Gestion des identités et des accès - Démystifions les concepts et terminologies

PRÉSENTÉ PAR YOUOVOP MARTIAL ET FRANCIS YUYA

SUPERVISÉ PAR ELIE MABO, CISSP, CASP

CAP2SEC
A consulting & InfoSec solutions firm



CAP2SEC
A consulting & InfoSec solutions firm

C'est quoi la GIA ?

La gestion des identités et des accès (GIA) se définit comme un ensemble de pratiques, de processus et de technologies qui permettent de gérer les identités numériques des utilisateurs et de contrôler leur accès aux ressources.

L'objectif de la GIA est de garantir que les bons sujets (personne, application, appareil, etc.) ont les bons accès aux objets (donnée, application, service, etc.), et ce, au bon moment et après autorisation.

CAP2SEC
A consulting & InfoSec solutions firm

Pourquoi la GIA est-elle importante ?

La GIA est un élément essentiel de la sécurité informatique, car elle permet de protéger les données et les systèmes contre les accès non autorisés. Dans un monde de plus en plus numérique, où les cyberattaques sont en constante augmentation, la GIA est un outil indispensable pour protéger les organisations et leurs utilisateurs.

CAP2SEC
A consulting & InfoSec solutions firm

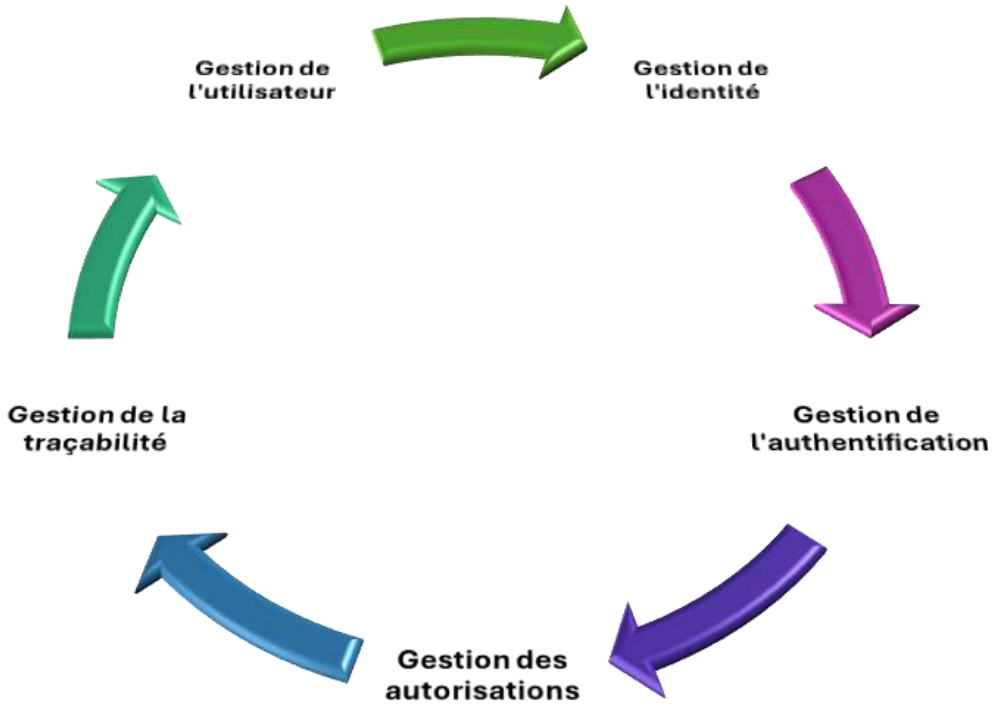
Que peut faire la GIA pour vous ?

La GIA peut vous aider à :

- ❑ Améliorer la sécurité de votre organisation en réduisant les risques de cyberattaques.
- ❑ Protéger vos données sensibles contre les accès non autorisés.
- ❑ Respecter les exigences de conformité en matière de protection des données (PCI-DSS, GDPR, HIPAA, PRP, etc.).
- ❑ Améliorer la productivité de vos utilisateurs en leur facilitant l'accès aux ressources dont ils ont besoin.

CAP2SEC
A consulting & InfoSec solutions firm

Les concepts clés de la GIA par domaine de service



CAP2SEC
A consulting & InfoSec solutions firm

Les concepts clés de la GIA – **Gestion de l'utilisateur**

Concepts liés à la gestion de l'utilisateur

- User
- Group
- Role

CAP2SEC
A consulting & InfoSec solutions firm

User

❑ Définition

Un utilisateur est une personne, une application ou un système qui accède aux ressources d'une organisation à des fins d'utilisation ou de gestion.

❑ Contexte d'utilisation

Le concept d'utilisateur est utilisé dans tous les aspects de la GIA, de l'authentification à l'autorisation.

❑ Quelques meilleures pratiques

- Vérifier les antécédents judiciaires des utilisateurs pour des fonctions sensibles;
- Sensibiliser et former les utilisateurs en matière de contrôle d'accès.
- Définir clairement et communiquer les rôles et responsabilités des utilisateurs.

❑ Quelques références

https://www.iso.org/isoiec-27001-information-security.html

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

https://docs.aws.amazon.com/fr_fr/IAM/latest/UserGuide/id_users.html



CAP2SEC
A consulting & InfoSec solutions firm

Group

❑ Définition

Un groupe est un ensemble d'utilisateurs qui partagent des caractéristiques communes.

❑ Contexte d'utilisation

Les groupes sont utilisés pour simplifier la gestion des accès aux ressources.

❑ Quelques meilleures pratiques

- Utiliser des groupes pour regrouper des utilisateurs ayant des besoins d'accès similaires.
- Définir des droits d'accès au niveau du groupe plutôt qu'au niveau de l'utilisateur individuel.
- Limiter le nombre de groupes auxquels un utilisateur appartient.

❑ Quelques références

https://docs.aws.amazon.com/fr_fr/IAM/latest/UserGuide/id_groups.html



CAP2SEC
A consulting & InfoSec solutions firm

Role

❑ Définition

Un rôle est un ensemble de droits et de responsabilités attribués à un utilisateur ou à un groupe d'utilisateurs.

❑ Contexte d'utilisation

Le rôle est utilisé dans tous les aspects de la sécurité informatique, de l'authentification à l'autorisation également utilisée pour suivre les activités des utilisateurs et pour auditer les accès aux ressources.



❑ Quelques meilleures pratiques

- Définir une politique de gestion des rôles.
- Définir des rôles précis et granulaires.
- Utiliser le principe de séparation des tâches.
- Attribuer les rôles aux utilisateurs ou aux groupes d'utilisateurs de manière minimale.

❑ Quelques références

https://esante.gouv.fr/sites/default/files/media_entity/documents/PGSSI-S_Guide_Pratique-Gestion%20des%20habilitations-V1.1.pdf

CAP2SEC
A consulting & InfoSec solutions firm

Profile Management

❑ Définition

consiste à créer des profils correspondant à certains types d'utilisateurs et à accorder des droits standard à chaque type ou profil d'utilisateurs, plutôt que de procéder au cas par cas.



