E. Dupuis - SEC101 - Quiz generated LaTeX's moodle (v1.0, 2023/01/28). Import the derived file `QUIZZ-EXAM-SEC101-moodle.xml` on Moodle.

SEC101 PACK 2024 Questions

(1) **Sécurité des Systèmes d'Information** tags: `M1Sec101`, `Risques`

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la première étape du processus de gestion des risques en sécurité de l'information ?

a. Analyse des menaces
b. Identification des actifs
c. Évaluation des vulnérabilités
d. Identification des risques ✓

(2) **Politiques de Sécurité** tags: `M2Sec101`, `PSSI`

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle politique de sécurité définit les règles de base pour l'utilisation des ressources informatiques d'une organisation ?

a. Politique d'utilisation acceptable ✓
b. Politique de cryptographie
c. Politique de pare-feu
d. Politique de sauvegarde

(3) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale menace à la sécurité liée à l'ingénierie sociale ?

a. Malware
b. Manipulation psychologique ✓
c. Attaque par déni de service (DDoS)
d. Vol de données

(4) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel composant d'un pare-feu est responsable de la vérification des paquets de données entrants et sortants ?

a. Filtre de paquets ✓
b. Processeur principal
c. Antivirus intégré
d. Répartiteur de charge

(5) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle norme de sécurité définit les exigences pour la gestion des informations sensibles par les organisations ?

a. ISO 9001
b. ISO 14001
c. ISO 27001 ✓
d. ISO 22000

(6) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale fonction d'une politique de pare-feu ?

a. Gérer les identités des utilisateurs
b. Gérer les mises à jour logicielles
c. Contrôler le trafic réseau ✓
d. Gérer les politiques de sauvegarde

(7) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle méthode de cryptographie utilise une clé publique et une clé privée pour chiffrer et déchiffrer les données ?

a. Cryptographie asymétrique ✓
b. Cryptographie symétrique
c. Cryptographie par transposition
d. Cryptographie quantique

(8) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle technologie est utilisée pour authentifier un utilisateur en utilisant des empreintes digitales, des iris ou des caractéristiques biométriques similaires ?

a. Biométrie ✓
b. Token d'authentification
c. Mot de passe
d. Carte à puce

(9) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la meilleure pratique pour se prémunir contre les attaques par phishing ?

a. Utiliser un pare-feu
b. Sensibiliser les employés à la sécurité ✓
c. Activer la détection d'intrusion
d. Mettre en place un VPN

(10) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle politique de sécurité définit les règles de stockage, de gestion et de protection des mots de passe ?

a. Politique de gestion des mots de passe ✓
b. Politique de pare-feu
c. Politique de cryptographie
d. Politique d'utilisation acceptable

(11) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel type d'attaque vise à saturer un réseau ou un service en submergeant de trafic malveillant ?

a. Attaque de phishing
b. Attaque par injection SQL
c. Attaque par déni de service distribué (DDoS)
d. Attaque par déni de service (DoS) ✓

(12) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel dispositif de sécurité est conçu pour empêcher les intrusions non autorisées en surveillant le trafic réseau et en bloquant les menaces potentielles ?

a. IDS (Système de Détection d'Intrusion) ✓
b. Antivirus
c. Firewall
d. VPN

(13) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle couche du modèle OSI est principalement responsable de la sécurité des données en transit ?

a. Couche application ✓
b. Couche transport
c. Couche liaison de données
d. Couche réseau ✓

(14) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle politique de sécurité permet de spécifier les niveaux d'accès aux ressources informatiques en fonction des rôles des utilisateurs ?

a. Politique de sauvegarde
b. Politique de contrôle d'accès ✓
c. Politique de cryptographie
d. Politique d'utilisation acceptable

(15) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale menace associée aux logiciels malveillants qui chiffrent les fichiers d'un utilisateur et demandent une rançon pour les déverrouiller ?

a. Ransomware ✓
b. Spyware
c. Adware
d. Worm

(16) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel composant réseau est utilisé pour segmenter un réseau en zones isolées afin de limiter la propagation des menaces ?

a. Routeur
b. Commutateur
c. Pare-feu de zone ✓
d. Répéteur

(17) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle méthode de chiffrement convertit chaque caractère individuellement dans un message en un caractère chiffré ?

a. Chiffrement de flux
b. Chiffrement par substitution ✓
c. Chiffrement de bloc
d. Chiffrement asymétrique

(18) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle action est recommandée pour une politique de sécurité en cas de perte ou de vol d'un dispositif mobile contenant des données sensibles ?

a. Ignorer la situation
b. Révoquer les privilèges d'accès aux utilisateurs
c. Signaler immédiatement la perte ou le vol ✓
d. Effectuer une sauvegarde des données

(19) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel type d'attaque tente d'exploiter les faiblesses connues dans les logiciels ou les systèmes pour prendre le contrôle de ces derniers ?

a. Attaque de phishing
b. Attaque par déni de service (DDoS)
c. Attaque par ingénierie sociale
d. Exploitation de vulnérabilités ✓

(20) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle technologie est utilisée pour surveiller en temps réel le trafic réseau à la recherche de comportements suspects ou malveillants ?

a. SIEM (Security Information and Event Management) ✓
b. Antivirus
c. Pare-feu
d. VPN

(21) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est l'objectif principal d'un système de gestion des identités (IdM) ?

a. Gérer les autorisations et l'authentification des utilisateurs ✓
b. Gérer les mises à jour logicielles
c. Surveiller le trafic réseau
d. Effectuer des analyses de vulnérabilité

(22) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel type de politique de sécurité spécifie les règles concernant le stockage, l'accès et la distribution des informations classifiées ?

a. Politique de contrôle d'accès
b. Politique de pare-feu
c. Politique de classification de l'information ✓
d. Politique de chiffrement

(23) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la meilleure pratique pour se protéger contre les attaques par force brute visant les mots de passe ?

a. Utiliser un pare-feu robuste
b. Ne pas utiliser de mots de passe
c. Utiliser des mots de passe forts et un mécanisme de verrouillage après plusieurs tentatives infructueuses ✓
d. Activer la détection d'intrusion

(24) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle technologie permet de masquer l'adresse IP réelle d'un dispositif en la remplaçant par une adresse IP publique ?

a. VPN
b. IDS
c. NAT (Network Address Translation) ✓
d. Pare-feu

(25) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle norme de sécurité est spécifiquement conçue pour protéger les informations de santé des patients dans le secteur de la santé ?

a. ISO 9001
b. HIPAA (USA)(Health Insurance Portability and Accountability Act) ou ISO 27799(Europe) ✓
c. ISO 27001
d. GDPR (General Data Protection Regulation)

(26) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la première étape dans la gestion d'une violation de données ?

a. Notifier les autorités gouvernementales
b. Identifier la source de la violation et la contenir ✓
c. Communiquer immédiatement à tous les employés
d. Engager une équipe de sécurité externe

(27) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale menace pour la sécurité des objets connectés (IoT) ?

a. Attaques par déni de service (DDoS)
b. Manque de mise à jour des logiciels et des micrologiciels ✓
c. Phishing ciblé
d. Utilisation de mots de passe forts

(28) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle méthode de chiffrement utilise une seule clé pour chiffrer et déchiffrer les données ?

a. Cryptographie symétrique ✓
b. Cryptographie asymétrique
c. Cryptographie par substitution
d. Cryptographie par transposition

(29) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel type d'attaque vise à tromper les utilisateurs en leur faisant croire qu'ils interagissent avec un site web légitime alors qu'il s'agit d'une fausse copie ?

a. Attaque de force brute
b. Attaque par déni de service (DDoS)
c. Attaque de phishing ✓
d. Attaque par injection SQL

(30) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle politique de sécurité spécifie les règles pour la gestion des certificats numériques utilisés dans les communications sécurisées ?

a. Politique de gestion des certificats ✓
b. Politique de contrôle d'accès
c. Politique de chiffrement
d. Politique de classification de l'information

(31) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel terme désigne une technique visant à vérifier l'authenticité d'un utilisateur en demandant quelque chose qu'il sait (comme un mot de passe) et quelque chose qu'il possède (comme un smartphone) ?

