QUIZZ MOODLE Module3
Architectures, Composants et Sécurité

Yann-Arzel LE VILLIO[1,2]*

Résumé
Liste des questions QUIZZ de la leçon, pour édition et vérifications.
Ce document présente les architectures, Composants de cybersécurité.
Il fait partie du cours introductif aux fondamentaux de la sécurité des systèmes d'information, de la cybersécurité, et de la cyberdéfense. Le cours est constitué d'un ensemble de notes de synthèse indépendantes compilées en un document unique, mais édité par chapitre dans le cadre de ce cours.
Ce document ne constitue pas à lui seul le référentiel du cours CYBERDEF101. Il compile des notes de cours mises à disposition de l'auditeur comme support pédagogique partiel à ce cours introductif à la cyberdéfense d'entreprise.

Mots clefs
Architectures, composants sécurité, SSI

[1] *Enseignant Sécurité ESIR*
[2] *Directeur Technique et Scientifique Orange CyberSchool*
***email** : yann-arzel.levillio@orange.com –

Module3

(1) **CyberEdu-X1.1**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Entourer les exemples d'enjeu de la cybersécurité ? (Voir ANSSI CyberEdu Slide n° 7 - Les enjeux de la sécurité des S.I.)

a. Augmenter les risques pesant sur le Système d'information (-100%)
b. Révéler les secrets (-100%)
c. Rendre difficile la vie des utilisateurs en ajoutant plusieurs contraintes comme les mots de passe longs et complexes (-100%)
d. Protéger le système d'information (100%)

(2) **CyberEdu-X1.2**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Impacts sur la vie privée ?

a. Impact sur l'image / le caractère / la vie privée : Diffamation de caractère , Divulgation d'informations personnelles (photos dénudées) Harcèlement (50%)
b. Impact sur l'identité : Usurpation d'identité (50%)

(3) **CyberEdu-X1.3**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Quels sont les trois principaux besoins de sécurité (Voir slide 23 - 24)

a. D : Disponibilité (33.33333%)
b. I : Intégrité (33.33333%)
c. C : Confidentialité (33.33333%)
d. P : Prouvabilité (-33.33333%)
e. A : InputAbilité (-33.33333%)

(4) **CyberEdu-X1.4**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Entourer la (ou les) phrase(s) correcte(s)

a. Le chiffrement permet de garantir que la donnée sera toujours disponible/accessible (-50%)
b. La sécurité physique permet d'assurer la disponibilité des équipements et des données (50%)
c. La signature électronique permet de garantir la confidentialité de la donnée (-50%)
d. Les dénis de service distribués (DDoS) portent atteinte à la disponibilité des données (50%)

(5) **CyberEdu-X1.5**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Vous développez un site web www.asso-etudiants-touristes.org pour une association qui regroupe les étudiants souhaitant effectuer des voyages ensemble à l'étranger. Sur ce site on retrouve les informations concernant les voyages proposés telles que : le pays, les villes à visiter, le prix du transport, les conditions d'hébergement, les dates potentielles du voyage. Ces informations ont un besoin en confidentialité :

a. Faible (100%)
b. Fort (-100%)

(6) **CyberEdu-X1.6**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Je viens de développer un site web pour une association qui regroupe les étudiants souhaitant effectuer des voyages en groupe à l'étranger. Les informations relatives aux étudiants inscrits sur le site (login et mot de passe, nom, prénom, numéro de téléphone, adresse), ont un besoin en confidentialité :

a. Faible (-100%)
b. Fort (100%)

(7) **CyberEdu-X1.6**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Je peux réussir une attaque sur un bien qui n'a aucune vulnérabilité (voir Slide 34 - Notions de vulnérabilité, menace, attaque - attaque) :

a. Vrai (-100%)
b. Faux (100%)

(8) **CyberEdu-X1.7**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Toutes les organisations et tous les individus font face aux mêmes menaces (voir slide 40 - Exemples de sources de menaces) :

a. Vrai (-100%)
b. Faux (100%)

(9) **CyberEdu-X1.8**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Entourer les attaques généralement de type ciblée (Voir ANSSI CyberEdu Slide n° 42 - 52 : Panorama de quelques menaces) :

a. Phishing ou hameçonnage (-50%)
b. Ransomware ou rançongiciel (-50%)
c. Social engineering ou ingénierie sociale (50%)
d. Spear phishing ou l'arnaque au président (50%)

