Quizz pour le cours de sensibilisation et initiation à la Cybersécurité

CyberEdu

CyberEdu

La sécurité par l'enseignement supérieur des NTIC

Avertissement !

Certaines réponses peuvent être sujettes à un sain débat en fonction de l'interprétation que chacun peut en faire avec sa vision d'expert ou d'administrateur ou d'utilisateur de l'outil informatique.

Ce document pédagogique a été rédigé par un consortium regroupant des enseignants-chercheurs et des professionnels du secteur de la cybersécurité.

Version 1.1 — Février 2017

1 Quizz pour le module 1 : « Cybersécurité : notions de base »

1. Sélectionner les enjeux de la cybersécurité ?

Réponses possibles :

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

2. Si vous étiez victime d'une attaque cybercriminelle, quelles pourraient être les conséquences (impacts) sur votre vie privée (deux exemples) ?

3. Citer les trois principaux besoins de sécurité.

4. Choisir la (ou les) phrase(s) correcte(s)

Réponses possibles :

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

5. Vous développez un site web www.asso-etudiants-touristes.org pour une association quiregroupe 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

Réponses possibles :

- **a.** Faible ;
- **b.** Fort.

6. Vous développez un site web www.asso-etudiants-touristes.org 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

Réponses possibles :

a. Faible ;

b. Fort.

7. Je peux réussir une attaque sur un objet qui n'a aucune vulnérabilité exploitable (faiblesse) :

Réponses possibles :

a. Vrai ;

b. Faux.

8. Toutes les organisations et tous les individus font face aux mêmes menaces :

Réponses possibles :

a. Vrai ;

b. Faux.

9. Entourer les attaques qui sont généralement de type « ciblée » :

Réponses possibles :

a. Phishing ou hameçonnage ;

b. Ransomware ou rançongiciel ;

c. Social engineering ou ingénierie sociale ;

d. Spear phishing ou « l'arnaque au président ».

10. Entourer les attaques qui sont généralement de type « non ciblées » :

Réponses possibles :

a. Intrusion informatique ;

b. Virus informatique ;

c. Déni de service distribué ;

d. Phishing ou hameçonnage.

11. Entourer les éléments facilitateurs des fraudes internes :

Réponses possibles :

a. Des comptes utilisateurs partagés entre plusieurs personnes ;
b. L'existence de procédures de contrôle interne ;
c. Peu ou pas de surveillance interne ;
d. Une gestion stricte et une revue des habilitations.

12. Entourer les éléments qui peuvent réduire ou empêcher des fraudes internes :

Réponses possibles :

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

13. Citer deux moyens (vecteurs d'infection) par lesquels les virus informatiques peuvent être transmis d'un système compromis (ou d'un attaquant) à un système sain.

14. Qu'est-ce qu'un botnet ?

15. Vous devez systématiquement donner votre accord avant de faire partie d'un réseau de botnets ?

Réponses possibles :

a. Vrai ;
b. Faux.

16. En France, la cybersécurité ne concerne que les entreprises du secteur privé et les individus :

Réponses possibles :

a. Vrai ;
b. Faux.

17. L'usage d'outils pour obtenir les clés Wifi et accéder au réseau Wifi du voisin tombe sous le coup de la loi :

Réponses possibles :

a. Vigipirate ;

b. Godfrain ;

c. Hadopi ;

d. Patriot Act.

18. 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 :

Réponses possibles :

a. J'encours des sanctions ;

b. Seul l'intrus encourt des sanctions ;

c. L'intrus et moi encourons des sanctions ;

d. Aucune sanction n'est encourue.

19. Donner un exemple de données à caractère personnel.

20. 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 ?

Réponses possibles :

a. Gendarmerie ;

b. Université ;

c. CNIL ;

d. Hadopi.

2 Quizz pour le module 2 « Les règles d'hygiène informatique »

21. Choisir ci-dessous 2 exemples de données électroniques sensibles pour un étudiant :

Réponses possibles :

a. Adresse postale ;
b. Nom et numéro de sécurité sociale ;
c. Numéro de carte bancaire ;
d. Nom de famille.