a. Authentification à deux facteurs ✓
b. Authentification biométrique
c. Authentification unique (SSO)

(32) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle politique de sécurité concerne la surveillance et la gestion des journaux d'activité pour détecter les incidents de sécurité ?

a. Politique de gestion des journaux (log) ✓
b. Politique de cryptographie
c. Politique de contrôle d'accès
d. Politique de pare-feu

(33) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle technique de sécurité permet de cacher les données sensibles dans un fichier ou un message sans altérer son apparence externe ?

a. Chiffrement asymétrique
b. Cryptographie par substitution
c. Stéganographie ✓
d. Vigenère cipher

(34) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel mécanisme de sécurité permet de garantir que les données n'ont pas été modifiées en transit entre l'expéditeur et le destinataire ?

a. Intégrité des données ✓
b. Confidentialité des données
c. Disponibilité des données
d. Authentification des données

(35) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel protocole de sécurité réseau est couramment utilisé pour établir des connexions VPN sécurisées ?

a. IPsec ✓
b. SSH
c. HTTP
d. RDP

(36) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale raison de l'application de mises à jour de sécurité régulières sur un système ?

a. Améliorer les performances
b. Ajouter de nouvelles fonctionnalités
c. Réduire les coûts d'exploitation
d. Corriger les vulnérabilités connues ✓

(37) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la méthode la plus courante pour protéger un réseau sans fil (Wi-Fi) contre les accès non autorisés ?

a. Chiffrement par substitution
b. Pare-feu de zone

c. Chiffrement WPA/WPA2 ✓
d. Biométrie

(38) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel type de pare-feu permet de surveiller le trafic entrant et sortant en analysant son contenu pour détecter les menaces ?

a. Pare-feu de zone
b. Pare-feu d'application
c. Pare-feu de nouvelle génération (NGFW) ✓
d. Pare-feu d'état

(39) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle méthode de sécurité consiste à rendre illisible une information en la transformant en un format inintelligible, réversible uniquement avec une clé de déchiffrement ?

a. Stéganographie
b. Chiffrement ✓
c. Biométrie
d. Token d'authentification

(40) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle politique de sécurité se concentre sur la définition des procédures et des responsabilités en cas d'incident de sécurité majeur ?

a. Politique de contrôle d'accès
b. Politique de sauvegarde
c. Politique de gestion des incidents de sécurité ✓
d. Politique de pare-feu

(41) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle mesure de sécurité consiste à supprimer complètement l'accès aux ressources d'un utilisateur lorsqu'il quitte une organisation ou un projet ?

a. Décommissionnement du compte ✓
b. Réinitialisation du mot de passe
c. Changement du nom d'utilisateur
d. Mise en quarantaine du compte

(42) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel type de pare-feu examine le trafic réseau à la recherche de comportements anormaux et peut prendre des mesures en temps réel pour bloquer les menaces ?

a. Pare-feu d'état
b. Pare-feu de zone
c. Pare-feu d'application
d. Pare-feu comportemental (BFW) ✓

(43) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle mesure de sécurité consiste à conserver une copie identique des données à un instant donné pour une éventuelle restauration en cas de perte de données ?

a. Sauvegarde ✓
b. Cryptographie
c. Archivage
d. Désactivation du compte

(44) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel concept de sécurité informatique vise à minimiser les risques en distribuant les ressources et les données sur plusieurs serveurs ou emplacements géographiques ?

a. Redondance ✓

b. Pare-feu
c. Authentification unique (SSO)
d. Chiffrement

(45) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle technique de protection de réseau identifie et isole automatiquement les appareils non conformes ou malveillants ?

a. Cryptographie quantique
b. Network Access Control (NAC) ✓
c. SIEM (Security Information and Event Management)
d. Pare-feu d'application

(46) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel type d'attaque consiste à intercepter et à détourner les communications entre deux parties pour les espionner ?

a. Attaque par déni de service (DoS)
b. Attaque de l'homme du milieu (Man-in-the-Middle) ✓
c. Attaque par injection SQL
d. Attaque par force brute

(47) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale raison de la mise en uvre de la gestion des identités et des accès (IAM) ?

a. Améliorer les performances du réseau
b. Réduire les coûts d'exploitation
c. Gérer les droits d'accès des utilisateurs ✓
d. Protéger les données sensibles

(48) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale raison de l'application de la politique de chiffrement des données ?

a. Contrôler l'accès aux ressources informatiques
b. Surveiller les journaux d'activité
c. Protéger la confidentialité des données ✓
d. Appliquer des mises à jour de sécurité

(49) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle technologie de sécurité vise à identifier les modèles de comportement suspects ou malveillants dans le trafic réseau ?

a. Antivirus
b. Analyse comportementale ✓
c. Pare-feu de nouvelle génération (NGFW)
d. Chiffrement WPA/WPA2

(50) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale fonction d'un proxy en matière de sécurité informatique ?

a. Filtrer et contrôler le trafic réseau ✓
b. Établir des connexions VPN
c. Analyser les journaux d'activité
d. Surveiller les vulnérabilités du système

(51) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle mesure de sécurité permet de s'assurer qu'un utilisateur a l'autorisation d'accéder à une ressource spécifique ?

a. Contrôle d'intégrité
b. Contrôle d'accès ✓
c. Contrôle de flux
d. Contrôle de routage

(52) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle politique de sécurité définit les règles et procédures pour la protection des informations sensibles lors de leur transmission par voie électronique ?

a. Politique de cryptographie
b. Politique de sauvegarde
c. Politique de sécurité des communications ✓
d. Politique d'utilisation acceptable

(53) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale mesure de sécurité pour empêcher l'accès non autorisé à un réseau sans fil (Wi-Fi) ?

a. VPN (Virtual Private Network)
b. Pare-feu de nouvelle génération (NGFW)
c. Chiffrement WPA3 ✓
d. Filtrage MAC

(54) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est l'objectif principal de la sécurité périmétrique d'un réseau ?

a. Protéger les données en transit
b. Contrôler l'accès aux données
c. Assurer la redondance des serveurs
d. Empêcher les menaces d'atteindre le réseau interne ✓

(55) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle technologie de sécurité permet de suivre les activités des utilisateurs et des systèmes afin de détecter les comportements anormaux ?

a. Pare-feu d'application
b. Chiffrement par substitution
c. SIEM (Security Information and Event Management) ✓
d. VPN (Virtual Private Network)

(56) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle politique de sécurité traite des procédures à suivre pour déclasser, détruire ou archiver des informations sensibles en fin de vie ?

a. Politique de gestion des mots de passe
b. Politique de sauvegarde
c. Politique de gestion de la fin de vie des données ✓
d. Politique de cryptographie

(57) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale menace liée aux attaques de type "zero-day" ?

a. L'absence de correctif de sécurité disponible ✓
b. L'absence de surveillance de sécurité
c. La lenteur des réponses aux incidents
d. L'absence de pare-feu

(58) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel mécanisme de sécurité permet de confirmer l'identité d'un utilisateur avant de lui accorder l'accès à un système ou à des données ?

a. Chiffrement des données
b. Authentification ✓
c. Contrôle d'intégrité
d. Chiffrement par substitution

(59) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la première étape du processus de gestion des incidents de sécurité ?

a. Détection de l'incident ✓

b. Analyse des causes profondes
c. Réponse immédiate à l'incident
d. Rapport de l'incident

(60) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle politique de sécurité concerne l'utilisation des clés de chiffrement, leur stockage et leur gestion ?

a. Politique de gestion des mots de passe
b. Politique de sauvegarde
c. Politique de gestion de la fin de vie des données
d. Politique de gestion des clés de chiffrement ✓

(61) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel terme désigne le processus de vérification de l'identité d'un utilisateur, généralement à l'aide d'un nom d'utilisateur et d'un mot de passe ?

a. Authentification ✓
b. Autorisation
c. Audit
d. Attribution

(62) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle technologie permet de créer un réseau privé virtuel (VPN) en utilisant une connexion sécurisée sur un réseau public, comme Internet ?