(10) **CyberEdu-X1.9**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Entourer les attaques généralement de type non ciblée (Voir ANSSI CyberEdu Slide n° 42 - 52 : Panorama de quelques menaces) :

a. Intrusion informatique (-50%)
b. Virus informatique (50%)
c. Déni de service distribué (-50%)
d. Phishing ou hameçonnage (50%)

(11) **CyberEdu-X1.10**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Quels sont les éléments facilitateurs de fraudes internes (Voir ANSSI CyberEdu Slide n° 47 - Panorama de quelques menaces : Fraude interne)

a. Des comptes utilisateurs partagés entre plusieurs personnes (50%)
b. L'existence de procédures de contrôle interne (-50%)
c. Peu ou pas de supervision des actions internes (50%)
d. Une gestion stricte et revue des habilitations (-50%)

(12) **CyberEdu-X1.11**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Entourer les éléments qui peuvent réduire ou empêcher des fraudes internes

a. Une gestion stricte et une revue des habilitations (33.33333%)
b. Une séparation des rôles des utilisateurs (33.33333%)
c. Peu ou pas de surveillance interne (-33.33333%)
d. Des comptes utilisateurs individuels pour chacun (33.33333%)

(13) **CyberEdu-X1.12**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Citer les vecteurs d'infection de virus

a. Une pièce jointe attachéà un message électronique (20%)
b. Un support amovible infecté par exemple une clé USB (20%)
c. Un site web malveillant ou ayant des pages web corrompues (20%)
d. Un partage réseau ouvert (20%)
e. Un système vulnérable (20%)

(14) **CyberEdu-X1.13**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Qu'est-ce qu'un botnet ? (Voir ANSSI CyberEdu Slide n° - Panorama de quelques menaces : Déni de service distribué)

a. un réseau d'ordinateurs infectés et contrôlés par une personne malveillante. (100%)
b. un logiciel maveillant s'autorepliquant sur internet (-100%)
c. un système controlé à distance par un logiciel malveillant (-100%)

(15) **CyberEdu-X1.14**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Vous devez systématiquement donner votre accord avant de faire partir d'un réseau de botnets ? (Voir ANSSI CyberEdu Slide n° 52 - Panorama de quelques menaces : Déni de service distribué - illustration d'un botnet)

a. Vrai (-100%)
b. Faux (100%)

(16) **CyberEdu-X1.15**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

En France, la cybersécurité ne concerne que les entreprises du secteur privé et les individus (Voir ANSSI CyberEdu Slide n° 54 : L'organisation de la sécurité en France)

a. Vrai (-100%)
b. Faux (100%)

(17) **CyberEdu-X1.16**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

L'usage d'outils pour obtenir les clés Wifi et accéder au réseau Wifi du voisin tombe sous le coup de la loi (Voir ANSSI CyberEdu Slide n° 58 - Dispositif juridique français de lutte contre la cybercriminalité) :

a. Vigipirate (-100%)
b. Godfrain (100%)
c. Hadopi (-100%)
d. Patriot act (-100%)

(18) **CyberEdu-X1.17**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Mon réseau wifi personnel est mal sécurisé, par exemple par l'usage d'une clé Wifi faible (exemple : 12345678). Une personne (intrus) se connecte à mon réseau pour effectuer des actions malveillantes comme attaquer un site gouvernemental :

a. J'encours des sanctions (-100%)
b. Seul l'intrus encourt des sanctions (-100%)
c. L'intrus et moi encourons des sanctions. (100%)
d. Aucune sanction n'est encourue (-100%)

(19) **CyberEdu-X1.18**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Données à caractère personnel lesquels ?

a. Nom, prénom (12.5%)
b. Nom, téléphone (12.5%)
c. Date de naissance et commune (12.5%)
d. Lieu de naissance (12.5%)
e. Nationalité ou pays de naissance des parents ou des grands parents (12.5%)
f. Adresse (12.5%)
g. No carte d'identité / No de passeport / No de permis de conduire, … (12.5%)
h. Empreinte digitale (12.5%)

(20) **CyberEdu-X1.20**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Lors de la création du site Web de notre association étudiante, si vous stockez les informations suivantes pour chaque membre : nom, prénom, adresse, adresse email. Auprès de quel organisme devez-vous faire une déclaration (Voir ANSSI CyberEdu Slide n° 60 - 64 : Droit de protection des données à caractère personnel) ?

a. Gendarmerie (-100%)
b. Université (-100%)
c. CNIL (100%)
d. Hadopi (-100%)

