Mastère Spécialisé Avancé

Haute Direction en Cybersécurité (CISO, Chief Information Security Officer)

tech Euromed University

tech Euromed University

Mastère Spécialisé Avancé
Haute Direction en Cybersécurité (CISO, Chief Information Security Officer)

- Modalité: **en ligne**
- Durée: **2 ans**
- Qualification: **TECH Euromed University**
- Accréditation: **120 ECTS**
- Horaire: **à votre rythme**
- Examens: **en ligne**

Accès au site web: www.techtitute.com/fr/informatique/mastere-specialise-avance/mastere-specialise-avance-haute-direction-cybersecurite-ciso-chief-information-security-officer

Sommaire

01

Présentation

Aujourd'hui, la cybersécurité est devenue un pilier fondamental pour protéger les individus et les entreprises contre le nombre croissant de menaces numériques. Cette discipline se concentre non seulement sur la sauvegarde des systèmes technologiques et des informations critiques des organisations, mais aussi sur la planification, la mise en œuvre et la supervision des stratégies de sécurité. Son principal objectif est donc d'atténuer les risques et de réagir efficacement aux cyberattaques et aux incidents. Parmi les principales responsabilités d'un Directeur de la Cybersécurité figurent la conception des politiques de sécurité, la gestion des risques technologiques et la direction d'équipes spécialisées. Face aux défis posés par le progrès technologique et la numérisation, ce programme a été spécialement conçu pour répondre à ces questions. TECH Euromed University se concentre non seulement sur la garantie de l'efficacité de la protection de l'information, mais aussi sur l'identification et la gestion des nouvelles vulnérabilités. Cela positionne le CISO comme l'élément le plus important pour la résilience de toute organisation.

Avec TECH Euromed University, spécialisez-vous et devenez un leader dans l'un des domaines les plus importants de l'informatique”

La Haute Direction en Cybersécurité a contribué à assurer la stabilité et la continuité des organisations dans un monde numérisé et hautement interconnecté. La mise en œuvre de stratégies de sécurité solides et l'adoption de technologies de pointe ont permis d'atténuer les risques et de prévenir des attaques catastrophiques. Dans les secteurs critiques tels que la banque, les soins de santé et les infrastructures publiques, la sécurité a été renforcée par la gouvernance et la conformité, sous l'impulsion de dirigeants spécialisés dans ce domaine.

Cette discipline a permis aux organisations de créer des environnements de travail numériques plus sûrs, renforçant ainsi la confiance des clients, des partenaires et des utilisateurs. Les résultats positifs ont permis d'économiser des millions de dollars en pertes économiques potentielles, tout en favorisant une culture organisationnelle dans laquelle la sécurité est une priorité partagée. En outre, il s'est avéré essentiel de protéger l'innovation, la réputation et la durabilité des organisations dans un paysage en constante évolution.

Le Mastère Spécialisé Avancé de TECH Euromed University est conçu pour spécialiser les professionnels dans la conduite de stratégies de sécurité efficaces. Tout au long du programme, les étudiants apprendront à leur propre rythme, en se concentrant sur le développement de compétences en gestion et d'un sens aigu des affaires stratégiques. En outre, ils auront accès à une spécialisation de pointe qui les préparera à exceller dans une carrière très demandée sur le marché mondial. Grâce à son format 100 % en ligne, les participants pourront combiner leurs études avec leurs responsabilités professionnelles, ce qui leur permettra de progresser sans compromettre leur activité professionnelle.

Ce **Mastère Spécialisé Avancé en Haute Direction en Cybersécurité (CISO, Chief Information Security Officer)** contient le programme le plus complet et le plus actualisé du marché. Ses caractéristiques sont les suivantes:

- Le développement d'études de cas présentées par des experts en informatique
- Le contenu graphique, schématique et éminemment pratique du programme fournit des informations scientifiques et pratiques sur les disciplines essentielles à la pratique professionnelle
- Les exercices pratiques où effectuer le processus d'auto-évaluation pour améliorer l'apprentissage
- Il met l'accent sur les méthodologies innovantes dans le domaine de la Haute Direction en Cybersécurité (CISO, Chief Information Security Officer)
- Cours théoriques, questions à l'expert, forums de discussion sur des sujets controversés et travail de réflexion individuel
- La possibilité d'accéder aux contenus depuis n'importe quel appareil fixe ou portable doté d'une connexion internet

Ce Mastère Spécialisé Avancé vous place à l'avant-garde de l'industrie et vous ouvre des perspectives de carrière infinies"

Développez les compétences dont vous avez besoin pour relever les défis de l'avenir sans négliger vos activités actuelles"

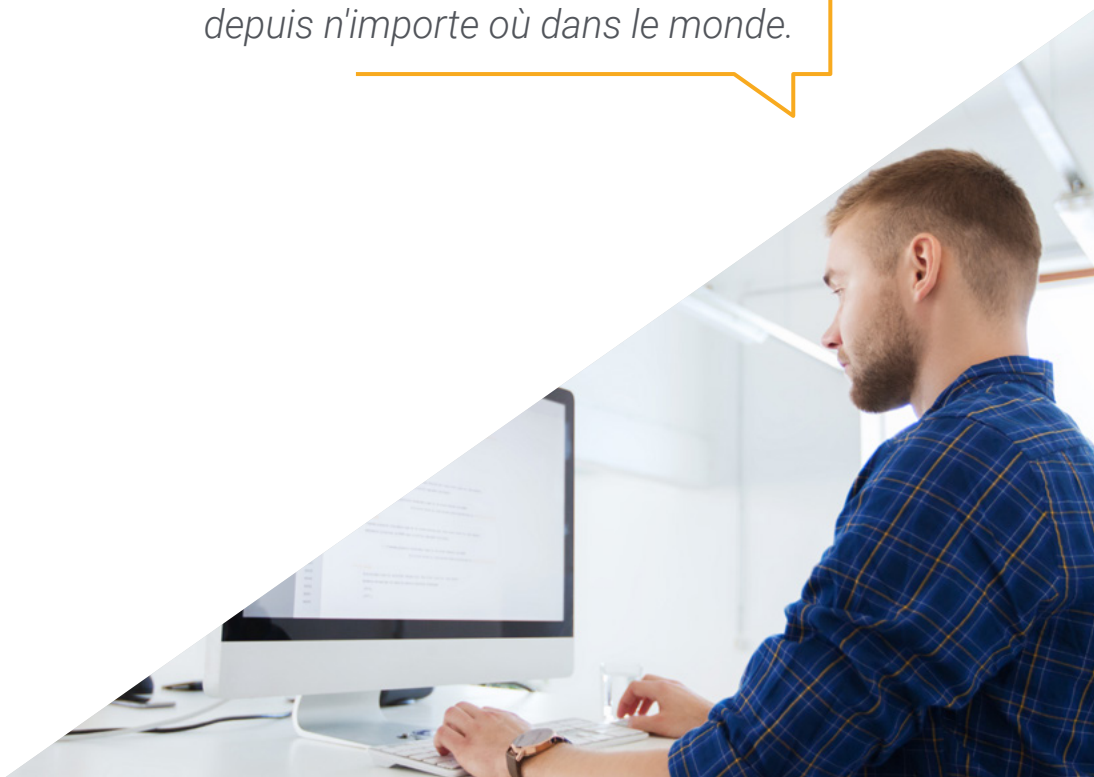
Devenez le protecteur des infrastructures technologiques grâce à la méthode Relearning qui s'adapte à votre rythme d'apprentissage.

Faites partie de la plus grande université numérique du monde et spécialisez-vous depuis n'importe où dans le monde.

Son corps enseignant comprend des professionnels de l'informatique, qui apportent l'expérience de leur travail 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 programme académique. Pour ce faire, le professionnel aura l'aide d'un système vidéo interactif innovant créé par des experts reconnus.



02

Pourquoi étudier à TECH?

TECH Euromed University est la plus grande Université Numérique du monde. Avec un catalogue impressionnant de plus de 14 000 programmes universitaires, disponibles en 11 langues, elle est leader en matière d'employabilité, avec un taux de placement de 99 %. Elle dispose également d'un vaste corps professoral composé de plus de 6 000 professeurs de renommée internationale.

Étudiez dans la plus grande université numérique du monde et assurez votre réussite professionnelle. L'avenir commence chez TECH Euromed University"

La meilleure université en ligne selon FORBES

Le prestigieux magazine Forbes, spécialisé dans les affaires et la finance, a désigné TECH Euromed University comme « la meilleure université en ligne du monde ». C'est ce qu'il a récemment déclaré dans un long article de son édition numérique dans lequel il se fait l'écho de la success story de cette institution, "grâce à l'offre académique qu'elle propose, à la sélection de son corps enseignant et à une méthode d'apprentissage innovante visant à former les professionnels du futur".

Un corps professoral international de premier plan

Le corps enseignant de TECH Euromed University est composé de plus de 6 000 professeurs jouissant du plus grand prestige international. Des professeurs, des chercheurs et des cadres supérieurs de multinationales, dont Isaiah Covington, entraîneur de performance des Boston Celtics, Magda Romanska, chercheuse principale au MetaLAB de Harvard, Ignacio Wistumba, président du département de pathologie moléculaire translationnelle au MD Anderson Cancer Center, et D.W. Pine, directeur de la création du magazine TIME, entre autres.

La plus grande université numérique du monde

TECH Euromed University est la plus grande université numérique du monde. Nous sommes le plus grand établissement d'enseignement, avec le meilleur et le plus vaste catalogue d'enseignement numérique, cent pour cent en ligne et couvrant la grande majorité des domaines de la connaissance. Nous proposons le plus grand nombre de diplômes propres, de diplômes officiels de troisième cycle et de premier cycle au monde. Au total, plus de 14 000 diplômes universitaires, dans dix langues différentes, ce qui fait de nous la plus grande institution éducative au monde.

Les programmes d'études les plus complets sur la scène universitaire

TECH Euromed University propose les programmes d'études les plus complets sur la scène universitaire, avec des cursus qui couvrent les concepts fondamentaux et, en même temps, les principales avancées scientifiques dans leurs domaines scientifiques spécifiques. De même, ces programmes sont continuellement mis à jour afin de garantir aux étudiants l'avant-garde académique et les compétences professionnelles les plus demandées. De cette manière, les diplômes de l'université fournissent à ses diplômés un avantage significatif pour propulser leur carrière vers le succès.

Une méthode d'apprentissage unique

TECH Euromed University est la première université à utiliser *Relearning* dans tous ses diplômes. Il s'agit de la meilleure méthode d'apprentissage en ligne, accréditée par des certifications internationales de qualité de l'enseignement délivrées par des agences éducatives prestigieuses. En outre, ce modèle académique perturbateur est complété par la "Méthode des Cas", configurant ainsi une stratégie d'enseignement en ligne unique. Des ressources pédagogiques innovantes sont également mises en œuvre, notamment des vidéos détaillées, des infographies et des résumés interactifs.

L'université en ligne officielle de la NBA

TECH Euromed University est l'université en ligne officielle de la NBA. Grâce à un accord avec la ligue majeure de basket-ball, elle offre à ses étudiants des programmes universitaires exclusifs, ainsi qu'une grande variété de ressources éducatives axées sur les affaires de la ligue et d'autres domaines de l'industrie du sport. Chaque programme est conçu de manière unique et fait appel à des conférenciers exceptionnels: des professionnels issus du monde du sport qui apportent leur expertise sur les sujets les plus pertinents.

Leaders en matière d'employabilité

TECH Euromed University a réussi à devenir la première université en termes d'employabilité. 99 % de ses étudiants trouvent un emploi dans le domaine académique qu'ils ont étudié, un an après avoir terminé l'un des programmes de l'université. Un nombre similaire d'entre eux bénéficient d'une amélioration immédiate de leur carrière. Tout cela grâce à une méthodologie d'étude qui fonde son efficacité sur l'acquisition de compétences pratiques, absolument nécessaires au développement professionnel.

Google Partner Premier

Le géant américain de la technologie a décerné à TECH Euromed University le badge Google Partner Premier. Ce prix, qui n'est décerné qu'à 3 % des entreprises dans le monde, souligne l'expérience efficace, flexible et adaptée que cette université offre aux étudiants. Cette reconnaissance atteste non seulement de la rigueur, de la performance et de l'investissement maximaux dans les infrastructures numériques de TECH Euromed University, mais place également cette université parmi les entreprises technologiques les plus avant-gardistes au monde.

L'université la mieux évaluée par ses étudiants

Les étudiants ont positionné TECH Euromed University comme l'université la mieux évaluée du monde dans les principaux portails d'opinion, soulignant sa note la plus élevée de 4,9 sur 5, obtenue à partir de plus de 1 000 évaluations. Ces résultats consolident TECH Euromed University en tant qu'institution universitaire de référence internationale, reflétant l'excellence et l'impact positif de son modèle éducatif.

03

Programme d'études

Le Mastère Spécialisé Avancé en Haute Direction en Cybersécurité (CISO) est conçu pour former des leaders stratégiques capables de gérer la sécurité de l'information dans les organisations mondiales. Grâce à une approche complète et actualisée, le programme couvre des domaines clés tels que la gouvernance de la cybersécurité et la gestion des risques. Ce faisant, les étudiants développeront des compétences managériales pour diriger des équipes performantes et mettre en œuvre des politiques de sécurité. En outre, tout en acquérant une connaissance des dernières tendances et des technologies émergentes, les diplômés apprendront à relever les défis de l'environnement numérique et à mener la sécurité vers l'avenir.