22. Choisir ci-dessous 2 exemples de données électroniques sensibles pour une université/école :

Réponses possibles :

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

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

Réponses possibles :

a. Le hotspot wifi offert aux visiteurs, par exemple dans une gare SNCF ;
b. Le réseau interne (où sont hébergés les postes des utilisateurs et les serveurs) ;
c. Le réseau Internet ;
d. Une zone démilitarisée (DMZ).

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

Réponses possibles :

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

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

Réponses possibles :

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

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

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

Réponses possibles :

a. Vrai ;
b. Faux.

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

Réponses possibles :

a. Utiliser un serveur d'authentification centralisé comme TACACS+ ;
b. Utiliser Internet ;
c. Utiliser un protocole sécurisé tel que telnet ou ftp ;
d. Utiliser un VPN.

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

Réponses possibles :

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

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

Réponses possibles :

- **a.** WEP ;
- **b.** WPA ;
- **c.** WPS ;
- **d.** WPA2.

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

Réponses possibles :

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

32. Pourquoi vérifier l'intégrité d'un logiciel ?

Réponses possibles :

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

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

Réponses possibles :

- **a.** Toujours gratuit ;
- **b.** Peut-être « open source » ;
- **c.** Peut contenir des logiciels espions ;
- **d.** Peut-être un programme malveillant.

34. Citer une bonne pratique de configuration de son antivirus :

Réponses possibles :

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

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

Réponses possibles :

- **a.** Peut détecter tous les virus et programmes malveillants, y compris ceux non découverts ;
- **b.** Protège de toutes les menaces ;
- **c.** Ne peut détecter que les virus qui sont connus dans sa base de signatures ;
- **d.** Doit être actif, et à jour pour être utile.

36. Choisir le (ou les) symptôme(s) potentiel(s) d'infection par un code malveillant :

Réponses possibles :

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

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

Réponses possibles :

- **a.** Vrai ;
- **b.** Faux.

38. Comment pouvez-vous protéger la confidentialité de vos données ?

Réponses possibles :

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

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

Réponses possibles :

- **a.** Modifier les mots de passe par défaut ;
- **b.** Désinstaller les logiciels inutiles ;
- **c.** Activer le mode « débogage USB » sur les téléphones ;
- **d.** Sécuriser le BIOS à l'aide d'un mot de passe.

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

Réponses possibles :

- **a.** « Tout ce qui n'est pas interdit, est autorisé » ;
- **b.** « Moindre privilège » ;
- **c.** « Besoin d'en connaitre » ;
- **d.** « Droit administrateur pour tous ».

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

Réponses possibles :

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

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

Réponses possibles :

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

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

Réponses possibles :

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

44. Citer deux moyens de sécurisation physique des biens/équipements :

Réponses possibles :

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

45. Sélectionner le (ou les) exemple(s) d'incident(s) de sécurité :

Réponses possibles :

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

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

Réponses possibles :

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

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

Réponses possibles :

a. Pour obtenir une certification ou un agrément ;

b. Pour trouver des faiblesses et les corriger ;

c. Pour évaluer le niveau de sécurité ;

d. Provoquer des incidents de sécurité.

3 Quizz pour le module 3 « Cybersécurité : les aspects réseaux et applicatifs »

48. La sécurité est au cœur de l'implémentation de la famille de protocoles IP :

Réponses possibles :

a. Vrai ;

b. Faux.

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

Réponses possibles :

a. Vrai ;

b. Faux.

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

Réponses possibles :

a. Vrai ;

b. Faux.

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

Réponses possibles :

a. Passive ;

b. Active ;

c. Hacktiviste ;

d. Discrète.

52. Choisir au moins 2 mécanismes de sécurité complémentaires pouvant servir à sécuriser les réseaux sur IP :

Réponses possibles :

a. L'utilisation d'Internet ;

b. Le chiffrement des communications ;

c. Le cloisonnement des réseaux ;

d. L'authentification des entités.

