoi les entreprises ont besoin d'experts en cybersécurité capables de répondre aux différents problèmes qui peuvent se poser dans ce domaine. L'un des profils les plus recherchés est celui de Directeur de la Cybersécurité, un poste qui implique une vision globale de ce domaine, et pour lequel ce Mastère Avancé offre une préparation complète. Ainsi, ce programme est une grande opportunité pour les informaticiens, car il leur fournira tous les derniers développements dans ce domaine, tout en les préparant à faire face à des décisions managériales qui requièrent les meilleures connaissances et compétences en matière de leadership.

Tout cela, sur la base d'une méthodologie d'apprentissage en ligne qui s'adaptera aux circonstances professionnelles de l'étudiant, tout en étant accompagné par un corps enseignant de grand prestige dans ce domaine de l'informatique. Vous aurez également à votre disposition la meilleure technologie éducative et les ressources didactiques les plus récentes: résumés interactifs, vidéos, classes de maître, analyses de cas et lectures complémentaires.

Ce **Mastère Avancé en Haute Direction en Cybersécurité** contient le programme académique le plus complet et le plus actuel du marché. Les principales caractéristiques sont les suivantes:

- Le développement d'études de cas présentées par des experts en informatique et cybersécurité
- Le contenu graphique, schématique et éminemment pratique du programme fournit des informations scientifiques et pratiques sur les disciplines essentielles à la pratique professionnelle
- Des exercices pratiques permettant de réaliser le processus d'auto-évaluation afin d'améliorer l'apprentissage
- Le développement d'études innovant en direction de cybersécurité
- Cours théoriques, questions à l'expert, forums de discussion sur des sujets controversés et travail de réflexion individuel
- La possibilité d'accéder au contenu à partir de n'importe quel appareil fixe
- Ou portable doté d'une connexion internet

Avec ce Mastère Avancé, vous pourrez approfondir la sécurité de l'IoT, l'informatique en nuage, la blockchain et vous apprendrez à réaliser des audits de haut niveau pour tous les types d'entreprises et d'organisations"

La gestion de la cybersécurité est un profil professionnel en pleine expansion et ce programme vous offre la possibilité, grâce à la méthodologie en ligne de TECH, d'accéder aux meilleures opportunités dans ce domaine"

Vous bénéficierez du soutien d'un corps enseignant prestigieux, qui veillera à ce que vous obteniez toutes les clés dans le domaine de la gestion de la cybersécurité.

Vous disposerez des dernières ressources pédagogiques pour garantir un apprentissage rapide et efficace.

Son corps enseignant comprend des professionnels de la cybersécurité que qui apportent leur expérience professionnelle à ce programme, ainsi que des spécialistes reconnus issus de grandes entreprises et d'universités prestigieuses.

Son contenu multimédia, développé avec les dernières technologies éducatives, permettra au professionnel un apprentissage situé et contextuel, c'est-à-dire un environnement simulé qui fournira un étude immersif programmé pour s'entraîner dans des situations réelles.

La conception de ce programme est axée sur l'Apprentissage par les Problèmes, grâce auquel l'étudiant doit essayer de résoudre les différentes situations de la pratique professionnelle qui se présentent tout au long du Certificat Avancé. Pour ce faire, le professionnel aura l'aide d'un système vidéo interactif innovant créé par des experts reconnus.

02

Objectifs

L'objectif principal de ce Mastère Avancé est de faire de l'informaticien un grand spécialiste dans ce domaine, lui permettant d'accéder aux meilleures opportunités professionnelles. À cette fin, il couvrira non seulement tous les derniers développements dans le domaine de la cybersécurité, mais vous fournira également les meilleurs outils pour obtenir une perspective globale des besoins des entreprises dans ce domaine. Ainsi, vous serez en mesure de travailler à la gestion de la sécurité des entreprises à tout moment, en connaissant les meilleures méthodes à suivre dans chaque cas.

Ce Mastère Avancé vous aidera à réaliser les progrès professionnels que vous recherchez, grâce à son contenu complet et actualisé, et à son corps enseignant prestigieux composé d'experts en cybersécurité en activité"

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
- Générer des connaissances spécialisées sur un système d'information, les types et les aspects de sécurité à prendre en compte
- Identifier les vulnérabilités d'un système d'information
- Développer la réglementation juridique et la criminalisation de la criminalité à l'encontre d'un système d'information
- Évaluer les différents modèles d'architecture de sécurité afin d'établir
- Le modèle le plus approprié pour l'organisation
- Identifier les cadres réglementaires d'application et leurs bases réglementaires de ces cadres
- Analyser la structure organisationnelle et fonctionnelle d'un domaine de la sécurité de l'information(bureau du CISO)
- Analyser et développer la notion de risque, d'incertitude dans l'environnement dans lequel nous vivons
- Examiner le Modèle de Gestion des Risques basé sur la norme Iso 31.000
- Examiner la science de la cryptologie et la relation avec ses branches: cryptographie, cryptanalyse, stéganographie et stégo-analyse
- Analyser les types de cryptographie en fonction du type d'algorithme et de leur utilisation
- Examiner les certificats numériques
- Examiner l'Infrastructure à Clé Publique (ICP)
- Développer le concept de gestion de l'identité
- Identifier les méthodes d'authentification
- Générer des connaissances spécialisées sur l'écosystème de la sécurité informatique
- Évaluer les connaissances en matière de cybersécurité
- Identifier les domaines de la sécurité du *cloud*
- Analyser les services et outils de chacun des domaines de sécurité
- Développer les spécifications de sécurité de chaque technologie LPWAN
- Analyse comparative de la sécurité des technologies LPWAN

Objectifs spécifiques

- 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
- Précisez les politiques de *backup* des données personnelles et professionnelles
- Évaluer les différents outils permettant d'apporter des solutions à des problèmes spécifiques de sécurité
- 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
- 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
- Examinez les différents vecteurs d'attaque pour éviter de devenir une cible facile
- Déterminer les principales attaques et les principaux types de logiciels malveillants 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
- 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
- Examiner les méthodes de l'IOSINT
- 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
- 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 le Sandboxing dans différents environnements
- Développer les différentes techniques d'analyse des logiciels malware
- Développer les différentes techniques d'analyse des malware
- 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
- 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
- Connaître les principes syntaxiques du langage graphique et appliquer ses règles pour décrire des objets et des idées de façon claire et précise
- Connaître l'origine des lettres et leur importance historique
- Reconnaître, étudier et appliquer de manière cohérente la typographie aux processus graphiques
- Connaître et appliquer les fondements esthétiques de la typographie
- Savoir analyser la disposition des textes dans l'objet de conception
- Être capable d'effectuer un travail professionnel basé sur la composition typographique
- Évaluer la sécurité d'un système d'information dans toutes ses composantes et couches
- Identifier les types actuels de menaces à la sécurité et leurs tendances
- Établir des lignes directrices en matière de sécurité en définissant des politiques et des plans de sécurité et d'urgence
- Analyser les stratégies et les outils permettant d'assurer l'intégrité et la sécurité des systèmes d'information
- Appliquer des techniques et des outils spécifiques pour chaque type d'attaque ou de faille de sécurité
- Protéger les informations sensibles stockées dans le système d'information
- Disposer du cadre juridique et de la typologie du délit, en complétant la vision par la typologie du délinquant et de sa victime
- Aligner le plan directeur de sécurité sur les objectifs stratégiques de l'organisation
- Établir un cadre de gestion continue des risques faisant partie intégrante du Plan Directeur de Sécurité
- Déterminer les indicateurs appropriés pour le suivi de la mise en œuvre du SGSI
- Établir une stratégie de sécurité fondée sur une politique
- Analyser les objectifs et les procédures associés au plan de sensibilisation des employés, des fournisseurs et des partenaires
- Identifier, dans le cadre réglementaire, les réglementations, certifications et lois applicables à chaque organisation
- Développer les éléments fondamentaux requis par la norme ISO 27001:2013
- Mettre en place un modèle de gestion de la vie privée conforme à la réglementation européenne GDPR/RGPD
- Identifier les différentes structures que peut avoir un domaine de sécurité de l'information
- Développer un modèle de sécurité basé sur trois lignes de défense
- Présenter les différents comités périodiques et extraordinaires dans lesquels intervient le domaine de la cybersécurité
- Identifier les outils technologiques qui soutiennent les principales fonctions de l'équipe des opérations de sécurité (SOC)
- Évaluer les mesures de contrôle des vulnérabilités appropriées à chaque scénario
- Développer le cadre des opérations de sécurité basé sur le NIST CSF
- Préciser la portée des différents types d'audits (Red Team, Pentesting, Bug Bounty, etc.)
- Proposer les activités à mener suite à un incident de sécurité