(21) **CyberEdu-X2.1**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Donner 2 exemples de données électroniques sensibles pour un étudiant :

a. Adresse postale (-50%)
b. Nom et numéro de sécurité sociale (50%)
c. Numéro de carte bancaire (50%)
d. Nom de famille (-50%)

(22) **CyberEdu-X2.2**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Donner 2 exemples de données électroniques sensibles pour une université/école :

a. Le nom et l'origine de l'université (-50%)
b. Les noms des professeurs (-50%)
c. Les brevets déposés (50%)
d. Les épreuves d'examens à venir (non encore passés) (50%)

(23) **CyberEdu-X2.3**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Dans un réseau, qu'est-ce qu'on entend par une zone de confiance ?

a. Le hotspot wifi offert aux visiteurs, exemple à la gare SNCF (-100%)
b. Le réseau interne (où sont hébergés les postes des utilisateurs et les serveurs) (100%)
c. Le réseau Internet (-100%)
d. Une zone démilitarisée (DMZ) (-100%)

(24) **CyberEdu-X2.4**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Quand parle-t-on d'une authentification mutuelle entre deux entités ?

a. Lorsque des deux entités sont administrées par la même personne (-100%)
b. Lorsque chacune des entités doit s'authentifier vis-à-vis de l'autre (100%)
c. Lorsque la communication entre les deux entités est chiffrée (-100%)
d. Lorsque les deux entités sont situées sur le même réseau (-100%)

(25) **CyberEdu-X2.5**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Dans un réseau, l'usage du BYOD peut entrainer (choisir la (ou les) proposition(s) vraie(s)) :

a. Une restriction du périmètre à sécuriser (-50%)
b. La propagation de codes malveillants (50%)
c. La fuite de données de l'entreprise (50%)
d. Une meilleure sécurité du SI (-50%)

(26) **CyberEdu-X2.6**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Quel est le principe célèbre en matière de gestion de flux sur un réseau ?

a. Tout ce qui n'est pas autorisé est interdit (100%)
b. Tout ce qui est autorisé n'est pas interdit (-100%)
c. Tout ce qui est interdit est interdit (-100%)

(27) **CyberEdu-X2.7**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Un pare-feu peut être aussi bien matériel (appliance dédiée) que logiciel ?

a. Vrai (100%)
b. Faux (-100%)

(28) **CyberEdu-X2.8**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Entourer la (ou les) proposition(s) vraie(s) qui peut (ou peuvent) servir de mesure de sécurisation des accès distants à un réseau :

a. Utiliser un serveur d'authentification centralisé comme TACACS+ (50%)
b. Utiliser Internet (-50%)
c. Utiliser un protocole sécurisé tel que telnet ou ftp (-50%)
d. Utiliser un VPN (50%)

(29) **CyberEdu-X2.9**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Entourer la (ou les) bonne(s) mesure(s) de sécurisation de l'administration

a. Rendre les interfaces d'administration disponibles à tous depuis Internet (-50%)
b. Tous les administrateurs doivent utiliser le même compte pour se connecter (-50%)
c. Utiliser un réseau dédié pour l'administration (50%)
d. Authentifier mutuellement les postes des administrateurs et les serveurs à administrer. (50%)

(30) **CyberEdu-X2.10**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Quelle est la technologie la plus appropriée pour sécuriser son accès Wifi :

a. WEP (-100%)
b. WPA (-100%)
c. WPS (-100%)
d. WPA2 (100%)

(31) **CyberEdu-X2.11**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Entourer la (ou les) proposition(s) vraie(s) lors de l'usage d'un hotspot Wifi ?

a. Il peut s'agir d'un faux point d'accès ; (50%)
b. Les autres personnes connectées peuvent voir mes communications (50%)
c. Je suis protégé des personnes malveillantes (-50%)
d. Je suis sur un réseau de confiance, je peux désactiver mon pare-feu. (-50%)

(32) **CyberEdu-X2.12**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Pourquoi vérifier l'intégrité d'un logiciel ?

a. Pour m'assurer qu'il ne contient pas de virus (-100%)
b. Pour m'assurer que le logiciel que je télécharge n'a pas été corrompu (100%)
c. Pour m'assurer que le logiciel fonctionne bien comme promis (-100%)
d. Pour m'assurer qu'il est gratuit (-100%)

(33) **CyberEdu-X2.13**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Laquelle (ou lesquelles) des expressions suivantes est (sont) vraie(s) pour un logiciel téléchargeable ?