❑ Contexte d'utilisation

Profile management est utilisée dans tous les aspects de la sécurité informatique, de l'authentification à l'autorisation également utilisée pour suivre les activités des utilisateurs et pour auditer les accès aux ressources.

❑ Quelques meilleures pratiques

- Définir une politique de gestion des profils.
- Définir des profils précis et granulaires.
- Attribuer les profils aux utilisateurs de manière minimale.

❑ Quelques références

https://www.youzer.net/articles/iam-gestion-identites-acces#:~:text=L%27Identity%20and%20Access%20Management%20est%20un%20ensemble%20de%20processus,réseau%20et%20aux%20applications%20cloud.

CAP2SEC
A consulting & InfoSec solutions firm

RBAC

❑ Définition

Le contrôle d'accès basé sur les rôles (RBAC) est un modèle de sécurité qui permet de contrôler l'accès aux ressources en fonction des rôles des utilisateurs.

❑ Contexte d'utilisation

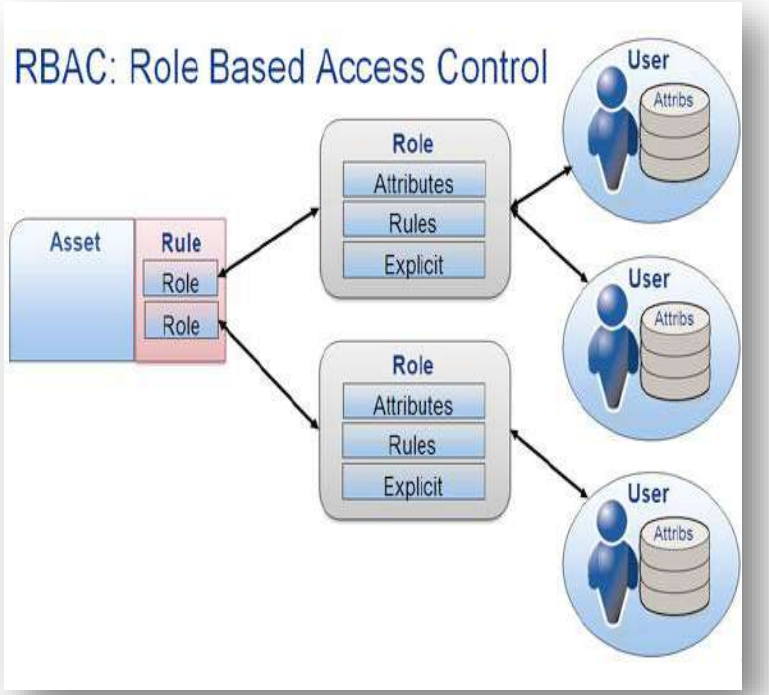
RBAC est utilisée dans tous les aspects de la sécurité informatique, de l'authentification à l'autorisation également utilisée pour suivre les activités des utilisateurs et pour auditer les accès aux ressources.

❑ Quelques meilleures pratiques

- Définir une politique de gestion des rôles.
- Définir des rôles précis et granulaires.
- Utiliser le principe de séparation des tâches.
- Surveiller les accès aux ressources.

❑ Quelques références

https://esante.gouv.fr/sites/default/files/media_entity/documents/PGSSI-S_Guide_Pratique-Gestion%20des%20habilitations-V1.1.pdf



CAP2SEC
A consulting & InfoSec solutions firm

ABAC

❑ Définition

Le contrôle d'accès basé sur les attributs (ABAC) est un modèle de sécurité qui permet de contrôler l'accès aux ressources en fonction des attributs des utilisateurs, des ressources et de l'environnement.

❑ Contexte d'utilisation

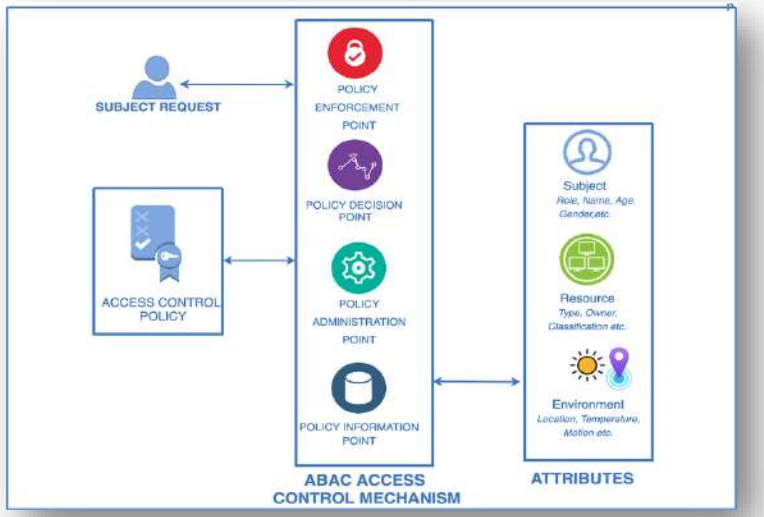
ABAC est utilisée dans tous les aspects de la sécurité informatique, de l'authentification à l'autorisation également utilisée pour suivre les activités des utilisateurs et pour auditer les accès aux ressources.

❑ Quelques meilleures pratiques

- Définir une politique de gestion des attributs.
- Définir des règles ABAC précises et granulaires.
- Utiliser le principe de séparation des tâches.

❑ Quelques références

https://esante.gouv.fr/sites/default/files/media_entity/documents/PGSSI-S_Guide_Pratique-Gestion%20des%20habilitations-V1.1.pdf



CAP2SEC
A consulting & InfoSec solutions firm

Les concepts clés de la GIA – **Gestion de l'identité**

Concepts liés à la gestion de l'identité

- Identity
- Identity Life-Cycle Management

CAP2SEC
A consulting & InfoSec solutions firm

Identity

❑ Définition

Ensemble d'attributs qui permettent d'identifier un utilisateur de manière unique.