53. Citer 2 mécanismes/technologies qui peuvent servir à sécuriser les réseaux sur IP :

Réponses possibles :

a. Le filtrage des flux ;

b. La supervision des équipements ;

c. L'usage des réseaux sans fil, comme le Wifi ;

d. Le BYOD (Bring your Own Device).

54. Entourer un équipement qui permet de définir et contrôler les flux autorisés et interdits entre deux réseaux ?

Réponses possibles :

a. Un routeur ;

b. Un pare-feu ;

c. Un hub ;

d. Un répartiteur de charge.

55. Quel rôle un proxy (serveur mandataire) peut-il jouer en matière de sécurité ?

Réponses possibles :

a. Il peut mettre en cache des pages Internet déjà demandées ;

b. Il peut autoriser ou interdire certains flux applicatifs ;

c. Il peut rechercher des éléments malveillants ;

d. Il peut chiffrer les communications.

56. Quel équipement peut aider à se protéger des dénis de services distribués (DDoS) ?

Réponses possibles :

a. Un antivirus ;

b. Un routeur ;

c. Un proxy ;

d. Un répartiteur de charge.

57. 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) ?

Réponses possibles :

a. Vrai ;

b. Faux.

58. Quel élément composant l'antivirus lui permet de détecter les codes malveillants connus ?

Réponses possibles :

a. Le nom de l'éditeur (Sophos, Trend Micro, McAfee. . .) ;

b. La matrice de flux ;

c. La base de données des signatures ;

d. Le moteur de chiffrement.

59. Quel équipement réseau peut être utilisé pour détecter une intrusion ?

Réponses possibles :

a. Un pare-feu ;

b. Un IDS ;

c. Un IPS ;

d. Un antivirus.

60. Quelle technologie permet de créer une communication sécurisée entre deux réseaux en s'appuyant sur un réseau qui n'est pas de confiance ?

Réponses possibles :

a. Internet ;
b. Wifi ;
c. VPN ;
d. 4G.

61. Complétez la phrase suivante : « Un VPN TLS est un tunnel établi au niveau de la couche » :

Réponses possibles :

a. Données ;
b. IP ;
c. Transport ;
d. Https.

62. La cryptographie est le seul moyen de créer des VPN de manière sécurisée :

Réponses possibles :

a. Vrai ;
b. Faux.

63. Les VLAN sont des réseaux virtuels implémentés sur les routeurs :

Réponses possibles :

a. Vrai ;
b. Faux.

64. Un proxy me permet de masquer mon adresse interne vis-à-vis d'Internet :

Réponses possibles :

a. Vrai ;
b. Faux.

65. Dans les règles de bonnes pratiques, les équipements qui communiquent directement avec Internet doivent être mis dans une DMZ :

Réponses possibles :

a. Vrai ;

b. Faux.

66. Comment s'appelle le processus de transformation d'un texte en clair en un texte illisible à l'aide d'un algorithme ?

67. 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 ?

Réponses possibles :

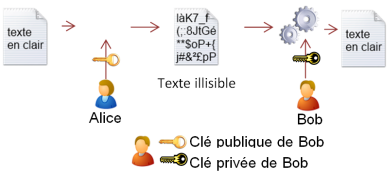
a. Cloisonnement ;

b. Chiffrement asymétrique ;

c. Chiffrement symétrique ;

d. Virtualisation.

68. 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 ?



Réponses possibles :

a. Chiffrement symétrique ;

b. Tokenisation ;

c. Envoi privé ;

d. Chiffrement asymétrique.

69. Considérant les besoins de sécurité, entourer le(s) besoin(s) assuré(s) par la signature électronique :

Réponses possibles :

a. Disponibilité ;

b. Intégrité ;

c. Confidentialité ;

d. Sûreté.

70. Entourer les éléments qu'on peut retrouver dans un certificat électronique d'une entité :

Réponses possibles :

a. Les noms, prénoms, URL de l'entité (ou son url) ;

b. La clé privée de l'entité ;

c. La signature d'un tiers de confiance (des autorités de certification) ;

d. La période de validité du certificat.

