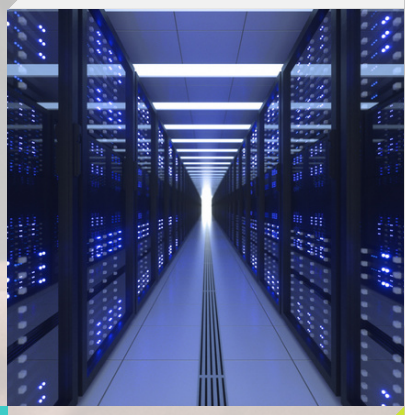
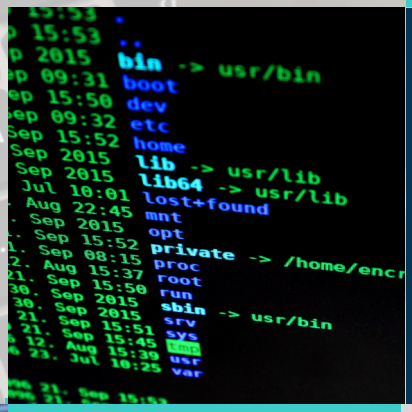
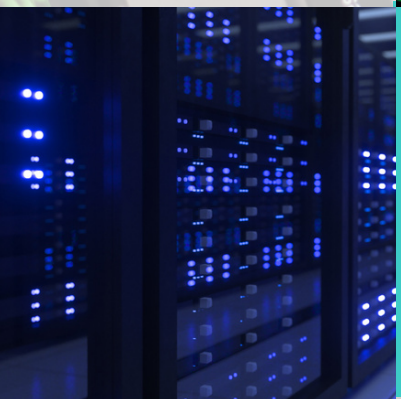
MAÎTRISER LA CYBERSÉCURITÉ

FORMATION CERTIFIANTE



VENUS CONSULTING





Objectifs et contexte de la certification

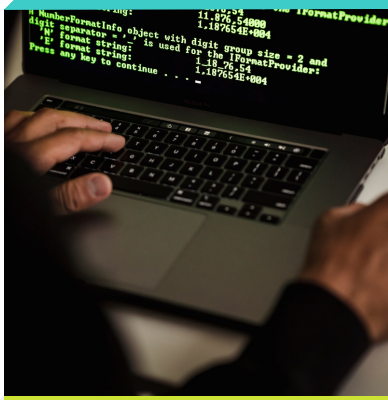
- La certification "Maîtriser la cybersécurité" permet au candidat de garantir sa trajectoire de carrière grâce à des compétences très recherchées par les entreprises.
- Cette certification contribue ainsi à l'amélioration de l'employabilité du candidat dans un domaine en pleine expansion, et lui permet de renforcer ses compétences en cybersécurité.
- Étant donné que les compétences acquises par le candidat, peuvent être transférées d'un secteur d'activité ou d'une entreprise à l'autre, cela augmentera la mobilité professionnelle du candidat ayant obtenu la certification.

Valeur ajoutée pour les entreprises du secteur privé ou du secteur public

Les bases de données informatiques sont sensibles aux attaques et peuvent être accessibles par n'importe qui. Dans contexte, les entreprises doivent être préparé à ces menaces et doivent connaitre leur niveau de sécurité.

Cette formation, permet de subvenir au manque considérable de ressources humaines à même de comprendre la cybersécurité et les risques que peuvent encourir les entreprises, avec ou sans connexion réseau.

Durant ce parcours, le candidat étudiera les types d'attaques menées par les pirates pour voler des informations personnelles, escroquer des individus et des entreprises, ou contrôler une machine à distance. Le candidat apprendra comment fonctionne un virus et comment les hackers manipulent leurs victimes avec des techniques d'ingénierie sociale.



À l'issue du parcours, le candidat sera en mesure de protéger des données à l'aide des moyens techniques et des bonnes pratiques de sécurité informatique.
Le candidat apprendra à protéger les données d'une entreprise des cybercriminels, en mettant en place des mesures techniques et organisationnelles appropriées, et en les gérant correctement.
Le candidat apprendra à comprendre les enjeux de la cybersécurité afin de prémunir une entreprise des risques et bâtir une vraie stratégie de gouvernance.