a. Commutateur Ethernet
b. Pare-feu de zone
c. Tunnel VPN (Virtual Private Network) ✓
d. Routeur sans fil

(63) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale menace associée à l'ingénierie inversée dans le domaine de la sécurité informatique ?

a. Divulgation de données
b. Perte de disponibilité
c. Perte de la confidentialité ✓
d. Perte d'intégrité

(64) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle politique de sécurité traite de la façon dont les données sensibles doivent être stockées, protégées et détruites à la fin de leur durée de vie utile ?

a. Politique de gestion des incidents de sécurité
b. Politique de contrôle d'accès
c. Politique de gestion de la confidentialité des données ✓
d. Politique de sauvegarde

(65) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est l'objectif principal d'un pare-feu d'application Web (WAF) ?

a. Bloquer les attaques de phishing
b. Contrôler l'accès aux données
c. Protéger les applications Web contre les vulnérabilités et les attaques ✓
d. Filtrer le trafic réseau

(66) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale mesure de sécurité pour protéger les systèmes contre les virus informatiques et les logiciels malveillants ?

a. Authentification à deux facteurs
b. Chiffrement des données
c. Logiciels antivirus ✓
d. Firewall d'application

(67) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est le rôle principal d'un proxy dans une architecture réseau sécurisée ?

a. Chiffrement des données
b. Faire office de mandataire (Intermédiaire) entre les utilisateurs et les ressources sur Internet ✓
c. Authentification des utilisateurs
d. Détection d'intrusion

(68) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle politique de sécurité concerne la classification et l'étiquetage des informations en fonction de leur sensibilité ?

a. Politique de gestion des incidents de sécurité
b. Politique de classification des données ✓
c. Politique de pare-feu
d. Politique de contrôle d'accès

(69) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle technologie de sécurité est conçue pour protéger un réseau local (LAN) contre les accès non autorisés de l'extérieur ?

a. VPN (Virtual Private Network)
b. IDS (Système de Détection d'Intrusion)
c. Pare-feu ✓
d. SIEM (Security Information and Event Management)

(70) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale menace associée à une attaque de type "man-in-the-middle" ?

a. Perte de disponibilité

b. Perte de la confidentialité
c. Altération des données en transit ✓

(71) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale menace pour la sécurité des informations stockées sur des supports physiques tels que des disques durs ou des clés USB perdus ou volés ?

a. Attaque de phishing
b. Attaque par déni de service (DDoS)
c. Attaque par ingénierie sociale
d. Perte ou vol de données ✓

(72) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel type de dispositif de sécurité inspecte le trafic réseau à la recherche de signatures de logiciels malveillants connus ?

a. IDS (Système de Détection d'Intrusion) ✓
b. Pare-feu d'application
c. VPN (Virtual Private Network)
d. Pare-feu de zone

(73) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle politique de sécurité définit les règles pour garantir la disponibilité et l'accès continu aux données en cas de catastrophe ?

a. Politique de contrôle d'accès
b. Politique de sauvegarde
c. Politique de continuité des activités (PCA) ✓
d. Politique de cryptographie

(74) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel type d'attaque informatique vise à perturber ou à détruire délibérément des systèmes informatiques ou des réseaux ?

a. Attaque par injection SQL
b. Attaque de phishing
c. Attaque par déni de service distribué (DDoS) ✓

(75) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel processus permet de rendre les données lisibles uniquement pour des utilisateurs autorisés, tout en empêchant les utilisateurs non autorisés d'y accéder ?

a. Authentification
b. Chiffrement
c. Biométrie
d. Contrôle d'accès ✓

(76) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle technologie permet de créer un réseau privé virtuel sécurisé en utilisant une connexion Internet publique ?

a. SIEM (Security Information and Event Management)
b. IDS (Système de Détection d'Intrusion)
c. VPN (Virtual Private Network) ✓
d. Pare-feu de nouvelle génération (NGFW)

(77) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle politique de sécurité définit les règles pour l'utilisation des médias sociaux au sein de l'entreprise ?

a. Politique de contrôle d'accès
b. Politique de gestion de la fin de vie des données
c. Politique des médias sociaux ✓
d. Politique de cryptographie

(78) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle mesure de sécurité consiste à diviser un réseau en segments logiques pour réduire la surface d'attaque ?

a. Chiffrement WPA/WPA2
b. Chiffrement par substitution
c. Segmentation réseau ✓
d. Authentification à deux facteurs

(79) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est le principal objectif de la sauvegarde régulière des données ?

a. Empêcher les attaques par injection SQL
b. Réduire la latence du réseau
c. Assurer la récupération des données en cas de perte ou de panne ✓
d. Renforcer le pare-feu

(80) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel protocole réseau est couramment utilisé pour sécuriser les communications entre un client et un serveur web ?

a. SSH (Secure Shell)
b. HTTPS (Hypertext Transfer Protocol Secure) ✓
c. FTP (File Transfer Protocol)
d. SMTP (Simple Mail Transfer Protocol)

(81) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle technologie permet de surveiller et de filtrer le trafic réseau pour détecter et bloquer les menaces en temps réel ?

a. IDS/IPS (Système de Détection et de Prévention des Intrusions) ✓
b. Pare-feu d'application
c. VPN (Virtual Private Network)
d. SIEM (Security Information and Event Management)

(82) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle politique de sécurité définit les règles concernant l'utilisation des ressources informatiques pendant les heures de travail ?

a. Politique de cryptographie
b. Politique de sauvegarde
c. Politique de gestion de la fin de vie des données
d. Politique de gestion du temps de travail sur les ordinateurs ✓

(83) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale menace associée aux attaques par hameçonnage (phishing) ?

a. Vol d'informations sensibles ✓
b. Corruption des fichiers système
c. Perte de connectivité réseau
d. Attaque par déni de service (DDoS)

(84) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle technologie est utilisée pour identifier les utilisateurs en se basant sur des caractéristiques physiques uniques, comme l'empreinte digitale ou l'iris ?

a. Authentification à deux facteurs
b. Token d'authentification
c. Biométrie ✓
d. Chiffrement asymétrique

(85) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle mesure de sécurité garantit que les données sont accessibles uniquement par des personnes autorisées et que leur contenu n'est pas modifié en transit ?

a. Chiffrement par substitution
b. Pare-feu de zone
c. Intégrité des données ✓
d. Authentification à deux éléments

(86) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle politique de sécurité définit les règles pour l'utilisation appropriée des équipements informatiques appartenant à l'entreprise ?

a. Politique de gestion des clés de chiffrement
b. Politique de cryptographie
c. Politique d'utilisation acceptable des équipements ✓
d. Politique de gestion de la fin de vie des données

(87) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle technique de sécurité consiste à tromper un attaquant en lui fournissant de fausses informations pour le détourner de la véritable cible ?

a. Leurre (Honeypot) ✓
b. Filtrage MAC
c. VPN (Virtual Private Network)
d. Chiffrement WPA3

(88) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel mécanisme de sécurité permet de garantir que l'expéditeur d'un message électronique est bien la personne qu'il prétend être ?

a. Chiffrement des données
b. Authentification à deux facteurs
c. Contrôle d'accès
d. Signature électronique ✓

(89) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle technologie permet de stocker les mots de passe de manière sécurisée en les transformant en une séquence aléatoire de caractères ?

a. Biométrie
b. Authentification à deux éléments
c. Hachage de mots de passe ✓
d. Chiffrement de fichiers

(90) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle politique de sécurité définit les procédures à suivre en cas de violation de la sécurité des données personnelles des clients ?

a. Politique de gestion des incidents de sécurité
b. Politique de cryptographie
c. Politique de notification de violation de données ✓
d. Politique de contrôle d'accès

(91) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel type d'attaque consiste à intercepter et à enregistrer le trafic réseau afin d'espionner les communications ?

a. Attaque de phishing
b. Attaque par déni de service (DDoS)
c. Attaque d'interception (sniffing) ✓
d. Attaque de ransomware