a. toujours gratuit (-33.33333%)
b. Peut être open source (33.33333%)
c. Peut contenir des logiciels espions (33.33333%)
d. Peut être un programme malveillant (33.33333%)

(34) **CyberEdu-X2.14**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Citer une bonne pratique de configuration de son antivirus

a. Avoir un antivirus d'un éditeur connu (-100%)
b. Avoir un jour installé un antivirus (-100%)
c. Tenir son antivirus à jour (mise à jour des signatures et du moteur) (100%)
d. Interdire l'analyse antivirale à certains répertoires ou périphériques. (-100%)

(35) **CyberEdu-X2.15**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Sélectionner la (ou les) proposition(s) vraie(s) parmi les suivantes. Un antivirus :

a. peut détecter tous les virus et programmes malveillants, y compris ceux non découverts (-50%)
b. protège de toutes les menaces (-50%)
c. ne peut détecter que les virus qui sont connus dans sa base de signatures (50%)
d. doit être actif, et à jour pour être utile (50%)

(36) **CyberEdu-X2.16**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Choisir un (ou des) symptôme(s) potentiel(s) d'infection par un code malveillant

a. Mon antivirus est désactivé (50%)
b. Mon ordinateur fonctionne plus lentement (50%)
c. J'ai plusieurs pages Web qui s'ouvrent toutes seules (-50%)
d. Des fichiers ou des répertoires sont créés automatiquement sur mon poste (-50%)

(37) **CyberEdu-X2.17**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Les mises à jour logicielles servent à améliorer les logiciels et à corriger les failles de sécurité

a. Vrai (100%)
b. Faux (-100%)

(38) **CyberEdu-X2.18**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Vous pouvez protéger la confidentialité vos données en :

a. Les chiffrant (100%)
b. En calculant leur empreinte de manière à vérifier leur intégrité (-100%)
c. En les envoyant vers des supports externes ou vers le Cloud (-100%)
d. En les publiant sur Internet (-100%)

(39) **CyberEdu-X2.19**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Sélectionner le (ou les) moyen(s) de durcissement d'une configuration

a. Modifier les mots de passe par défaut (33.33333%)
b. Désinstaller les logiciels inutiles (33.33333%)
c. Activer le mode débogage USB sur les téléphones (-33.33333%)
d. Sécuriser le BIOS à l'aide d'un mot de passe (33.33333%)

(40) **CyberEdu-X2.20**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Sélectionner le (ou les) principes(s) à prendre en compte lors de l'attribution de privilèges utilisateurs

a. Tout ce qui n'est pas interdit, est autorisé (-50%)
b. Moindre privilège (50%)
c. Besoin d'en connaitre (50%)
d. Droit administrateur pour tous (-50%)

(41) **CyberEdu-X2.21**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Entourer la (ou les) mauvaise(s) pratique(s) pour les mots de passe

a. Je crée un mot de passe très long et très complexe, dont je ne me souviens pas (25%)
b. Ma date de naissance me sert de mot de passe (25%)
c. Je stocke mes mots de passe en clair dans un fichier texte (25%)
d. Mon mot de passe doit avoir au plus 7 caractères (25%)

(42) **CyberEdu-X2.22**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Entourer la (ou les) bonne(s) pratique(s) pour les mots de passe

a. J'enregistre mes mots de passe sur chaque navigateur Internet (-50%)
b. Je crée un mot de passe long et complexe dont je peux me souvenir * facilement (50%)
c. J'écris mon mot de passe sur un post-it que je cache sous mon clavier/PC (-50%)
d. J'utilise un porte-clés de mots de passe (50%)

(43) **CyberEdu-X2.23**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Entourer la (ou les) bonne(s) pratique(s) de navigation sur Internet

a. Je suis victime de ransomware, je paye la rançon (-100%)
b. J'évite de communiquer avec des inconnus (100%)
c. J'accepte toutes les demandes sur les médias sociaux (-100%)
d. Je donne mon mot de passe de messagerie à l'administrateur lorsqu'il me le demande. (-100%)

(44) **CyberEdu-X2.24**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Citer deux moyens de sécurisation physique des biens/équipements

a. Mettre les équipements sensibles dans une salle sans contrôle d'accès (-50%)
b. Attacher les équipements sensibles avec des câbles de sécurité (50%)
c. Nommer tous les équipements de la même façon (-50%)
d. Utiliser des filtres de confidentialité pour les écrans (50%)