TECH Euromed University vous prépare à devenir le stratège qui prévient, détecte et atténue les Cybermenaces dans l'environnement commercial mondial"

Module 1. Cyber intelligence et cybersécurité

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

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

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

1.7. Menaces et types de sécurité
- 1.7.1. Types de menaces
- 1.7.2. Sécurité physique
- 1.7.3. Sécurité en 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 *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. les vulnérabilités
1.9.5. Évaluation des risques
1.9.6. Traitement du risque
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 de 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 VPC en Cloud
  - 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 du *malware* et des IOCs
- 3.6.2. Problèmes de moteur antivirus

3.7. Systèmes de protection du courrier
- 3.7.1. Antispam
  - 3.7.1.1. Liste blanche et liste noire
  - 3.7.1.2. Filtres bayésiens
- 3.7.2. Mail Gateway (MGW)

3.8. SIEM
- 3.8.1. Composants et architecture
- 3.8.2. Règles de corrélation et cas d'utilisation
- 3.8.3. Les défis actuels des systèmes SIEM

3.9. SOAR
- 3.9.1. SOAR et SIEM: ennemis ou alliés
- 3.9.2. L'avenir des systèmes SOAR

3.10. Autres systèmes en réseau
- 3.10.1. WAF
- 3.10.2. NAC
- 3.10.3. HoneyPots y HoneyNets
- 3.10.4. CASB

Module 4. La sécurité sur les smartphones

4.1. Le monde de l'appareil mobile
- 4.1.1. Types de plateformes mobiles
- 4.1.2. Dispositifs Ios
- 4.1.3. Dispositifs Android

4.2. Gestion de la sécurité mobile
- 4.2.1. Projet de sécurité mobile de l'OWASP
  - 4.2.1.1. Les 10 principales vulnérabilités
- 4.2.2. Communications, réseaux et modes de connexion

4.3. Le dispositif mobile dans l'environnement professionnel
- 4.3.1. Risques
- 4.3.2. Politiques de sécurité
- 4.3.3. Surveillance des dispositifs
- 4.3.4. Gestion des dispositifs mobiles (MDM)

4.4. Vie privée des utilisateurs et sécurité des données
- 4.4.1. États d'information
- 4.4.2. Protection des données et confidentialité
  - 4.4.2.1. Permissions
  - 4.4.2.2. Cryptage
- 4.4.3. Stockage sécurisé des données
  - 4.4.3.1. Stockage sécurisé sur iOS
  - 4.4.3.2. Stockage sécurisé sur Android
- 4.4.4. Bonnes pratiques en matière de développement d'applications

4.5. Vulnérabilités et vecteurs d'attaque
- 4.5.1. Vulnérabilités
- 4.5.2. Vecteurs d'attaque
  - 4.5.2.1. Malware
  - 4.5.2.2. Exfiltration de données
  - 4.5.2.3. Manipulation des données

4.6. Principales menaces
- 4.6.1. Utilisateur non 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 *dispositifs* iOS: mécanismes et outils
- 4.8.4. Hacking des *appareils* Android: mécanismes et outils

4.9. Tests de pénétration
- 4.9.1. iOS *PenTesting*
- 4.9.2. Android *PenTesting*
- 4.9.3. Outils

4.10. Sûreté et sécurité
- 4.10.1. Paramètres de sécurité
  - 4.10.1.1. Sur les appareils iOS
  - 4.10.1.2. Sur les appareils 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. Piratage éthique

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

6.2. 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 d' *exploits* connus
- 6.9.2. Utilisation des *metasploit*
- 6.9.3. Utilisation des *Malware*
  - 6.9.3.1. Définition et champ d'application
  - 6.9.3.2. Génération de *malware*
  - 6.9.3.3. Bypass des solutions anti-virus

6.10. Persistance
- 6.10.1. Installation de *rootkits*
- 6.10.2. Utilisation de ncat
- 6.10.3. Utilisation de tâches planifiées pour les backdoors
- 6.10.4. Création d'utilisateurs
- 6.10.5. Détection HIDS

Module 7. Ingénierie inverse

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

7.2. Types d'analyse de compilateur
- 7.2.1. Analyse lexicale
  - 7.2.1.1. Terminologie
  - 7.2.1.2. Composante lexicale
  - 7.2.1.3. Analyseur Lexical LEX
- 7.2.2. Analyse syntaxique
  - 7.2.2.1. Grammaires sans contexte
  - 7.2.2.2. Types d'analyse syntaxique
    - 7.2.2.2.1. Analyse syntaxique descendante
    - 7.2.2.2.2. Analyse ascendante
  - 7.2.2.3. Arbres syntaxiques et dérivations

7.2.2.4. Types d'analyseurs syntaxiques
7.2.2.4.1. Analyseurs LR(*Left To Right*)
7.2.2.4.2. 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 d'un *sandbox*
7.9.2. Évasion d'un *sandbox*
7.9.3. Techniques de détection
7.9.4. Techniques d'évasion
7.9.5. Contre-mesures
7.9.6. Sandbox sur Linux
7.9.7. Sandbox sur Windows
7.9.8. Sandbox sur MacOS
7.9.9. Sandbox sur Android
7.10. Analyse des *malware*
7.10.1. Méthodes d'analyse des *malware*
7.10.2. Techniques d'obscurcissement des *malware*
7.10.2.1. Obfuscation des exécutables
7.10.2.2. Restriction des environnements d'exécution
7.10.3. Outils d'analyse des *malware*

Module 8. Développement 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 de *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. Implémentation des politiques de sécurité de software et hardware

9.1. Implémentation des politiques de sécurité de software et hardware
- 9.1.1. Implémentation de l'identification et de l'autorisation
- 9.1.2. Implémentation des techniques d'identification
- 9.1.3. Mesures techniques d'autorisation

9.2. Technologies d'identification et d'autorisation
- 9.2.1. Identificateur et OTP
- 9.2.2. Clé USB ou carte à puce PKI
- 9.2.3. La touche "Confidentiel Défense"
- 9.2.4. Le RFID Actif

9.3. Politiques de sécurité d'accès aux logiciels et aux systèmes
- 9.3.1. Implémentation des politiques de contrôle d'accès
- 9.3.2. Implémentation des politiques d'accès aux communications
- 9.3.3. Types d'outils de sécurité pour le contrôle d'accès

9.4. Gestion des accès des utilisateurs
- 9.4.1. Gestion des droits d'accès
- 9.4.2. Séparation des rôles et des fonctions d'accès
- 9.4.3. Mise en œuvre des droits d'accès dans les systèmes

9.5. Contrôle d'accès aux systèmes et applications
- 9.5.1. Règlementation d'accès minimal
- 9.5.2. Technologies de connexion sécurisée
- 9.5.3. Politiques de sécurité des mots de passe

9.6. Technologies des systèmes d'identification
- 9.6.1. Active Directory
- 9.6.2. OTP
- 9.6.3. PAP, CHAP
- 9.6.4. KERBEROS, DIAMETER, NTLM

9.7. Contrôles CIS pour la base des systèmes
- 9.7.1. Contrôles CIS de base
- 9.7.2. Contrôles CIS fondamentaux
- 9.7.3. Contrôles CIS organisationnels

9.8. Sécurité opérationnelle
- 9.8.1. Protection contre les codes malveillants
- 9.8.2. Copies de sauvegarde
- 9.8.3. Enregistrement des activités et suivi

9.9. Gestion des vulnérabilités techniques
- 9.9.1. Vulnérabilités techniques
- 9.9.2. Gestion des vulnérabilités techniques
- 9.9.3. Restrictions relatives dans l'installation du software

9.10. Mise en œuvre des pratiques de la politique de sécurité
- 9.10.1. Vulnérabilités logiques
- 9.10.2. Implémentation des politiques de défense

Module 10. Analyse médico-légale

10.1. Acquisition et réplication des données
- 10.1.1. Acquisition de données volatiles
  - 10.1.1.1. Informations sur le système
  - 10.1.1.2. Informations sur le réseau
  - 10.1.1.3. Ordre de volatilité
- 10.1.2. Acquisition de données statiques
  - 10.1.2.1. Création d'une image dupliquée
  - 10.1.2.2. Préparation d'un document de chaîne de contrôle

10.1.3. Méthodes de validation des données acquises
10.1.3.1. Méthodes pour Linux
10.1.3.2. Méthodes pour Windows
10.2. Évaluation et défaite des techniques anti-forensic
10.2.1. Objectifs des techniques médico-légales
10.2.2. Effacement des données
10.2.2.1. Effacement des données et des fichiers
10.2.2.2. Récupération de fichiers
10.2.2.3. Récupération de partitions supprimées
10.2.3. Protection par mot de passe
10.2.4. Stéganographie
10.2.5. Effacement sécurisé des dispositifs
10.2.6. Cryptage
10.3. Analyse judiciaire des systèmes d'exploitation
10.3.1. Analyse légale de Windows
10.3.2. Analyse légale de Linux
10.3.3. Analyse légale de Mac
10.4. Analyse judiciaire des réseaux
10.4.1. Analyse des logs
10.4.2. Corrélation des données
10.4.3. Enquête sur le réseau
10.4.4. Étapes à suivre pour l'analyse criminelle du réseau
10.5. Analyse légale Web
10.5.1. Enquête sur les attaques sur Internet
10.5.2. Détection des attaques
10.5.3. Localisation de l'adresse IP
10.6. Police scientifique des bases de données
10.6.1. Analyse légale de MSSQL
10.6.2. Analyse légale de MySQL
10.6.3. Analyse légale de PostgreSQL
10.6.4. Analyse légale de MongoDB
10.7. Analyse légale en Cloud
10.7.1. Types de délits en Cloud
10.7.1.1. Le Cloud comme sujet
10.7.1.2. Le cloud comme objet
10.7.1.3. Le cloud comme outil
10.7.2. Les défis légaux du Cloud
10.7.3. Recherche sur les services de stockage en Cloud
10.7.4. Outils d'analyse forensique pour Cloud
10.8. Enquêtes sur les crimes par courriel
10.8.1. Systèmes de courrier
10.8.1.1. Clients de messagerie
10.8.1.2. Serveur de messagerie
10.8.1.3. Serveur SMTP
10.8.1.4. Serveur POP3
10.8.1.5. Serveur IMAP4
10.8.2. Délits de courrier
10.8.3. Message de courrier
10.8.3.1. En-têtes standard
10.8.3.2. En-têtes étendus
10.8.4. Étapes de l'enquête sur ces crimes
10.8.5. Outils d'analyse des e-mails
10.9. Analyse légale des mobiles
10.9.1. Réseaux cellulaires
10.9.1.1. Types de réseaux
10.9.1.2. Contenu du CDR
10.9.2. *Subscriber Identity Module* (SIM)
10.9.3. Acquisition logique
10.9.4. Acquisition physique
10.9.5. Acquisition du système de fichiers
10.10. Rédaction et soumission de rapports légaux
10.10.1. Aspects importants d'un rapport légal
10.10.2. Classification et types de rapports
10.10.3. Guide pour la rédaction d'un rapport
10.10.4. Présentation du rapport
10.10.4.1. Préparation préalable au témoignage
10.10.4.2. Dépôt
10.10.4.3. Traiter avec les médias

Module 11. Sécurité dans la conception et la développement de systèmes

11.1. Systèmes d'information
- 11.1.1. Domaines des systèmes 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. Commerciaux
  - 11.2.1.2. Stratégiques
  - 11.2.1.3. Selon le domaine d'application
  - 11.2.1.4. Spécifiques
- 11.2.2. Systèmes d'information Exemples concrets
- 11.2.3. Évolution des systèmes d'information: Phases
- 11.2.4. Méthodologie 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: Délits
- 11.3.4. Procédures d'entretien d'un système 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. Intégration
  - 11.4.1.2. Confidencialité
  - 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. Types de mesures de sécurité
  - 11.5.2.1. Prévention
  - 11.5.2.2. Détection
  - 11.5.2.3. Correction
- 11.5.3. Système de contrôle d'accès. Typologie
- 11.5.4. Cryptographie

11.6. Sécurité sur les réseaux et internet
- 11.6.1. Firewalls
- 11.6.2. Identification numérique
- 11.6.3. Virus et vers informatiques
- 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. Attaque. Typologies
- 11.7.4. Le cas à la réalité virtuelle
- 11.7.5. Profils des délinquants et des victimes. Pénalisation de la criminalité
- 11.7.6. Criminalité informatique. Exemples et cas réels

11.8. Plan de sécurité d'un 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. Plan de sécurité. Exemples

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

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

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

12.1. Architecture de sécurité de l'information
- 12.1.1. SGSI / 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. Basés sur des politiques de sécurité
- 12.2.2. Basés sur les outils de protection
- 12.2.3. Basés psur des équipes 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, fournisseurs, 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 opérationnels 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. Opérations commerciales 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 homogénéisation 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. Règlements sectoriels
- 12.8.2. Certifications
- 12.8.3. Législations

12.9. La 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. Systèmes de Gestion de Sécurité de Information (SGSI)

13.1. Sécurité de l'information. Aspects clés
- 13.1.1. Sécurité de l'information
  - 13.1.1.1. Confidencialité
  - 13.1.1.2. Intégration
  - 13.1.1.3. Disponibilité
  - 13.1.1.4. Mesures de sécurité de l'Information

13.2. Systèmes de gestion de la sécurité de l'information
- 13.2.1. Modèles de gestion de la sécurité de l'information
- 13.2.2. Documents pour la mise en œuvre d'un SGSI
- 13.2.3. Niveaux et contrôles d'un SGSI

13.3. Normes et standards internationaux
- 13.3.1. Normes internationales en matière de sécurité de l'information
- 13.3.2. Origine et évolution de la norme
- 13.3.3. Normes internationales de gestion de la sécurité de l'information
- 13.3.4. Autres normes de référence

13.4. Normes ISO/IEC 27000
- 13.4.1. Objectif et domaines d'application
- 13.4.2. Structure de la norme
- 13.4.3. Certification
- 13.4.4. Étapes de l'accréditation
- 13.4.5. Avantages des normes ISO/IEC 27.000

13.5. Conception et mise en œuvre d'un système général de sécurité de l'information
- 13.5.1. Phases de mise en œuvre d'un système général de sécurité de l'information
- 13.5.2. Plan de continuité des activités

13.6. Phase I: diagnostic
- 13.6.1. Diagnostic préliminaire
- 13.6.2. Identification du niveau de stratification
- 13.6.3. Niveau de conformité aux normes

13.7. Phase II: Préparation
- 13.7.1. Contexte de l'organisation
- 13.7.2. Analyse des règles de sécurité applicables
- 13.7.3. Portée du système global de sécurité de l'information
- 13.7.4. Politique générale du système de sécurité des informations
- 13.7.5. Objectifs du système général de sécurité de l'information

13.8. Phase III: Planification
- 13.8.1. Classification des actifs
- 13.8.2. Évaluation des risques
- 13.8.3. Identification des menaces et des risques

13.9. Phase IV: Mise en œuvre et suivi
- 13.9.1. Analyse des résultats
- 13.9.2. Attribution des responsabilités
- 13.9.3. Calendrier du plan d'action
- 13.9.4. Suivi et audits

13.10. Politiques de sécurité en gestion des incidents
- 13.10.1. Phases
- 13.10.2. Catégorisation des incidents
- 13.10.3. Procédures et gestion des incidents

Module 14. Gestion de la sécurité IT

14.1. Gestion de la sécurité
- 14.1.1. Opérations de sécurité
- 14.1.2. Aspects juridique et réglementaire
- 14.1.3. Qualification des entreprises
- 14.1.4. Gestion des risques
- 14.1.5. Gestion des identités et des accès

14.2. Structure du domaine de la sécurité. Le bureau du CISO
- 14.2.1. Structure de l'organisation Position du CISO dans la structure
- 14.2.2. Les lignes de défense
- 14.2.3. Organigramme du bureau du CISO
- 14.2.4. Gestion du budget