(92) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel composant réseau est conçu pour bloquer le trafic réseau non autorisé en fonction de règles prédéfinies ?

a. SIEM (Security Information and Event Management)
b. IDS (Système de Détection d'Intrusion)
c. Pare-feu ✓
d. VPN (Virtual Private Network)

(93) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle politique de sécurité définit les règles pour l'accès physique aux locaux informatiques, aux serveurs et aux équipements ?

a. Politique de gestion des mots de passe
b. Politique des médias sociaux
c. Politique de sécurité physique ✓
d. Politique de cryptographie

(94) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale caractéristique d'une attaque de type "phishing" ?

a. Elle vise à saturer un réseau de trafic malveillant
b. Elle consiste à détruire physiquement les systèmes informatiques
c. Elle cherche à tromper les victimes en se faisant passer pour une source de confiance ✓
d. Elle exploite des vulnérabilités logicielles connues

(95) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel mécanisme de sécurité permet de garantir l'intégrité des données en vérifiant si elles ont été altérées pendant le transport ?

a. Chiffrement asymétrique
b. Authentification à deux facteurs
c. Fonction de hachage (hash) ✓
d. Authentification biométrique

(96) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle technologie de sécurité est utilisée pour empêcher les programmes malveillants d'accéder à certaines ressources du système ?

a. IDS (Système de Détection d'Intrusion)

b. SIEM (Security Information and Event Management)
c. VPN (Virtual Private Network)
d. Contrôle d'accès aux applications ✓

(97) **Politiques de Sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle politique de sécurité traite des procédures pour la gestion des certificats numériques ?

a. Politique de sauvegarde
b. Politique de gestion de la fin de vie des données
c. Politique de gestion des certificats ✓
d. Politique de cryptographie

(98) **Cybersécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle mesure de sécurité implique la création de copies de données et leur stockage hors site pour la récupération en cas de sinistre ?

a. Authentification forte
b. Sauvegarde et récupération des données ✓
c. Chiffrement de bout en bout
d. Contrôle d'accès

(99) **Sécurité des Systèmes d'Information**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale menace associée à l'utilisation de mots de passe faibles ou faciles à deviner ?

a. Attaque de phishing
b. Attaque par injection SQL
c. Attaque par déni de service (DDoS)
d. Attaque par force brute ✓

(100) **Architectures de Sécurité Informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel type de pare-feu permet de prendre des décisions basées sur l'état actuel des connexions réseau, plutôt que sur des règles statiques ?

a. Pare-feu d'application
b. Pare-feu de zone
c. VPN (Virtual Private Network)
d. Pare-feu d'état ✓

(101) **Vulnérabilités informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une vulnérabilité informatique ?

a. Une attaque contre les données
b. Un logiciel antivirus
c. Une faiblesse dans un système qui peut être exploitée ✓
d. Une méthode de chiffrement

(102) **Vulnérabilités informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel type de vulnérabilité est généralement corrigé par un correctif de sécurité ?

a. Vulnérabilité physique
b. Vulnérabilité humaine
c. Vulnérabilité logicielle ✓
d. Vulnérabilité matérielle

(103) **Vulnérabilités informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une analyse de vulnérabilité ?

a. Une attaque ciblée
b. L'évaluation des faiblesses potentielles dans un système ✓
c. Le chiffrement des données sensibles
d. La gestion des incidents de sécurité

(104) **Vulnérabilités informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est le rôle d'un scanner de vulnérabilités ?

a. Identifier et rapporter les vulnérabilités dans un système ✓

b. Défendre contre les attaques DDoS
c. Chiffrer les communications réseau
d. Gérer les identités utilisateur

(105) **Vulnérabilités informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale raison de la présence de vulnérabilités dans les systèmes informatiques ?

a. Manque de pare-feu
b. Complexité des logiciels et des systèmes ✓
c. Faible utilisation de l'authentification à deux facteurs
d. Trop de correctifs de sécurité

(106) **Vulnérabilités informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une menace informatique ?

a. Un événement ou une situation potentiellement nuisible pour les systèmes informatiques ✓
b. Une mise à jour logicielle
c. Un certificat SSL
d. Un programme antivirus

(107) **Vulnérabilités informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est le principal objectif d'une menace informatique de type "ransomware" ?

a. Chiffrer les données de la victime et demander une rançon ✓
b. Dérober des informations confidentielles
c. Détecter les vulnérabilités dans un système
d. Corrompre les fichiers système

(108) **Vulnérabilités informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la caractéristique commune des attaques de type "phishing" ?

a. L'utilisation de l'ingénierie sociale pour tromper les utilisateurs ✓
b. L'exploitation de failles logicielles
c. La diffusion de logiciels malveillants par courriel
d. L'effacement de données sensibles

(109) **Vulnérabilités informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un attaquant "hacker" ?

a. Un employé de sécurité informatique
b. Une personne qui exploite des failles de sécurité pour accéder illégalement à un système ✓
c. Un utilisateur légitime du réseau
d. Un concepteur de logiciels

(110) **Vulnérabilités informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale motivation derrière les attaques informatiques ?

a. Curiosité
b. Génération de profit financier ✓
c. Amélioration des compétences techniques
d. Amélioration de la réputation en ligne

(111) **Computer Emergency Response Team**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un logiciel malveillant (malware) ?

a. Un programme informatique conçu pour causer des dommages ou compromettre la sécurité ✓
b. Un programme antivirus
c. Un outil de sauvegarde
d. Un dispositif de chiffrement

(112) **Codes malveillants**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale caractéristique d'un virus informatique ?

a. Capacité de se reproduire en infectant d'autres fichiers ✓
b. Chiffrer des données sensibles
c. Exploitation de failles de sécurité
d. Détection des vulnérabilités réseau

(113) **Codes malveillants**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un cheval de Troie (trojan) dans le contexte des codes malveillants ?

a. Un programme apparemment légitime qui contient un logiciel malveillant ✓
b. Un virus informatique
c. Un dispositif de chiffrement
d. Une attaque par déni de service (DDoS)

(114) **Codes malveillants**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est l'objectif d'un ransomware ?

a. Collecter des informations de navigation
b. Chiffrer les fichiers de la victime et demander une rançon ✓
c. Détruire physiquement le matériel informatique
d. Infecter les utilisateurs avec des publicités indésirables

(115) **Codes malveillants**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale méthode de propagation d'un ver informatique ?

a. Exploitation des vulnérabilités réseau ✓
b. Ingénierie sociale
c. Chiffrement des fichiers système
d. Utilisation de courriels frauduleux

(116) **Incidents informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un incident informatique ?

a. Une mise à jour logicielle
b. Un certificat SSL
c. Un événement qui compromet la sécurité des systèmes informatiques ✓
d. Une attaque DDoS

(117) **Incidents informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la première étape dans la gestion d'un incident informatique ?

a. Détection et identification de l'incident ✓
b. Isolation du système affecté
c. Notification des autorités
d. Analyse post-incident

(118) **Incidents informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale responsabilité d'une équipe de réponse aux incidents (IRT) ?

a. Investigation et gestion des incidents de sécurité ✓
b. Mise en uvre des politiques de sécurité
c. Maintenance des serveurs
d. Développement de logiciels sécurisés

(119) **Incidents informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une analyse post-incident ?

a. Examen et évaluation des événements survenus après un incident de sécurité ✓
b. Prévention des incidents futurs
c. Détection des vulnérabilités
d. Réponse immédiate à un incident

(120) **Incidents informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est l'objectif d'une politique de gestion des incidents ?

a. Chiffrer les données sensibles
b. Fournir des directives pour répondre efficacement aux incidents de sécurité ✓
c. Gérer les vulnérabilités du réseau
d. Analyser les journaux d'activité

(121) **Security Operation Center**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un Security Operation Center (SOC) ?

a. Un logiciel antivirus
b. Un centre qui surveille et répond aux incidents de sécurité ✓
c. Un dispositif de chiffrement
d. Un pare-feu

(122) **Security Operation Center**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est le rôle principal d'un SOC dans une organisation ?