(45) **CyberEdu-X2.25**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Choisir l' (ou les) exemple(s) d'incidents de sécurité

a. Le vol d'un équipement/terminal (33.33333%)
b. La création d'un compte utilisateur pour un nouvel étudiant (-33.33333%)
c. La présence d'un code malveillant sur un poste (33.33333%)
d. La divulgation sur un forum des noms, prénoms, et numéros de sécurité sociale des étudiants (33.33333%)

(46) **CyberEdu-X2.26**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Choisir la (ou les) bonne(s) réaction(s) face à un incident de sécurité :

a. Désactiver/désinstaller son antivirus (-50%)
b. Appliquer les règles/consignes reçues par exemple dans la charte informatique (50%)
c. Chercher à identifier la cause de l'incident (50%)
d. Désactiver son pare-feu (personnel par exemple) (-50%)

(47) **CyberEdu-X2.27**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Sélectionner la (ou les) raison(s) pour laquelle (ou lesquelles) les audits de sécurité peuvent être effectués :

a. Pour obtenir une certification ou un agrément (33.33333%)
b. Pour trouver des faiblesses et les corriger (33.33333%)
c. Pour évaluer le niveau de sécurité (33.33333%)
d. Provoquer des incidents de sécurité (-33.33333%)

(48) **CyberEdu-X3.1**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

La sécurité est au coeur de l'implémentation de la famille de protocoles IP :

a. Vrai (-100%)
b. Faux (100%)

(49) **CyberEdu-X3.2**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Lors de l'utilisation du protocole IP, il est nativement possible d'authentifier les émetteurs et récepteurs d'un datagramme IP :

a. Vrai (-100%)
b. Faux (100%)

(50) **CyberEdu-X3.3**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Le chiffrement des données transportées est automatiquement pris en compte dans la famille de protocole IP au niveau de la couche de Transport :

a. Vrai (-100%)
b. Faux (100%)

(51) **CyberEdu-X3.4**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Lorsqu'un attaquant C peut écouter et modifier les informations échangées entre A et B, on parle d'écoute :

a. Passive (-100%)
b. Active (100%)
c. Hacktiviste (-100%)
d. Discrète (-100%)

(52) **CyberEdu-X3.5**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Entourer au moins 2 mécanismes de sécurité complémentaires pouvant servir à sécuriser les réseaux sur IP

a. L'utilisation d'Internet (-33.33333%)
b. Le chiffrement des communications (33.33333%)
c. Le cloisonnement des réseaux (33.33333%)
d. L'authentification des entités (33.33333%)

(53) **CyberEdu-X3.6**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Entourer 2 mécanismes/technologies qui peuvent servir à sécuriser les réseaux sur IP

a. Le filtrage des flux (50%)
b. La supervision des équipements (50%)
c. L'usage des réseaux sans fil, comme le Wifi (-50%)
d. Le BYOD (Bring your Own Device) (-50%)

(54) **CyberEdu-X3.7**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Entourer un équipement qui permet de définir et contrôler les flux autorisés et interdits entre deux réseaux ? (Voir ANSSI CyberEdu Slide n° Pare-feu)

a. Un routeur (-100%)
b. Un pare-feu (100%)
c. Un hub (-100%)
d. Un répartiteur de charge (-100%)

(55) **CyberEdu-X3.8**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Quel rôle un proxy (serveur mandataire) peut-il jouer en matière de sécurité ? (Voir ANSSI CyberEdu Slide n° Pare-feu : 13)

a. Il peut mettre en cache des pages Internet déjà demandées. (-100%)
b. Il peut autoriser ou interdire certains flux applicatifs. (100%)
c. Il peut rechercher des éléments malveillants (-100%)
d. Il peut chiffrer les communications (-100%)

(56) **CyberEdu-X3.9**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Quel équipement peut aider à se protéger des dénis de services distribués ? (Voir ANSSI CyberEdu Slide n° 14 : Répartiteur de charge)

a. Un antivirus (-100%)
b. Un routeur (-100%)
c. Un proxy (-100%)
d. Un répartiteur de charge (100%)

(57) **CyberEdu-X3.10**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Mon antivirus me protège suffisamment. Je suis à l'abri de tous les virus, y compris des virus à paraitre non encore détectés (0-day) ? (Voir ANSSI CyberEdu Slide n° Antivirus : 16)

a. Vrai (-100%)
b. Faux (100%)

(58) **CyberEdu-X3.11**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Quel élément composant l'antivirus lui permet de détecter les codes malveillants connus ? (Voir ANSSI CyberEdu Slide n° 16 : Antivirus)

a. Le nom de l'éditeur (Sophos, Trend Micro, McAfee, …) (-100%)
b. La matrice de flux (-100%)
c. La base de données des signatures (100%)
d. Le moteur de chiffrement (-100%)