14.3. Gouvernance de la sécurité
- 14.3.1. Comité de sécurité
- 14.3.2. Comité de suivi des risques
- 14.3.3. Comité d'audit
- 14.3.4. Comité de crise

14.4. Gouvernance de la sécurité. Fonctions
- 14.4.1. Politiques et normes
- 14.4.2. Plan directeur de la sécurité
- 14.4.3. Tableaux de bord
- 14.4.4. Sensibilisation et formation
- 14.4.5. Sécurité de la chaîne d'approvisionnement

14.5. Opérations de sécurité
- 14.5.1. Gestion des identités et des accès
- 14.5.2. Configuration des règles de sécurité du réseau Firewalls
- 14.5.3. Gestion des plateformes IDS/IPS
- 14.5.4. Analyse des vulnérabilités

14.6. Cadre de cybersécurité. NIST CSF
- 14.6.1. Méthodologie NIST
  - 14.6.1.1. Identifier
  - 14.6.1.2. Protéger
  - 14.6.1.3. Détecter
  - 14.6.1.4. Répondre
  - 14.6.1.5. Récupérer

14.7. Centre des opérations de sécurité (SOC). Fonctions
- 14.7.1. Protection *Red Team, pentesting, threat intelligence*
- 14.7.2. Détection. SIEM, *user behavior analytics, fraud prevention*
- 14.7.3. Réponse

14.8. Audit de sécurité
- 14.8.1. Tests de pénétration
- 14.8.2. Exercices de *red team*
- 14.8.3. Audits du code source. Développement sécurisé
- 14.8.4. Sécurité des composants (*software supply chain*)
- 14.8.5. Analyse médico-légale

14.9. Réponse aux incidents
- 14.9.1. Préparation
- 14.9.2. Détection, analyse et rapport
- 14.9.3. Confinement, éradication et récupération
- 14.9.4. Activité post-incident
  - 14.9.4.1. Conservation des preuves
  - 14.9.4.2. Analyse médico-légale
  - 14.9.4.3. Gestion des écarts
- 14.9.5. Guides officiels de gestion des cyberincidents

14.10. Gestion des vulnérabilités
- 14.10.1. Analyse des vulnérabilités
- 14.10.2. Évaluation de vulnérabilité
- 14.10.3. Base de données système
- 14.10.4. Vulnérabilités au jour 0 Zero-day

Module 15. Politiques de gestion des incidents de sécurité

15.1. Politiques de gestion des incidents de sécurité informatique et leurs avancées
- 15.1.1. Gestion des incidents
- 15.1.2. Responsabilités et procédures
- 15.1.3. Notification d'événement

15.2. Systèmes de détection et de prévention des intrusions (IDS/IPS)
- 15.2.1. Données relatives au fonctionnement du système
- 15.2.2. Types de systèmes de détection d'intrusion
- 15.2.3. Critères de localisation des IDS/IPS

15.3. Réponse aux incidents de sécurité
- 15.3.1. Procédure de collecte d'informations
- 15.3.2. Procédure de vérification des intrusions
- 15.3.3. Organismes CERT

15.4. Processus de notification et gestion des tentatives d'intrusion
- 15.4.1. Responsabilité sur le processus de notification
- 15.4.2. Classification des incidents
- 15.4.3. Processus de résolution et de rétablissement

15.5. Analyse criminalistique en tant que politique de sécurité
- 15.5.1. Preuves volatiles et non volatiles
- 15.5.2. Analyse et collecte de preuves électroniques
  - 15.5.2.1. Analyse des preuves électroniques
  - 15.5.2.2. Collecte de preuves électroniques

15.6. Outils de systèmes de détection et de prévention des intrusions (IDS/IPS)
- 15.6.1. Snort
- 15.6.2. Suricata
- 15.6.3. Solar-Winds

15.7. Outils de centralisation des événements
- 15.7.1. SIM
- 15.7.2. SEM
- 15.7.3. SIEM

15.8. Guide de sécurité CCN-STIC 817
- 15.8.1. Gestion des cyberincidents
- 15.8.2. Mesures et Indicateurs

15.9. NIST SP800-61
- 15.9.1. Capacité de réponse aux incidents de sécurité informatique
- 15.9.2. Gestion d'un incident
- 15.9.3. Coordination et partage d'informations

15.10. Norme ISO 27035
- 15.10.1. Norme ISO 27035. Principes de gestion des incidents
- 15.10.2. Lignes directrices pour l'élaboration d'un plan de gestion des incidents
- 15.10.3. Lignes directrices pour une réponse aux incidents

Module 16. Analyse des risques et environnement de sécurité TI

16.1. Analyse de l'environnement
- 16.1.1. Analyse de la situation conjoncturelle
  - 16.1.1.1. Environnements VUCA
    - 16.1.1.1.1. Volatils
    - 16.1.1.1.2. Incertains
    - 16.1.1.1.3. Complexes
    - 16.1.1.1.4. Ambigus
  - 16.1.1.2. Environnements BANI
    - 16.1.1.2.1. Fragiles
    - 16.1.1.2.2. Anxieux
    - 16.1.1.2.3. Non linéaires
    - 16.1.1.2.4. Incompréhensibles
- 16.1.2. Analyse de l'environnement général. PESTEL
  - 16.1.2.1. Politique
  - 16.1.2.2. Économique
  - 16.1.2.3. Social
  - 16.1.2.4. Technologique
  - 16.1.2.5. Écologique / Ambiental
  - 16.1.2.6. Juridique
- 16.1.3. Analyse de la situation interne. SWOT
  - 16.1.3.1. Objectifs
  - 16.1.3.2. Menaces
  - 16.1.3.3. Opportunités
  - 16.1.3.4. Points forts

16.2. Risque et incertitude
- 16.2.1. Risques
- 16.2.2. Gestion des risques
- 16.2.3. Normes de gestion des risques

16.3. Directrices pour la gestion de risques ISO 31000:2018
- 16.3.1. Objet
- 16.3.2. Principes
- 16.3.3. Cadre de référence
- 16.3.4. Processus

16.4. Méthodologie d'analyse et de gestion des risques liés aux systèmes d'information (MAGERIT)
- 16.4.1. Méthodologie MAGERIT
  - 16.4.1.1. Objectifs
  - 16.4.1.2. Méthode
  - 16.4.1.3. Éléments
  - 16.4.1.4. Techniques
  - 16.4.1.5. Outils disponibles (PILAR)

16.5. Transfert du risque cybernétique
- 16.5.1. Transfert de risques
- 16.5.2. Les cyber-risques. Typologie
- 16.5.3. Assurance des cyber-risques

16.6. Méthodologies agiles pour la gestion des risques
- 16.6.1. Méthodologies agiles
- 16.6.2. Scrum pour la gestion des risques
- 16.6.3. *Agile risk management*

16.7. Technologies pour la gestion des risques
- 16.7.1. Intelligence artificielle appliquée à la gestion des risques
- 16.7.2. *Blockchain* et cryptographie. Méthodes de préservation de la valeur
- 16.7.3. L'informatique quantique. Opportunités et menaces

16.8. Cartographie des risques informatiques basée sur les méthodologies agiles
- 16.8.1. Représentation de la probabilité et de l'impact dans les environnements agiles
- 16.8.2. Le risque en tant que menace pour la valeur
- 16.8.3. Réévolution de la gestion de projet agile et des processus agiles basés sur les KRIs

16.9. *Risk driven* dans la gestion des risques
- 16.9.1. *Risk driven*
- 16.9.2. *Risk driven* dans la gestion des risques
- 16.9.3. Développement d'un modèle de gestion d'entreprise axé sur le risque

16.10. Innovation et transformation numérique dans la gestion des risques informatiques
- 16.10.1. La gestion agile des risques comme source d'innovation commerciale
- 16.10.2. Transformer les données en informations utiles à la prise de décision
- 16.10.3. Vue holistique de l'entreprise à travers le risque

Module 17. Politiques de sécurité pour l'analyse des menaces dans les systèmes informatiques

17.1. La gestion des menaces dans les politiques de sécurité
- 17.1.1. Gestion des risques
- 17.1.2. Risque de sécurité
- 17.1.3. Méthodologies de gestion des menaces
- 17.1.4. Implémentation des méthodologies

17.2. Phases de la gestion des menaces
- 17.2.1. Identification
- 17.2.2. Analyse
- 17.2.3. Localisation
- 17.2.4. Mesures de sauvegarde

17.3. Systèmes d'audit pour la localisation des menaces
- 17.3.1. Classification et flux d'informations
- 17.3.2. Analyse des processus vulnérables

17.4. Classification des risques
- 17.4.1. Types de risques
- 17.4.2. Calcul de la probabilité de la menace
- 17.4.3. Risque résiduel

17.5. Traitement du Risque
- 17.5.1. Implémentation des mesures de sauvegarde
- 17.5.2. Transfert ou prise en charge

17.6. Contrôle des risques
- 17.6.1. Processus continu de gestion des risques
- 17.6.2. Implémentation de mesures de sécurité
- 17.6.3. Modèle stratégique des mesures de sécurité de l'information

17.7. Méthodologies pratiques d'analyse et de surveillance des menaces
- 17.7.1. Catalogue des menaces
- 17.7.2. Catalogue des mesures de contrôle
- 17.7.3. Catalogue des sauvegardes

17.8. Norme ISO 27005
- 17.8.1. Identification des risques
- 17.8.2. Analyse des risques
- 17.8.3. Évaluation des risques

17.9. Matrice des risques, incidences et menaces
- 17.9.1. Données, systèmes et personnel
- 17.9.2. Probabilité de la menace
- 17.9.3. Ampleur des dommages

17.10. Conception des phases et processus dans l'analyse des menaces
- 17.10.1. Identification des éléments critiques de l'organisation
- 17.10.2. Détermination des menaces et des impacts
- 17.10.3. Analyse des impacts et des risques
- 17.10.4. Méthodologie

Module 18. Mise en œuvre pratique des politiques de sécurité contre les attaques

18.1. *System Hacking*
- 18.1.1. Risques et vulnérabilités
- 18.1.2. Contre-mesures

18.2. DoS dans les services
- 18.2.1. Risques et vulnérabilités
- 18.2.2. Contre-mesures

18.3. *Session Hijacking*
- 18.3.1. Le processus de *Hijacking*
- 18.3.2. Contre-mesures au *Hijacking*

18.4. Évasion des IDS, *Firewalls and Honeypots*
- 18.4.1. Techniques d'évasion
- 18.4.2. Implémentation de contre-mesures

18.5. *Hacking Web Servers*
- 18.5.1. Attaques contre les serveurs web
- 18.5.2. Implémentation de mesures de défense

18.6. *Piratage des applications Web*
- 18.6.1. Attaques contre les application web
- 18.6.2. Implémentation de mesures de défense

18.7. *Hacking Wireless Networks*
- 18.7.1. Vulnérabilités des réseaux wifi
- 18.7.2. Implémentation de mesures de défense

18.8. *Hacking Mobile Platforms*
- 18.8.1. Vulnérabilités des plateformes mobiles
- 18.8.2. Implémentation de contre-mesures

18.9. *Ransomware*
- 18.9.1. Vulnérabilités à l'origine du Ransomware
- 18.9.2. Implémentation de contre-mesures

18.10. Ingénierie sociale
- 18.10.1. Types d'ingénierie sociale
- 18.10.2. Contre-mesures en matière d'ingénierie sociale

Module 19. Cryptographie dans les TI

19.1. Cryptographie
- 19.1.1. Cryptographie
- 19.1.2. Fondements mathématiques

19.2. Cryptologie
- 19.2.1. Cryptologie
- 19.2.2. Cryptanalyse
- 19.2.3. Stéganographie et analyse stégoscopique

19.3. Protocoles cryptographiques
- 19.3.1. Blocs de base
- 19.3.2. Protocoles de base
- 19.3.3. Protocoles intermédiaires
- 19.3.4. Protocoles avancés
- 19.3.5. Protocoles exotériques

19.4. Techniques cryptographiques
- 19.4.1. Longueur des clés
- 19.4.2. Gestion des clés
- 19.4.3. Types d'Algorithmes
- 19.4.4. Fonctions de synthèse. *Hash*
- 19.4.5. Générateurs de nombres pseudo-aléatoires
- 19.4.6. Utilisation d'algorithmes

19.5. Cryptographie symétrique
- 19.5.1. Chiffrement par blocs
- 19.5.2. DES (*Data Encryption Standard*)
- 19.5.3. Algorithme RC4
- 19.5.4. AES (*Advance Encryption Standard*)
- 19.5.5. Combinaison de chiffrements par blocs
- 19.5.6. Dérivation des clés

19.6. Cryptographie assymétrique
- 19.6.1. Diffie-Hellman
- 19.6.2. DSA (*Digital Signature Algorithm*)
- 19.6.3. RSA (Rivest, Shamir y Adleman)
- 19.6.4. Courbe elliptique
- 19.6.5. Cryptographie asymétrique. Typologie

19.7. Certificats numériques
- 19.7.1. Signature numérique
- 19.7.2. Certificats X509
- 19.7.3. Infrastructure à clé publique (PKI)

19.8. Mise en œuvre
- 19.8.1. Kerberos
- 19.8.2. IBM CCA
- 19.8.3. *Pretty Good Privacy* (PGP)
- 19.8.4. ISO *Authentication Framework*
- 19.8.5. SSL et TLS
- 19.8.6. Cartes à puce dans les moyens de paiement (EMV)
- 19.8.7. Protocoles de téléphonie mobile
- 19.8.8. *Blockchain*

19.9. Stéganographie
- 19.9.1. Stéganographie
- 19.9.2. Analyse du stégo
- 19.9.3. Applications et utilisations

19.10. Cryptographie quantique
- 19.10.1. Algorithmes quantiques
- 19.10.2. Protection des algorithmes contre l'informatique quantique
- 19.10.3. Distribution des clés quantiques

Module 20. Gestion des identités et des accès dans la sécurité TI

20.1. Gestion des identités et des accès (IAM)
- 20.1.1. Identité numérique
- 20.1.2. Gestion de l'identité
- 20.1.3. Fédération d'identités

20.2. Contrôle d'accès physique
- 20.2.1. Systèmes de protection
- 20.2.2. Sécurité des zones
- 20.2.3. Installations de récupération

20.3. Contrôle d'accès logique
- 20.1.1. Authentification: Typologie
- 20.1.2. Protocoles d'authentification
- 20.1.3. Attaques d'authentification

20.4. Contrôle d'accès logique Authentification MFA
- 20.4.1. Contrôle d'accès logique Authentification MFA
- 20.4.2. Mots de passe. Importance
- 20.4.3. Attaques d'authentification