❑ Contexte d'utilisation

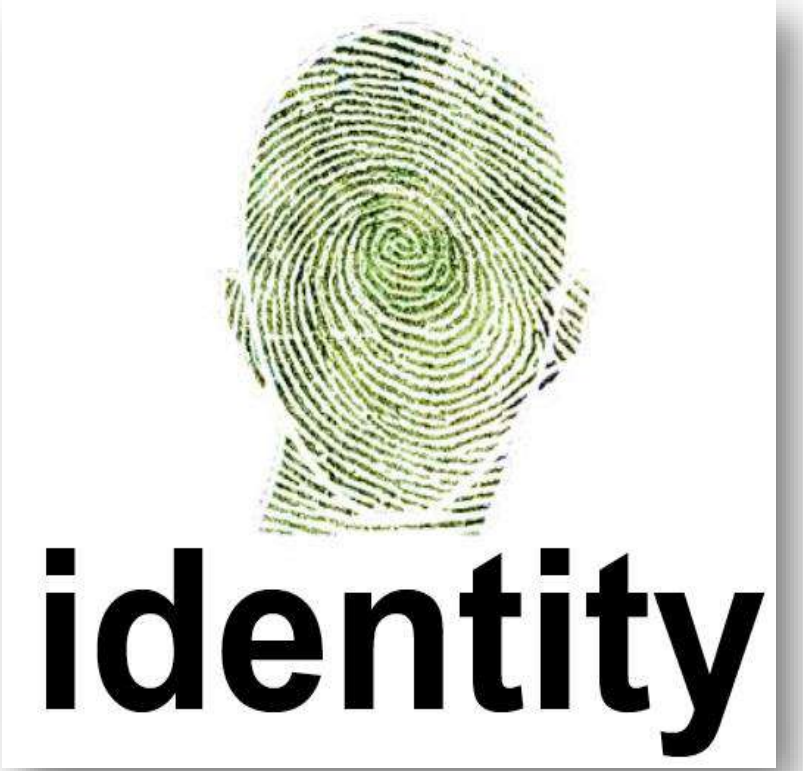
L'identité est utilisée dans tous les aspects de la sécurité informatique, de l'authentification à l'autorisation également utilisée pour suivre les activités des utilisateurs et pour auditer les accès aux ressources.

❑ Quelques meilleures pratiques

- Toujours vérifier l'identité d'une entité
- Assurer l'unicité de l'identité
- Mettre en place une politique de mot de passe robuste.
- Gérer les identités de manière centralisée.

❑ Quelques références

https://www.ckseven.com/identifiant-informatique-qu-est-ce-que-c-est



CAP2SEC
A consulting & InfoSec solutions firm

Identity Life-Cycle Management

❑ Définition

Le cycle de vie de l'identité est le processus de création, de gestion et de suppression des identités numériques.

❑ Contexte d'utilisation

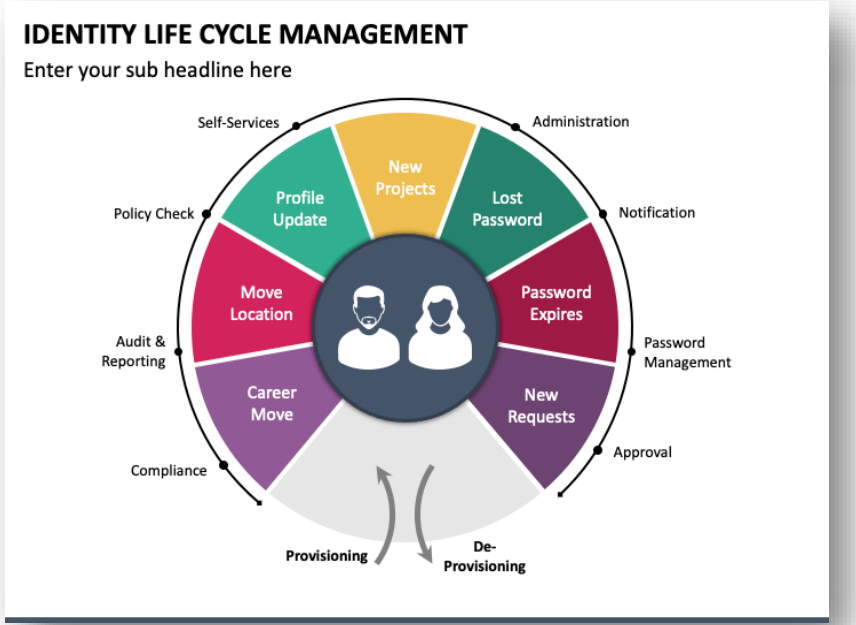
L'identité life cycle management est utilisée dans tous les aspects de la sécurité informatique, de l'authentification à l'autorisation également utilisée pour suivre les activités des utilisateurs et pour auditer les accès aux ressources.

❑ Quelques meilleures pratiques

- Définir une politique de gestion du cycle de vie de l'identité.
- Utiliser des noms d'utilisateurs uniques et forts.
- Gérer les identités de manière centralisée.

❑ Quelques références

https://learn.microsoft.com/fr-fr/entra/id-governance/what-is-identity-lifecycle-management



CAP2SEC
A consulting & InfoSec solutions firm

Gestion des identités privilégiés (PIM)

❑ Définition

La gestion des identités privilégiés (PIM) est un ensemble de processus et de technologies visant à gérer le cycle de vie des identités numériques aux ressources.



❑ Contexte d'utilisation

PIM est utilisée dans tous les aspects de la sécurité informatique, de l'authentification à l'autorisation également utilisée pour suivre les activités des utilisateurs et pour auditer les accès aux ressources.

❑ Quelques meilleures pratiques

- Définir une politique de gestion des identités et des accès.
- Définir des identités précises et granulaires.
- Utiliser le principe de séparation des tâches.

❑ Quelques références

https://www.microsoft.com/fr-fr/security/business/identity-access/microsoft-entra-privileged-identity-management-pim

CAP2SEC
A consulting & InfoSec solutions firm

Les concepts clés de la GIA – **Gestion de l'authentification**

Concepts liés à la gestion de l'authentification

- Multifactor Authentication
- 2FA
- Single Sign On (SSO)

CAP2SEC
A consulting & InfoSec solutions firm

Multifactor Authentication (MFA)

❑ Définition

L'authentification multifacteur (MFA) est une méthode de sécurité qui exige de l'utilisateur de fournir plusieurs facteurs d'authentification pour se connecter à un système ou à une application.



❑ Contexte d'utilisation

La MFA peut être utilisée pour protéger l'accès à une large gamme de systèmes et d'applications, notamment :

- Comptes bancaires
- Réseaux sociaux

❑ Quelques meilleures pratiques

- Activer le MFA pour tous les comptes à hauts privilèges.
- Utiliser des facteurs d'authentification forts, tels que les applications d'authentification à deux facteurs ou les clés de sécurité.

❑ Quelques références

https://aws.amazon.com/fr/what-is/mfa/#:~:text=L%27authentification%20multifactorielle%20(MFA)%20est%20un%20processus%20de%20connexion,un%20simple%20mot%20de%20passe.

CAP2SEC
A consulting & InfoSec solutions firm

Authentification à deux facteurs (2FA)

❑ Définition

L'authentification à deux facteurs (2FA) est une méthode de sécurité qui exige de l'utilisateur de fournir deux facteurs d'authentification pour se connecter à un système ou à une application.



❑ Contexte d'utilisation

Le 2FA peut être utilisé pour protéger l'accès à une large gamme de systèmes et d'applications, notamment :

- Comptes bancaires
- Réseaux sociaux

❑ Quelques meilleures pratiques

- Activer le 2FA pour tous les comptes à hauts privilèges.