(59) **CyberEdu-X3.12**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Quel équipement réseau peut être utilisé pour détecter une intrusion ? (Voir ANSSI CyberEdu Slide n° 18 : IDS et IPS)

a. Un pare-feu (-100%)
b. Un IDS (100%)
c. Un IPS (-100%)
d. Un antivirus (-100%)

(60) **CyberEdu-X3.13**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Quelle technologie permet de créer une communication (tunnel) sécurisée entre deux réseaux en s'appuyant sur un réseau qui n'est pas de confiance ? (Voir ANSSI CyberEdu Slide n° 20 : VPN)

a. Internet (-100%)

b. Wifi (-100%)
c. VPN (100%)
d. 4G (-100%)

(61) **CyberEdu-X3.14**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Entourer les bonnes réponses. Un VPN TLS est un tunnel est établi au niveau de la couche de : (Voir ANSSI CyberEdu Slide n° 22 : VPN)

a. Données (-100%)
b. IP (-100%)
c. Transport (100%)
d. Https (-100%)

(62) **CyberEdu-X3.15**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

La cryptographie est seul moyen de créer des VPN de manière sécurisée : (Voir ANSSI CyberEdu Slide n° 23 : VPN)

a. Vrai (-100%)
b. Faux (100%)

(63) **CyberEdu-X3.16**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Les VLAN sont des réseaux virtuels implémentés sur les routeurs : (Voir ANSSI CyberEdu Slide n° 26 : Segmentation)

a. Vrai (-100%)
b. Faux (100%)

(64) **CyberEdu-X3.17**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Un proxy me permet de masquer mon adresse interne vis-à-vis d'Internet : (Voir ANSSI CyberEdu Slide n° 37 : Exemple pratique de sécurisation avec un réseau simple)

a. Vrai (100%)
b. Faux (-100%)

(65) **CyberEdu-X3.18**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Dans les règles de bonnes pratiques, les équipements qui communiquent directement avec Internet doivent être mis dans une DMZ : (Voir ANSSI CyberEdu Slide n° 37 : Exemple pratique de sécurisation avec un réseau simple)

a. Vrai (100%)
b. Faux (-100%)

(66) **CyberEdu-X3.19**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Comment s'appelle le processus de transformation d'un texte en clair en un texte illisible à l'aide d'un algorithme ? (Voir ANSSI CyberEdu Slide n° 42 : Vocabulaire)

a. Le chiffrement (100%)
b. Le cryptage (-100%)
c. La signature (-100%)

(67) **CyberEdu-X3.20**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

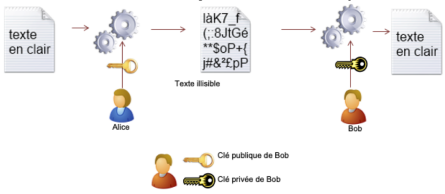
Lorsque la clé utilisée pour transformer un texte en clair en texte illisible est la même pour rendre, le texte illisible en texte en clair , on parle de ? (Voir ANSSI CyberEdu Slide n° 50 : Chiffrement symétrique)

a. Cloisonnement (-100%)
b. Chiffrement asymétrique (-100%)
c. Chiffrement symétrique (100%)
d. Virtualisation (-100%)

(68) **CyberEdu-X3.21**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Lorsque pour envoyer un message privé à Bob, Alice utilise la clé publique de Bob pour rendre illisible le texte en clair , et que Bob utilise sa clé privée pour transformer le texte illisible en texte en clair , on parle de ? (Voir ANSSI CyberEdu Slide n° 52 : Chiffrement asymétrique)



a. Chiffrement symétrique (-100%)
b. Tokenisation (-100%)
c. Envoi privé (-100%)
d. Chiffrement asymétrique (100%)

(69) **CyberEdu-X3.22**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Considérant les besoins de sécurité, entourer le(s) besoin(s) assuré(s) par la signature électronique : (Voir ANSSI CyberEdu Slide n° 54 : Signature électronique)

a. Disponibilité, (-100%)
b. Intégrité (100%)
c. Confidentialité (-100%)
d. Sureté (-100%)