20.5. Contrôle d'accès logique Authentification biométrique
- 20.5.1. Contrôle d'Accès Logique. Authentification biométrique
  - 20.5.1.1. Authentification biométrique. Exigences
- 20.5.2. Fonctionnement
- 20.5.3. Modèles et techniques

20.6. Systèmes de gestion de l'authentification
- 20.6.1. *Single sign on*
- 20.6.2. Kerberos
- 20.6.3. Systèmes AAA

20.7. Systèmes de gestion de l'authentification: Systèmes AAA
- 20.7.1. TACACS
- 20.7.2. RADIUS
- 20.7.3. DIAMETER

20.8. Services de contrôle des accès
- 20.8.1. FW - Pare-feu
- 20.8.2. VPN- Réseaux Privés Virtuels
- 20.8.3. IDS - Système de Détection des Intrusions

20.9. Systèmes de contrôle d'accès au réseau
- 20.9.1. NAC
- 20.9.2. Architecture et éléments
- 20.9.3. Fonctionnement et normalisation

20.10. Accès aux réseaux sans fil
- 20.10.1. Types de réseaux sans fil
- 20.10.2. Sécurité dans les réseaux sans fil
- 20.10.3. Attaques dans les réseaux sans fil

Module 21. Sécurité dans les communications et opération software

21.1. Sécurité Informatique dans les communications et opération software
- 21.1.1. Sécurité informatique
- 21.1.2. Cybersécurité
- 21.1.3. Sécurité dans le cloud

21.2. Sécurité informatique dans les communications et opération software. Typologie
- 21.2.1. Sécurité physique
- 21.2.2. Sécurité logique

21.3. Sécurité dans les communications
- 21.3.1. Principaux éléments
- 21.3.2. Sécurité des réseaux
- 21.3.3. Meilleures pratiques

21.4. Cyber Intelligence
- 21.4.1. Ingénierie sociale
- 21.4.2. *Deep web*
- 21.4.3. *Phishing*
- 21.4.4. *Malware*

21.5. Développement sécurité dans les communications et opération software
- 21.1.1. Développement sécurisé. Protocole HTTP
- 21.1.2. Développement sécurisé. Cycle de vie
- 21.1.3. Développement sécurisé. Sécurité PHP
- 21.1.4. Développement sécurisé. Sécurité NET
- 21.1.5. Développement sécurisé. Meilleures pratiques

21.6. Systèmes de gestion de la sécurité de l'information dans les communications et opération software
- 21.6.1. GDPR
- 21.6.2. ISO 27021
- 21.6.3. ISO 27017/18

21.7. Technologies SIEM
- 21.7.1. Technologies SIEM
- 21.7.2. Fonctionnement du SOC
- 21.7.3. SIEM *vendors*

21.8. Le rôle de la sécurité dans les organisations
- 21.8.1. Rôles dans les organisations
- 21.8.2. Rôle des spécialistes de l'IoT dans les entreprises
- 21.8.3. Certifications reconnues sur le marché

21.9. Analyse médico-légale
- 21.9.1. Analyse médico-légale
- 21.9.2. Analyse médico-légale. Méthodologie
- 21.9.3. Analyse médico-légale. Outils et mise en œuvre

21.10. La cybersécurité aujourd'hui
- 21.10.1. Principales cyberattaques
- 21.10.2. Prévisions en matière d'employabilité
- 21.10.3. Défis

Module 22. Sécurité dans les environnements *cloud*

22.1. Sécurité dans les environnements *cloud computing*
- 22.1.1. Sécurité dans les environnements *cloud computing*
- 22.1.2. Sécurité dans les environnements *cloud computing* Menaces et risques pour la sécurité
- 22.1.3. Sécurité dans les environnements *cloud computing*. Principaux aspects de la sécurité

22.2. Types d'infrastructures *cloud*
- 22.2.1. Publique
- 22.2.2. Privée
- 22.2.3. Hybride

22.3. Modèle de gestion partagé
- 22.3.1. Éléments de sécurité gérés par fournisseur
- 22.3.2. Éléments gérés par le client
- 22.3.3. Définition de la stratégie de sécurité

22.4. Mécanismes de prévention
- 22.4.1. Systèmes de gestion de l'authentification
- 22.4.2. Systèmes de gestion d'autorisation Politiques d'accès
- 22.4.3. Systèmes de gestion des clés

22.5. Sécurisation des systèmes
- 22.5.1. Sécurisation des systèmes de stockage
- 22.5.2. Protection de systèmes de bases de données
- 22.5.3. Sécurisation des données en transit

22.6. Protection de l'infrastructure
- 22.6.1. Conception et mise en œuvre d'un réseau sécurisé
- 22.6.2. Sécurité des ressources informatiques
- 22.6.3. Outils et ressources pour la protection des infrastructures

22.7. Détection des menaces et des attaques
- 22.7.1. Systèmes d'audit, *logging* et de surveillance
- 22.7.2. Systèmes d'événements et d'alarmes
- 22.7.3. Systèmes SIEM

22.8. Réponse aux incidents
- 22.8.1. Plan de réponse aux incidents
- 22.8.2. La continuité des affaires
- 22.8.3. Analyse médico-légale et remédiation d'incidents de même nature

22.9. Sécurité dans les *clouds* publics
- 22.9.1. AWS (Amazon Web Services)
- 22.9.2. Microsoft Azure
- 22.9.3. Google GCP
- 22.9.4. Oracle Cloud

22.10. Réglementation et conformité
- 22.10.1. Respect des règles de sécurité
- 22.10.2. Gestion des risques
- 22.10.3. Personnes et processus dans les organisations

Module 23. Outils de surveillance des politiques de sécurité des systèmes d'information

23.1. Politiques de surveillance des systèmes d'information
- 23.1.1. Surveillance du système
- 23.1.2. Métriques
- 23.1.3. Types de mesures

23.2. Vérification et enregistrement dans les systèmes
- 23.2.1. Audit et journalisation de Windows
- 23.2.2. Journalisation et audit de Linux

23.3. Protocole SNMP. *Simple Network Management Protocol*
- 23.3.1. Protocole SNMP
- 23.3.2. Fonctionnement de SNMP
- 23.3.3. Outils SNMP

23.4. Surveillance du réseau
- 23.4.1. Surveillance du réseau dans les systèmes de contrôle
- 23.4.2. Outils de surveillance des systèmes de contrôle

23.5. Nagios. Système de surveillance du réseau
- 23.5.1. Nagios
- 23.5.2. Fonctionnement de Nagios
- 23.5.3. Installation de Nagios

23.6. Zabbix. Système de surveillance du réseau
- 23.6.1. Zabbix
- 23.6.2. Fonctionnement de Zabbix
- 23.6.3. Installation de Zabbix

23.7. Cacti. Système de surveillance du réseau
- 23.7.1. Cacti
- 23.7.2. Fonctionnement de Cacti
- 23.7.3. Installation de Cacti

23.8. Pandora. Système de surveillance du réseau
- 23.8.1. Pandora
- 23.8.2. Fonctionnement de Pandora
- 23.8.3. Installation de Pandora

23.9. SolarWinds. Système de surveillance du réseau
- 23.9.1. SolarWinds
- 23.9.2. Fonctionnement de SolarWinds
- 23.9.3. Installation de SolarWinds

23.10. Réglementation en matière de surveillance
- 23.10.1. Contrôles CIS sur l'audit et l'enregistrement
- 23.10.2. NIST 800-123 (ÉTATS-UNIS)

Module 24. Sécurité dans les communications des dispositifs de l'IoT

24.1. De la télémétrie à l'IoT
- 24.1.1. Télémétrie
- 24.1.2. Connectivité M2M
- 24.1.3. Démocratisation de la télémétrie

24.2. Modèles de référence de l'IoT
- 24.2.1. Modèle de référence de l'IoT
- 24.2.2. Architecture simplifiée de l'IoT

24.3. Vulnérabilités de sécurité de l'IoT
- 24.3.1. Dispositifs IoT
- 24.3.2. Dispositifs IoT. Casuistique d'utilisation
- 24.3.3. Dispositifs IoT. Vulnérabilités

24.4. Connectivité de l'IoT
- 24.4.1. Réseaux PAN, LAN, WAN
- 24.4.2. Technologies sans fil non liées à l'IoT
- 24.4.3. Technologies sans fil LPWAN

24.5. Technologies LPWAN
- 24.5.1. Le triangle de fer des réseaux LPWAN
- 24.5.2. Bandes de fréquences libres vs. Bandes sous licence
- 24.5.3. Options technologiques LPWAN

24.6. Technologie LoRaWAN
- 24.6.1. Technologie LoRaWAN
- 24.6.2. Cas d'utilisation de LoRaWAN. Éco-système
- 24.6.3. Sécurité dans LoRaWAN

24.7. Technologie Sigfox
- 24.7.1. Technologie Sigfox
- 24.7.2. Cas d'utilisation SigFox. Éco-système
- 24.7.3. Sécurité dans Sigfox

24.8. Technologie Mobile IoT
- 24.8.1. Technologie Mobile IoT (NB-IoT et LTE-M)
- 24.8.2. Cas d'utilisation de l'IoT mobile. Éco-système
- 24.8.3. Sécurité de l'IoT mobile

24.9. Technologie WiSUN
- 24.9.1. Technologie WiSUN
- 24.9.2. Cas d'utilisation WiSUN. Éco-système
- 24.9.3. Sécdurité dans WiSUN

24.10. Autres technologies IoT
- 24.10.1. Autres technologies IoT
- 24.10.2. Cas d'utilisation et éco-système des autres technologies IoT
- 24.10.3. Sécurité dans les autres technologies IoT

Module 25. Plan de continuité des activités associé à la sécurité

25.1. Plan de continuité des activités
- 25.1.1. Plans de continuité des activités (PCA)
- 25.1.2. Plan de continuité des activités (PCN). Aspects clés
- 25.1.3. Plan de continuité d'activité (PCA) pour l'évaluation des entreprises

25.2. Paramètres d'un plan de continuité des activités (PCA)

25.2.1. *Recovery time objective* (RTO) et *recovery point objective* (RPO)
25.2.2. Durée maximale tolérable (DMT)
25.2.3. Niveaux de récupération minimaux (ROL)
25.2.4. Objectif de point de récupération (RPO)
25.3. Projets de continuité. Typologie
25.3.1. Plan de continuité des activités (PCA)
25.3.2. Plan de continuité des TIC (PCTIC)
25.3.3. Plan de reprise après sinistre (PRS)
25.4. Gestion des risques associés au PCA
25.4.1. Analyse de l'impact sur les activités
25.4.2. Avantages de la mise en œuvre d'un PCA
25.4.3. Réflexion basée sur les risques
25.5. Cycle de vie d'un plan de continuité des activités
25.5.1. Phase 1: Analyse organisationnelle
25.5.2. Phase 2: Détermination de la stratégie de continuité
25.5.3. Phase 3: Réponse aux imprévus
25.5.4. Phase 4: Essais, entretien et révision
25.6. Phase d'analyse organisationnelle d'un PCA
25.6.1. Identification des processus entrant dans le champ d'application du PCA
25.6.2. Identification des domaines d'activité critiques
25.6.3. Identification des dépendances entre les domaines et les processus
25.6.4. Détermination des MTD appropriées
25.6.5. Produits livrables. Création d'un plan
25.7. Phase de détermination de la stratégie de continuité dans un PCA
25.7.1. Rôles dans la phase de détermination de la stratégie
25.7.2. Tâches dans la phase de définition de la stratégie
25.7.3. Produits livrables
25.8. Phase d'intervention d'urgence d'un PCA
25.8.1. Rôles dans la phase d'intervention
25.8.2. Tâches au cours de cette phase
25.8.3. Produits livrables
25.9. Phase d'essais, d'entretien et de révision d'un PCA
25.9.1. Rôles dans la phase d'essais, d'entretien et de révision
25.9.2. Tâches dans la phase d'essais, d'entretien et de révision
25.9.3. Produits livrables
25.10. Normes ISO associées aux plans de continuité d'activité (PCA)
25.10.1. ISO 22301:2019
25.10.2. ISO 22313:2020
25.10.3. Autres normes ISO et internationales connexes

Module 26. Politique pratique de sécurité en cas de catastrophe

26.1. DRP. Plan de Récupération après un Désastre
26.1.1. Objectif d'un DRP
26.1.2. Avantages d'un DRP
26.1.3. Conséquences de l'absence d'un DRP et sans mise à jour
26.2. Orientations pour la définition d'un plan de reprise après sinistre (DRP)
26.2.1. Champ d'application et objectifs
26.2.2. Conception de la stratégie de reprise
26.2.3. Attribution des rôles et des responsabilités
26.2.4. Inventaire du matériel, des logiciels et des services
26.2.5. Tolérance des temps d'arrêt et des pertes de données
26.2.6. Déterminer les types spécifiques de DRP requis
26.2.7. Mise en œuvre d'un plan de formation, de sensibilisation et de communication
26.3. Portée et objectifs d'un DRP (Plan de Reprise après Désastre)
26.3.1. Garantie de réponse
26.3.2. Composants technologiques
26.3.3. Champ d'application de la politique de continuité
26.4. Conception d'une stratégie de reprise après sinistre (DRP)
26.4.1. Stratégie de Plan de Reprise après Désastre
26.4.2. Budget

26.4.3. Ressources Humaines et Matérielles
26.4.4. Postes d'encadrement à risque
26.4.5. Technologie
26.4.6. Données
26.5. Continuité des processus d'information
26.5.1. Planification de la continuité
26.5.2. Implantation de la continuité
26.5.3. Vérification de l'évaluation de la continuité
26.6. Champ d'application d'un PCA (Plan de Continuité des Affaires)
26.6.1. Détermination des processus les plus critiques
26.6.2. Approche basée sur les actifs
26.6.3. Approche par processus
26.7. Implémentation de procédures commerciales sécurisées
26.7.1. Activités prioritaires (AP)
26.7.2. Temps de récupération idéaux (TRI)
26.7.3. Stratégies de survie
26.8. Analyse organisationnelle
26.8.1. Collecte d'informations
26.8.2. Analyse d'impact sur l'entreprise (BIA)
26.8.3. Analyse des risques organisationnels
26.9. Réponse aux imprévus
26.9.1. Plan de crise
26.9.2. Plans de rétablissement de l'environnement opérationnel
26.9.3. Procédures techniques de travail ou d'incident
26.10. Norme Internationale ISO 27031 BCP
26.10.1. Objectifs
26.10.2. Conditions et définitions
26.10.3. Opération

Module 27. Mettre en œuvre des politiques de sécurité physique et environnementale dans l'entreprise

27.1. Zones sécurisées
27.1.1. Périmètre de sécurité physique
27.1.2. Travailler dans des zones sécurisées
27.1.3. Sécurité des bureaux, des locaux et des ressources
27.2. Contrôles physiques des entrées
27.2.1. Politiques de contrôle d'accès physique
27.2.2. Systèmes de contrôle des entrées physiques
27.3. Vulnérabilités de l'accès physique
27.3.1. Principales vulnérabilités physiques
27.3.2. Implémentation des mesures de sauvegarde
27.4. Systèmes biométriques physiologiques
27.4.1. Empreintes digitales
27.4.2. Reconnaissance faciale
27.4.3. Reconnaissance de l'iris et de la rétine
27.4.4. Autres systèmes biométriques physiologiques
27.5. Systèmes biométriques du comportement
27.5.1. Reconnaissance de la signature
27.5.2. Reconnaissance du scripteur
27.5.3. Reconnaissance de la parole
27.5.4. Autres systèmes comportementaux biométriques
27.6. Gestion des risques de la biométrie
27.6.1. Implémentation des systèmes biométriques
27.6.2. Vulnérabilités des systèmes biométriques
27.7. Mise en œuvre des politiques d'hosts
27.7.1. Installation d'approvisionnement et sécurité du câblage
27.7.2. Emplacement de l'équipement
27.7.3. Sortie du matériel en dehors des locaux
27.7.4. Matériel informatique non surveillé et politique claire en matière d'étalage

27.8. Protection de l'environnement
- 27.8.1. Systèmes de protection contre l'incendie
- 27.8.2. Systèmes de protection face aux tremblements de terre
- 27.8.3. Systèmes de protection anti tremblements de terre

27.9. Sécurité du centre de traitement des données
- 27.9.1. Portes de sécurité
- 27.9.2. Systèmes de vidéosurveillance (CCTV)
- 27.9.3. Contrôle de sécurité

27.10. Règlements internationaux en matière de sécurité physique
- 27.10.1. IEC 62443-2-1 (europe)
- 27.10.2. NERC CIP-005-5 (U.S.A.)
- 27.10.3. NERC CIP-014-2 (U.S.A.)

