

Sujet : Gestion des identités et des accès

1. Quels sont les challenges qu'a une entreprise en IAM? (plusieurs réponses possibles)

- ☒ a) Persistance d'accès historiques
- ☐ b) Laxisme dans l'ajout de droits
- ☒ c) Manque de confiance entre services
- ☐ d) Homonymes trop fréquents

2. Qu'est-ce que l'IAM?

- ☐ a) Assurer la redondance des infrastructures
- ☐ b) Empêcher la perte de données de l'entreprise
- ☒ c) Gérer les utilisateurs et contrôler les accès aux ressources dont ils ont besoin pour travailler

3. Qu'est-ce que l'IAG?

- ☐ a) Evaluation de la qualité des données présentes dans un système IAM
- ☒ b) Ensemble des processus et règles fonctionnelles essentiels au bon pilotage d'un projet d'IAM
- ☐ c) Convention de nommage des comptes

4. L'accès temporaire à une application est ?

- ☐ a) Un accès métier
- ☐ b) Un accès structurel
- ☒ c) Un accès exceptionnel

5. Donnez les avantages d'un système UBAC? (plusieurs réponses possibles)

- ☒ a) Respect du moindre privilège
- ☐ b) Bonne prise en charge des accès standard
- ☒ c) Bonne gestion des coûts de licence
- ☐ d) Cartographie des droits simples

6. Donnez les avantages d'un système ABAC? (plusieurs réponses possibles)

- ☒ a) Ajout de nouvelles règles
- ☒ b) Prise en charge des accès standards
- ☒ c) Gestion des exceptions
- ☒ d) Simple à mettre en œuvre

7. Donnez les avantages d'un système RBAC? (plusieurs réponses possibles)

- ☒ a) Intégration simple de nouvelles équipes
- ☒ b) Gestion des exceptions

- ☒ c) Recommandé par l'ANSSI
- ☒ d) Facile à superviser

8. Quels sont les actions standards de gestion du cycle de vie des identités? (plusieurs réponses possibles)

- ☒ a) Joiner
- ☒ b) Leaver
- ☒ c) Mover
- ☒ d) Manager

9. Quels sont les objectifs de la re-certification? (plusieurs réponses possibles)

- ☒ a) Auditer simplement
- ☒ b) Optimiser les coûts
- ☒ c) Informer des modifications RHs

10. Quelle re-certification n'est généralement pas conduite en entreprise ?

- ☐ a) La re certification des rôles métiers
- ☐ b) La rectification des profils techniques
- ☒ c) La re certification des privilèges

11. Quel est l'objectif de la séparation des pouvoirs?

- ☐ a) S'assurer que les employés sont dans les bonnes équipes
- ☐ b) Définir l'organigramme de l'entreprise simplement
- ☒ c) S'assurer qu'aucune action sensible ne peut être réalisée par une seule équipe ou personne

12. Qu'est-ce que l'AM?

- ☒ a) Authentifier les utilisateurs afin de garantir la légitimité d'un accès à une ressource.
- ☐ b) Authentifier fortement les utilisateurs (double facteur)
- ☐ c) Avoir une identité unique sur toutes les applications

13. Quels sont les moyens d'authentification composant une authentification forte?
(plusieurs réponses possibles)

- ☒ a) Quelque chose que l'on sait
- ☒ b) Quelque chose que l'on comprend
- ☒ c) Quelque chose que l'on possède
- ☒ d) Quelque chose que l'on est

14. Combien faut-il de facteurs au minimum pour faire une authentification forte?

- ☐ a) 1
- ☒ b) 2

- c) 3
- d) 4

15. Qu'est-ce que l'authentification out of band?

- a) C'est une authentification qui s'adapte à l'utilisateur connecté en fonction du contexte
- b) Elle consiste à comparer le comportement de l'utilisateur par rapport à son « empreinte comportementale ».
- c) C'est une authentification qui s'adapte à l'utilisateur connecté en fonction du risque
- ☒ d) Elle consiste à recourir, pour un facteur d'authentification, à un canal différent de celui utilisé pour accéder à l'application.