(70) **CyberEdu-X3.23**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Entourer les éléments qu'on peut retrouver dans un certificat électronique d'une entité : (Voir ANSSI CyberEdu Slide n° 61 : Certificats électroniques)

a. Les noms, prénoms, URL de l'entité (ou son url) (33.33333%)
b. La clé privée de l'entité (-33.33333%)
c. La signature d'un tiers de confiance (des autorités de certification) (33.33333%)
d. La période de validité du certificat (33.33333%)

(71) **CyberEdu-X3.24**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Lors de la navigation sur Internet, les fichiers temporaires créés et gérés par les navigateurs Web afin de stocker les informations concernant les utilisateurs telles que : (Voir ANSSI CyberEdu Slide n° 67 : Usurpation d'identité via les cookies), (Son identifiant, Les thèmes et les préférences d'affichage) sont appelés

a. les logs (-100%)
b. La clé privée de l'entité (-100%)
c. les fichiers INI (-100%)
d. les cookies (100%)

(72) **CyberEdu-X3.25**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Depuis Internet, lorsqu'un attaquant réussit à contourner les mécanismes d'authentification et à interroger directement la base de données par écriture de commandes spécifiques on parle de (Voir ANSSI CyberEdu Slide n° 72 : Injection SQL)

a. Hacking (-100%)
b. XSS (Cross Site Scripting) (-100%)
c. Injection SQL (100%)
d. Malware (-100%)

(73) **CyberEdu-X3.26**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Lors de la navigation en https sur un site Web, entourer les propositions ci-dessous qui sont vraies : (Voir ANSSI CyberEdu Slide n° 63 : Certificats électroniques)

a. Le site web dispose d'un certificat électronique (50%)
b. Tous les échanges entre le site Web et mon navigateur doivent être chiffrés (50%)
c. Tous les échanges entre le site Web et mon navigateur sont analysés par mon antivirus (-50%)
d. Le débit des communications Internet est plus rapide (-50%)

(74) **CyberEdu-X3.27**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Lors de la navigation en https sur un site Web, il faut faire attention à :

a. La validité du certificat annoncé par le site (le certificat n'a pas encore expiré) (33.33333%)
b. L'autorité ayant accordé le certificat (par exemple, il ne faudrait que le certificat soit auto-signé ou issue d'une autorité non reconnue) (33.33333%)
c. L'alerte de mon navigateur indiquant que le certificat présenté par le site n'est pas de confiance (33.33333%)
d. Il n'y pas de raison de faire attention, https signifie que je peux naviguer en toute confiance. (-33.33333%)

(75) **CyberEdu-X4.1**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

De quelle famille de normes internationales, une organisation peut-elle s'inspirer pour intégrer la sécurité en son sein ?

a. 27000 (100%)
b. 9000 (-100%)
c. 14000 (-100%)

(76) **CyberEdu-X4.2**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Citer un exemple représentatif d'une organisation devant avoir recours à une certification de sécurité.

a. pour respecter une réglementation (50%)
b. pour s'améliorer (50%)
c. pour se protéger contre des menaces spécifiques (-50%)

(77) **CyberEdu-X4.3**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Très souvent dans les entreprises, les informations ont toutes le même niveau de confidentialité toutes non confidentielles

a. Vrai (-100%)
b. Faux. (100%)

(78) **CyberEdu-X4.4**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Pour une bonne intégration de la sécurité dans l'organisation, le personnel doit être sensibilisé à la sécurité conformément à leurs fonctions

a. Vrai (100%)
b. Faux. (-100%)

(79) **CyberEdu-X4.5**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Citer les procédures de gestion des départs du personnel indispensables impactant la sécurité

a. Retrait des accès (50%)
b. Restitution du matériel fourni (badge, ordinateur, …) (50%)
c. Solde de tout compte (-50%)

(80) **CyberEdu-X4.6**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

La sécurité c'est comme la cerise sur le gâteau elle doit être prise en compte à la fin d'un projet

a. Vrai (-100%)
b. Faux. (100%)

(81) **CyberEdu-X4.7**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Le but d'une analyse de risques est de déterminer pour un périmètre donné (projet par exemple), les risques qui peuvent porter sur les biens non sensibles

a. Vrai (-100%)
b. Faux (100%)

(82) **CyberEdu-X4.8**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Sélectionner la phase qui résume le plus la démarche d'analyse de risques

a. Identifier les agents menacants et les neutraliser (-100%)
b. Identifier les acteurs importants du projet (-100%)
c. Inventorier les biens (-100%)
d. Déterminer les risques et les traiter (100%)