❑ Quelques références

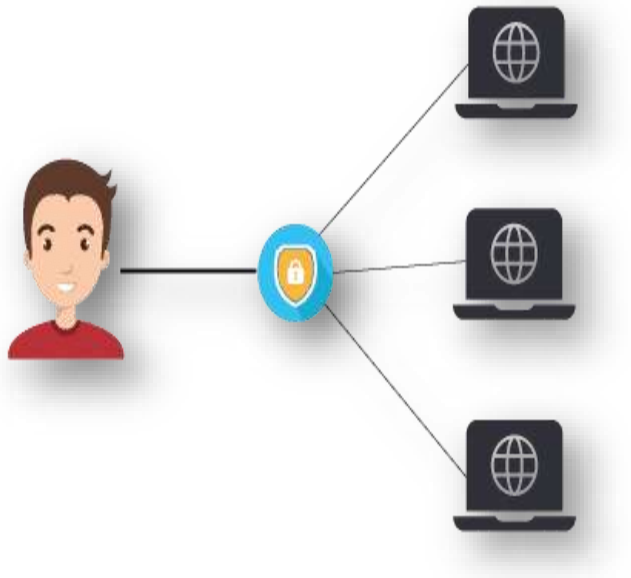
https://aws.amazon.com/fr/what-is/mfa/#:~:text=L%27authentification%20multifactorielle%20(MFA)%20est%20un%20processus%20de%20connexion,un%20simple%20mot%20de%20passe.

CAP2SEC
A consulting & InfoSec solutions firm

Authentification unique (SSO)

❑ Définition

L'authentification unique (SSO) est une méthode d'authentification qui permet aux utilisateurs de s'authentifier une seule fois pour accéder à plusieurs applications ou systèmes.



❑ Contexte d'utilisation

Le SSO peut être utilisé dans divers contextes, y compris :

- Application mobile: simplification l'expérience de connexion des utilisateurs
- Application cloud: possibilité de se connecter à l'aide des identifiants d'entreprise

❑ Quelques meilleures pratiques

- Choisir une solution SSO adaptée aux besoins de l'organisation.
- Mettre en place des processus de contrôle et d'audit.
- Sensibiliser les utilisateurs aux risques liés à la sécurité informatique.

❑ Quelques références

https://www.onelogin.com/fr-fr/learn/how-single-sign-on-works

CAP2SEC
A consulting & InfoSec solutions firm

Les concepts clés de la GIA – **Gestion des autorisations**

Concepts liés à la gestion des autorisations

- Permission
- PAM

CAP2SEC
A consulting & InfoSec solutions firm

Permissions

❑ Définition

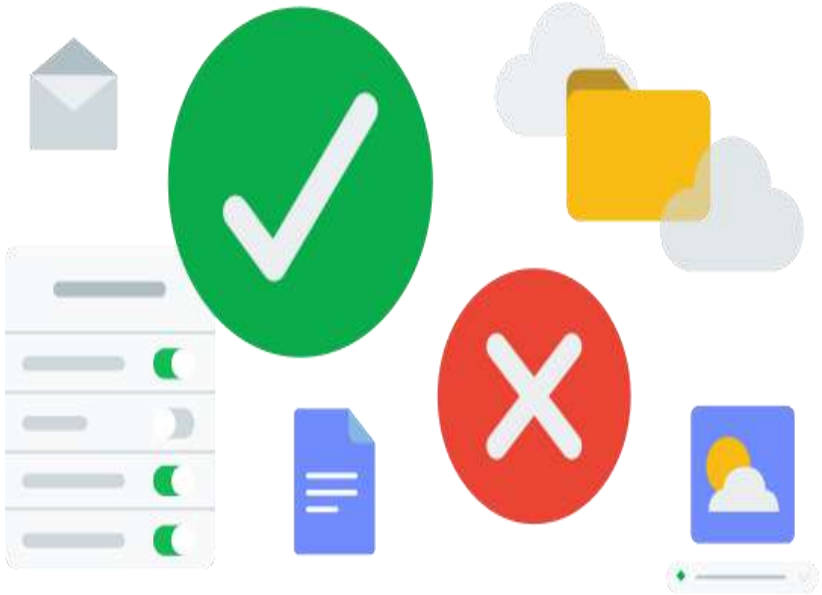
Les permissions définissent les actions qu'un utilisateur peut effectuer sur une ressource.

❑ Contexte d'utilisation

Permissions est utilisée dans tous les aspects de la sécurité informatique, de l'authentification à l'autorisation également utilisée pour suivre les activités des utilisateurs et pour auditer les accès aux ressources.

❑ Quelques meilleures pratiques

- Définir une politique de gestion des permissions.
- Définir des permissions précises et granulaires.
- Utiliser le principe de séparation des tâches.
- Supprimer les permissions des utilisateurs lorsqu'elles ne sont plus nécessaires.



❑ Quelques références

https://esante.gouv.fr/sites/default/files/media_entity/documents/PGSSI-S_Guide_Pratique-Gestion%20des%20habilitations-V1.1.pdf

CAP2SEC
A consulting & InfoSec solutions firm

Gestion des accès privilégiés (PAM)

❑ Définition

La gestion des accès privilégiés (PAM) est un ensemble de processus et de technologies visant à contrôler et à auditer l'accès aux comptes et aux ressources privilégiés.

❑ Contexte d'utilisation

PAM est utilisée dans tous les aspects de la sécurité informatique, de l'authentification à l'autorisation également utilisée pour suivre les activités des utilisateurs et pour auditer les accès aux ressources.

❑ Quelques meilleures pratiques

- Définir une politique de gestion des accès privilégiés.
- Définir des comptes privilégiés précis et granulaires.
- Utiliser le principe de séparation des tâches.

❑ Quelques références

https://www.microsoft.com/en-ca/security/business/security-101/what-is-privileged-access-management-pam



CAP2SEC
A consulting & InfoSec solutions firm

Les concepts clés de la GIA – **Gestion de la traçabilité**

Concepts liés à la gestion de la traçabilité

- Rights
- Moindre Privilèges
- Just-In-Time
- Authentication – Autorisation – Audit (AAA)
- ACL
- MAC
- DAC
- One-Time-Password (OTP)

CAP2SEC
A consulting & InfoSec solutions firm

Gestion des droits (Rights Management)

❑ Définition

La gestion des droits (Rights Management) est un ensemble de processus et de technologies visant à contrôler l'utilisation des données et des ressources numériques.