Durant ce parcours, le candidat sera amené à réfléchir sur différente problématiques liées aux risques et aux menaces. Pour cela seron des moyens pour mettre en place une gouvernance efficace de cybersécurité, ainsi que les éléments de base nécessaires à compréhension des aspects techniques.

VENUS CONSULTING

PROGRAMME

VENUS CONSULTING

4 thématiques

1. Les fondements de la sécurité informatique et de la cybersécurité

2. Découvrir la cryptographie et la sécurité des réseaux

3. La sécurité des applications et des protocoles réseau

4. Cybersécurité et gouvernance

Modalités d'évaluation

VENUS CONSULTING

1. Les fondements de la sécurité informatique et de la cybersécurité

a) Réaliser un état des lieux de la cybersécurité

- Définir la cybersécurité
- Saisir l'ampleur de la cybercriminalité
- Comprendre que tout le monde est une cible
- Mesurer la sensibilité des accès publics
- Appréhender la menace interne

b) Évaluer les menaces des malwares

- Aborder la contamination par un malware
- Avoir une vue globale des différents malwares
- Comprendre les caractéristiques des virus
- Définir les vers
- Evaluer les dangers des ransomwares et des cryptolocker
- Observer le comportement d'un poste infecté par un cryptolocker
- Définir les trojans et les spywares
- Comprendre les botnets
- Aborder le fonctionnement du botnet Umbra
- Lutter contre les idées préconçues

c) Comprendre l'ingénierie sociale

- Evaluer la menace critique
- Comprendre le processus de prise de décision
- Biaiser la prise de décision
- Comprendre et détecter le phishing
- Examiner les bases d'une attaque social ingineering
- Aborder l'ingénierie sociale sur les applications mobiles

d) Protéger son poste de travail et suivre les bonnes pratiques

- Comprendre un antivirus et choisir une solution
- Découvrir les fonctions supplémentaires et comparer les solutions
- Comprendre l'utilité d'un firewall
- Mesurer l'intérêt du multisession et des permissions
- Protéger son poste physique à l'aide de la virtualisation
- Gérer des identifiants et des mots de passes
- Comprendre les attaques sur les mots de passe
- Mieux gérer et renforcer l'authentification
- Mettre en place un coffre-fort en ligne bien sécurisé

2. Découvrir la cryptographie et la sécurité des réseaux

Lab virtuel

a) Introduction
- S'initier au prérequis
- Mettre en place le Lab

b) Définir la sécurité des réseaux
- Découvrir les CIA
- Comprendre les attaques réseau
- Visualiser une démonstration du MITM
- Découvrir les protocoles de sécurité réseau
- S'initier à la cryptographie
- Définir la cryptographie moderne
- Aborder le protocole Secure Socket Layer
- Effectuer une analyse protocolaire
- Prendre en main les certificats électroniques

c) Découvrir le chiffrement symétrique
- Définir le chiffrement symétrique
- Aborder l'algorithme AES
- Comprendre la cryptanalyse

d) Découvrir le chiffrement asymétrique et la signature digitale
- Définir le chiffrement asymétrique
- Utiliser le chiffrement asymétrique au niveau du Lab
- Comprendre les PKI

e) Définir le hachage
- Mettre en place l'algorithme de hachage
- Utiliser l'algorithme de hachage dans un Lab
- Exploiter les rainbow tables
- Surveiller les attaques sur les mots de passe

f) Sécuriser les e-mails
- Sécuriser les échanges par e-mail
- Mettre en place un protocole PGP

g) Découvrir la stéganographie
- Explorer les techniques de stéganographie
- Appliquer la stéganographie dans le Lab