- Mettre en place un centre de commandement de la sécurité de l'information englobant tous
- Les acteurs concernés (autorités, clients, fournisseurs, etc.)
- Examiner, dans une perspective globale, l'environnement dans lequel nous opérons
- Identifier les principaux risques et opportunités susceptibles d'affecter la réalisation de nos objectifs
- Analyser les risques sur la base des meilleures pratiques dont nous disposons
- Évaluer l'impact potentiel de ces risques et opportunités
- Développer des techniques qui nous permettent de gérer les risques et les opportunités de manière à maximiser notre contribution à la valeur ajoutée
- Examiner en profondeur les différentes techniques de transfert de risque et de valeur
- Générer de la valeur à partir de la conception de modèles propriétaires pour la gestion agile des risques
- Examiner les résultats afin de proposer des améliorations continues dans la gestion de projet et les processus basés sur des modèles de gestion axés sur le risque ou *risk-driven*
- Innover et transformer les données générales en informations pertinentes pour la prise de décision basée sur le risque
- Compiler les opérations fondamentales (XOR, grands nombres, substitution et transposition) et les différents composants (fonctions unidirectionnelles, hachage, générateurs de nombres aléatoires)
- Analyser les techniques cryptographiques
- Développer différents algorithmes cryptographiques numériques
- Évaluer les systèmes de gestion des clés et l'importance de la longueur des clés cryptographiques
- Examiner les algorithmes de dérivation des clés
- Analyser le cycle de vie des clés
- Évaluer les modes de chiffrement par bloc et de chiffrement par flot
- Déterminer les générateurs de nombres pseudo-aléatoires
- Développer des cas d'application cryptographiques réels, tels que Kerberos, PGP ou les cartes à puce
- Examiner les associations et organismes concernés, tels que l'ISO, le NIST ou le NCSC
- Déterminer les défis de la cryptographie de l'informatique quantique
- Développer le concept d'identité numérique
- Évaluer le contrôle d'accès physique à l'information
- Principes fondamentaux de l'authentification biométrique et de l'authentification MFA
- Évaluer les attaques contre la confidentialité des informations
- Analyser la fédération d'identité
- Mettre en place un contrôle d'accès au réseau
- Développer une expertise en matière de sécurité physique et logique

- Démontrer ses connaissances en matière de communications et de réseaux
- Identifier les principales attaques malveillantes
- Établir un cadre de développement sécurisé
- Démontrer une compréhension des principales réglementations relatives aux systèmes de gestion de la sécurité de l'information
- Démontrer sa compréhension du fonctionnement d'un centre opérationnel de cybersécurité
- Démontrer l'importance de mettre en place des pratiques de cybersécurité en cas de catastrophes organisationnelles
- Identifier les risques liés au déploiement d'une infrastructure de *cloud* public
- Définir les exigences de sécurité
- Élaborer un plan de sécurité pour le déploiement d'une infrastructure *cloud*
- Identifier les services *cloud* à déployer pour la mise en œuvre d'un plan de sécurité
- Déterminer les opérations requises pour les mécanismes de prévention
- Établir les lignes directrices d'un système de *logging* et de surveillance
- Proposer des actions de réponse aux incidents
- Présenter l'architecture simplifiée de l'IoT
- Justifier les différences entre les technologies de connectivité généralistes et les technologies de connectivité pour l'IoT
- Établir le concept du triangle de fer de la connectivité de l'IoT
- Analyser les spécifications de sécurité des technologies LoRaWAN, NB-IoT et WiSUN
- Justifier le choix de la technologie IoT appropriée pour chaque projet
- Présenter les éléments clés de chaque phase et Analyser les caractéristiques du Plan de Continuité des Activités (PCA)
- Justifier la nécessité d'un Plan de Continuité des Activités
- Déterminer les cartes de succès et de risques pour chaque phase du Plan de Continuité des Activités
- Préciser comment établir un Plan d'Action pour la mise en œuvre
- Évaluer l'exhaustivité d'un Plan de Continuité des Activités (PCA)
- Élaborer un Plan pour la Mise en œuvre réussie d'un Plan de continuité pour nos activités

03

Compétences

Tout au long de ce Mastère Avancé, le professionnel acquerra une série d'outils et de compétences qui lui permettront de travailler dans la gestion de la cybersécurité d'une grande entreprise. C'est pourquoi ce programme ne se concentre pas uniquement sur les aspects informatiques, mais s'intéresse également au processus de numérisation, aux technologies émergentes et à la manière dont ces éléments ont affecté les activités courantes et quotidiennes des organisations. De cette manière, le diplômé sera capable de s'adapter au contexte actuel, en connaissant les meilleures solutions de sécurité pour chaque entreprise.

Améliorez vos compétences pour devenir le spécialiste de la cybersécurité dans votre environnement"

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
- Appliquer les mesures de sécurité les plus appropriées en fonction des menaces
- Déterminer la politique et le plan de sécurité dans le système d'information d'une entreprise, en achevant la conception et la mise en œuvre du Plan d'Urgence
- Établir un programme d'audit qui répond aux besoins d'auto-évaluation de la cybersécurité de l'organisation
- Développer un programme d'analyse et de surveillance des vulnérabilités et un plan de réponse aux incidents de cybersécurité
- Maximiser les opportunités et éliminer l'exposition à tous les risques potentiels liés à la conception
- Compiler les systèmes de gestion des clés
- Évaluer la sécurité de l'information d'une entreprise
- Analyser les systèmes d'accès à l'information
- Développer les meilleures pratiques en matière de développement sécurisé
- Présenter les risques pour les entreprises de ne pas disposer d'un environnement de sécurité informatique

Ce programme vous fera découvrir l'avenir de la cybersécurité"

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 éthique et protéger une entreprise d'une cyberattaque
- Être capable d'enquêter sur un incident de cybersécurité
- Connaître les différentes techniques d'attaque et de défense disponibles
- Analyse du rôle du Responsable de la Sécurité de l'Information (Chief Information Security Officer)
- Comprendre le fonctionnement de l'ingénierie sociale et ses méthodes
- Développer un Système de Management de la Sécurité de l'Information (SMSI)
- Identifier les éléments clés qui composent un SMSI
- Appliquer la méthodologie MAGERIT pour faire évoluer le modèle et aller plus loin
- Concevoir de nouvelles méthodologies propres de gestion des risques, basées sur le concept *agile risk management*
- Identifier, analyser, évaluer et traiter les risques auxquels le professionnel est confronté dans une nouvelle perspective commerciale basée sur un modèle *risk-driven* ou sur les risques qui permet non seulement de survivre dans son propre environnement, mais aussi d'apporter sa propre contribution à la valeur ajoutée
- Examiner le processus de conception d'une stratégie de sécurité lors du déploiement de services d'entreprise en *cloud*
- Évaluer les différences entre les implémentations concrètes des différents vendeurs de *cloud* publics
- Évaluer les options de connectivité IoT pour répondre à un projet, en mettant l'accent sur les technologies LPWAN
- Présenter les spécifications de base des principales technologies LPWAN pour l'IoT

04

Direction de la formation

TECH a compilé les informations les plus récentes dans le domaine de la gestion des systèmes d'information afin que les informaticiens puissent trouver, dans un seul programme, le soutien didactique nécessaire pour améliorer leur formation et devenir un directeur des systèmes d'information performant. Sans aucun doute, un Mastère Avancé qui marquera un avant et un après dans leur formation et qui leur donnera l'opportunité d'augmenter leurs options d'employabilité.