❑ Contexte d'utilisation

La gestion des droits peut être utilisée pour protéger une large gamme de données et de ressources numériques, notamment :

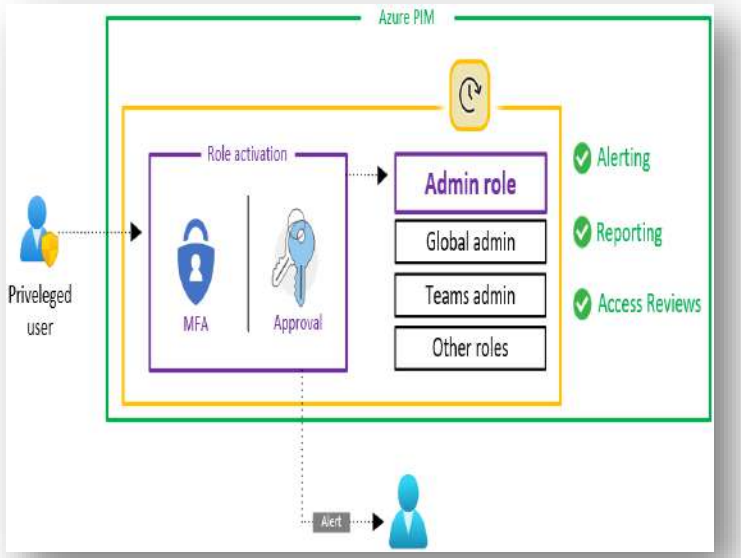
- Fichiers
- Logiciels

❑ Quelques meilleures pratiques

- Définir une politique de gestion des droits.
- Définir les droits d'accès pour chaque utilisateur ou groupe d'utilisateurs.

❑ Quelques références

https://www.ibm.com/fr-fr/topics/identity-access-management#:~:text=La%20gestion%20des%20identités%20et%20des%20accès%2C%20ou%20IAM%2C%20est,qu%27elles%20souhaitent%20utiliser.%20.



CAP2SEC
A consulting & InfoSec solutions firm

Entitlement Management

❑ Définition

L'entitlement management (gestion des habilitations) est un ensemble de processus et de technologies visant à contrôler l'accès aux ressources informatiques en fonction des rôles et des responsabilités des utilisateurs.

❑ Contexte d'utilisation

L'entitlement management peut être utilisé dans tous les types d'organisations, y compris

- Entreprises
- Administrations

❑ Quelques meilleures pratiques

- Définir une politique d'entitlement management.
- Identifier les ressources informatiques qui doivent être protégées.
- Définir les rôles et les responsabilités des utilisateurs.

❑ Quelques références

https://www.gartner.com/en/documents/4348799



CAP2SEC
A consulting & InfoSec solutions firm

Principe du moindre privilège (Least Privilege)

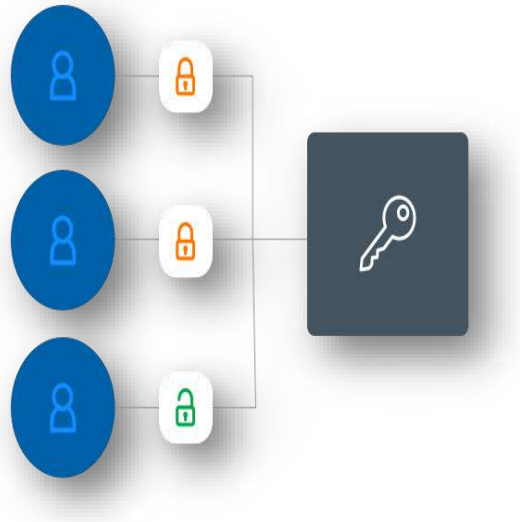
❑ Définition

Le principe du moindre privilège est une stratégie de sécurité qui vise à accorder aux utilisateurs et aux processus le minimum d'autorisations nécessaires pour accomplir leurs tâches.

❑ Contexte d'utilisation

Le principe du moindre privilège peut être utilisé dans tous les types d'organisations, y compris :

- Entreprises
- Administrations



❑ Quelques meilleures pratiques

- Appliquer le principe du moindre privilège à tous les utilisateurs et processus.
- Accorder les autorisations au besoin et les supprimer lorsqu'elles ne sont plus nécessaires.
- Utiliser des contrôles d'accès granulaires.

❑ Quelques références

https://www.cyberark.com/fr/what-is/least-privilege/

CAP2SEC
A consulting & InfoSec solutions firm

Just-in-Time (JIT)

❑ Définition

Le Just-in-Time (JIT) est un mécanisme de sécurité qui permet de fournir un accès privilégié élevé et granulaire à une application ou un système, uniquement lorsqu'un utilisateur en a besoin pour effectuer une tâche spécifique et pendant une durée précise.



❑ Contexte d'utilisation

Le JIT peut être utilisé dans tous les types d'organisations, y compris :

- Entreprises
- Administrations

❑ Quelques meilleures pratiques

- Négocier et supprimer l'accès.
- Accorder une élévation temporaire de privilège.

❑ Quelques références

Qu'est-ce que l'accès juste-à-temps ? Explication de l'accès JAT (cyberark.com)

CAP2SEC
A consulting & InfoSec solutions firm

Authentification, Autorisation et Audit (AAA)

❑ Définition

L'authentification, l'autorisation et la comptabilité (AAA) est un cadre de sécurité qui contrôle l'accès aux ressources informatiques, applique des politiques et audite l'utilisation

❑ Contexte d'utilisation

AAA peut être utilisé dans tous les types d'organisations, y compris :

- Entreprises
- Administrations

❑ Quelques meilleures pratiques

- Utiliser des mécanismes d'authentification forts.
- Définir des politiques d'autorisation strictes.
- Mettre en place un système d'audit complet.

❑ Quelques références

https://www.fortinet.com/fr/resources/cyberglossary/aaa-security#:~:text=Qu%27est-ce%20que%20l,politiques%20et%20audite%20l%27utilisation.



CAP2SEC
A consulting & InfoSec solutions firm

Listes de contrôle d'accès (ACL)

❑ Définition

Les listes de contrôle d'accès (ACL) sont des mécanismes de sécurité qui permettent de contrôler l'accès aux ressources informatiques.

❑ Contexte d'utilisation

Les ACL peut être utilisé dans tous les types d'organisations, y compris :

- Entreprises
- Administrations

❑ Quelques meilleures pratiques

- Définir des ACL strictes.
- Utiliser des noms d'utilisateurs et des mots de passe forts.
- Mettre en place un système d'audit pour surveiller l'utilisation des ACL.

❑ Quelques références

https://www.manageengine.com/fr/network-configuration-manager/access-control-list-cisco.html#:~:text=Une%20liste%20de%20contrôle%20d%27accès%20(ACL)%20est%20un,interface%20pour%20contrôler%20le%20trafic.



CAP2SEC
A consulting & InfoSec solutions firm

Accès conditionnel

❑ Définition

L'accès conditionnel est une stratégie de sécurité qui permet de contrôler l'accès aux ressources en fonction de conditions spécifiques.