71. Lors de la navigation sur Internet, les _____ sont des fichiers temporaires créés et gérés par les navigateurs Web afin de stocker les informations concernant les utilisateurs telles que :

Réponses possibles :

a. Son identifiant ;

b. Les thèmes et les préférences d'affichage.

72. 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 :

Réponses possibles :

a. Hacking ;

b. XSS (Cross Site Scripting) ;

c. Injection SQL ;

d. Malware.

73. Lors de la navigation en https sur un site web, entourer la (ou les) proposition(s) ci-dessous qui sont vraie(s) :

Réponses possibles :

a. Le site web dispose d'un certificat électronique ;

b. Tous les échanges entre le site Web et mon navigateur doivent être chiffrés ;

c. Tous les échanges entre le site Web et mon navigateur sont analysés par mon antivirus ;

d. Le débit des communications Internet est plus rapide.

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

Réponses possibles :

a. La validité du certificat annoncé par le site (le certificat n'a pas encore expiré) ;

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) ;

c. L'alerte de mon navigateur indiquant que le certificat présenté par le site n'est pas de confiance ;

d. Il n'y pas de raison de faire attention ! « `https` » signifie que je peux naviguer en toute confiance.

4 Quizz pour le module 4 « La gestion de la cybersécurité au sein d'une organisation »

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

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

77. Très souvent dans les entreprises, les informations ont toutes le même niveau de confidentialité : « toutes non confidentielles » :

Réponses possibles :

a. Vrai ;

b. Faux.

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

Réponses possibles :

a. Vrai ;

b. Faux.

79. Citer une procédure de gestion des départs du personnel.

80. La sécurité c'est comme « la cerise sur le gâteau », elle doit être prise en compte à la fin d'un projet :

Réponses possibles :

a. Vrai ;

b. Faux.

81. 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 :

Réponses possibles :

a. Vrai ;

b. Faux.

82. Sélectionner la phrase qui résume le plus la démarche d'analyse de risques :

Réponses possibles :

a. Identifier les agents menaçants et les neutraliser ;

b. Identifier les acteurs importants du projet ;

c. Inventorier les biens ;

d. Déterminer les risques et les traiter.

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

84. Choisir la (les) proposition(s) correcte(s). Au cours de l'analyse de risques, les mesures de réduction de risque peuvent être :

Réponses possibles :

- **a.** techniques et organisationnelles ;
- **b.** techniques uniquement ;
- **c.** organisationnelles uniquement ;
- **d.** déclinées des objectifs de sécurité définis.

85. Choisir la (les) proposition(s) correcte(s) :

Réponses possibles :

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

86. 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 :

Réponses possibles :

- **a.** Vrai ;
- **b.** Faux.

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

Réponses possibles :

- **a.** les exigences légales relatives aux données hébergées ;
- **b.** les mécanismes de sécurité tels que le chiffrement des données stockées proposés par le fournisseur du service ;
- **c.** le devenir des données hébergées à la fin du contrat ;
- **d.** les certifications dont dispose le fournisseur du service Cloud.

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

Réponses possibles :

a. Vrai ;

b. Faux.

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

Réponses possibles :

a. Vrai ;

b. Faux.

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

Réponses possibles :

a. Vrai ;

b. Faux.

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

Réponses possibles :

a. d'envoyer les données sensibles de l'organisation en clair vers le Cloud ;

b. d'utiliser une capacité de traitement de manière à effectuer l'analyse d'évènements de sécurité en temps réel ;

c. de corréler les traces provenant de différents équipements réseau pour détecter des menaces persistantes avancées (APT) ;

d. de surveiller le trafic réseau en temps réel pour détecter les botnets.

92. Citer un métier SSI sollicité dans chaque phase d'un cycle d'un projet :

Réponses possibles :

a. Expression de besoin

b. Développement

c. Validation

d. Exploitation

93. Les compétences recherchées en cybersécurité sont uniquement techniques :

Réponses possibles :

a. Vrai ;

b. Faux.

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

Réponses possibles :

a. Vrai ;

b. Faux.

Ce document pédagogique a été rédigé par un consortium regroupant des enseignants-chercheurs et des professionnels du secteur de la cybersécurité.

Version 1.1 — Février 2017