Un programme complet qui vous introduira aux derniers concepts en matière de gestion d'entreprise et de systèmes informatiques pour devenir un directeur des systèmes d'information performant"

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 Disruptives.** 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. Pendant 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 très pertinents, tous liés au **renseignement criminel, au maintien de l'ordre, 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 être Professeur de Pratique et 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 Disruptives à l'Université de Georgetown
- Directeur du Master en Gestion des Technologies de l'Information à l'Université de Georgetown
- Directeur du Master en Gestion des Technologies, Université de Georgetown
- Directeur du Master en Gestion des Risques de Cybersécurité à l'Université de Georgetown
- Directeur du Master en Intelligence Appliquée à l'Université de Georgetown
- Professeur de Stage à l'Université de Georgetown
- Doctorat en Criminologie de l'École de Criminologie de l'Université de Montréal
- Licence en Sociologie, Mineure en Psychologie, Université de Laval
- Membre de: New Program Roundtable Committee, Université de Georgetown

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

Direction

Mme Fernández Sapena, Sonia

- Formatrice en Sécurité Informatique et Ethical Hacking au Centre National de Référence pour l'Informatique et les Télécommunications
- Formatrice en Sécurité Informatique et Piratage Ethique au Centre National de Référence pour l'Informatique et les Télécommunications à Getafe, Madrid
- Formatrice Agréée E-Council
- Formatrice en: EXIN Ethical Hacking Foundation et EXIN Cyber & IT Security Foundation Madrid
- Formatrice Spécialisée accréditée par le CAM pour les Certificats Professionnels suivants: Sécurité Informatique (IFCT0190), Gestion des Réseaux de Voix et de Données (IFCM0310), Administration des Réseaux Départementaux (IFCT0410), Gestion des Alarmes de Réseaux de Télécommunications (IFCM0410), Opérateur de Réseaux de Voix et Données (IFCM0110), et Administration des Services Internet (IFCT0509)
- Collaboratrice Externe CSO/SSA (*Chief Security Officer/Senior Security Architect*) à l'Université des Iles Baléares
- Ingénierie Informatique, Université d'Alcalá de Henares de Madrid
- Master en DevOps: Docker and Kubernetes Cas-Training
- Microsoft Azure Security Techonologies E-Council

M. Olalla Bonal, Martín

- Responsable de la Pratique *Blockchain* chez EY
- Spécialiste Technique Client *Blockchain* pour IBM
- Directeur de l'Architecture de Blocknitive
- Coordinateur de l'Équipe Bases de Données Distribuées non Relationnelles pour wedoIT, Filiale d'IBM
- Architecte d'Infrastructure chez Bankia
- Chef du Département Mise en Page chez T-Systems
- Coordinateur de Département pour Bing Data España SL

Professeurs

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
- Technicienne en Système pour la Migration des Équipements et pour la Gestion, la Maintenance et la Formation des PDA Mobiles
- Ingénieure Technique en Systèmes Informatiques par l'Université Ouverte de Catalogne
- Master en Sécurité Informatique et Piratage Éthique Officielle EC- Council et CompTIA par l'École Professionnelle des Nouvelles Technologies CICE

M. Peralta Alonso, Jon

- Consultant Senior - Protection des Données et Cybersécurité chez Altia
- Avocat / Conseiller Juridique chez Arriaga Associés Assessorat Juridique et Economique S.L
- Conseiller Juridique / Stagiaire dans un Cabinet Professionnel: Oscar Padura
- Licence en Droit de l'Université Publique du Pays Basque
- Master en Protection des Données Délégué de l'EIS Innovative School
- Master en Droit de l'Université Publique du Pays Basque
- Master Spécialisé en Pratique du Contentieux Civil de l'Université Internationale Isabel I de Castille
- Professeur du Master en Protection des Données Personnelles, Cybersécurité et Droit des TIC

M. Redondo, Jesús Serrano

- Développeur web et technicien en cybersécurité
- Développeur Web chez Roams, Palencia
- Développeur *FrontEnd* chez Telefónica, Madrid
- Développeur *FrontEnd* chez Best Pro Consulting SL, Madrid
- Installateur d'Équipements et de Services de Télécommunications à Grupo Zener, Castille et Léon
- Installateur d'Équipements et de Services de Télécommunications chez Lican Comunicaciones SL, Castille et Léon
- Certificat en Sécurité informatique, CFTIC Getafe, Madrid
- Technicien Supérieur en Télécommunications et Systèmes Informatiques par l'IES Trinité Arroyo, Palencia
- Technicien Supérieur en Installations Electrotechniques MT et BT, Lycée Trinité Arroyo, Palencia
- Formation en Rétro-Ingénierie, Sténographie et Cryptage par Incibe Hacker Academy

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

M. Nogales Ávila, Javier

- Enterprise Cloud and Sourcing Senior Consultant chez Quint
- Cloud et Technology Consultant chez Indra
- Consultant Technologique Associé chez Accenture
- Diplômé en Ingénierie de la Gestion Industrielle de l'Université de Jaén
- MBA en Administration et Gestion des Entreprises par ThePower Business School

M. Gómez Rodríguez, Antonio

- Ingénieur Principal de Solutions Cloud chez Oracle
- Co-organisateur de Malaga Developer Meetup
- Consultant Spécialisé pour Sopra Group et Everis
- Chef d'équipe chez System Dynamics
- Développeur de Logiciels chez SGO Software
- Master en E-Business de l'École de Commerce de La Salle
- Diplôme en Technologies et Systèmes d'Information, Institut Catalan de Technologie
- Licence en Génie Supérieur des Télécommunications de l'Université Polytechnique de Catalogne

M. Catalá Barba, José Francisco

- Technicien en Électronique Expert en Cybersécurité
- Développeur d'Applications Mobiles
- Technicien en Électronique au Service de Commandement Intermédiaire du Ministère de la Défense Espagnol
- Technicien en Électronique à l'usine Ford Sita, à Valence

M. Gonzalo Alonso, Félix

- Directeur Général et Fondateur de Smart REM Solutions
- Responsable de l'Ingénierie des Risques et de l'Innovation chez Dynargy
- Directeur et Partenaire Fondateur de Risknova, une Société de Conseil en Technologie
- Master en Gestion des Assurances de l'Institut pour la Collaboration entre les Compagnies d'Assurances
- Diplôme en Ingénierie Technique Industrielle, spécialité Électronique Industrielle de l'Université Pontificale de Comillas

M. Entrenas, Alejandro

- Chef de Projet en Cybersécurité
- Chef de projet en Cybersécurité Entelgy Innotec Security
- Consultant en Cybersécurité Entelgy
- Analyste en Sécurité de l'Information Innovery Espagne
- Analyste en Sécurité de l'Information Atos
- Licence en Ingénierie Technique des Systèmes Informatiques de l'Université de Cordoue
- Master en Gestion de la Sécurité de l'Information de l'Université Polytechnique de Madrid
- ITIL v4 Foundation Certificate in IT Service Management. ITIL Certified
- IBM Security QRadar SIEM 7.1 Advanced. Avnet
- IBM Security QRadar SIEM 7.1 Foundations. Avnet

M. Del Valle Arias, Jorge

- Ingénieur en Télécommunications avec Expertise en Développement d'Affaires
- Smart City Solutions & Software Business Development Manager Espagne Itron, Inc Consultant IoT
- Directeur Commercial IoT par Intérim TCOMET
- Responsable de l'Unité Commerciale IoT, Industrie 4.0 Diode Espagne
- Directeur de la Zone de Ventes de l'IoT et des Télécommunications Aicox Solutions
- Directeur Technique (CTO) et Directeur du Développement des Affaires Consultation TELYC
- Fondateur et PDG de Sensor Intelligence
- Chef des Opérations et des Projets Codio
- Directeur des Opérations chez Codium Networks
- Ingénieur en Chef de la Conception du hardware et du firmware AITEMIN
- Responsable Régional de la Planification et de l'Optimisation RF - Réseau LMDS 3.5 GHz Clearwire
- Ingénieur en Télécommunications de l'Université Polytechnique de Madrid
- Executive MBA de l'International Graduate School de La Salle de Madrid
- Master en Énergies Renouvelables CEPYME

M. Gozalo Fernández, Juan Luis

- Gestionnaire de Produits basés sur la blockchain pour Open Canarias
- Directeur Blockchain DevOps chez Alastria
- Responsable de la Technologie des Niveaux de Service chez Santander Espagne
- Directeur du Développement des Applications Mobiles Tinkerlink chez Cronos Telecom
- Directeur de la Technologie de Gestion des Services Informatiques à la Barclays Bank Espagne

- Diplôme en Ingénierie Informatique à l'UNED
- Spécialisation en *Deep Learning* chez DeepLearning.ai

Mme Jurado Jabonero, Lorena

- Responsable de la Sécurité de l'Information (CISO) chez Groupe Pascual
- Cybersecurity Manager en KPMG. Espagne
- Consultante en Processus Informatique et Contrôle d'Infrastructure et en Gestion de Projet chez Bankia
- Ingénieuse en Outils d'Exploitation chez Dalkia
- Développeur au Sein du Groupe Banco Popular
- Développeur des Applications à l'Université Polytechnique de Madrid
- Diplômé en Ingénierie Informatique de l'Université Alfonso X el Sabio
- Ingénieuse Technique en Gestion Informatique de l'Université Polytechnique de Madrid
- Certified Data Privacy Solutions Engineer (CDPSE) par l'ISACA

M. Ortega Esteban, Octavio

- Spécialiste du Marketing et du Développement Web
- Programmeur d'Applications Informatiques et Développeur Web Indépendant
- *Chief Operating Officer* chez Smallsquid SL
- Administrateur du E-commerce pour Ortega et Serrano
- Conférencier pour les cours de Certificat de Professionnalisme en Informatique et Communications
- Conférencier pour les cours de Sécurité Informatique
- Licence en Psychologie de l'Université Ouverte de Catalogne
- Technicien Supérieur d'Analyse, de Conception et de Solutions Logicielles
- Technicien Supérieur en Programmation Avancée