Module 28. Politiques de communications sécurisées dans l'entreprise

28.1. Gestion de la sécurité des réseaux
- 28.1.1. Contrôle et surveillance du réseau
- 28.1.2. Séparation des réseaux
- 28.1.3. Systèmes de sécurité du réseau

28.2. Protocoles de communication sécurisés
- 28.2.1. Modèle TCP/IP
- 28.2.2. Protocole IPSEC
- 28.2.3. Protocole TLS

28.3. Protocole TLS 1.3
- 28.3.1. Phases d'un processus TLS1.3
- 28.3.2. Protocole *Handshake*
- 28.3.3. Protocole d'enregistrement
- 28.3.4. Différences avec TLS 1.2

28.4. Algorithmes cryptographiques
- 28.4.1. Algorithmes cryptographiques utilisés dans les communications
- 28.4.2. *Cipher-suites*
- 28.4.3. Algorithmes cryptographiques autorisés pour TLS 1.3

28.5. Fonctions de digestion
- 28.5.1. MD6
- 28.5.2. SHA

28.6. PKI. Infrastructure à clé publique
- 28.6.1. PKI et ses entités
- 28.6.2. Certificat numérique
- 28.6.3. Types de certificats numériques

28.7. Communications par tunnel et transport
- 28.7.1. Communications par tunnel
- 28.7.2. Communications de transport
- 28.7.3. Implémentation d'un tunnel crypté

28.8. SSH *Secure Shell*
- 28.8.1. SSH Capsule sécurisée
- 28.8.2. Fonctionnement de SSH
- 28.8.3. Outils SSH

28.9. Vérification des systèmes cryptographiques
- 28.9.1. Tests d'intégration
- 28.9.2. Test des systèmes cryptographiques

28.10. Systèmes cryptographiques
- 28.10.1. Vulnérabilités des systèmes cryptographiques
- 28.10.2. Sauvegardes en cryptographie

Module 29. Aspects organisationnels de la politique de sécurité de l'information

29.1. Organisation interne
- 29.1.1. Attribution des responsabilités
- 29.1.2. Séparation des tâches
- 29.1.3. Contacts avec les autorités
- 29.1.4. Sécurité de l'information dans la gestion de projets

29.2. Gestion des actifs
- 29.2.1. Responsabilité des actifs
- 29.2.2. Classification des informations
- 29.2.3. Traitement des supports de stockage

29.3. Politiques de sécurité dans les processus d'entreprise
- 29.3.1. Analyse des processus opérationnels vulnérables
- 29.3.2. Analyse de l'impact sur les activités
- 29.3.3. Classement des processus en fonction de leur impact sur les activités

29.4. Politiques de sécurité liées aux Ressources Humaines
- 29.4.1. Avant le recrutement
- 29.4.2. Pendant le recrutement
- 29.4.3. Fin de contrat ou changement de poste

29.5. Politiques de sécurité de la direction
- 29.5.1. Directives de gestion sur la sécurité de l'information
- 29.5.2. BIA - Analyse de l'impact
- 29.5.3. Le plan de reprise en tant que politique de sécurité

29.6. Acquisition et maintenance des systèmes d'information
- 29.6.1. Exigences d'une Sécurité des systèmes d'information
- 29.6.2. Sécurité des données de développement et soutien
- 29.6.3. Données de l'essai

29.7. Sécurité avec les fournisseurs
- 29.7.1. Sécurité informatique avec les fournisseurs
- 29.7.2. Gestion de la prestation du service avec garantie
- 29.7.3. Sécurité de la chaîne d'approvisionnement

29.8. Sécurité des opérations
- 29.8.1. Responsabilités opérationnelles
- 29.8.2. Protection contre les codes malveillants
- 29.8.3. Copies de sauvegarde
- 29.8.4. Registres d'activité et de suivi

29.9. Gestion de la sécurité et de la réglementation
- 29.9.1. Respect des exigences légales
- 29.9.2. Examens de la sécurité de l'information

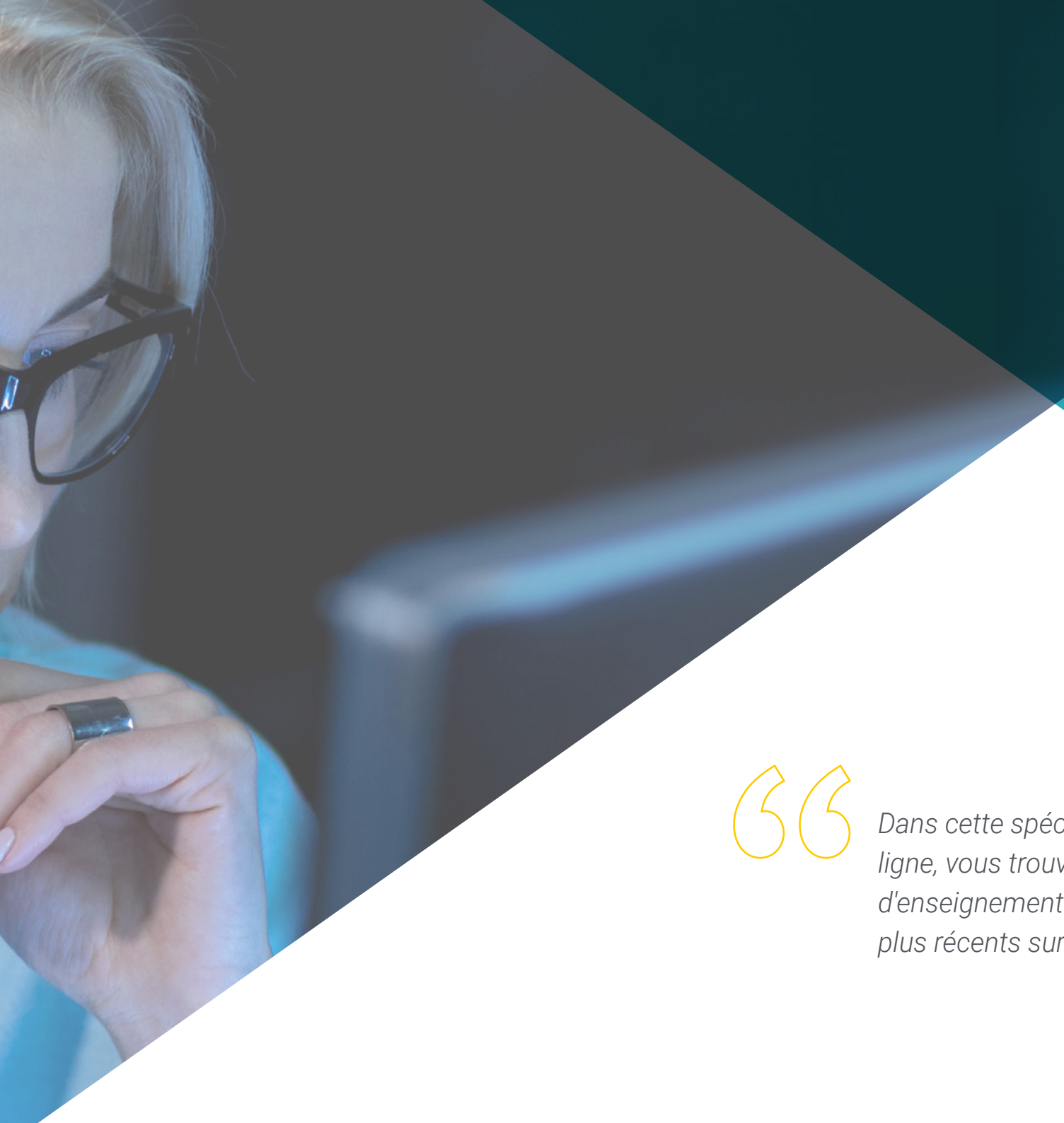
29.10. Sécurité dans la gestion de la continuité des activités
- 29.10.1. Continuité de la sécurité de l'information
- 29.10.2. Redondances

Un programme d'études de TECH Euromed University complet vous apprendra à devenir un leader visionnaire qui assure la protection à long terme de l'organisation"

04

Objectifs

Le Mastère Spécialisé Avancé en Haute Direction en Cybersécurité (CISO) vise à former des leaders stratégiques capables de gérer la sécurité de l'information dans tout type d'organisation. Tout au long du programme, les participants développeront des compétences pour identifier, évaluer et atténuer les cyber-risques, et mettre en œuvre des politiques de sécurité efficaces. En outre, ils acquerront une connaissance approfondie des technologies émergentes et des meilleures pratiques en matière d'architecture de sécurité, garantissant la protection des données et la continuité des activités. Le programme favorise également une vision commerciale intégrée de la cybersécurité, en alignant les initiatives sur les objectifs de l'entreprise et en garantissant la conformité avec les réglementations internationales. Les étudiants seront préparés à être des agents de changement et à promouvoir une culture organisationnelle axée sur la protection numérique.



Dans cette spécialisation 100% en ligne, vous trouverez le matériel d'enseignement et la recherche les plus récents sur la scène universitaire"

Objectifs généraux

- Former des leaders stratégiques en cybersécurité capables de gérer la protection des actifs numériques et des infrastructures technologiques des organisations mondiales
- Intégrer la cybersécurité dans la stratégie de l'entreprise, en alignant les initiatives de protection numérique sur les objectifs généraux de l'organisation
- Former à la mise en œuvre de politiques de cybersécurité et de cadres réglementaires qui garantissent la conformité réglementaire et la protection des informations dans les environnements numériques
- Favoriser le leadership et la gestion des équipes de cybersécurité, en améliorant la capacité à prendre des décisions stratégiques dans des situations de crise et à gérer des projets de sécurité au niveau de l'organisation

Rejoignez TECH Euromed University et développez les compétences nécessaires pour devenir un leader qui anticipe les menaces et renforce les opportunités"

Objectifs spécifiques

Module 1. Cyber intelligence et cybersécurité

- Développer les compétences nécessaires pour mettre en œuvre des stratégies de cyberveille et de Cybersécurité
- Protéger les systèmes informatiques des cybermenaces par la collecte, l'analyse et l'utilisation de renseignements numériques

Module 2. Sécurité de l'Hôte

- Former à la mise en œuvre des mesures de sécurité sur les systèmes hôtes
- Assurer la protection des serveurs et des appareils contre les vulnérabilités, les*malware* et les accès non autorisés

Module 3. Sécurité des réseaux (périmètre)

- Fournir les connaissances nécessaires pour protéger les réseaux informatiques au niveau du périmètre
- Manipuler les techniques et les outils de sécurité tels que les pare-feu, les VPN et les systèmes de détection d'intrusion

Module 4. Sécurité pour *smartphones*

- Fournir une compréhension complète de la sécurité des appareils mobiles
- Approfondir la protection contre les menaces telles que les *malware*, la perte de données et les attaques par le biais d'applications mobiles

Module 5. Sécurité IoT

- Permettre la mise en œuvre de politiques de sécurité pour les appareils IoT
- Protéger l'infrastructure et les données générées par les appareils connectés via les réseaux et plateformes IoT

Module 6. Piratage éthique

- Développer les compétences nécessaires pour effectuer des tests de pénétration et des audits de sécurité en utilisant des techniques de piratage éthique
- Être capable d'identifier les vulnérabilités et de prévenir les attaques

Module 7. Ingénierie inverse

- Maîtriser les techniques d'ingénierie inverse pour analyser et comprendre le fonctionnement des logiciels et du *hardware*
- Identifier les vulnérabilités potentielles et les solutions de sécurité

Module 8. Développement sécurisé

- Enseigner les meilleures pratiques en matière de développement de logiciels sécurisés
- Appliquer les principes de sécurité tout au long du cycle de développement afin de minimiser les risques et les vulnérabilités des applications

Module 9. Implémentation des politiques de sécurité de software et *hardware*

- Fournir les connaissances nécessaires pour concevoir et mettre en œuvre des politiques de sécurité des logiciels et du hardware
- Assurer la protection contre les menaces internes et externes

Module 10. Analyse médico-légale

- Développer des compétences en matière d'analyse criminalistique numérique
- Analyser la collecte, la conservation et l'analyse des preuves numériques dans les cas d'incidents de sécurité informatique

Module 11. Sécurité dans la conception et la développement de systèmes
- Traiter de l'intégration des mesures de sécurité dès les phases de conception et de développement des systèmes informatiques
- Assurer la protection contre les vulnérabilités potentielles dès le début du projet

Module 12. Architectures et modèle de sécurité de l'information
- Fournir les connaissances nécessaires sur les architectures et les modèles de sécurité de l'information
- Concevoir et mettre en œuvre des systèmes robustes qui protègent les données et les ressources de l'organisation

Module 13. Systèmes de Gestion de Sécurité de Information (SGSI)
- Mettre en œuvre un Système de Gestion de la Sécurité de l'Information
- Protéger efficacement les informations de l'entreprise, en veillant au respect des réglementations et des bonnes pratiques