❑ Contexte d'utilisation

L'accès conditionnel peut être utilisé dans tous les types d'organisations, y compris :

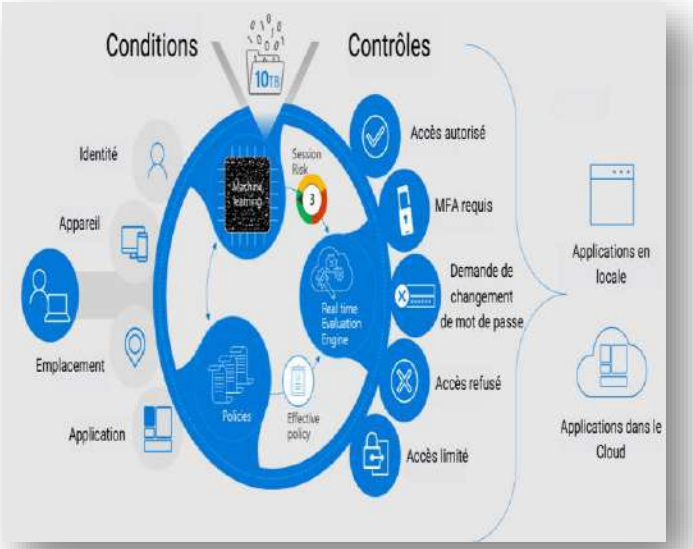
- Entreprises
- Administrations

❑ Quelques meilleures pratiques

- Définir des politiques d'accès conditionnel strictes.
- Utiliser des technologies d'authentification multifacteurs (MFA).

❑ Quelques références

https://www.microsoft.com/fr-ca/security/business/identity-access/microsoft-entra-conditional-access#:~:text=L%27accès%20conditionnel%20est%20un,aux%20ressources%20d%27une%20entreprise.



Mandatory Access Control (MAC)

❑ Définition

Le contrôle d'accès obligatoire (MAC) est un modèle de sécurité informatique qui permet de contrôler l'accès aux ressources en fonction de la classification de sécurité des utilisateurs et des ressources.

❑ Contexte d'utilisation

Le MAC conditionnel peut être utilisé dans tous les types d'organisations, y compris :

- Entreprises
- Administrations



❑ Quelques meilleures pratiques

- Définir des politiques de sécurité claires et concises.
- Utiliser des outils de sécurité pour automatiser l'application du MAC.

❑ Quelques références

https://www.microsoft.com/fr-ca/security/business/identity-access/microsoft-entra-conditional-access#:~:text=L%27accès%20conditionnel%20est%20un,aux%20ressources%20d%27une%20entreprise.

CAP2SEC
A consulting & InfoSec solutions firm

Discretionary Access Control (DAC)

❑ Définition

Le contrôle d'accès discrétionnaire (DAC) est un modèle de sécurité informatique qui permet aux utilisateurs de contrôler l'accès à leurs propres ressources.

❑ Contexte d'utilisation

Le DAC conditionnel peut être utilisé dans tous les types d'organisations, y compris :

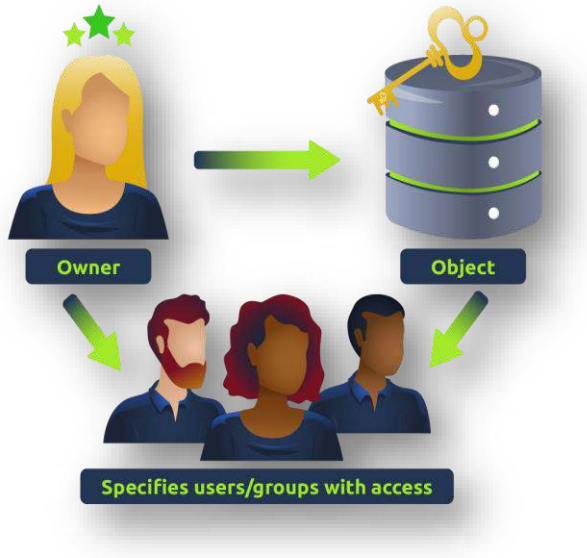
- Entreprises
- Administrations

❑ Quelques meilleures pratiques

- Définir des autorisations d'accès strictes.
- Utiliser des groupes d'utilisateurs pour simplifier la gestion des autorisations.
- Surveiller l'activité des utilisateurs et détecter les anomalies.

❑ Quelques références

https://www.microsoft.com/fr-ca/security/business/identity-access/microsoft-entra-conditional-access#:~:text=L%27accès%20conditionnel%20est%20un,aux%20ressources%20d%27une%20entreprise.



CAP2SEC
A consulting & InfoSec solutions firm

Separation of Duties

❑ Définition

La séparation des tâches (SoD) est un principe de sécurité informatique qui vise à prévenir les erreurs et les fraudes en répartissant les tâches critiques entre plusieurs personnes.



❑ Contexte d'utilisation

La SoD conditionnel peut être utilisé dans tous les types d'organisations, y compris :

- Entreprises
- Administrations

❑ Quelques meilleures pratiques

- Identifier les tâches critiques et les risques associés.
- Définir des politiques de SoD claires et concises.
- Mettre en place des contrôles techniques pour automatiser l'application de la SoD.

❑ Quelques références

https://www.synetis.com/pourquoi-faire-de-la-segregation-of-duties-sod/

CAP2SEC
A consulting & InfoSec solutions firm

Password

❑ Définition

Un mot de passe est une séquence de caractères utilisée pour authentifier un utilisateur et lui accorder l'accès à un système ou à une ressource.

❑ Contexte d'utilisation

Les mots de passe sont utilisés dans tous les types d'environnements, y compris :

- Ordinateurs personnels
- Sites Web
- Applications



❑ Quelques meilleures pratiques

- Utiliser des mots de passe longs et complexes.
- Ne pas utiliser le même mot de passe pour plusieurs comptes.
- Utiliser un gestionnaire de mots de passe pour stocker vos mots de passe en toute sécurité.

❑ Quelques références

https://www.microsoft.com/fr-ca/security/business/security-101/what-is-password-protection

CAP2SEC
A consulting & InfoSec solutions firm

Password Policy

❑ Définition

La politique de mot de passe est un ensemble de règles qui définissent les exigences relatives aux mots de passe utilisés dans un système ou une organisation.

❑ Contexte d'utilisation

La politique de mot de passe peut être utilisé dans tous les types d'organisations, y compris :

- Entreprises
- Administrations



❑ Quelques meilleures pratiques

- Définir des mots de passe longs et complexes.
- Ne pas utiliser le même mot de passe pour plusieurs comptes.
- Mettre en place un processus de vérification et d'application de la politique.

❑ Quelques références

https://www.blogdumoderateur.com/comment-mettre-en-place-politique-mot-de-passe-efficace/

CAP2SEC
A consulting & InfoSec solutions firm

Credential

❑ Définition

Un identifiant est un ensemble d'informations qui permet d'authentifier un utilisateur et de lui accorder l'accès à un système ou à une ressource.