M. Embid Ruiz, Mario

- Avocat Expert en TIC et protection des données chez Martínez-Echevarría Avocats
- Directeur Juridique de Branddocs SL
- Analyste des Risques dans le Segment PME de BBVA
- Chargé de cours dans le cadre d'études universitaires de troisième cycle en rapport avec le Droit
- Licence en Droit de l'Université Roi Juan Carlos
- Licence en Administration et Gestion d'Entreprises à l'Université Roi Juan Carlos
- Master en Droit des Nouvelles Technologies, de l'Internet et de l'Audiovisuel du Centre d'Etudes Universitaires Villanueva

M. Rodrigo Estébanez, Juan Manuel

- Co-fondateur d'Ismet Tech
- Directeur de la Sécurité de l'Information chez Ecix Group
- Operational Security Officer chez Atos IT Solutions and Services A/S
- Chargé de cours en Gestion de la Cybersécurité dans le cadre d'Études Universitaires
- Diplôme d'Ingénieur de l'Université de Valladolid
- Master en Systèmes de Gestion Intégrée de l'Université CEU San Pablo

05

Structure et contenu

Ce Mastère Avancé en Haute Direction en Cybersécurité est composé de 20 modules, et a été soigneusement conçu pour rapprocher les professionnels des derniers développements dans ce domaine. Ainsi, vous découvrirez les avancées les plus récentes dans des domaines tels que la sécurité des *smartphones*, la sécurité dans l'internet des objets, le développement sécurisé, la cryptographie et la sécurité dans les environnements de *cloud computing*. Avec ce programme, l'informaticien aura donc accès aux connaissances les plus récentes et les plus complètes, ce qui le préparera rapidement à devenir un spécialiste de la cybersécurité très prestigieux.

Vous ne trouverez pas de contenu plus complet pour vous mettre à jour dans le domaine de la cybersécurité"

Module 1. Cyber Intelligence et Cybersécurité

1.1. Cyber Intelligence
- 1.1.1. Cyber Intelligence
  - 1.1.1.1. Renseignement
    - 1.1.1.1.1. Cycle du renseignement
  - 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 de 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. OWISAP
- 1.3.7. PTES
- 1.3.8. OSSTM

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. L'anonymat sur le Net
- 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'intrusion-HIDS
- 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. Pare-feu pour Linux
- 2.4.3. Pare-feu 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. StickyPassword
- 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. Pare-feu courants du 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 journaux du système
  - 3.2.4.1. TCP Wrappers
  - 3.2.4.2. BlockHosts et DenyHosts
  - 3.2.4.3. Fai2ban

3.3. Systèmes de Détection et Prévention des Intrusions (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 Pare-feu 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. ACLs du Cloud
  - 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 de l'entreprise
- 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 forcé
- 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. Test 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 Android
- 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. Transports
- 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. Transports
- 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'exercice et de la fréquence cardiaque
- 5.8.2. Surveillance des patients et des personnes âgées
- 5.8.3. Implantation
- 5.8.4. Robots chirurgicaux

5.9. Connectivité
- 5.9.1. Wi-Fi/Gateway
- 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. Hacking 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. Système de Virtualisation
- 6.1.3. *Sandbox*
- 6.1.4. Déploiement des laboratoires

6.2. Méthodologie
- 6.2.1. OSSTM
- 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 Vulnérabilités
  - 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. Wi-Fi 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. SQLinjection

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 codes
- 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. Analyseurs 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. Tableaux
- 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
- 7.5.3. 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 de 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 Sécurisé

8.1. Développement Sécurisé
- 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 d'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 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 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 Forense

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 technique non-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. Analyse Légale 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 Légaux 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 Courrier Électronique
- 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 du Courrier Electronique
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 Covid19
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

Module 11. La sécurité dans la conception et le développement des systèmes

11.1. Systèmes d'information
- 11.1.1. Domaines d'un système d'information
- 11.1.2. Composants des systèmes d'information
- 11.1.3. Activités d'un système d'information
- 11.1.4. Cycle de vie d'un système d'information
- 11.1.5. Ressources d'un système d'information

11.2. Systèmes d'information. Typologie
- 11.2.1. Types de systèmes d'information
  - 11.2.1.1. Commerciale
  - 11.2.1.2. Stratégique
  - 11.2.1.3. Selon le domaine d'application
  - 11.2.1.4. Spécifique
- 11.2.2. Systèmes d'information Exemples concrets
- 11.2.3. Évolution des systèmes d'information: Étapes
- 11.2.4. Méthodologies des systèmes d'information

11.3. Sécurité des systèmes d'information. Implications juridiques
- 11.3.1. Accès aux données
- 11.3.2. Menaces sur la sécurité: Vulnérabilités
- 11.3.3. Implications juridiques: Crimes
- 11.3.4. Procédures de maintenance des systèmes d'information

11.4. Sécurité d'un système d'information. Protocole de sécurité
- 11.4.1. Sécurité d'un système d'information
  - 11.4.1.1. Intégrité
  - 11.4.1.2. Confidentialité
  - 11.4.1.3. Disponibilité
  - 11.4.1.4. Authentification
- 11.4.2. Services de sécurité
- 11.4.3. Protocoles de sécurité de l'information. Typologie
- 11.4.4. Sensibilité d'un système d'information

11.5. Sécurité d'un système d'information Mesures et systèmes de contrôle d'accès
- 11.5.1. Mesures de sécurité
- 11.5.2. Type de mesures de sécurité
  - 11.5.2.1. Prévention
  - 11.5.2.2. Détection
  - 11.5.2.3. Correction
- 11.5.3. Systèmes de contrôle d'accès Typologie
- 11.5.4. Cryptographie

11.6. Sécurité dans les réseaux sur l'internet
- 11.6.1. Firewalls
- 11.6.2. Identification numérique
- 11.6.3. Virus et vers
- 11.6.4. Hacking
- 11.6.5. Exemples et cas réels

11.7. Criminalité informatique
- 11.7.1. Criminalité informatique
- 11.7.2. Criminalité informatique Typologie
- 11.7.3. Criminalité informatique L'attaque Typologie
- 11.7.4. Le cas de la réalité virtuelle
- 11.7.5. Profils des auteurs et des victimes Typification de la criminalité
- 11.7.6. Criminalité informatique Exemples et cas réels

11.8. Plan de sécurité du système d'information
- 11.8.1. Plan de sécurité. Objectifs
- 11.8.2. Plan de sécurité. Planification
- 11.8.3. Plan de risque Analyse
- 11.8.4. Politique de sécurité. Mise en œuvre dans l'organisation
- 11.8.5. Plan de sécurité. Mise en œuvre dans l'organisation
- 11.8.6. Procédures de sécurité. Types
- 11.8.7. Plans de sécurité Exemples

11.9. Plan de contingence
- 11.9.1. Plan de contingence Fonctions
- 11.9.2. Plan d'urgence: Éléments et objectifs
- 11.9.3. Plan d'urgence dans l'organisation Mise en œuvre
- 11.9.4. Plans de contingence Exemples

11.10. Gouvernance de la sécurité des systèmes d'information
- 11.10.1. Réglementation juridique
- 11.10.2. Normes
- 11.10.3. Certifications
- 11.10.4. Technologies

Module 12. Architectures et modèles de sécurité de l'information

12.1. Architecture de la sécurité de l'information
- 12.1.1. SMSI/PDS
- 12.1.2. Alignement stratégique
- 12.1.3. Gestion des risques
- 12.1.4. Mesure de la performance

12.2. Modèles de sécurité de l'information
- 12.2.1. Modèles de sécurité fondés sur des politiques
- 12.2.2. Basés sur des outils de protection
- 12.2.3. Basé sur l'équipe de travail

12.3. Modèle de sécurité. Éléments clés
- 12.3.1. Identification des risques
- 12.3.2. Définition des contrôles
- 12.3.3. Évaluation continue des niveaux de risque
- 12.3.4. Plan de sensibilisation des employés, des fournisseurs, des partenaires, etc

12.4. Processus de gestion des risques
- 12.4.1. Identification des actifs
- 12.4.2. Identification des menaces
- 12.4.3. Évaluation des risques
- 12.4.4. Hiérarchisation des contrôles
- 12.4.5. Réévaluation et risque résiduel

12.5. Processus d'entreprise et sécurité de l'information
- 12.5.1. Processus d'entreprise
- 12.5.2. Évaluation des risques sur la base des paramètres de l'entreprise
- 12.5.3. Analyse de l'impact sur l'entreprise
- 12.5.4. Les opérations d'entreprise et sécurité de l'information

12.6. Processus d'amélioration continue
- 12.6.1. Le cycle de Deming
  - 12.6.1.1. Planification
  - 12.6.1.2. Faire
  - 12.6.1.3. Vérifier
  - 12.6.1.4. Agir