Module 14. Gestion de la sécurité IT
- Fournir les connaissances nécessaires pour gérer efficacement la sécurité des infrastructures technologiques de l'entreprise
- Minimiser les risques et garantir la continuité opérationnelle

Module 15. Politiques de gestion des incidents de sécurité
- Former à la création et à l'application de politiques efficaces de gestion des incidents de sécurité
- Établir des protocoles clairs pour la détection, l'analyse et la réponse aux violations de la sécurité

Module 16. Analyse des risques et environnement de sécurité TI
- Fournir les connaissances nécessaires pour effectuer une analyse des risques de l'environnement informatique, en identifiant les menaces et les vulnérabilités
- Appliquer des stratégies d'atténuation pour sécuriser l'infrastructure technologique

Module 17. Politiques de sécurité pour l'analyse des menaces dans les systèmes informatiques
- Former à l'élaboration de politiques de sécurité pour identifier, analyser et atténuer les menaces dans les systèmes informatiques
- Utiliser les outils et les méthodes appropriés pour protéger les actifs numériques de l'organisation

Module 18. Mise en œuvre pratique des politiques de sécurité contre les attaques
- Mettre en œuvre des politiques de sécurité efficaces face à d'éventuelles attaques
- Assurer la protection des systèmes et des informations critiques de l'organisation

Module 19. Cryptographie dans les TI
- Enseigner les principes fondamentaux et les applications de la cryptographie dans le domaine des technologies de l'information
- Mettre en œuvre des algorithmes de cryptage et de sécurité dans la transmission de données

Module 20. Gestion des identités et des accès dans la sécurité TI
- Développer les compétences nécessaires à la gestion des identités et des accès dans les systèmes TI
- Mettre en place des politiques d'authentification et de contrôle d'accès pour protéger les ressources et les données de l'organisation

Module 21. Sécurité dans les communications et opération software

- Former à la protection des communications numériques et à la mise en œuvre de mesures de sécurité dans l'exploitation des logiciels
- Assurer la confidentialité, l'intégrité et la disponibilité des informations

Module 22. Sécurité dans les environnements cloud

- Mettre en œuvre des politiques de sécurité dans les environnements de cloud computing
- S'assurer que les données et les applications sont protégées contre les accès non autorisés et les attaques

Module 23. Outils de Surveillance dans les Politiques de Sécurité des Systèmes d'Information

- Former à l'utilisation des outils de surveillance pour évaluer l'efficacité des politiques de sécurité dans les systèmes d'information
- Approfondir la détection précoce des vulnérabilités et des attaques

Module 24. Sécurité dans les communications des dispositifs de l'IoT

- Développer des compétences dans la mise en œuvre de mesures de sécurité pour protéger les communications entre les appareils IoT
- Minimiser les risques associés à l'échange de données entre les appareils connectés

Module 25. Plan de continuité des activités associé à la sécurité

- Élaborer un plan de continuité des activités pour assurer la protection et la récupération rapide des systèmes
- Établir des protocoles pour sécuriser les données critiques en cas d'incidents de sécurité

Module 26. Politique pratique de sécurité en cas de catastrophe

- Élaborer des politiques de reprise après sinistre
- Assurer la restauration rapide des systèmes et la protection des données en cas de sinistre

Module 27. Mettre en œuvre des politiques de sécurité physique et environnementale dans l'entreprise

- Former à la mise en œuvre des politiques de sécurité physique et environnementale afin de protéger les ressources physiques de l'organisation
- Garantir un environnement propice au fonctionnement sécurisé des systèmes technologiques

Module 28. Politiques de communications sécurisées dans l'entreprise

- Fournir les connaissances nécessaires à l'élaboration de politiques de communication sécurisées au sein de l'organisation
- Protéger les réseaux et canaux de communication contre l'espionnage et les fuites d'informations

Module 29. Aspects organisationnels de la politique de sécurité de l'information

- Fournir les outils nécessaires à la mise en œuvre des politiques organisationnelles de gestion de la sécurité de l'information
- Établir les rôles, les responsabilités et les processus appropriés pour protéger les actifs informationnels

05

Opportunités de carrière

À l'issue du Mastère Spécialisé Avancé en Haute Direction en Cybersécurité (CISO), les diplômés seront pleinement qualifiés pour assumer des rôles clés dans la protection et la gestion de la sécurité de l'information au sein de diverses organisations. Ils seront également en mesure de diriger des stratégies de sécurité dans des entreprises multinationales, en gérant et en atténuant les cyber-risques. De même, ils seront prêts à occuper des postes exigeant des compétences pour mener des initiatives de cybersécurité et assurer la protection des actifs numériques dans n'importe quel secteur.

Avec ce Mastère Spécialisé Avancé, vous vous spécialiserez en tant que Directeur capable d'anticiper les risques et de protéger les informations critiques"

Profil des diplômés

Le diplômé du Mastère Spécialisé Avancé en Haute Direction en Cybersécurité (CISO) sera un leader stratégique doté d'une connaissance approfondie de la sécurité de l'information dans le contexte des organisations mondiales. Il sera capable de concevoir et de mettre en œuvre des politiques de sécurité avancées et de diriger des équipes pluridisciplinaires. Il possédera également de solides compétences en matière de gestion et de gouvernance, ce qui lui permettra de relever les défis de la cybersécurité dans divers secteurs et d'assurer la protection des actifs numériques. Cette opportunité lui fournira les outils dont il a besoin pour rester à la pointe des dernières tendances technologiques et s'adapter à l'évolution rapide du paysage numérique.

Préparez-vous à faire partie des meilleurs professionnels, à minimiser l'impact des cyber-attaques et à reprendre rapidement le cours normal de vos activités.

- **Leadership stratégique et capacité d'adaptation:** Capacité à diriger des équipes pluridisciplinaires et à gérer des politiques de sécurité, en s'adaptant aux changements technologiques rapides et aux nouvelles évolutions dans le domaine de la cybersécurité
- **Gestion des risques et prise de décision éclairée:** Capacité à identifier, évaluer et atténuer les cyberrisques, en prenant des décisions fondées sur des données et des analyses détaillées
- **Analyse critique et gestion des incidents:** Capacité à identifier les vulnérabilités, à gérer les incidents de sécurité et à coordonner la réponse aux crises, en assurant la continuité des activités
- **Communication efficace et réflexion stratégique:** Capacité à communiquer clairement les risques et les solutions aux différentes parties prenantes, en adoptant une approche holistique et stratégique de la protection des actifs numériques

À l'issue de ce Mastère Spécialisé Avancé, vous serez en mesure d'utiliser vos connaissances et vos compétences pour occuper les postes suivants:

1. **Chief Information Security Officer (CISO):** Responsable stratégique de la protection de l'information et de la cybersécurité au sein de l'organisation, chargé d'élaborer des politiques et de superviser l'infrastructure de sécurité numérique.
2. **Directeur de la Cybersécurité:** Responsable de la gestion et de la supervision des équipes de sécurité informatique, il élabore et met en œuvre des stratégies visant à protéger l'infrastructure technologique de l'entreprise.
3. **Responsable de la Sécurité Informatique:** Responsable de la gestion et de la coordination des politiques de sécurité numérique, il supervise la protection des données et des systèmes informatiques contre les menaces éventuelles.
4. **Consultant en Cybersécurité:** Expert qui conseille les entreprises sur la meilleure façon de mettre en œuvre et de gérer les politiques de cybersécurité, en les aidant à réduire les risques et à se conformer aux réglementations internationales.
5. **Responsable de la Gestion des Risques Informatiques:** Responsable de l'identification, de l'évaluation et de l'atténuation des cyber-risques susceptibles d'affecter la sécurité des systèmes d'information et de technologie de l'organisation
6. **Chef de la Sécurité de l'Information:** Responsable de la supervision et de la coordination de toutes les initiatives liées à la protection des données et des systèmes informatiques au sein de l'organisation

Vous êtes à deux doigts d'améliorer votre vie professionnelle grâce à ce Mastère Spécialisé Avancé que seule TECH Euromed University peut vous offrir"

06

Méthodologie d'étude

TECH Euromed University est la première au monde à combiner la méthodologie des ***case studies*** avec ***Relearning***, un système d'apprentissage 100% en ligne basé sur la répétition guidée.

Cette stratégie d'enseignement innovante est conçue pour offrir aux professionnels la possibilité d'actualiser leurs connaissances et de développer leurs compétences de manière intensive et rigoureuse. Un modèle d'apprentissage qui place l'étudiant au centre du processus académique et lui donne le rôle principal, en s'adaptant à ses besoins et en laissant de côté les méthodologies plus conventionnelles.

TECH Euromed University vous prépare à relever de nouveaux défis dans des environnements incertains et à réussir votre carrière"

L'étudiant: la priorité de tous les programmes de TECH Euromed University

Dans la méthodologie d'étude de TECH Euromed University, l'étudiant est le protagoniste absolu.

Les outils pédagogiques de chaque programme ont été sélectionnés en tenant compte des exigences de temps, de disponibilité et de rigueur académique que demandent les étudiants d'aujourd'hui et les emplois les plus compétitifs du marché.

Avec le modèle éducatif asynchrone de TECH Euromed University, c'est l'étudiant qui choisit le temps qu'il consacre à l'étude, la manière dont il décide d'établir ses routines et tout cela dans le confort de l'appareil électronique de son choix. L'étudiant n'a pas besoin d'assister à des cours en direct, auxquels il ne peut souvent pas assister. Les activités d'apprentissage se dérouleront à votre convenance. Vous pouvez toujours décider quand et où étudier.

"À TECH Euromed University, vous n'aurez PAS de cours en direct (auxquelles vous ne pourrez jamais assister)"

Les programmes d'études les plus complets au niveau international

TECH Euromed University se caractérise par l'offre des itinéraires académiques les plus complets dans l'environnement universitaire. Cette exhaustivité est obtenue grâce à la création de programmes d'études qui couvrent non seulement les connaissances essentielles, mais aussi les dernières innovations dans chaque domaine.

Grâce à une mise à jour constante, ces programmes permettent aux étudiants de suivre les évolutions du marché et d'acquérir les compétences les plus appréciées par les employeurs. Ainsi, les diplômés de TECH Euromed University reçoivent une préparation complète qui leur donne un avantage concurrentiel significatif pour progresser dans leur carrière.

De plus, ils peuvent le faire à partir de n'importe quel appareil, PC, tablette ou smartphone.

> *Le modèle de TECH Euromed University est asynchrone, de sorte que vous pouvez étudier sur votre PC, votre tablette ou votre smartphone où vous voulez, quand vous voulez et aussi longtemps que vous le voulez"*

Case studies ou Méthode des cas

La méthode des cas est le système d'apprentissage le plus utilisé par les meilleures écoles de commerce du monde. Développée en 1912 pour que les étudiants en Droit n'apprennent pas seulement le droit sur la base d'un contenu théorique, sa fonction était également de leur présenter des situations réelles et complexes. De cette manière, ils pouvaient prendre des décisions en connaissance de cause et porter des jugements de valeur sur la manière de les résoudre. Elle a été établie comme méthode d'enseignement standard à Harvard en 1924.

Avec ce modèle d'enseignement, ce sont les étudiants eux-mêmes qui construisent leurs compétences professionnelles grâce à des stratégies telles que *Learning by doing* ou le *Design Thinking*, utilisées par d'autres institutions renommées telles que Yale ou Stanford.

Cette méthode orientée vers l'action sera appliquée tout au long du parcours académique de l'étudiant avec TECH Euromed University. Vous serez ainsi confronté à de multiples situations de la vie réelle et devrez intégrer des connaissances, faire des recherches, argumenter et défendre vos idées et vos décisions. Il s'agissait de répondre à la question de savoir comment ils agiraient lorsqu'ils seraient confrontés à des événements spécifiques complexes dans le cadre de leur travail quotidien.

Méthode Relearning

À TECH Euromed University, les *case studies* sont complétées par la meilleure méthode d'enseignement 100% en ligne: le *Relearning*.

Cette méthode s'écarte des techniques d'enseignement traditionnelles pour placer l'apprenant au centre de l'équation, en lui fournissant le meilleur contenu sous différents formats. De cette façon, il est en mesure de revoir et de répéter les concepts clés de chaque matière et d'apprendre à les appliquer dans un environnement réel.

Dans le même ordre d'idées, et selon de multiples recherches scientifiques, la répétition est le meilleur moyen d'apprendre. C'est pourquoi TECH Euromed University propose entre 8 et 16 répétitions de chaque concept clé au sein d'une même leçon, présentées d'une manière différente, afin de garantir que les connaissances sont pleinement intégrées au cours du processus d'étude.

Le Relearning vous permettra d'apprendre plus facilement et de manière plus productive tout en développant un esprit critique, en défendant des arguments et en contrastant des opinions: une équation directe vers le succès.

Un Campus Virtuel 100% en ligne avec les meilleures ressources didactiques

Pour appliquer efficacement sa méthodologie, TECH Euromed University se concentre à fournir aux diplômés du matériel pédagogique sous différents formats: textes, vidéos interactives, illustrations et cartes de connaissances, entre autres. Tous ces supports sont conçus par des enseignants qualifiés qui axent leur travail sur la combinaison de cas réels avec la résolution de situations complexes par la simulation, l'étude de contextes appliqués à chaque carrière professionnelle et l'apprentissage basé sur la répétition, par le biais d'audios, de présentations, d'animations, d'images, etc.

Les dernières données scientifiques dans le domaine des Neurosciences soulignent l'importance de prendre en compte le lieu et le contexte d'accès au contenu avant d'entamer un nouveau processus d'apprentissage. La possibilité d'ajuster ces variables de manière personnalisée aide les gens à se souvenir et à stocker les connaissances dans l'hippocampe pour une rétention à long terme. Il s'agit d'un modèle intitulé *Neurocognitive context-dependent e-learning* qui est sciemment appliqué dans le cadre de ce diplôme d'université.