3. La sécurité des applications et des protocoles réseau

Laboratoire de simulation

a) Contrôler les applications et les services disponibles sur le réseau

- Mettre en place le lab
- Comprendre la notion de port
- Identifier des machines sur le réseau avec un scanner de ports
- Scanner un serveur avec Nmap
- Découvrir les fonctions avancés de Nmap
- Utiliser le scanner SPARTA
- Utiliser un moteur de recherche spécialisé
- Comprendre l'origine des vulnérabilités
- Rechercher des vulnérabilités sur un service découvert
- Etudier les failles potentielles d'un serveur avec OpenVAS
- Eviter les configurations par défaut
- Comprendre un service protégé par des identifiants trop faibles

b) Comprendre les attaques sur les protocoles réseau

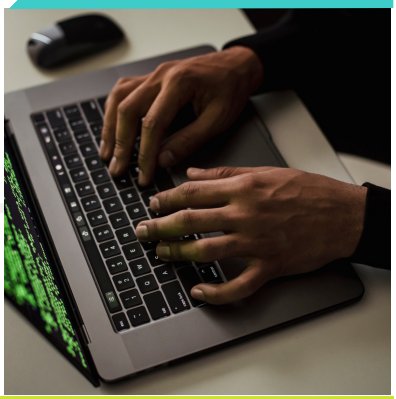
- Comprendre le principe de l'attaque de l'homme du milieu
- Étudier le fonctionnement du protocole ARP et de l'attaque ARP poisoning
- Compromettre une communication via une attaque MITM
- Empêcher les attaques d'empoisonnement de cache ARP
- Réduire les impacts d'une attaque MITM réussie
- Étudier le fonctionnement du DNS et des noms de domaine
- Comprendre les attaques d'empoisonnement de cache sur le DNS
- Comprendre les attaques d'usurpation sur le DNS
- Se protéger des attaques sur le DNS
- Comprendre les attaques basées sur des serveurs DHCP pirates
- Aborder un scénario typique d'attaque sur le DHCP
- Illustrer une attaque par rogue DHCP server

3. La sécurité des applications et des protocoles réseau (suite)

Laboratoire de simulation

c) Exploiter les vulnérabilié au niveau applicatif

- Attaquer une application par débordement de tampon
- Comprendre le danger des failles zero day
- Recenser les types d'injections de code sur une application
- Intercepter une session web et modifier des variables envoyées
- Illustrer un buffer overflow pour compromettre une application web
- Découvrir le framework Metasploit
- Automatiser la recherche et l'exploitation de vulnérabilités avec Armitage
- Rechercher des vulnérabilités sur une cible déterminée
- Exploiter une vulnérabilité spécifique sur une plateforme VPN SSL



4. Cybersécurité et gouvernance

a) Comprendre les concepts clés de la cybersécurité

- Aborder les notions de besoins de sécurité de l'information
- Comprendre ce qu'est un risque et comment le traiter
- Adopter une approche par les risques
- Défendre en profondeur

b) Mesurer les nouveaux défis de la cybersécurité

- Identifier les vecteurs d'attaque les plus utilisés
- Découvrir les risques les plus critiques
- Comprendre les motivations des attaquants
- Évaluer le facteur humain dans la gestion des risques
- Définir le rôle de la direction dans la gouvernance de la cybersécurité

c) Étudier les normes et les standards pour la cybersécurité et la gouvernance

- Avoir une vue d'ensemble du framework du NIST
- Renforcer la sécurité de l'information avec la norme ISO 27001
- Gérer la sécurité de l'information avec COBIT

d) Sensibiliser à la cybersécurité

- Définir un programme de sensibilisation
- Choisir les cibles et identifier les objectifs à atteindre
- S'outiller pour mieux sensibiliser

e) Aborder les enjeux économiques et règlementaires

- Comprendre l'impact de la cybersécurité sur la performance d'une entreprise
- Intégrer la cybersécurité dans des processus de due diligence et de M&A
- Intégrer la cybersécurité dans une entreprise vitale pour un État
- Utiliser la cybersécurité dans le cadre de la conformité au RGPD

Modalités d'évaluation

1) Évaluation écrite individuelle (durée 6 heures)
Épreuves : Mise en situation, simulation au sein d'une entreprise (du secteur privé ou du secteur public), il est demandé au candidat de réaliser un état des lieux de la cybersécurité et d'évaluer les menaces des malwares.

2) Evaluation individuelle orale devant jury (durée 1 heure)
Le candidat doit réaliser une présentation devant les membres du jury, oralement avec l'aide d'un support visuel (exemple PowerPoint)

VENUS CONSULTING

VENUS CONSULTING

Téléphone : 09 72 63 83 89
E-mail : contact@venusconsulting.fr

97, rue Sauveur Tobelem
13007 Marseille

www.venusconsulting.fr