12.7. Architectures de sécurité
- 12.7.1. Sélection et normalisation des technologies
- 12.7.2. Gestion de l'identité Authentification
- 12.7.3. Gestion des accès Autorisation
- 12.7.4. Sécurité de l'infrastructure du réseau
- 12.7.5. Technologies et solutions de chiffrement
- 12.7.6. Sécurité des équipements terminaux (EDR)

12.8. Le cadre réglementaire
- 12.8.1. Réglementations sectorielles
- 12.8.2. Certifications
- 12.8.3. Législation

12.9. Norme ISO 27001
- 12.9.1. Mise en œuvre
- 12.9.2. Certification
- 12.9.3. Audits et tests de pénétration
- 12.9.4. Gestion continue des risques
- 12.9.5. Classification des informations

12.10. Législation en matière de protection de la vie privée RGPD (GDPR)
- 12.10.1. Champ d'application du règlement général sur la protection des données (RGPD)
- 12.10.2. Données personnelles
- 12.10.3. Rôles dans le traitement des données à caractère personnel
- 12.10.4. Droits de l'ARCO
- 12.10.5. Le DPO Fonctions

Module 13. Gestion de la sécurité IT

13.1. Gestion de la sécurité
- 13.1.1. Opérations de sécurité
- 13.1.2. Aspects juridique et réglementaire
- 13.1.3. Qualification des entreprises
- 13.1.4. Gestion des risques
- 13.1.5. Gestion des identités et des accès

13.2. Structure du domaine de la sécurité. Le bureau du CISO
- 13.2.1. Structure de l'organisation Position du CISO dans la structure
- 13.2.2. Les lignes de défense
- 13.2.3. Organigramme du bureau du CISO
- 13.2.4. Gestion du budget

13.3. Gouvernance de la sécurité
- 13.3.1. Comité de sécurité
- 13.3.2. Comité de suivi des risques
- 13.3.3. Comité d'audit
- 13.3.4. Comité de crise

13.4. Gouvernance de la sécurité. Fonctions
- 13.4.1. Politiques et normes
- 13.4.2. Plan directeur de la sécurité
- 13.4.3. Tableaux de bord
- 13.4.4. Sensibilisation et formation
- 13.4.5. Sécurité de la chaîne d'approvisionnement

13.5. Opérations de sécurité
- 13.5.1. Gestion des identités et des accès
- 13.5.2. Configuration des règles de sécurité du réseau Firewalls
- 13.5.3. Gestion des plateformes IDS/IPS
- 13.5.4. Analyse des vulnérabilités

13.6. Cadre de cybersécurité. NIST CSF
- 13.6.1. Méthodologie NIST
  - 13.6.1.1. Identifier
  - 13.6.1.2. Protéger
  - 13.6.1.3. Détecter
  - 13.6.1.4. Répondre
  - 13.6.1.5. Récupérer

13.7. Centre des opérations de sécurité (SOC). Fonctions
- 13.7.1. Protection *Red Team, pentesting, threat intelligence*
- 13.7.2. Détection. SIEM, *user behavior analytics, fraud prevention*
- 13.7.3. Réponse

13.8. Audit de sécurité
- 13.8.1. Tests de pénétration
- 13.8.2. Exercices de *red team*
- 13.8.3. Audits du code source. Développement sécurisé
- 13.8.4. Sécurité des composants (*software supply chain*)
- 13.8.5. Analyse médico-légale

13.9. Réponse aux incidents
- 13.9.1. Préparation
- 13.9.2. Détection, analyse et rapport
- 13.9.3. Confinement, éradication et récupération
- 13.9.4. Activité post-incident
  - 13.9.4.1. Conservation des preuves
  - 13.9.4.2. Analyse médico-légale
  - 13.9.4.3. Gestion des écarts
- 13.9.5. Guides officiels de gestion des cyberincidents

13.10. Gestion des vulnérabilités
- 13.10.1. Analyse des vulnérabilités
- 13.10.2. Évaluation de vulnérabilité
- 13.10.3. Base de données système
- 13.10.4. Vulnérabilités au jour 0 Zero-day

Module 14. Analyse des risques et environnement de sécurité IT

14.1. Analyse de l'environnement
- 14.1.1. Analyse de la situation économique
  - 14.1.1.1. Environnement VUCA
    - 14.1.1.1.1. Volatilité
    - 14.1.1.1.2. Incertain
    - 14.1.1.1.3. Complexe
    - 14.1.1.1.4. Ambiguë:

14.1.1.2. Environnement BANI
14.1.1.2.1. Fragile
14.1.1.2.2. Anxieux
14.1.1.2.3. Non linéaire
14.1.1.2.4. Incompréhensible
14.1.2. Analyse de l'environnement général PESTEL
14.1.2.1. Politique
14.1.2.2. Économique
14.1.2.3. Social
14.1.2.4. Technologique
14.1.2.5. Écologique/Environnemental
14.1.2.6. Juridique
14.1.3. Analyse de la situation interne. SWOT
14.1.3.1. Objectifs
14.1.3.2. Menaces
14.1.3.3. Opportunités
14.1.3.4. Points forts
14.2. Risques et incertitudes
14.2.1. Risques
14.2.2. Gestion des risques
14.2.3. Normes de gestion des risques
14.3. Lignes directrices ISO 31.000:2018 relatives au management du risque
14.3.1. Objet
14.3.2. Principes
14.3.3. Cadre de référence
14.3.4. Processus
14.4. Méthodologie d'analyse et de gestion des risques liés aux systèmes d'information (MAGERIT)
14.4.1. Méthodologie MAGERIT
14.4.1.1. Objectifs
14.4.1.2. Méthode
14.4.1.3. Éléments
14.4.1.4. Techniques
14.4.1.5. Outils disponibles (PILAR)
14.5. Transfert du risque cybernétique
14.5.1. Transfert de risque
14.5.2. Les cyber-risques Typologie
14.5.3. Assurance des cyber-risques
14.6. Méthodologies agiles pour la gestion des risques
14.6.1. Méthodologies agiles
14.6.2. Scrum pour la gestion des risques
14.6.3. *Agile risk management*
14.7. Technologies pour la gestion des risques
14.7.1. Intelligence artificielle appliquée à la gestion des risques
14.7.2. *Blockchain* et cryptographie Méthodes de préservation de la valeur
14.7.3. L'informatique quantique Opportunité ou menace
14.8. Cartographie des risques IT basée sur les méthodologies agiles
14.8.1. Représentation de la probabilité et de l'impact dans les environnements agiles
14.8.2. Le risque en tant que menace pour la valeur
14.8.3. Réévolution dans la gestion de projet agile et les processus agiles basés sur les KRIs
14.9. *Risk driven* en matière de gestion des risques
14.9.1. *Risk driven*
14.9.2. *Risk driven* en matière de gestion des risques
14.9.3. Développer un modèle de gestion d'entreprise axé sur le risque
14.10. Innovation et transformation numérique dans la gestion des risques Informatiques
14.10.1. La gestion agile des risques comme source d'innovation commerciale
14.10.2. Transformation des données dans informations utiles à la prise de décision
14.10.3. Vue holistique de l'entreprise à travers le risque

Module 15. Cryptographie dans les IT

15.1. Cryptographie
15.1.1. Cryptographie
15.1.2. Fondements mathématiques
15.2. Cryptologie
15.2.1. Cryptologie
15.2.2. Cryptanalyse
15.2.3. Stéganographie et stégananalyse

15.3. Protocoles cryptographiques
- 15.3.1. Blocs de base
- 15.3.2. Protocoles de base
- 15.3.3. Protocoles intermédiaires
- 15.3.4. Protocoles avancés
- 15.3.5. Protocoles exotériques

15.4. Techniques cryptographiques
- 15.4.1. Longueur de clé
- 15.4.2. Traitement des clés
- 15.4.3. Types d'Algorithmes
- 15.4.4. Fonctions récapitulatives *Hash*
- 15.4.5. Générateurs de nombres pseudo-aléatoires
- 15.4.6. Utilisation d'algorithmes

15.5. Cryptographie symétrique
- 15.5.1. Chiffrement par blocs
- 15.5.2. DES (*Data Encryption Standard*)
- 15.5.3. Algorithme RC4
- 15.5.4. AES (*Advanced Encryption Standard*)
- 15.5.5. Combinaison de chiffrement par blocs
- 15.5.6. Dérivation des clés

15.6. Cryptographie symétrique
- 15.6.1. Diffie-Hellman
- 15.6.2. DSA (*Digital Signature Algorithm*)
- 15.6.3. RSA (*Rivest, Shamir y Adleman*)
- 15.6.4. Courbe elliptique
- 15.6.5. Cryptographie asymétrique Typologie