(83) Identifier les agents menaçants et les neutraliser

(84) Identifier les acteurs importants du projet

(85) Inventorier les biens

(86) * Déterminer les risques et les traiter

(87) **CyberEdu-X4.9**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Est-ce que tous les risques issus d'une analyse de risques doivent-ils être traités par une mesure de réduction des risques ?

a. Non seuls ceux dont le niveau de criticité est supérieur au seuil de tolérance (100%)
b. Oui tous les risques doivent être couverts (-100%)

(88) **CyberEdu-X4.10**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Choisir la (les) proposition(s) correcte(s). Au cours de l'analyse de risques, les contre-mesures sont des mesures de réduction de risque qui peuvent être

a. techniques et organisationnelles (50%)
b. techniques uniquement (-50%)
c. organisationnelles uniquement (-50%)
d. déclinées des objectifs de sécurité définis. (50%)

(89) **CyberEdu-X4.11**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Choisir la (les) proposition(s) correcte(s)

a. Il est plus facile d'attaquer un système que de le rendre invulnérable (50%)
b. Il est facile de créer un système sans aucune vulnérabilité (-50%)
c. Pour défendre un système, il suffit de le protéger de manière périmétrique (-50%)
d. La défense en profondeur peut être appliquée pour protéger un système. (50%)

(90) **CyberEdu-X4.12**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Choisir la (les) proposition(s) correcte(s). La défense en profondeur est un principe d'origine militaire qui consiste à avoir plusieurs lignes de défense constituant des barrières autonomes pour défense un système

a. Vrai (100%)
b. Faux. (-100%)

(91) **CyberEdu-X4.13**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Choisir la (les) proposition(s) correcte(s). Pour une organisation, l'usage des services du Cloud doit prendre en compte

a. les exigences légales relatives aux données hébergées (25%)
b. les mécanismes de sécurité tels que le chiffrement des données stockées proposés par le fournisseur du service (25%)
c. le devenir des données hébergées à la fin du contrat (25%)

d. les certifications dont dispose le fournisseur du service Cloud. (25%)

(92) **CyberEdu-X4.14**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

L'une des difficultés de l'intégration de la sécurité dans une organisation, est celle des choix éclairés en matière de produits de confiance

a. Vrai (100%)
b. Faux. (-100%)

(93) **CyberEdu-X4.15**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Dans une organisation, la sécurité est critique. Elle doit être imposée à tous sans consultation

a. Vrai (-100%)
b. Faux. (100%)

(94) **CyberEdu-X4.16**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Le Shadow IT ou Shadow Cloud est une pratique qui consiste pour les utilisateurs à souscrire directement aux services Cloud sans la consultation et aval de leur DSI et en souvent en dépit de la politique de sécurité

a. Vrai (100%)
b. Faux (-100%)

(95) **CyberEdu-X4.17**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Choisir la (les) proposition(s) correcte(s). Le Big Data peut constituer une opportunité en sécurité car il peut permettre de

a. d'envoyer les données sensibles de l'organisation en clair vers le Cloud (-33.33333%)
b. d'utiliser une capacité de traitement de manière à effectuer l'analyse d'évènements de sécurité en temps réel (33.33333%)
c. de corréler les traces provenant de différents équipements réseau pour détecter des menaces persistantes avancées (APT) (33.33333%)
d. de surveiller le trafic réseau en temps réel pour détecter les botnets. (33.33333%)

(96) **CyberEdu-X4.18**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Citer un métier, avec une principale activité associée, sollicité dans chaque phase d'un cycle d'un projet

a. Expression de besoin Chef de projet/consultant MOA pour définir les exigences de sécurité issues d'une analyse de risque (25%)

b. Développement Chef de projet/consultant MOE, architecte, concepteur/développeur pour spécifier, concevoir/développer les mesures de sécurité (25%)
c. Validation auditeur technique ou organisationnel pour contrôler la conformité et l'efficacité des mesures de sécurité (25%)
d. Exploitation technicien ou administrateur pour maintenir en condition de sécurité (mise à jour des patchs et des bases de signature), analyste pour faire la veille sur les vulnérabilités ou détecter des incidents de sécurité (25%)

(97) **CyberEdu-X4.19**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

Les compétences recherchées en cybersécurité sont uniquement techniques

a. Vrai (-100%)
b. Faux. (100%)

(98) **CyberEdu-X4.20**

QCM | noté sur 1.0 | pénalité 0.10 | Plusieurs réponses possibles | Mélanger

La cybersécurité est un secteur ayant peu de perspective d'embauche

a. Vrai (-100%)
b. Faux. (100%)

Total des points : 94