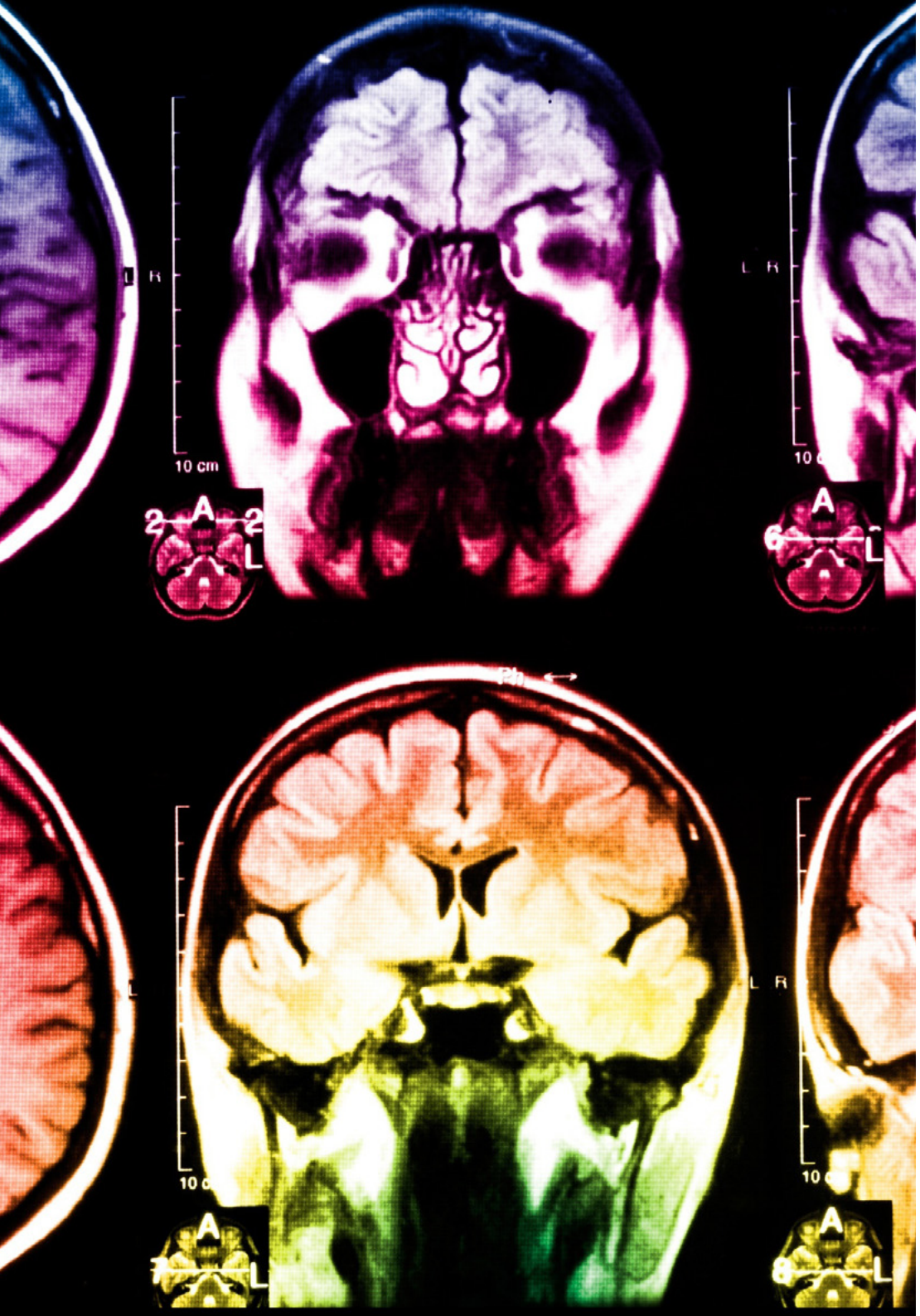
D'autre part, toujours dans le but de favoriser au maximum les contacts entre mentors et mentorés, un large éventail de possibilités de communication est offert, en temps réel et en différé (messagerie interne, forums de discussion, service téléphonique, contact par courrier électronique avec le secrétariat technique, chat et vidéoconférence).

De même, ce Campus Virtuel très complet permettra aux étudiants TECH Euromed University d'organiser leurs horaires d'études en fonction de leurs disponibilités personnelles ou de leurs obligations professionnelles. De cette manière, ils auront un contrôle global des contenus académiques et de leurs outils didactiques, mis en fonction de leur mise à jour professionnelle accélérée.

> *Le mode d'étude en ligne de ce programme vous permettra d'organiser votre temps et votre rythme d'apprentissage, en l'adaptant à votre emploi du temps"*

L'efficacité de la méthode est justifiée par quatre acquis fondamentaux:

1. Les étudiants qui suivent cette méthode parviennent non seulement à assimiler les concepts, mais aussi à développer leur capacité mentale au moyen d'exercices pour évaluer des situations réelles et appliquer leurs connaissances.
2. L'apprentissage est solidement traduit en compétences pratiques ce qui permet à l'étudiant de mieux s'intégrer dans le monde réel.
3. L'assimilation des idées et des concepts est rendue plus facile et plus efficace, grâce à l'utilisation de situations issues de la réalité.
4. Le sentiment d'efficacité de l'effort investi devient un stimulus très important pour les étudiants, qui se traduit par un plus grand intérêt pour l'apprentissage et une augmentation du temps passé à travailler sur le cours.



La méthodologie universitaire la mieux évaluée par ses étudiants

Les résultats de ce modèle académique innovant sont visibles dans les niveaux de satisfaction générale des diplômés de TECH Euromed University.

L'évaluation par les étudiants de la qualité de l'enseignement, de la qualité du matériel, de la structure et des objectifs des cours est excellente. Sans surprise, l'institution est devenue l'université la mieux évaluée par ses étudiants sur la plateforme d'évaluation Global Score, avec une note de 4,9 sur 5.

Accédez aux contenus de l'étude depuis n'importe quel appareil disposant d'une connexion Internet (ordinateur, tablette, smartphone) grâce au fait que TECH Euromed University est à la pointe de la technologie et de l'enseignement.

Vous pourrez apprendre grâce aux avantages offerts par les environnements d'apprentissage simulés et à l'approche de l'apprentissage par observation: le Learning from an expert.

Ainsi, le meilleur matériel pédagogique, minutieusement préparé, sera disponible dans le cadre de ce programme:

Matériel didactique

Tous les contenus didactiques sont créés par les spécialistes qui enseignent les cours. Ils ont été conçus en exclusivité pour le programme afin que le développement didactique soit vraiment spécifique et concret.

Ces contenus sont ensuite appliqués au format audiovisuel afin de mettre en place notre mode de travail en ligne, avec les dernières techniques qui nous permettent de vous offrir une grande qualité dans chacune des pièces que nous mettrons à votre service.

Pratique des aptitudes et des compétences

Vous effectuerez des activités visant à développer des compétences et des aptitudes spécifiques dans chaque domaine. Pratiques et dynamiques permettant d'acquérir et de développer les compétences et les capacités qu'un spécialiste doit acquérir dans le cadre de la mondialisation dans laquelle nous vivons.

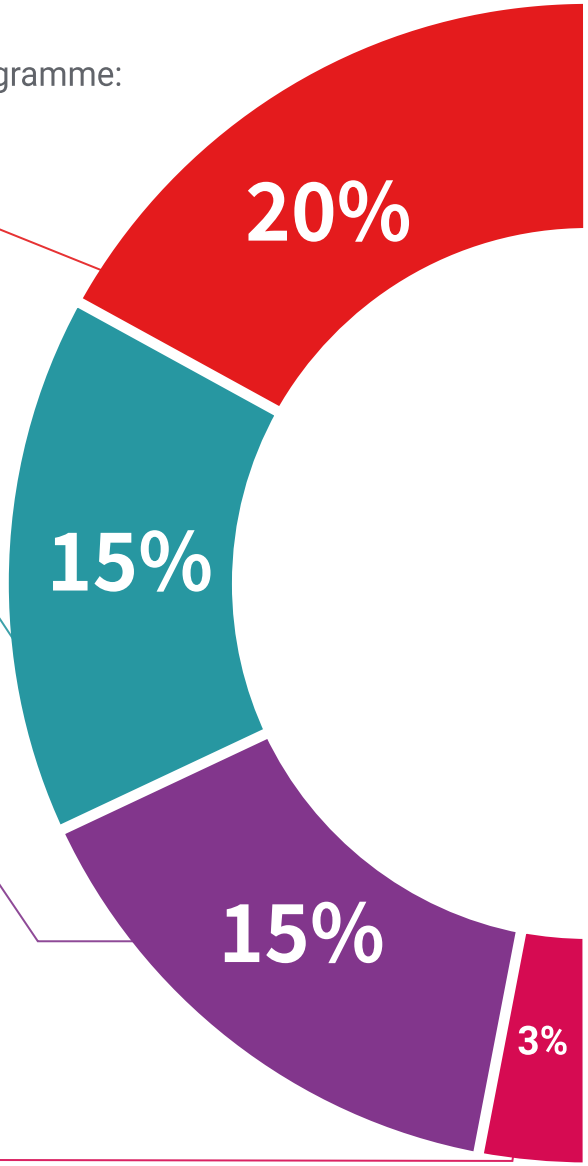
Résumés interactifs

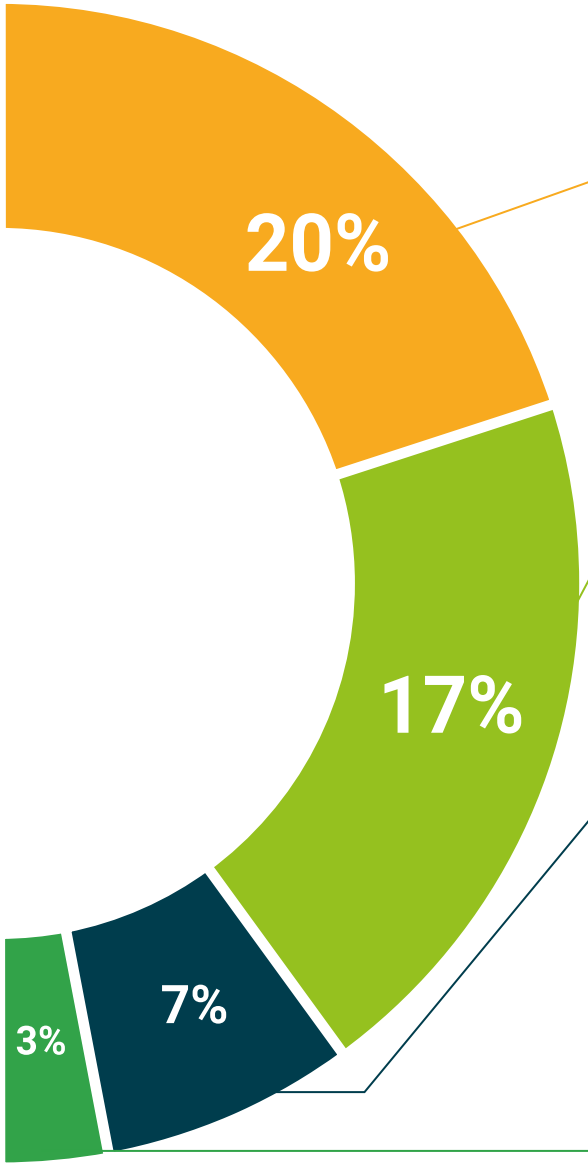
Nous présentons les contenus de manière attrayante et dynamique dans des dossiers multimédias qui incluent de l'audio, des vidéos, des images, des diagrammes et des cartes conceptuelles afin de consolider les connaissances.

Ce système éducatif unique de présentation de contenu multimédia a été récompensé par Microsoft en tant que»European Success Story".

Lectures complémentaires

Articles récents, documents de consensus, guides internationaux, etc... Dans notre bibliothèque virtuelle, vous aurez accès à tout ce dont vous avez besoin pour compléter votre formation.





Case Studies

Vous réaliserez une sélection des meilleures case studies dans le domaine. Des cas présentés, analysés et encadrés par les meilleurs spécialistes internationaux.

Testing & Retesting

Nous évaluons et réévaluons périodiquement vos connaissances tout au long du programme. Nous le faisons sur 3 des 4 niveaux de la Pyramide de Miller.

Cours magistraux

Il existe des preuves scientifiques de l'utilité de l'observation par un tiers expert.

La méthode Learning from an Expert permet au professionnel de renforcer ses connaissances ainsi que sa mémoire, puis lui permet d'avoir davantage confiance en lui concernant la prise de décisions difficiles.

Guides d'action rapide

TECH Euromed University propose les contenus les plus pertinents du programme sous forme de fiches de travail ou de guides d'action rapide. Un moyen synthétique, pratique et efficace pour vous permettre de progresser dans votre apprentissage.

07

Corps Enseignant

Ce Mastère Spécialisé Avancé en Haute Direction en Cybersécurité (CISO, Chief Information Security Officer) dispose d'un corps enseignant composé de professionnels en activité qui connaissent parfaitement l'état actuel de ce domaine, et qui transmettront donc à l'étudiant toutes les clés de la cybersécurité actuelle. De cette manière, il est garanti que l'étudiant de ce programme obtiendra les dernières avancées dans ce domaine, en pouvant y accéder grâce au prestigieux corps enseignant que TECH Euromed University a sélectionné.

TECH Euromed University met à votre disposition les Directeurs et les Enseignants les plus spécialisés pour que votre approche et votre apprentissage soient les meilleurs”

Directeur International Invité

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. Au cours de sa carrière professionnelle, il a conceptualisé et dirigé des programmes académiques de pointe dans plusieurs institutions renommées, telles que **l'Université de Montréal**, **l'Université George Washington** et **l'Université de Georgetown**.