15.7. Certificats numériques
- 15.7.1. Signature numérique
- 15.7.2. Certificats X509
- 15.7.3. Infrastructure à clé publique(PKI)

15.8. Mise en œuvre
- 15.8.1. Kerberos
- 15.8.2. IBM CCA
- 15.8.3. *Pretty Good Privacy* (PGP)
- 15.8.4. ISO *Authentication Framework*
- 15.8.5. SSL y TLS
- 15.8.6. Cartes à puce dans les moyens de paiement (EMV)
- 15.8.7. Protocoles de téléphonie mobile
- 15.8.8. *Blockchain*

15.9. Stéganographie
- 15.9.1. Stéganographie
- 15.9.2. Stéganalyse
- 15.9.3. Applications et utilisations

15.10. Cryptographie quantique
- 15.10.1. Algorithmes quantiques
- 15.10.2. Protection des algorithmes contre l'informatique quantique
- 15.10.3. Distribution quantique des clés

Module 16. Gestion des identités et des accès dans le cadre de la sécurité Informatique

16.1. Gestion des identités et des accès (IAM)
- 16.1.1. Identité numérique
- 16.1.2. Gestion des identités
- 16.1.3. Fédération d'identité

16.2. Contrôle d'accès physique
- 16.2.1. Systèmes de protection
- 16.2.2. Sécurité des zones
- 16.2.3. Installations de récupération

16.3. Contrôle d'accès logique
- 16.3.1. Authentification Typologie
- 16.3.2. Protocoles d'authentification
- 16.3.3. Attaques d'authentification

16.4. Contrôle d'accès logique Authentification MFA
- 16.4.1. Contrôle d'accès logique Authentification MFA
- 16.4.2. Mots de passe Importance
- 16.4.3. Attaques d'authentification

16.5. Contrôle d'accès logique Authentification biométrique
- 16.5.1. Contrôle d'Aaccès Logique Authentification biométrique
  - 16.5.1.1. Authentification biométrique Exigences
- 16.5.2. Fonctionnement
- 16.5.3. Modèles et techniques

16.6. Systèmes de gestion de l'authentification
- 16.6.1. *Single sign on*
- 16.6.2. Kerberos
- 16.6.3. Systèmes AAA

16.7. Systèmes de gestion de l'authentification: Systèmes AAA
- 16.7.1. TACACS
- 16.7.2. RADIUS
- 16.7.3. DIAMETER

16.8. Services de contrôle d'accès
- 16.8.1. FW - Pare-feu
- 16.8.2. VPN - Réseaux Privés Virtuels
- 16.8.3. IDS - Système de Détection d'Intrusion

16.9. Systèmes de contrôle d'accès au réseau
- 16.9.1. NAC
- 16.9.2. Architecture et éléments
- 16.9.3. Fonctionnement et normalisation

16.10. Accès aux réseaux sans fil
- 16.10.1. Types de réseaux sans fil
- 16.10.2. Sécurité dans les réseaux sans fil
- 16.10.3. Attaques contre les réseaux sans fil

Module 17. Sécurité des communications et du fonctionnement des logiciels

17.1. Sécurité informatique dans les communications et l'exploitation des logiciels
- 17.1.1. Sécurité informatique
- 17.1.2. Cybersécurité
- 17.1.3. Sécurité dans le cloud

17.2. Sécurité informatique dans les communications et l'exploitation des logiciels Typologie
- 17.2.1. Sécurité physique
- 17.2.2. Sécurité logique

17.3. Sécurité des communications
- 17.3.1. Principaux éléments
- 17.3.2. Sécurité des réseaux
- 17.3.3. Meilleures pratiques

17.4. Cyber Intelligence
- 17.4.1. Ingénierie sociale
- 17.4.2. *Deep web*
- 17.4.3. *Phishing*
- 17.4.4. *Malware*

17.5. Développement sécurisé des communications et de l'exploitation des logiciels
- 17.5.1. Développement sécurisé Protocole HTTP
- 17.5.2. Développement sécurisé Cycle de vie
- 17.5.3. Développement sécurisé Sécurité de PHP
- 17.5.4. Développement sécurisé Sécurité de NET
- 17.5.5. Développement sécurisé Meilleures pratiques

17.6. Systèmes de gestion de la sécurité de l'information dans les communications et le fonctionnement des logiciels
- 17.6.1. GDPR
- 17.6.2. ISO 27021
- 17.6.3. ISO 27017/18

17.7. Technologies SIEM
- 17.7.1. Technologies SIEM
- 17.7.2. Opérations SOC
- 17.7.3. SIEM *vendors*

17.8. Le rôle de la sécurité dans les organisations
- 17.8.1. Rôles dans les organisations
- 17.8.2. Rôle des spécialistes de l'IdO dans les entreprises
- 17.8.3. Certifications reconnues sur le marché

17.9. Analyse médico-légale
- 17.9.1. Analyse médico-légale
- 17.9.2. Analyse médico-légale Méthodologie
- 17.9.3. Analyse médico-légale Outils et mise en œuvre

17.10. La cbersécurité aujourd'hui
- 17.10.1. Principales cyberattaques
- 17.10.2. Prévisions en matière d'employabilité
- 17.10.3. Défis

Module 18. Sécurité dans les environnements *cloud*

18.1. La sécurité dans les environnements *cloud computing*
- 18.1.1. La sécurité dans les environnements *cloud computing*
- 18.1.2. Sécurité dans les environnements *cloud computing* Menaces et risques pour la sécurité
- 18.1.3. Sécurité dans les environnements *cloud computing* Aspects clés de la sécurité

18.2. Types d'infrastructures *cloud*
- 18.2.1. Public
- 18.2.2. Privé
- 18.2.3. Hybride

18.3. Modèle de gestion partagé
- 18.3.1. Éléments de sécurité gérés par fournisseur
- 18.3.2. Éléments gérés par le client
- 18.3.3. Définition de la stratégie de sécurité

18.4. Mécanismes de prévention
- 18.4.1. Systèmes de gestion de l'authentification
- 18.4.2. Système de gestion des autorisations Politiques d'accès
- 18.4.3. Systèmes de gestion des clés

18.5. Sécurisation des systèmes
- 18.5.1. Sécurisation des systèmes de stockage
- 18.5.2. Protection de systèmes de bases de données
- 18.5.3. Sécurisation des données en transit

18.6. Protection de l'infrastructure
- 18.6.1. Conception et mise en œuvre d'un réseau sécurisé
- 18.6.2. Sécurité des ressources informatiques
- 18.6.3. Outils et ressources pour la protection des infrastructures

18.7. Détection des menaces et des attaques
- 18.7.1. Systèmes d'audit, *logging* et de surveillance
- 18.7.2. Systèmes d'événements et d'alarmes
- 18.7.3. Systèmes SIEM

18.8. Réponse aux incidents
- 18.8.1. Plan de réponse aux incidents
- 18.8.2. Continuité des activités
- 18.8.3. Analyse médico-légale et remédiation d'incidents de même nature

18.9. Sécurité dans les *clouds* publics
- 18.9.1. AWS (Amazon Web Services)
- 18.9.2. Microsoft Azure
- 18.9.3. Google GCP
- 18.9.4. Oracle Cloud

18.10. Réglementation et conformité
- 18.10.1. Respect des règles de sécurité
- 18.10.2. Gestion des risques
- 18.10.3. Les personnes et les processus dans les organisations

Module 19. Sécurité des communications des dispositifs IoT

19.1. De la télémétrie à IoT
- 19.1.1. La télémétrie
- 19.1.2. Connectivité M2M
- 19.1.3. Démocratisation de la télémétrie

19.2. Modèles de référence IoT
- 19.2.1. Modèle de référence IoT
- 19.2.2. Architecture simplifiée IoT

19.3. Vulnérabilités de la sécurité IoT
- 19.3.1. Dispositifs IoT
- 19.3.2. Dispositifs IoT. Études de cas d'utilisation
- 19.3.3. Dispositifs IoT. Vulnérabilités

19.4. Connectivité IoT
- 19.4.1. Réseaux PAN, LAN, WAN
- 19.4.2. Technologies sans fil non liées à IoT
- 19.4.3. Technologies sans fil LPWAN

19.5. Technologies LPWAN
- 19.5.1. Le triangle de fer des LPWAN
- 19.5.2. Bandes de fréquences libres vs. Bandes sous licence
- 19.5.3. Options technologiques LPWAN

19.6. Technologie LoRaWAN
- 19.6.1. Technologie LoRaWAN
- 19.6.2. Cas d'utilisation LoRaWAN Éco-système
- 19.6.3. Sécurité dans LoRaWAN