❑ Contexte d'utilisation

Les identifiants sont utilisés dans tous les types d'environnements, y compris :

- Sites Web
- Applications



❑ Quelques meilleures pratiques

- Ne pas utiliser le même identifiant pour plusieurs comptes.
- Modifier régulièrement vos identifiants.
- Utiliser un gestionnaire de mots de passe pour stocker vos identifiants en toute sécurité.
- Ne jamais partager vos identifiants avec d'autres personnes.

❑ Quelques références

https://www.cyber.gc.ca/fr/orientation/gestion-de-lidentite-des-justificatifs-didentite-et-de-lacces-gijia-itsap30018

CAP2SEC
A consulting & InfoSec solutions firm

Keys

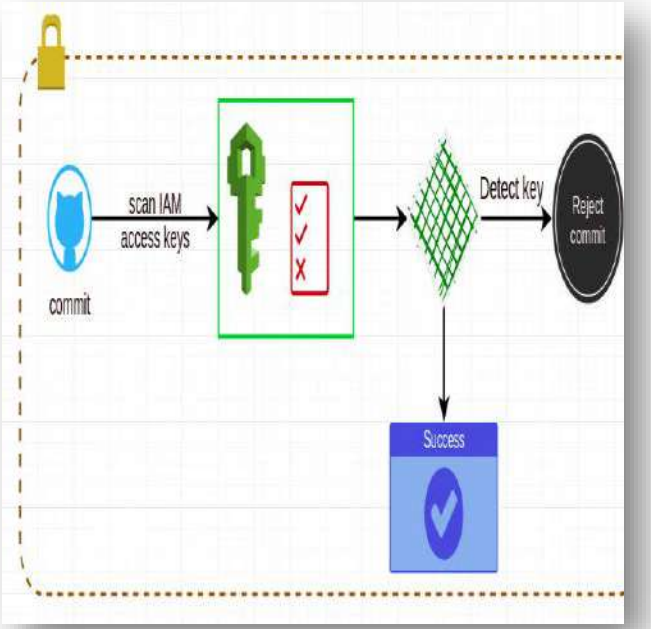
❑ Définition

La clé est Informations utilisées pour crypter et décrypter des données.

❑ Contexte d'utilisation

Clés:

- Cryptage des données stockées sur les ordinateurs et les appareils mobiles.
- Sécurisation des communications en ligne, telles que les e-mails et les VPN.
- Signature numérique des documents électroniques.



❑ Quelques meilleures pratiques

- Stocker les clés dans un endroit sûr et sécurisé.
- Utiliser des algorithmes de cryptage forts.
- Gérer les clés de manière à garantir leur confidentialité et leur intégrité.

❑ Quelques références

https://www.entrust.com/fr/resources/learn/what-is-encryption-key-management

CAP2SEC
A consulting & InfoSec solutions firm

Secret

❑ Définition

Un secret est une information confidentielle qui ne doit pas être divulguées.

❑ Contexte d'utilisation

Secrets:

- Authentification des utilisateurs et des systèmes.
- Accès aux ressources sensibles, telles que les bases de données et les applications.
- Gestion des configurations des systèmes et des applications.



❑ Quelques meilleures pratiques

- Ne jamais partager les secrets avec d'autres personnes.
- Stocker les secrets dans un endroit sûr et sécurisé.
- Utiliser des techniques de hachage pour protéger les secrets.

❑ Quelques références

https://cloud.ibm.com/docs/secrets-manager?topic=secrets-manager-what-is-secret&locale=fr#:~:text=Un%20secret%20est%20une%20donnée,de%20ce%20point%20d%27accès.

CAP2SEC
A consulting & InfoSec solutions firm

Certificate

❑ Définition

Certificats sont documents numériques qui permettent de vérifier l'identité d'une personne ou d'une organisation.

❑ Contexte d'utilisation

Certificats:

- Sécurisation des sites Web et des applications web.
- Signature numérique des e-mails et des documents électroniques.
- Authentification des utilisateurs et des appareils.



❑ Quelques meilleures pratiques

- Obtenir les certificats d'une autorité de certification de confiance.
- Stocker les certificats dans un endroit sûr et sécurisé.
- Vérifier la validité des certificats avant de les utiliser.

❑ Quelques références

https://www.entrust.com/fr/resources/learn/certificate-authority

CAP2SEC
A consulting & InfoSec solutions firm

Privilege escalation

❑ Définition

Escalade de privilèges est une technique utilisée par un attaquant pour obtenir un accès non autorisé à des ressources ou des systèmes avec des privilèges plus élevés que ceux qui lui sont initialement accordés.

❑ Contexte d'utilisation

L'escalade de privilèges peut être utilisée dans tous les types d'environnements, y compris :

- Entreprises
- Administrations



❑ Quelques meilleures pratiques

- Appliquer le principe du moindre privilège.
- Former les utilisateurs aux risques liés à l'escalade de privilège.

❑ Quelques références

https://www.proofpoint.com/fr/threat-reference/privilege-escalation#:~:text=Il%20s%27agit%20d%27une,confidentielles%2C%20la%20consultation%20d%27informations

CAP2SEC
A consulting & InfoSec solutions firm

Biometric access control

❑ Définition

Le contrôle d'accès biométrique est une technologie qui utilise les caractéristiques physiques uniques d'une personne pour l'authentifier et lui accorder l'accès à un système ou à une zone sécurisée.

❑ Contexte d'utilisation

Le contrôle d'accès biométrique peut être utilisé dans une grande variété d'applications, notamment :

- **Informatique et réseaux:** Authentification aux ordinateurs, aux applications et aux réseaux.
- **Terminaux de paiement:** Authentification des paiements par carte bancaire et mobile.



❑ Quelques meilleures pratiques

- Choisir la technologie biométrique la plus appropriée pour les besoins spécifiques de l'organisation.
- Mettre en place des mesures de sécurité pour protéger les données biométriques collectées.
- Former les utilisateurs à l'utilisation du système de contrôle d'accès biométrique.

❑ Quelques références

https://www.boschsecurity.com/fr/fr/solutions/controle-dacces/biometric-access-control/

CAP2SEC
A consulting & InfoSec solutions firm

Strong authentication

❑ Définition

Authentification forte est une méthode d'authentification qui utilise plusieurs facteurs pour vérifier l'identité d'un utilisateur.