a. Mise en uvre des politiques de sécurité
b. Gestion des identités utilisateurs
c. Surveillance continue de la sécurité et réponse aux incidents ✓
d. Maintenance des serveurs

(123) **Security Operation Center**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une alerte de sécurité dans le contexte d'un SOC ?

a. Une notification signalant une activité suspecte ou un incident de sécurité ✓
b. Un test de pénétration automatisé
c. Un rapport sur les performances du réseau
d. Une mise à jour logicielle

(124) **Security Operation Center**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale différence entre un SOC et un CERT ?

a. Un SOC se concentre sur la surveillance et la réponse aux incidents, tandis qu'un CERT se concentre sur la coordination des réponses aux incidents au niveau national ou sectoriel ✓
b. Un SOC est uniquement responsable de la gestion des vulnérabilités
c. Un CERT est une extension d'un SOC
d. Un SOC et un CERT sont des termes interchangeables

(125) **Security Operation Center**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est l'avantage d'utiliser des outils d'automatisation dans un SOC ?

a. Réduction du temps de réponse aux incidents ✓
b. Augmentation de la complexité des opérations
c. Diminution de la surveillance
d. Amélioration de la gestion des identités utilisateurs

(126) **Computer Emergency Response Team**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un Computer Emergency Response Team (CERT) ?

a. Une équipe spécialisée dans la gestion des incidents de sécurité au niveau national ou sectoriel ✓
b. Un groupe de pirates informatiques
c. Un logiciel antivirus
d. Un centre de formation en cybersécurité

(127) **Computer Emergency Response Team**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est le rôle principal d'un CERT ?

a. Maintenance des serveurs
b. Gestion des identités utilisateurs
c. Coordination des réponses aux incidents au niveau national ou sectoriel ✓
d. Mise en uvre des politiques de sécurité

(128) **Computer Emergency Response Team**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale responsabilité d'un CERT pendant une cyber-attaque majeure ?

a. Maintenance des serveurs
b. Coordination des efforts de réponse et d'information ✓
c. Développement de logiciels sécurisés
d. Mise en uvre des politiques de sécurité

(129) **Computer Emergency Response Team**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une déclaration d'incidents électroniques ?

a. Une communication formelle informant le CERT d'un incident de sécurité ✓
b. Un rapport sur les performances du réseau
c. Un test de pénétration automatisé
d. Un certificat SSL

(130) **Computer Emergency Response Team**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale différence entre un SOC et un CERT ?

a. Un SOC se concentre sur la surveillance et la réponse aux incidents, tandis qu'un CERT se concentre sur la coordination des réponses aux incidents au niveau national ou sectoriel ✓
b. Un SOC est uniquement responsable de la gestion des vulnérabilités
c. Un CERT est une extension d'un SOC
d. Un SOC et un CERT sont des termes interchangeables

(131) **Vulnérabilités informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un test d'intrusion ?

a. Un logiciel antivirus

b. Une analyse post-incident
c. Une simulation d'attaque pour identifier les vulnérabilités ✓
d. Un programme de gestion des incidents

(132) **Vulnérabilités informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est le principal facteur contribuant aux vulnérabilités logicielles ?

a. Complexité du code ✓
b. Mises à jour fréquentes
c. Utilisation d'authentification forte
d. Isolation des systèmes

(133) **Menaces informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un logiciel espion (spyware) ?

a. Un programme conçu pour collecter des informations sans le consentement de l'utilisateur ✓
b. Un dispositif de chiffrement
c. Un outil de gestion des identités
d. Une mise à jour logicielle

(134) **Menaces informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale caractéristique d'une attaque par déni de service distribué (DDoS) ?

a. Inondation d'un service en ligne par un trafic excessif ✓
b. Chiffrer des fichiers système
c. Utilisation de l'ingénierie sociale
d. Exploitation de vulnérabilités réseau

(135) **Codes malveillants**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un virus polymorphique ?

a. Un virus capable de changer son apparence pour éviter la détection ✓

b. Un cheval de Troie
c. Une alerte de sécurité
d. Un programme antivirus

(136) **Codes malveillants**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est l'objectif principal d'un ver informatique ?

a. Se propager rapidement à travers les réseaux ✓
b. Chiffrer les fichiers de la victime
c. Collecter des informations sans autorisation
d. Corrompre les fichiers système

(137) **Incidents informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une analyse forensique ?

a. L'analyse des preuves numériques après un incident pour en déterminer la cause ✓
b. Un test d'intrusion
c. La gestion des identités utilisateurs
d. La coordination des réponses aux incidents

(138) **Incidents informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est le rôle d'un responsable de la réponse aux incidents ?

a. Coordination des efforts pour résoudre les incidents de sécurité ✓
b. Développement de politiques de sécurité
c. Maintenance des serveurs
d. Analyse post-incident

(139) **Security Operation Center**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un SIEM (Security Information and Event Management) ?

a. Un programme antivirus

b. Un dispositif de chiffrement
c. Un système qui analyse et corrèle les données liées à la sécurité ✓
d. Une équipe de réponse aux incidents

(140) **Security Operation Center**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est l'objectif principal de la surveillance continue dans un SOC ?

a. Identifier et répondre rapidement aux incidents de sécurité ✓
b. Gérer les politiques de sauvegarde
c. Développer des logiciels sécurisés
d. Fournir une formation en cybersécurité

(141) **Vulnérabilités informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un test de sécurité "black-box" ?

a. Une évaluation externe sans connaissance préalable du système ✓
b. Une analyse post-incident
c. Une simulation d'attaque interne
d. Un test de pénétration automatisé

(142) **Vulnérabilités informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est le principal objectif d'une évaluation de la sécurité physique ?

a. La détection d'attaques DDoS
b. La collecte d'informations sensibles
c. L'identification des vulnérabilités physiques d'un site ✓
d. Le suivi des journaux d'activité réseau

(143) **Menaces informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un attaquant "script kiddie" ?

a. Une personne qui utilise des outils préexistants sans comprendre leur fonctionnement ✓
b. Un professionnel de la cybersécurité

c. Un pirate informatique expérimenté
d. Un membre d'une équipe de réponse aux incidents

(144) **Menaces informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale caractéristique d'une attaque par "zero-day" ?

a. Exploitation d'une vulnérabilité non corrigée ✓
b. Utilisation d'attaques sophistiquées
c. Attaque pendant une journée spécifique
d. Détection préalable par les systèmes de sécurité

(145) **Codes malveillants**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un cheval de Troie (trojan) dans le contexte des codes malveillants ?

a. Un programme apparemment légitime qui contient un logiciel malveillant ✓
b. Un virus polymorphique
c. Une alerte de sécurité
d. Un certificat SSL

(146) **Codes malveillants**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale caractéristique d'un ransomware ?

a. Chiffrer les fichiers de la victime et demander une rançon ✓
b. Collecter des informations sans autorisation
c. Se propager rapidement à travers les réseaux
d. Corrompre les fichiers système

(147) **Incidents informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale responsabilité d'une équipe d'analystes forensiques ?

a. Collecter et analyser des preuves numériques après un incident ✓

b. Coordination des réponses aux incidents
c. Mise en uvre des politiques de sécurité
d. Maintenance des serveurs

(148) **Incidents informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une déclaration d'incidents électroniques ?

a. Un test d'intrusion automatisé
b. Une communication formelle informant d'un incident de sécurité ✓
c. Un programme antivirus
d. Un rapport sur les performances du réseau

(149) **Security Operation Center**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un indicateur de compromission (IoC) dans le contexte d'un SOC ?

a. Un outil de chiffrement
b. Une donnée observable qui indique une activité suspecte ou malveillante ✓
c. Une équipe de réponse aux incidents
d. Un certificat SSL

(150) **Security Operation Center**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale fonction d'un tableau de bord de sécurité (Security Dashboard) dans un SOC ?

a. Afficher en temps réel les indicateurs de sécurité et les alertes ✓
b. Gérer les vulnérabilités du réseau
c. Coordonner les réponses aux incidents
d. Chiffrer les données sensibles