19.7. Technologie Sigfox
- 19.7.1. Technologie Sigfox
- 19.7.2. Cas d'utilisation de Sigfox Éco-système
- 19.7.3. La sécurité dans Sigfox

19.8. Technologie Cellulaire IoT
- 19.8.1. Technologie Cellulaire IoT (NB-IoT et LTE-M)
- 19.8.2. Cas d'utilisation Cellulaire IoT Éco-système
- 19.8.3. Sécurité en Cellulaire IoT

19.9. Technologie WiSUN
- 19.9.1. Technologie WiSUN
- 19.9.2. Cas d'utilisation de WiSUN Éco-système
- 19.9.3. Sécurité du WiSUN

19.10. Autres technologies IoT
- 19.10.1. Autres technologies IoT
- 19.10.2. Cas d'utilisation et écosystème des autres technologies IoT
- 19.10.3. Sécurité dans les autres technologies IoT

Module 20. Plan de continuité des activités associé à la sécurité

20.1. Plan de continuité des activités
- 20.1.1. Les plans de continuité d'activité (PCA)
- 20.1.2. Plan de continuité des activités (PCA) Aspects clés
- 20.1.3. Plan de continuité des activités (PCA) pour l'évaluation de l'entreprise

20.2. Mesures dans un plan de continuité d'activité (PCA)
- 20.2.1. *Recovery time objective* (RTO) et *recovery point objective* (RPO)
- 20.2.2. Délai maximum tolérable (MTD)
- 20.2.3. Niveaux minimaux de récupération (ROL)
- 20.2.4. Objectif de point de récupération (RPO)

20.3. Projets de continuité Typologie
- 20.3.1. Plan de continuité des activités (PCA)
- 20.3.2. Plan de continuité des TIC (PCTIC)
- 20.3.3. Plan de reprise après sinistre (PRS)

20.4. Gestion des risques associés au PCA
- 20.4.1. Analyse de l'impact sur les activités
- 20.4.2. Avantages de la mise en œuvre d'un PCA
- 20.4.3. Réflexion basée sur les risques

20.5. Cycle de vie d'un plan de continuité des activités
- 20.5.1. Phase 1: Analyse de l'organisation
- 20.5.2. Phase 2: détermination de la stratégie de continuité
- 20.5.3. Phase 3: réponse à l'urgence
- 20.5.4. Phase 4: essais, maintenance et révision

20.6. Phase d'analyse organisationnelle d'un PCA
- 20.6.1. Identification des processus entrant dans le champ d'application du PCA
- 20.6.2. Identification des domaines d'activité critiques
- 20.6.3. Identification des dépendances entre les domaines et les processus
- 20.6.4. Détermination des MTD appropriées
- 20.6.5. Produits livrables Création d'un plan

20.7. Phase de détermination de la stratégie de continuité dans un PCA
- 20.7.1. Rôles dans la phase de détermination de la stratégie
- 20.7.2. Tâches dans la phase de définition de la stratégie
- 20.7.3. Produits livrables

20.8. Phase d'intervention d'urgence d'un PCA
- 20.8.1. Rôles dans la phase de réponse
- 20.8.2. Tâches au cours de cette phase
- 20.8.3. Produits livrables

20.9. Phase de test, de maintenance et de révision d'un PCA
- 20.9.1. Rôles dans la phase de test, de maintenance et de révision
- 20.9.2. Tâches de la phase de test, de maintenance et de révision
- 20.9.3. Produits livrables

20.10. Normes ISO associées aux plans de continuité d'activité (PCA)
- 20.10.1. ISO 22301:2019
- 20.10.2. ISO 22313:2020
- 20.10.3. Autres normes ISO et internationales connexes

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

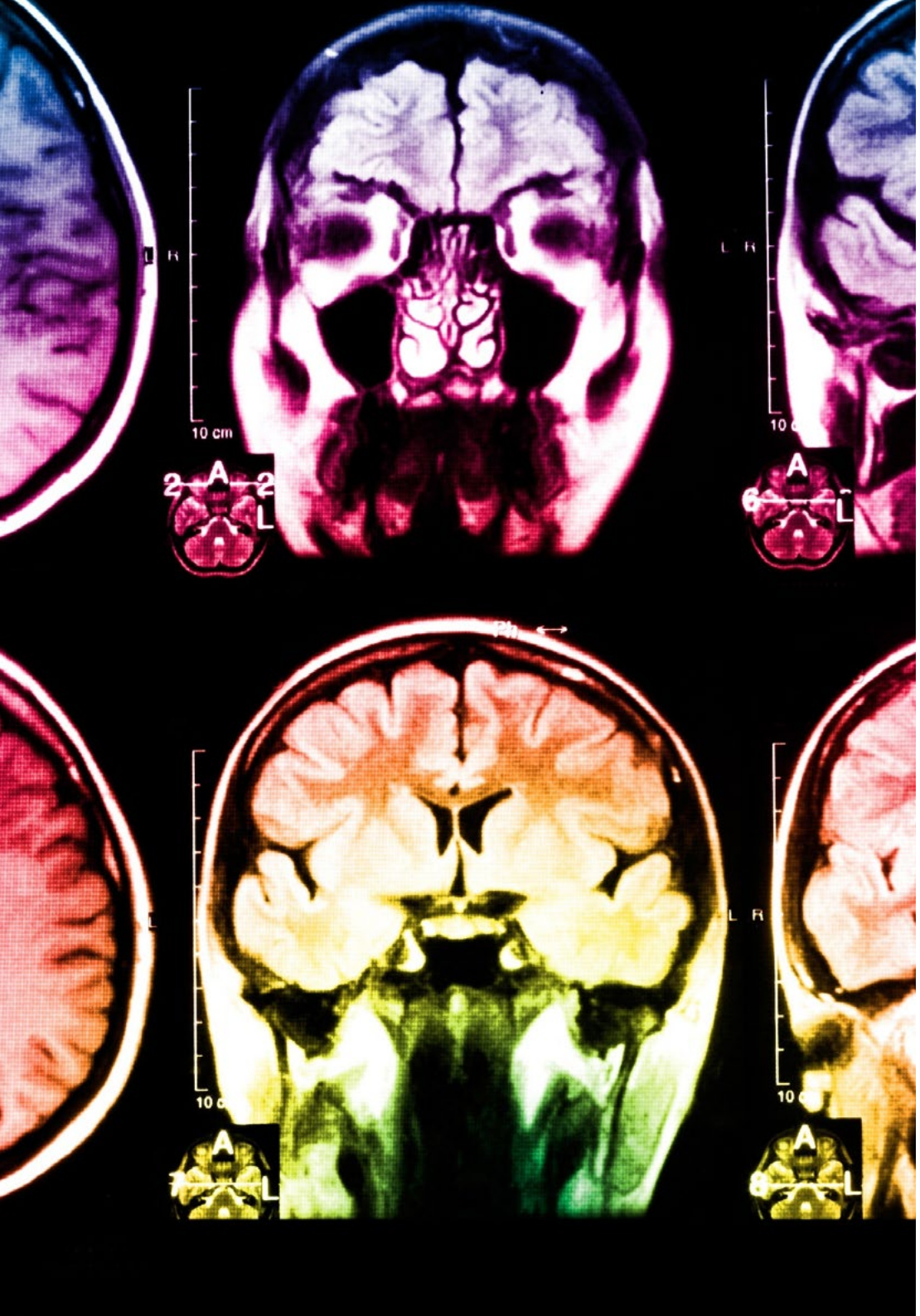
TECH combine efficacement la méthodologie des Études de Cas avec un système d'apprentissage 100% en ligne basé sur la répétition, qui associe différents éléments didactiques dans chaque leçon.

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.