16. Quel est l'objectif du eSSO?

- a) Le principe de base est d'intercepter les requêtes entre le client et le serveur, et indiquer au serveur que le client est bien authentifié
- ☒ b) Cela consiste à entrer à la place de l'utilisateur, ses informations de connexion préalablement connues.

17. Quels sont les intérêts de la fédération d'identité? (plusieurs réponses possibles)

- ☒ a) La protection de la vie privée
- ☒ b) Le fournisseur de service (SP) ne gère plus les identités, il fait confiance à l'IDP.
- ☒ c) L'accès transparent aux fournisseurs de service
- ☒ d) Chiffrer les mots de passe

18. Quelle est la version du SAML déployée aujourd'hui ?

- a) SAML 1.0
- ☒ b) SAML 2.0
- c) SAML 2.1

19. Quel est le rôle de l'Identity Provider ?

- ☒ a) C'est celui qui construit et transmet une assertion à destination de l'application cible
- b) C'est celui qui protège l'application cible contre les accès non authentifiés ;
- c) C'est celui qui crée une session pour l'utilisateur sur l'application cible.

20. Quelle est la bonne cinématique SAML ?

- a) L'utilisateur accède au Service Provider, est redirigé vers l'Identity Provider, s'authentifie à l'Identity Provider, est redirigé vers le Service Provider avec une réponse SAML ;
- ☒ b) L'utilisateur accède à l'Identity Provider, est redirigé vers le SP, s'authentifie au Service Provider, est redirigé vers l'Identity Provider avec une réponse SAML ;
- c) L'utilisateur s'authentifie sur l'application, est redirigé vers le Service Provider, reçoit une réponse SAML et la transmet à l'Identity Provider pour validation.

21. A l'état de l'art, toutes les applications internes en entreprise :

- a) Ont un référentiel d'identité uniques pour simplifier la gestion ;
- ☒ b) S'authentifient avec des mots de passe différents par application pour diminuer le risque ;
- c) Ont un référentiel par application pour être indépendantes.



22. Quel est l'objectif du cIAM ?

- ☒ a) Avoir une vision unifiée des clients, partenaires et grand public à la fois sécurité et métier ;
- b) Avoir un mot de passe unique pour tous les clients ;
- c) Permettre un audit simple des comptes à privilèges.



23. Quelles sont les briques couvertes par le cIAM? (plusieurs réponses possibles)

- ☒ a) Enregistrement et Accès
- ☒ b) Stockage et Traitement
- ☒ c) Offrir un service de SSO sur les périphériques mobiles tels que les smartphones et les tablettes.



24. Quelle affirmation est vraie ?

- a) Il est plus important d'avoir des performances sur les applications internes que cIAM ;
- ☒ b) Il y a plus d'utilisateurs gérés dans des projets cIAM que IAM ;
- c) Les RHs sont la source d'information unique des données pour les comptes clients.



25. Quels comptes sont des comptes à privilèges? (plusieurs réponses possibles)

- a) Un compte bancaire
- b) Un compte réseau social d'entreprise
- ☒ c) Un compte d'administration
- d) Un compte royal canin



26. Quels sont les standards les plus connus en fédération d'identités? (plusieurs réponses possibles)

- ☒ a) OAuth2
- b) SSH
- ☒ c) OpenIDConnect
- ☒ d) SAML



27. Les comptes applicatifs sont-ils des comptes à privilèges?

- a) Oui
- b) Non
- ☒ c) Cela dépend des contextes



28. Les comptes d'administration sont-ils des comptes à privilèges?

- ☒ a) Oui
- ☐ b) Non
- ☐ c) Cela dépend des contextes



29. Quelle affirmation est vraie ?

- ☒ a) A l'état de l'art du modèle RBAC, chaque utilisateur bénéficie d'un seul rôle métier ;
- ☐ b) Dans un modèle RBAC, les utilisateurs qui ont le même rôle métier n'ont pas les mêmes accès ;
- ☐ c) Le modèle RBAC est le modèle le plus mature sur le marché.



30. Pour bâtir un modèle RBAC depuis un modèle UBAC, il faut commencer par :
- ☒ a) Définir les rôles métiers ;
 - ☐ b) Définir les rôles techniques ;
 - ☐ c) Définir le niveau de confiance dans l'authentification.