(151) **Vulnérabilités informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une vulnérabilité "day-zero" ?

a. Une vulnérabilité qui est exploitée avant qu'un correctif ne soit disponible ✓
b. Une vulnérabilité identifiée zéro jour après son apparition
c. Une vulnérabilité qui affecte seulement les systèmes de production
d. Une vulnérabilité découvert zéro jours après sa correction

(152) **Vulnérabilités informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est le rôle principal d'un scanner de vulnérabilités dans le contexte de la sécurité informatique ?

a. Une protection contre les attaques DDoS
b. Identifier et signaler les vulnérabilités dans un système ✓
c. Un dispositif de chiffrement des données
d. Un outil de détection de malware

(153) **Menaces informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une attaque de type "man-in-the-middle" ?

a. Une attaque par force brute
b. Une attaque où un attaquant intercepte et altère la communication entre deux parties ✓
c. Une attaque de déni de service distribué (DDoS)
d. Une attaque par script kiddie

(154) **Menaces informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est l'objectif principal d'une attaque de type "phishing" ?

a. Corrompre les fichiers système
b. Utiliser des techniques d'ingénierie sociale pour tromper les utilisateurs et obtenir des informations sensibles ✓
c. Collecter des informations de navigation
d. Lancer des attaques DDoS

(155) **Codes malveillants**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un ver informatique ?

a. Un programme autonome capable de se propager à travers les réseaux ✓
b. Un virus polymorphique
c. Une équipe de réponse aux incidents
d. Un outil de chiffrement

(156) **Codes malveillants**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale caractéristique d'un cheval de Troie (trojan) ?

a. Un programme apparemment légitime qui cache un logiciel malveillant ✓
b. Une alerte de sécurité
c. Un outil de détection de malware
d. Un virus capable de se reproduire en infectant d'autres fichiers

(157) **Incidents informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une analyse post-incident ?

a. L'examen et l'évaluation des événements survenus après un incident de sécurité ✓
b. Une simulation d'attaque pour identifier les vulnérabilités
c. Un test de pénétration automatisé
d. La collecte des preuves numériques pendant un incident

(158) **Incidents informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale responsabilité d'une équipe de réponse aux incidents (IRT) ?

a. La gestion des identités utilisateurs
b. Investigation et gestion des incidents de sécurité ✓
c. Maintenance des serveurs
d. Mise en uvre des politiques de sécurité

(159) **Security Operation Center**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un indicateur de compromission (IoC) fournit par un CERT ?

a. Une donnée de vulnérabilité
b. Une donnée observable qui indique une activité suspecte ou malveillante ✓
c. Un outil de chiffrement
d. Une signature de programme malveillant ✓

(160) **Security Operation Center**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est le rôle principal d'un analyste de sécurité dans un SOC ?

a. Surveiller et analyser les activités de sécurité, détecter les incidents et fournir une réponse initiale ✓
b. Développer des politiques de sécurité
c. Gérer les vulnérabilités du réseau
d. Coordonner les efforts de réponse aux incidents

(161) **Vulnérabilités informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une vulnérabilité "zero-day" ?

a. Une vulnérabilité qui n'a jamais été exploitée
b. Une vulnérabilité qui ne nécessite aucune correction
c. Une vulnérabilité qui est exploitée avant qu'un correctif ne soit disponible ✓
d. Une vulnérabilité qui n'affecte que les anciennes versions de logiciels

(162) **Vulnérabilités informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est le rôle d'un test d'intrusion "gray-box" ?

a. Une évaluation externe sans connaissance préalable du système
b. Une évaluation avec une connaissance partielle du système ✓

c. Une simulation d'attaque interne
d. Un test de pénétration automatisé

(163) **Menaces informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une attaque par force brute ?

a. Une attaque utilisant des tactiques furtives
b. Une attaque essayant toutes les combinaisons possibles de mots de passe ✓
c. Une attaque exploitant les failles matérielles
d. Une attaque par déni de service distribué (DDoS)

(164) **Menaces informatiques**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale caractéristique d'une menace persistante avancée (APT) ?

a. Une menace de courte durée
b. Une menace discrète et soutenue visant à accéder à un système de manière non détectée ✓
c. Une menace uniquement basée sur l'ingénierie sociale
d. Une menace affectant uniquement les utilisateurs inexpérimentés

(165) **Codes malveillants**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un logiciel espion (spyware) ?

a. Un programme conçu pour collecter des informations sans le consentement de l'utilisateur ✓
b. Un virus capable de se reproduire en infectant d'autres fichiers
c. Un cheval de Troie
d. Un outil de détection de malware

(166) **Codes malveillants**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale caractéristique d'un ransomware ?

a. Chiffrer les fichiers de la victime et demander une rançon ✓
b. Collecter des informations sans autorisation
c. Se propager rapidement à travers les réseaux
d. Corrompre les fichiers système

(167) **Incidents informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une déclaration d'incidents électroniques ?

a. Un test d'intrusion automatisé
b. Une communication formelle informant d'un incident de sécurité ✓
c. Un programme antivirus
d. Un rapport sur les performances du réseau

(168) **Incidents informatique**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la première étape dans la gestion d'un incident informatique ?

a. L'analyse post-incident
b. La détection et l'identification de l'incident ✓
c. La coordination des réponses aux incidents
d. L'analyse forensique

(169) **Security Operation Center**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un tableau de bord de sécurité (Security Dashboard) dans un SOC ?

a. Un outil de chiffrement
b. Un outil visuel affichant en temps réel les indicateurs de sécurité et les alertes ✓
c. Une équipe de réponse aux incidents
d. Un certificat SSL

(170) **Security Operation Center**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est l'objectif principal de la surveillance continue dans un SOC ?

a. Gérer les vulnérabilités du réseau
b. Identifier et répondre rapidement aux incidents de sécurité ✓
c. Fournir une formation en cybersécurité
d. Coordonner les réponses aux incidents

(171) **Gestion de crise cyber**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale responsabilité d'une équipe de gestion de crise cyber pendant un incident majeur ?

a. Maintenance des serveurs
b. Coordination des actions pour minimiser les impacts et restaurer les opérations normales ✓
c. Surveillance des journaux d'activité réseau
d. Gestion des vulnérabilités du réseau

(172) **Gestion de crise cyber**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un plan de gestion de crise cyber ?

a. Un programme antivirus
b. Une équipe de réponse aux incidents
c. Un ensemble de procédures définissant les actions à prendre pendant une cybercrise ✓
d. Un logiciel de détection de malware

(173) **Gestion de crise cyber**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est le rôle principal d'un coordinateur de crise cyber ?

a. La maintenance des serveurs
b. Coordonner les actions et les communications pendant une crise ✓
c. La gestion des vulnérabilités du réseau
d. Analyser les journaux d'activité réseau

(174) **Gestion de crise cyber**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la première étape d'une gestion efficace de crise cyber ?

a. La coordination des réponses aux incidents
b. La détection et la compréhension de la cyberattaque ✓
c. La maintenance des serveurs
d. Le déploiement d'un logiciel antivirus

(175) **Gestion de crise cyber**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une communication proactive pendant une crise cyber ?

a. Fournir des mises à jour régulières aux parties prenantes ✓
b. Une analyse post-incident
c. La gestion des identités utilisateurs
d. La collecte des preuves numériques pendant un incident

(176) **Gestion de crise cyber**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est le rôle d'une équipe de communication de crise cyber ?

a. La maintenance des serveurs
b. Gérer la communication interne et externe pendant une crise ✓
c. La coordination des réponses aux incidents
d. L'analyse forensique

(177) **Gestion de crise cyber**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un exercice de simulation de crise cyber ?

a. Une simulation d'une situation de crise pour tester la préparation de l'équipe ✓
b. Un test d'intrusion automatisé
c. La gestion des vulnérabilités du réseau
d. Une alerte de sécurité

(178) **Gestion de crise cyber** tags: `M3Sec101`, `Secops`

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale responsabilité d'une équipe de résilience cyber ?