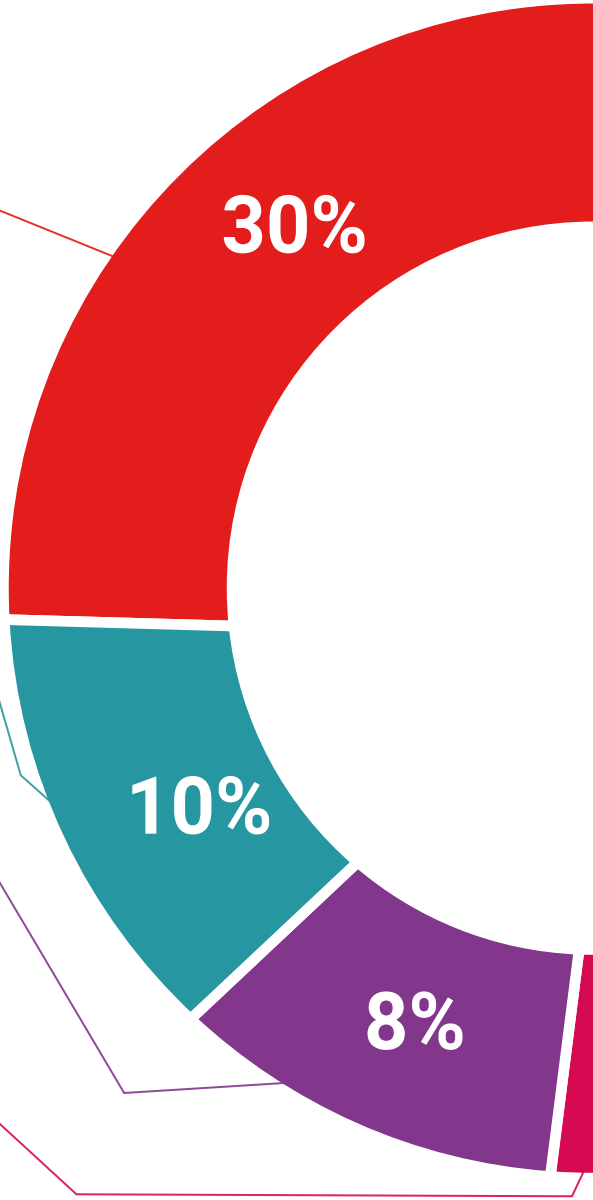
La méthode "Learning from an Expert" renforce les connaissances et la mémoire, et donne confiance dans les futures décisions difficiles.

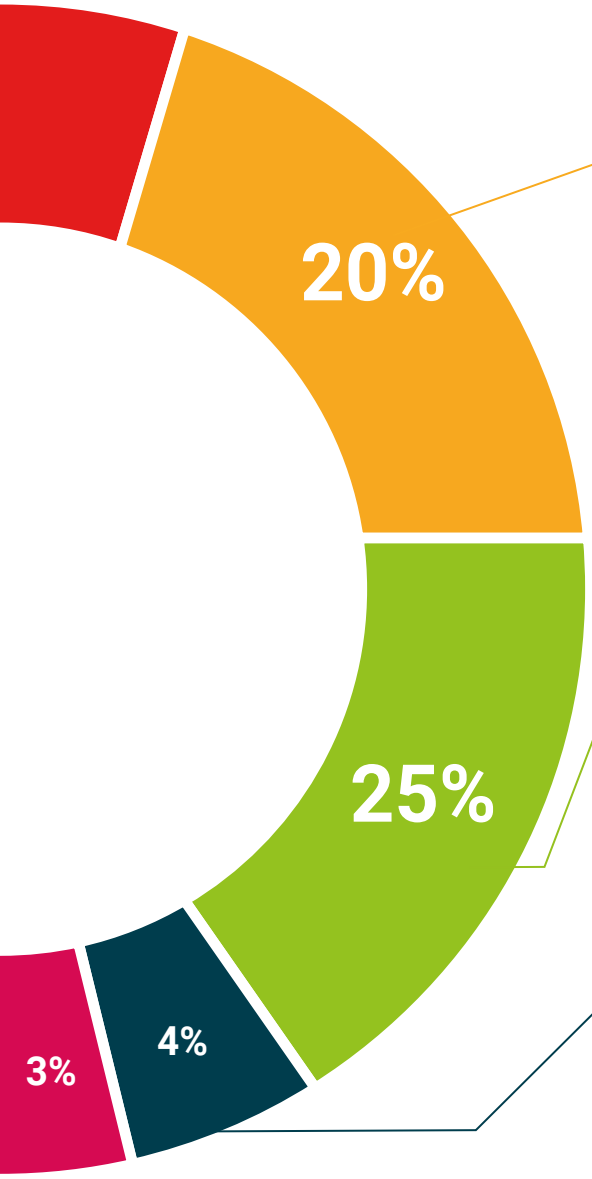
Pratiques en compétences et aptitudes

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 Avancé en Haute Direction en Cybersécurité vous garantit, en plus de la formation la plus rigoureuse et la plus actuelle, l'accès à un diplôme universitaire de Mastère Avancé délivré par TECH Université Technologique.

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

Ce **Mastère Avancé en Haute Direction en Cybersécurité** contient le programme le plus complet et le plus à jour du marché.

Après avoir réussi l'évaluation, l'étudiant recevra par courrier postal* avec accusé de réception son correspondant diplôme de **Mastère Avancé** délivré par **TECH Université Technologique.**

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

Diplôme: **Mastère Avancé en Haute Direction en Cybersécurité**

Nº d'heures officielles: **3.000h.**

tech université technologique

Délivre le présent

DIPLÔME

à

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

Pour avoir finalisé et accrédité avec succès le programme de

MASTÈRE AVANCÉ

Haute Direction en Cybersécurité

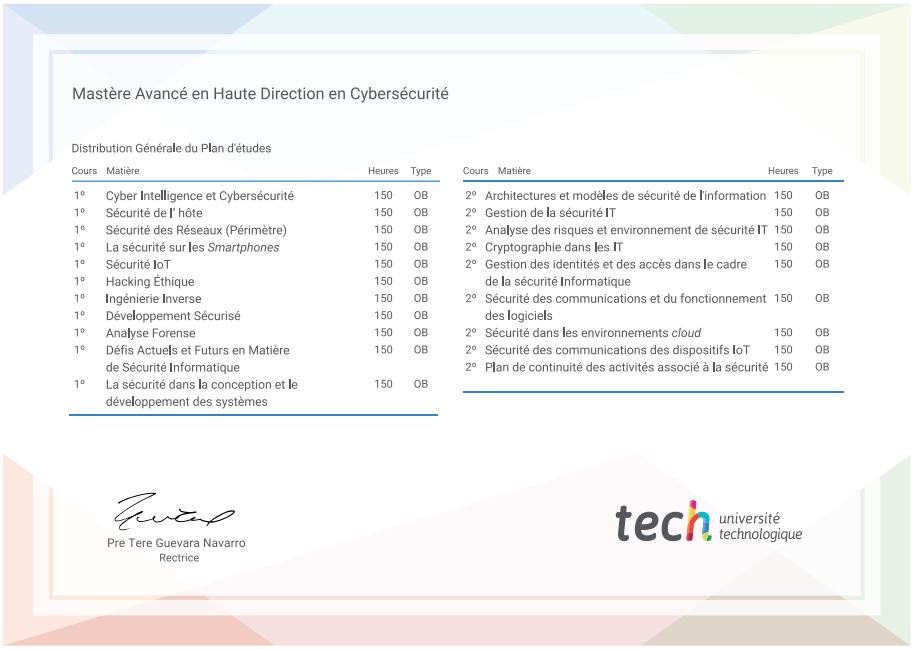
Il s'agit d'un diplôme spécialisé octroyé par cette Université d'une durée de 3.000 heures, débutant le dd/mm/aaaa et finalisant le dd/mm/aaaa.

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

Ce diplôme doit être impérativement accompagné d'un diplôme universitaire reconnu par les autorités compétentes pour exercer la profession dans chaque pays. Code Unique TECH: AFWOR23S techtitute.com/diplômes



Mastère Avancé en Haute Direction en Cybersécurité

Distribution Générale du Plan d'études

Cours	Matière	Heures	Type
1º	Cyber Intelligence et Cybersécurité	150	OB
1º	Sécurité de l' hôte	150	OB
1º	Sécurité des Réseaux (Périmètre)	150	OB
1º	La sécurité sur les *Smartphones*	150	OB
1º	Sécurité IoT	150	OB
1º	Hacking Éthique	150	OB
1º	Ingénierie Inverse	150	OB
1º	Développement Sécurisé	150	OB
1º	Analyse Forense	150	OB
1º	Défis Actuels et Futurs en Matière de Sécurité Informatique	150	OB
1º	La sécurité dans la conception et le développement des systèmes	150	OB
2º	Architectures et modèles de sécurité de l'information	150	OB
2º	Gestion de la sécurité IT	150	OB
2º	Analyse des risques et environnement de sécurité IT	150	OB
2º	Cryptographie dans les IT	150	OB
2º	Gestion des identités et des accès dans le cadre de la sécurité Informatique	150	OB
2º	Sécurité des communications et du fonctionnement des logiciels	150	OB
2º	Sécurité dans les environnements *cloud*	150	OB
2º	Sécurité des communications des dispositifs IoT	150	OB
2º	Plan de continuité des activités associé à la sécurité	150	OB

Pre Tere Guevara Navarro
Rectrice

tech université technologique

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

tech université technologique

Mastère Avancé
Haute Direction en Cybersécurité

- Modalité: **en ligne**
- Durée: **2 ans**
- Quali ication: **TECH Université Technologique**
- Horaire: **à votre rythme**
- Examens: **en ligne**

Mastère Avancé

Haute Direction en Cybersécurité

tech université technologique