Tout au long de son parcours, 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, qui traitent de la lutte contre la criminalité lors de catastrophes majeures, de la lutte contre le terrorisme, des agences de renseignement et de 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. Ainsi, sa prestigieuse carrière universitaire l'a amené à être Professeur de Pratiques et Directeur de la Faculté 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

- Directeur du Master en Cybersecurity Risk Management à l'Université de Georgetown, Washington, États-Unis
- Directeur du Master en Technology Management à l'Université de Georgetown
- Directeur du Master en Applied Intelligence à l'Université de Georgetown
- Professeur de Stages Pratiques à l'Université de Georgetown
- Doctorat en Criminologie de la School of Criminology de l'Université de Montréal
- Licence en Sociologie et Minor Degree en Psychologie de l'Université de Laval
- Membre de: New Program Roundtable Committee, Université de Georgetown

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

Direction

Mme Fernández Sapena, Sonia

- Formatrice en Sécurité Informatique et Piratage Éthique au Centre National de Référence pour l'Informatique et les Télécommunications à Getafe à Madrid
- Instructrice agréée E-Council
- Formatrice dans les certifications suivantes: EXIN Ethical Hacking Foundation et EXIN Cyber & IT Security Foundation. Madrid
- Formatrice experte accréditée par la 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
- Ingénieure en Informatique de l'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 de *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

- Développeuse d'applications mobiles natives Android chez B60. UK
- Analyste Programmeuse pour la Gestion, la Coordination et la Documentation d'un Environnement d'Alarme de Sécurité Virtualisé
- Analyste Programmeuse d'Applications Java pour les guichets automatiques bancaires
- Professionnelle du Développement de *Software* pour une Application de Validation de Signature et de Gestion de Documents
- Technicienne des Systèmes pour la Migration des Équipements et pour la Gestion, la Maintenance et la Formation des PDA Mobiles
- Ingénieure Technique en Systèmes Informatiques de l'Université Ouverte de Catalogne
- Master en Sécurité Informatique et Hacking Éthique Officiel de EC- Council et CompTIA de l'École Profesionelle des Nouvelles Technologies CICE

M. Entrenas, Alejandro

- Chef de Projet en Cybersécurité. Entelgy Innotec Security
- Consultant en Cybersécurité. Entelgy
- Analyste de la Sécurité de l'Information. Innovery España
- Analyste de la Sécurité de l'Information. Atos
- Licence en Ingénierie Technique en Informatique des Systèmes de l'Université de Cordoue
- Master en Direction et 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. Catalá Barba, José Francisco

- Technicien en Électronique Expert en Cybersécurité
- Développeur d'Applications pour Dispositifs Mobiles
- Technicien en Électronique dans L'Encadrement Intermédiaire au sein du Ministère Espagnol de la Défense
- Technicien en Électronique à l'Usine Ford Sita à Valence

M. Peralta Alonso, Jon

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

M. Gonzalo Alonso, Félix

- PDG 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 d'Assurance de l'Institut pour la Collaboration entre les Compagnies d'Assurance
- Diplôme en Ingénierie Technique Industrielle, avec spécialisation en Électronique Industrielle, de l'Université Pontificale de Comillas

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 du CICE
- Cours Avancé en Cybersécurité de la Formation Deusto

M. Redondo, Jesús Serrano

- Développeur Web et Technicien en Cybersécurité
- Développeur Web à Roams, Palencia
- Développeur FrontEnd chez Telefónica, Madrid
- Développeur FrontEnd chez Best Pro Consulting SL, Madrid
- Installateur d'Équipements et de Services de Télécommunications chez Groupe Zener, Castille et León
- Installateur d'Équipements et de Services de Télécommunications chez Lican Comunicaciones SL, Castille et León
- Certificat en Sécurité Informatique, CFTIC Getafe, Madrid
- Technicien Supérieur en Télécommunications et Systèmes Informatiques de l'IES Trinidad Arroyo, Palencia
- Technicien Supérieur en Installations Electrotechniques MT et BT de l'IES Trinidad Arroyo, Palencia
- Formation en Ingénierie Inverse, Sténographie et Cryptage de Incibe Hacker Academy

M. Nogales Ávila, Javier

- Enterprise Cloud y Sourcing Senior Consultant à Quint
- Cloud y Technology Consultant a Indra
- Associate Technology Consultant à Accenture
- Diplôme d'Ingénieur d'Organisation Industrielle de l'Université de Jaén
- MBA en Administration et Gestion des Entreprises deThePower 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 de l'Institut Catalan de Technologie
- Licence en Génie Supérieur des Télécommunications de l'Université Polytechnique de Catalogne

M. Rodrigo Estébanez, Juan Manuel

- Co-fondateur d'Ismet Tech
- Responsable de la Sécurité de l'Information chez Ecix Group
- *Operational Security Officer* chez Atos IT Solutions and Services A/S
- Enseignant 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

M. Del Valle Arias, Jorge

- Ingénieur en Télécommunications, expert en Développement d'Affaires
- Smart City Solutions & Software Business Development Manager Espagne. Itron, Inc
- Consultant IoT
- Responsable Intérimaire des Activités IoT. TCOMET
- Responsable de l'Unité Commerciale IoT, Industrie 4.0. Diode Espagne
- Directeur Commercial de Zone pour l'IoT et les Télécommunications Aicox Soluciones
- Directeur Technique (CTO) et Directeur du Développement Commercial. TELYC Consulting
- 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 chez KPMG. Espagne
- Consultante en Processus Informatiques et en Contrôle et Gestion de Projets d'Infrastructure chez Bankia
- Ingénieure en Outils d'Exploitation chez Dalkia
- Développeuse au sein du Groupe Banque Populaire
- Développeuse d'Applications à l'Université Polytechnique de Madrid
- Diplôme en Ingénierie Informatique de l'Université Alfonso X el Sabio
- Ingénieure Technique en Informatique de Gestion de l'Université Polytechnique de Madrid
- Certified Data Privacy Solutions Engineer (CDPSE) de l'ISACA

M. Ortega Esteban, Octavio

- Spécialiste en Marketing et Développement Web
- Programmeur d'Applications Informatiques et Développeur Web *Freelance*
- *Chief Operating Officer* à Smallsquid SL
- Administrateur du e-commerce chez Ortega y Serrano
- Enseignant dans les cours de Certificats Professionnels en Informatique et Communications
- Enseignant des cours de Sécurité Informatique
- Licence en Psychologie de l'Université Ouverte de Catalogne
- Technicien Supérieur Universitaire en Analyse, Conception et Solutions de *Software*
- Technicien Supérieur Universitaire en Programmation Avancée

M. Embid Ruiz, Mario

- Avocat Spécialisé dans les TIC et la Protection des Données chez Martínez-Echevarría Abogados
- Responsable juridique de Branddocs SL
- Analyste des Risques dans le Segment PME de BBVA
- Enseignant dans le cadre d'études universitaires de troisième cycle en Droit
- Licence en Droit de l'Université Rey Juan Carlos
- Licence en Administration et Gestion des Entreprises de l'Université Rey Juan Carlos
- Master en Droit des Nouvelles Technologies, de l'Internet et de l'Audiovisuel du Centre d'Études Universitaires Villanueva

Profitez de l'occasion pour vous informer sur les derniers développements dans ce domaine afin de les appliquer à votre pratique quotidienne"

08

Diplôme

Le Mastère Spécialisé Avancé en Haute Direction en Cybersécurité (CISO, Chief Information Security Officer) garantit, outre la formation la plus rigoureuse et la plus actualisée, l'accès à un diplôme de Mastère Spécialisé Avancé délivré par TECH Euromed University.

Terminez ce programme avec succès et obtenez votre diplôme universitaire sans avoir à vous déplacer ou à passer par des procédures fastidieuses"

Le programme du **Mastère Spécialisé Avancé en Haute Direction en Cybersécurité (CISO, Chief Information Security Officer)** est le programme le plus complet sur la scène académique actuelle. Après avoir obtenu leur diplôme, les étudiants recevront un diplôme d'université délivré par TECH Global University et un autre par Université Euromed de Fès.

Ces diplômes de formation continue et et d'actualisation professionnelle de TECH Global University et d'Université Euromed de Fès garantissent l'acquisition de compétences dans le domaine de la connaissance, en accordant une grande valeur curriculaire à l'étudiant qui réussit les évaluations et accrédite le programme après l'avoir suivi dans son intégralité.

Ce double certificat, de la part de deux institutions universitaires de premier plan, représente une double récompense pour une formation complète et de qualité, assurant à l'étudiant l'obtention d'une certification reconnue au niveau national et international. Ce mérite académique vous positionnera comme un professionnel hautement qualifié, prêt à relever les défis et à répondre aux exigences de votre secteur professionnel.

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

Modalité: **en ligne**

Durée: **2 ans**

Accréditation **120 ECTS**

tech Global University

M./Mme _____, titulaire du document d'identité _____
a réussi et obtenu le diplôme de:

Mastère Spécialisé Avancé en Haute Direction en Cybersécurité (CISO, Chief Information Security Officer)

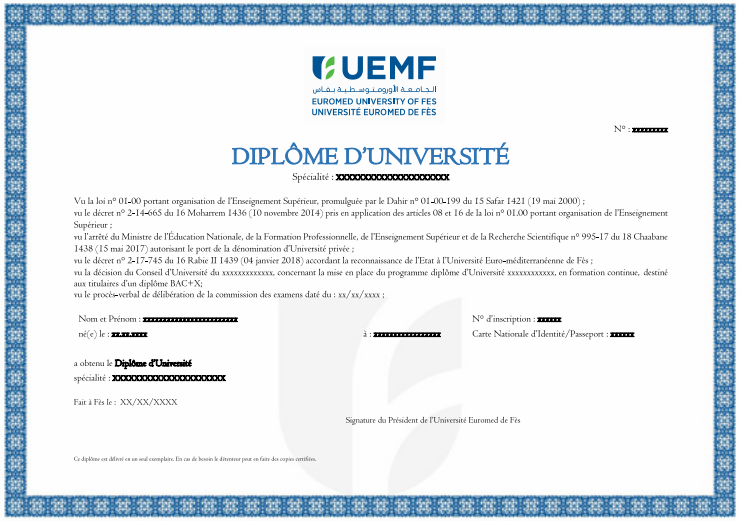
Il s'agit d'un diplôme propre à l'université de 3.600 heures, équivalant à 120 ECTS, dont la date de début est le jj/mm/aaaa et la date de fin le jj/mm/aaaa.

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

À Andorre-la-Vieille, 28 février 2024

Dr Pedro Navarro Illana
Recteur

Code Unique TECH: AFWOR23S techtitute.com/diplômes



UEMF
EUROMED UNIVERSITY OF FES
UNIVERSITÉ EUROMED DE FÈS

N° : xxxxxxxxx

DIPLÔME D'UNIVERSITÉ

Spécialité : xxxxxxxxxxxxxxxxxxxxxxxx

Vu la loi n° 01-00 portant organisation de l'Enseignement Supérieur, promulguée par le Dahir n° 01-00-199 du 15 Safar 1421 (19 mai 2000) ;
vu le décret n° 2-14-665 du 16 Moharrem 1436 (10 novembre 2014) pris en application des articles 08 et 16 de la loi n° 01.00 portant organisation de l'Enseignement Supérieur ;
vu l'arrêté du Ministre de l'Éducation Nationale, de la Formation Professionnelle, de l'Enseignement Supérieur et de la Recherche Scientifique n° 995-17 du 18 Chaabane 1438 (15 mai 2017) autorisant le port de la dénomination d'Université privée ;
vu le décret n° 2-17-745 du 16 Rabie II 1439 (04 janvier 2018) accordant la reconnaissance de l'Etat à l'Université Euro-méditerranéenne de Fès ;
vu la décision du Conseil d'Université du xxxxxxxxxxxxx, concernant la mise en place du programme diplôme d'Université xxxxxxxxxxxx, en formation continue, destiné aux titulaires d'un diplôme BAC+?X;
vu le procès-verbal de délibération de la commission des examens daté du : xx/xx/xxxx ;

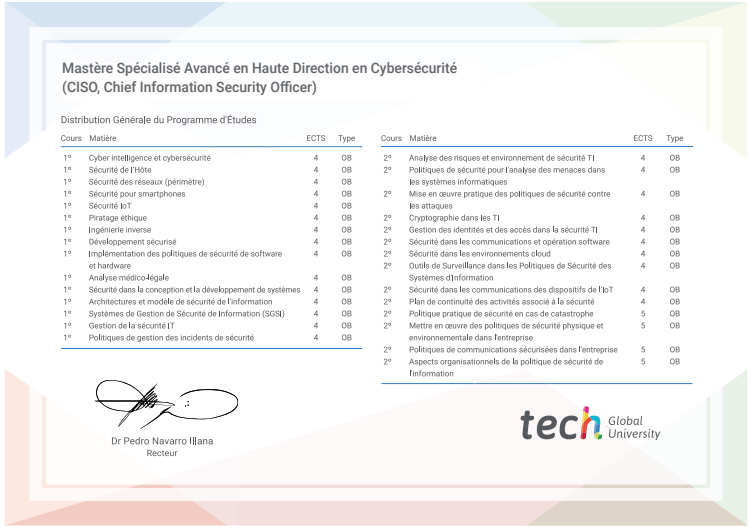
Nom et Prénom : xxxxxxxxxxxxxxxxxxxxxxxx
né(e) le : xx.xx.xxxx à : xxxxxxxxxxxxxxxx
N° d'inscription : xxxxxx
Carte Nationale d'Identité/Passeport : xxxxxx

a obtenu le **Diplôme d'Université**
spécialité : xxxxxxxxxxxxxxxxxxxxxxxx

Fait à Fès le : XX/XX/XXXX

Signature du Président de l'Université Euromed de Fès

Ce diplôme est délivré en un seul exemplaire. En cas de besoin le détenteur peut en faire des copies certifiées.



Mastère Spécialisé Avancé en Haute Direction en Cybersécurité (CISO, Chief Information Security Officer)

Distribution Générale du Programme d'Études

Cours	Matière	ECTS	Type
1°	Cyber intelligence et cybersécurité	4	OB
1°	Sécurité de l'Hôte	4	OB
1°	Sécurité des réseaux (périmètre)	4	OB
1°	Sécurité pour smartphones	4	OB
1°	Sécurité IoT	4	OB
1°	Piratage éthique	4	OB
1°	Ingénierie inverse	4	OB
1°	Développement sécurisé	4	OB
1°	Implémentation des politiques de sécurité de software et hardware	4	OB
1°	Analyse médico-légale	4	OB
1°	Sécurité dans la conception et la développement de systèmes	4	OB
1°	Architectures et modèle de sécurité de l'information	4	OB
1°	Systèmes de Gestion de Sécurité de Information (SGSI)	4	OB
1°	Gestion de la sécurité IT	4	OB
1°	Politiques de gestion des incidents de sécurité	4	OB
2°	Analyse des risques et environnement de sécurité TI	4	OB
2°	Politiques de sécurité pour l'analyse des menaces dans les systèmes informatiques	4	OB
2°	Mise en œuvre pratique des politiques de sécurité contre les attaques	4	OB
2°	Cryptographie dans les TI	4	OB
2°	Gestion des identités et des accès dans la sécurité TI	4	OB
2°	Sécurité dans les communications et opération software	4	OB
2°	Sécurité dans les environnements cloud	4	OB
2°	Outils de Surveillance dans les Politiques de Sécurité des Systèmes d'Information	4	OB
2°	Sécurité dans les communications des diapositifs de l'IoT	4	OB
2°	Plan de continuité des activités associé à la sécurité	4	OB
2°	Politique pratique de sécurité en cas de catastrophe	5	OB
2°	Mettre en œuvre des politiques de sécurité physique et environnementale dans l'entreprise	5	OB
2°	Politiques de communications sécurisées dans l'entreprise	5	OB
2°	Aspects organisationnels de la politique de sécurité de l'information	5	OB

Dr Pedro Navarro Illana
Recteur

tech Global University

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

tech Euromed University

Mastère Spécialisé Avancé

Haute Direction en Cybersécurité (CISO, Chief Information Security Officer)

- Modalité: **en ligne**
- Durée: **2 ans**
- Qualification: **TECH Euromed University**
- Accréditation: **120 ECTS**
- Horaire: **à votre rythme**
- Examens: **en ligne**

Mastère Spécialisé Avancé

Haute Direction en Cybersécurité (CISO, Chief Information Security Officer)

tech Euromed University