a. La coordination des réponses aux incidents
b. Assurer la continuité des opérations et la reprise après une cyberattaque ✓
c. La maintenance des serveurs
d. La gestion des identités utilisateurs

(179) **Gestion de crise cyber**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est l'objectif principal d'une communication externe pendant une crise cyber ?

a. Maintenir la confiance du public et des partenaires ✓
b. La collecte des preuves numériques pendant un incident
c. La gestion des vulnérabilités du réseau
d. Une analyse post-incident

(180) **Gestion de crise cyber**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la différence entre une gestion de crise cyber et une réponse aux incidents ?

a. La gestion de crise est l'étape suivante d'une réponse à incident qui dépasse les capacités de décisions et de remédiation de la direction ✓
b. Il n'y a pas de différence
c. Une réponse à incident englobe toutes les actions dont la gestion de crise ✓
d. La gestion de crise cyber est réservée aux équipes techniques

(181) **Gestion de crise cyber**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une évaluation post-crise cyber ?

a. L'évaluation des actions prises et des leçons apprises après la gestion d'une crise cyber ✓
b. La coordination des réponses aux incidents
c. La maintenance des serveurs
d. Une simulation d'attaque pour identifier les vulnérabilités

(182) **ISO27001**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale caractéristique de la norme ISO 27001?

a. Elle fournit un cadre pour établir, mettre en uvre, maintenir et améliorer un système de management de la sécurité de l'information. ✓
b. Elle spécifie des exigences précises pour la conception d'un pare-feu.
c. Elle définit les protocoles de cryptage pour les réseaux sans fil.
d. Elle établit les exigences pour les logiciels antivirus.

(183) **Système de management de la sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est le principal objectif d'un SMSI (Système de Management de la Sécurité de l'Information)?

a. Assurer la confidentialité, l'intégrité et la disponibilité de l'information. ✓
b. Gérer les ressources humaines de l'entreprise.
c. Optimiser les processus de marketing.
d. Accroître les bénéfices financiers de l'entreprise.

(184) **Politique de sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est l'élément essentiel d'une politique de sécurité?

a. La définition des règles et des responsabilités en matière de sécurité. ✓
b. L'installation de logiciels antivirus sur tous les ordinateurs.
c. L'utilisation de mots de passe simples pour faciliter l'accès.
d. La réduction des coûts liés à la sécurité informatique.

(185) **Architectures fonctionnelles de sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est le principal avantage d'une architecture de sécurité en couches?

a. Elle permet une défense en profondeur contre les menaces. ✓
b. Elle réduit le nombre de dispositifs de sécurité nécessaires.
c. Elle rend la maintenance du réseau plus complexe.

d. Elle simplifie la configuration des pare-feux.

(186) **ISO27001**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce que la certification ISO 27001 garantit?

a. La conformité aux normes internationales en matière de sécurité de l'information. ✓
b. La protection absolue contre toutes les menaces informatiques.
c. La réduction des coûts de maintenance des serveurs.
d. La compatibilité avec tous les systèmes d'exploitation.

(187) **Système de management de la sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la première étape dans la mise en uvre d'un SMSI?

a. L'engagement de la direction. ✓
b. L'achat de matériel de sécurité de haute technologie.
c. La formation du personnel informatique.
d. La rédaction de politiques de sécurité détaillées.

(188) **Politique de sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est l'une des principales raisons pour lesquelles les politiques de sécurité échouent souvent?

a. Le manque de sensibilisation et de formation du personnel. ✓
b. L'existence de politiques trop strictes.
c. L'absence de surveillance des activités en ligne.
d. La dépendance excessive aux logiciels de sécurité.

(189) **Architectures fonctionnelles de sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel composant d'une architecture de sécurité est responsable de la limitation du trafic réseau entrant et sortant?

a. Le pare-feu. ✓
b. Le commutateur réseau.

c. Le serveur DNS.
d. Le routeur.

(190) **ISO27001**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce que l'évaluation des risques dans le cadre de la norme ISO 27001?

a. L'identification des menaces potentielles et de leurs impacts sur l'organisation. ✓
b. La mise en place de pare-feux sur tous les points d'accès au réseau.
c. La vérification de la conformité des politiques de sécurité.
d. La classification des employés en fonction de leur niveau d'accès à l'information.

(191) **Système de management de la sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un processus clé dans un SMSI?

a. L'amélioration continue. ✓
b. La désactivation des mises à jour automatiques.
c. La réduction des effectifs informatiques.
d. La suppression périodique des journaux d'activité.

(192) **ISO27001**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est l'objectif principal de l'ISO 27001?

a. Établir, mettre en uvre, maintenir et améliorer un système de management de la sécurité de l'information. ✓
b. Définir les normes pour la gestion des ressources humaines.
c. Élaborer des politiques de sécurité spécifiques pour les entreprises.
d. Créer des pare-feux personnalisés pour chaque organisation.

(193) **Système de management de la sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un audit de sécurité?

a. Une évaluation systématique de la sécurité d'un système ou d'une organisation. ✓
b. Une mise à jour régulière des logiciels de sécurité.
c. Un processus pour réduire les coûts de sécurité.
d. Une analyse des tendances de sécurité sur les réseaux sociaux.

(194) **Politique de sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une politique de classification de l'information?

a. Une directive indiquant comment l'information doit être étiquetée et gérée en fonction de sa sensibilité. ✓
b. Une liste de logiciels approuvés pour une utilisation sur le réseau de l'entreprise.
c. Une procédure pour l'installation de mises à jour logicielles.
d. Une politique interdisant l'utilisation de médias sociaux sur le lieu de travail.

(195) **Architectures fonctionnelles de sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est l'avantage d'une architecture de sécurité en périphérie?

a. Elle permet de protéger le réseau interne en contrôlant le trafic entrant et sortant. ✓
b. Elle réduit la nécessité d'avoir des politiques de sécurité claires.
c. Elle rend la configuration des pare-feux plus complexe.
d. Elle augmente le risque de compromission des données sensibles.

(196) **ISO27001**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est le rôle d'un responsable de la sécurité de l'information selon l'ISO 27001?

a. Superviser la mise en uvre et le maintien du SMSI (Système de Management de la Sécurité de l'Information). ✓
b. Gérer les ressources financières de l'entreprise.
c. Assurer la sécurité physique des locaux de l'entreprise.
d. Développer des logiciels de sécurité personnalisés.

(197) **Système de management de la sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce que la roue de Deming dans le contexte de la sécurité de l'information?

a. Un cycle d'amélioration continue composé des étapes Plan-Do-Check-Act. ✓
b. Un modèle de menace largement utilisé dans l'industrie de la cybersécurité.
c. Un algorithme de cryptage asymétrique.
d. Un protocole pour la détection des intrusions.

(198) **Politique de sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Pourquoi est-il important de sensibiliser régulièrement les employés à la sécurité de l'information?

a. Pour réduire les risques d'attaques basées sur l'ingénierie sociale. ✓
b. Pour éviter les pannes matérielles.
c. Pour augmenter la vitesse de connexion Internet.
d. Pour permettre l'accès à des sites Web non sécurisés.

(199) **Architectures fonctionnelles de sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un proxy dans une architecture de sécurité?

a. Un serveur intermédiaire qui agit comme un intermédiaire entre les utilisateurs et Internet. ✓
b. Un type de pare-feu spécialement conçu pour les réseaux sans fil.
c. Un protocole de sécurité utilisé pour crypter les communications.
d. Un dispositif qui contrôle l'accès physique aux locaux de l'entreprise.

(200) **ISO27001**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une analyse des risques selon l'ISO 27001?

a. Une évaluation des menaces potentielles et de leurs impacts sur l'organisation. ✓
b. Un test de pénétration des systèmes informatiques.
c. Un examen de la conformité des politiques de sécurité.
d. Une vérification de la disponibilité des mises à jour logicielles.

(201) **Système de management de la sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une revue de direction dans le contexte de la sécurité de l'information?

a. Une évaluation régulière de la performance du SMSI par la direction de l'entreprise. ✓
b. Un processus pour réviser les politiques de sécurité chaque année.
c. Un audit externe mené par des experts en sécurité.
d. Un examen des journaux d'activité informatique.

(202) **Politique de sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale raison pour laquelle les politiques de sécurité doivent être adaptées à chaque organisation?

a. Chaque organisation a des besoins, des risques et des environnements informatiques uniques. ✓
b. Les politiques de sécurité standard sont suffisantes pour toutes les entreprises.
c. Il est moins coûteux de copier les politiques d'autres entreprises.
d. Les politiques de sécurité ne sont pas importantes pour la plupart des organisations.

(203) **Architectures fonctionnelles de sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est l'objectif principal d'un pare-feu dans une architecture réseau?

a. Contrôler le trafic entrant et sortant pour protéger le réseau contre les menaces. ✓
b. Réduire la vitesse de connexion Internet.
c. Surveiller les activités des utilisateurs en ligne.

d. Fournir un stockage sécurisé des données sensibles.

(204) **ISO27001**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la différence entre une politique de sécurité et une procédure de sécurité?

a. Une politique de sécurité énonce les règles générales, tandis qu'une procédure de sécurité décrit les étapes spécifiques à suivre. ✓
b. Une politique de sécurité est utilisée pour contrôler l'accès au réseau, tandis qu'une procédure de sécurité gère les mises à jour logicielles.
c. Une politique de sécurité est mise en uvre par les utilisateurs finaux, tandis qu'une procédure de sécurité est gérée par le département informatique.
d. Une politique de sécurité concerne uniquement la sécurité physique, tandis qu'une procédure de sécurité concerne la sécurité informatique.

(205) **Système de management de la sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est l'objectif principal d'une évaluation des risques dans le cadre d'un SMSI?

a. Identifier les menaces potentielles et évaluer leur impact sur l'organisation. ✓
b. Établir des politiques de sécurité strictes.
c. Optimiser les processus de marketing.
d. Améliorer l'efficacité des communications internes.

(206) **Politique de sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est l'une des principales raisons pour lesquelles les politiques de sécurité sont souvent contournées par les employés?

a. Les politiques de sécurité peuvent être perçues comme étant trop contraignantes ou inefficaces. ✓
b. Les employés sont généralement bien formés sur les politiques de sécurité.

c. Les politiques de sécurité sont souvent trop laxistes.
d. Les employés ne sont pas conscients des politiques de sécurité de leur entreprise.

(207) **Architectures fonctionnelles de sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un DMZ (zone démilitarisée) dans une architecture réseau?

a. Un sous-réseau situé entre le réseau interne et Internet, utilisé pour héberger des services accessibles au public. ✓
b. Une zone réservée aux employés de l'entreprise pour leurs activités de loisirs en ligne.
c. Un espace de stockage sécurisé pour les données sensibles.
d. Un dispositif qui bloque les attaques provenant de l'extérieur du réseau.

(208) **ISO27001**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un actif de l'information selon l'ISO 27001?

a. Tout élément qui a de la valeur pour une organisation et qui nécessite une protection appropriée. ✓
b. Un logiciel antivirus installé sur les ordinateurs.
c. Un dispositif de sécurité physique comme une serrure de porte.
d. Un fichier de sauvegarde stocké sur un disque dur externe.

(209) **Système de management de la sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est le rôle d'un responsable de la sécurité de l'information dans un SMSI?

a. Planifier, mettre en uvre et maintenir le système de management de la sécurité de l'information. ✓
b. Gérer les opérations quotidiennes du service informatique.
c. Rédiger des rapports financiers pour la direction de l'entreprise.
d. Développer des applications logicielles personnalisées pour l'entreprise.

(210) **Politique de sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une attaque par hameçonnage (phishing)?

a. Une tentative d'obtenir des informations sensibles en se faisant passer pour une entité de confiance. ✓
b. Une technique pour intercepter les communications sans fil.
c. Un type d'attaque qui vise à submerger un système de requêtes malveillantes.
d. Un processus pour créer des sauvegardes de données régulières.

(211) **Architectures fonctionnelles de sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quel est l'objectif principal d'un IPS (Système de Prévention des Intrusions)?

a. Détecter et empêcher les intrusions non autorisées sur le réseau. ✓
b. Contrôler l'accès physique aux locaux de l'entreprise.
c. Crypter les communications sur le réseau.
d. Surveiller l'activité des utilisateurs sur les ordinateurs de l'entreprise.

(212) **ISO27001**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la principale différence entre la certification ISO 27001 et la conformité à la norme?

a. La certification est délivrée par un organisme de certification tiers, tandis que la conformité est auto-déclarée. ✓
b. La conformité est obligatoire, tandis que la certification est facultative.
c. La certification est moins contraignante que la conformité.
d. La certification est valable pour une année, tandis que la conformité est permanente.

(213) **Système de management de la sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est la première étape dans le processus de gestion des incidents de sécurité?

a. Identifier et classer l'incident. ✓
b. Isoler le système affecté du réseau.
c. Notifier les autorités locales.
d. Réparer les dommages causés par l'incident.

(214) **Politique de sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une politique de gestion des mots de passe?

a. Une directive qui établit des règles pour la création et l'utilisation de mots de passe sécurisés. ✓
b. Un document qui répertorie tous les mots de passe utilisés dans l'entreprise.
c. Un processus pour réinitialiser les mots de passe oubliés.
d. Une politique qui interdit l'utilisation de mots de passe pour accéder au système.

(215) **Architectures fonctionnelles de sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un VPN (réseau privé virtuel)?

a. Un réseau sécurisé qui permet aux utilisateurs d'accéder à des ressources informatiques à distance. ✓
b. Un logiciel antivirus pour les ordinateurs personnels.
c. Un dispositif de surveillance de l'activité Internet des employés.
d. Un protocole de cryptage pour les réseaux sans fil.

(216) **ISO27001**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une analyse d'impact sur la sécurité?

a. Une évaluation des consé
quences potentielles des menaces sur les actifs de l'information. ✓
b. Un test de vulnérabilité des systèmes informatiques.
c. Un processus pour vérifier la conformité aux politiques de sécurité.

d. Une enquête sur les incidents de sécurité passés.

(217) **Système de management de la sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un tableau de bord de sécurité?

a. Un outil pour surveiller et mesurer les performances du SMSI. ✓
b. Un dispositif de sécurité physique installé dans les locaux de l'entreprise.
c. Un document décrivant les procédures de réponse aux incidents de sécurité.
d. Un logiciel de gestion des mots de passe.

(218) **Politique de sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Quelle est l'une des meilleures pratiques pour assurer la sécurité des courriels?

a. Utiliser le chiffrement pour protéger les données sensibles. ✓
b. Ouvrir tous les courriels sans les examiner.
c. Partager les mots de passe par courriel.
d. Cliquer sur tous les liens dans les courriels, même s'ils semblent suspects.

(219) **Architectures fonctionnelles de sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'un NIDS (Système de Détection d'Intrusion sur Réseau)?

a. Un système conçu pour détecter les activités suspectes sur un réseau. ✓
b. Un dispositif de sécurité physique installé sur les ordinateurs.
c. Un logiciel antivirus pour les serveurs de messagerie.
d. Un protocole de cryptage pour les communications en ligne.

(220) **ISO27001**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce qu'une politique de sauvegarde des données?

a. Une directive qui établit des règles pour la sauvegarde régulière et sécurisée des données. ✓
b. Un processus pour supprimer définitivement les données obsolètes.
c. Un protocole pour crypter les données lors de leur transmission.
d. Un dispositif de stockage sécurisé des données sensibles.

(221) **Système de management de la sécurité**

MULTIPLE CHOICE | marked out of 1 | penalty 0.10 | One answer only | Shuffle

Qu'est-ce que la sensibilisation à la sécurité?

a. L'éducation des employés sur les pratiques sécuritaires et les risques potentiels. ✓
b. L'installation de logiciels de sécurité sur tous les ordinateurs.
c. La surveillance constante des activités en ligne des employés.
d. La restriction de l'accès à Internet sur le lieu de travail.

Total of marks: 221