❑ Contexte d'utilisation

L'authentification forte peut être utilisé dans une grande variété d'applications, notamment :

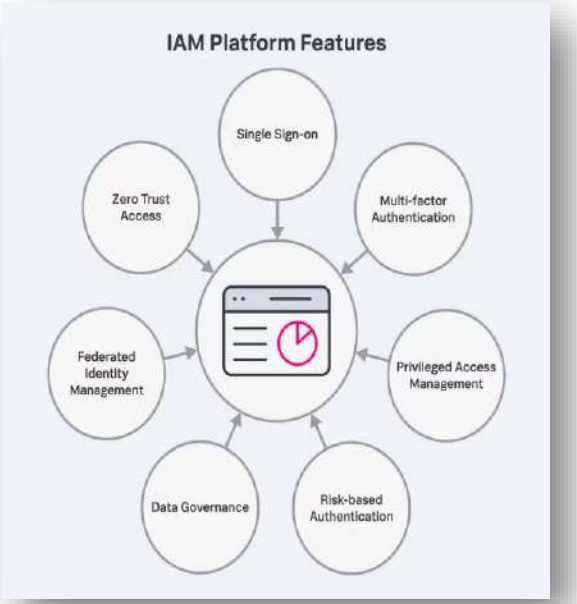
- **Informatique et réseaux:** Authentification aux ordinateurs, aux applications et aux réseaux.

❑ Quelques meilleures pratiques

- Choisir la méthode d'authentification forte la plus appropriée pour les besoins spécifiques de l'organisation.
- Mettre en place une politique de sécurité pour l'utilisation de l'authentification forte.

❑ Quelques références

https://www.abe-infoservice.fr/banque/moyens-de-paiement/quest-ce-que-lauthentification-forte#:~:text=L%27authentification%20forte%20est%20un,de%20coordonnées%2C%20etc.).



CAP2SEC
A consulting & InfoSec solutions firm

Zero-Trust Principle

❑ Définition

Principe du Zéro Trust est un Modèle de sécurité qui ne suppose aucune confiance par défaut, ni à l'intérieur ni à l'extérieur du périmètre du réseau.

❑ Contexte d'utilisation

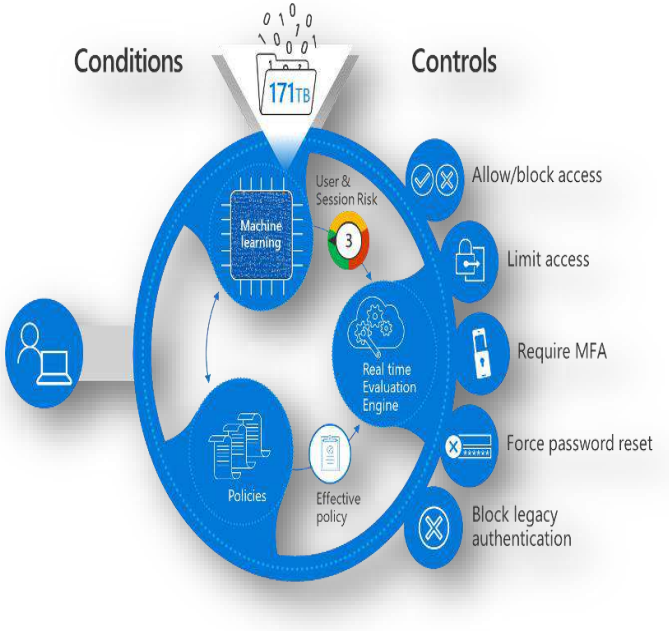
- Peut être utilisé dans tous types d'organisations, y compris :
  - Entreprises
  - Administrations
- Particulièrement utile pour les organisations qui:
  - Ont des données sensibles ou confidentielles

❑ Quelques meilleures pratiques

- Appliquer le principe du moindre privilège.
- Surveiller et auditer l'activité des utilisateurs et des applications.

❑ Quelques références

https://www.cyberark.com/fr/what-is/zero-trust/



CAP2SEC
A consulting & InfoSec solutions firm

Passwordless authentication

❑Définition

Authentification sans mot de passe est une méthode d'authentification qui n'utilise pas de mot de passe pour vérifier l'identité d'un utilisateur.

❑Contexte d'utilisation

L'authentification sans mot de passe peut être utilisée dans une grande variété d'applications, notamment :

- Authentification aux ordinateurs et aux applications.
- Paiements en ligne.



❑ Quelques meilleures pratiques

- Choisir la méthode d'authentification sans mot de passe la plus appropriée pour les besoins spécifiques de l'organisation.
- Mettre en place des mesures de sécurité pour protéger les données d'authentification.
- Mettre en place une politique de sécurité pour l'utilisation de l'authentification sans mot de passe.

❑ Quelques références

https://www.trustbuilder.com/fr/passwordless

CAP2SEC
A consulting & InfoSec solutions firm

Local Access

❑ Définition

Accès local est la capacité d'accéder à un système ou à un réseau informatique en étant physiquement présent sur le site.

❑ Contexte d'utilisation

L'accès local est souvent utilisé dans les environnements suivants :

- Petites entreprises et organisations
- Environnements où la sécurité physique est élevée



❑ Quelques meilleures pratiques

- Mettre en place des mesures de sécurité pour protéger les systèmes et les données accessibles localement.
- Utiliser des mots de passe forts et une authentification multifacteur.
- Mettre à jour régulièrement les logiciels et les systèmes.

❑ Quelques références

https://www.okta.com/fr/blog/2019/05/putting-the-8-principles-of-infrastructure-access-into-practice/

CAP2SEC
A consulting & InfoSec solutions firm

Remote Access

❑ Définition

Accès à distance est la capacité d'accéder à un système ou à un réseau informatique à partir d'un emplacement distant.



❑ Contexte d'utilisation

L'accès à distance est souvent utilisé dans les environnements suivants :

- Grandes entreprises et organisations
- Environnements où la mobilité est importante

❑ Quelques meilleures pratiques

- Utiliser un VPN pour sécuriser la connexion.
- Utiliser des mots de passe forts et une authentification multifacteur.
- Former les utilisateurs aux risques de sécurité lié à l'accès à distance.

❑ Quelques références

https://www.hpe.com/ca/fr/what-is/remote-access.html#:~:text=L%27accès%20à%20distance%20est,depuis%20n%27importe%20quel%20endroit.

CAP2SEC
A consulting & InfoSec solutions firm

Physical Access

❑ Définition

Accès physique est la capacité d'accéder à un système ou à un réseau informatique en étant physiquement présent sur le site.



❑ Contexte d'utilisation

L'accès physique est souvent utilisé dans les environnements suivants :

- Petites entreprises et organisations
- Environnements où la sécurité physique est élevée

❑ Quelques meilleures pratiques

- Mettre en place des mesures de sécurité pour protéger les systèmes et les données accessibles localement.
- Utiliser des contrôles d'accès physiques, tels que des badges et des serrures biométriques.
- Surveiller l'accès aux locaux et aux installations.

❑ Quelques références

https://www.entrust.com/fr/resources/learn/what-is-physical-access-control-system

CAP2SEC
A consulting & InfoSec solutions firm

Access Certification

❑ Définition

Certification d'accès est le processus de vérification et de validation de l'identité d'un utilisateur avant de lui accorder l'accès à des ressources.

❑ Contexte d'utilisation

La certification d'accès est souvent utilisée dans les environnements suivants :

- Grandes entreprises et organisations
- Environnements où la sécurité est une priorité absolue



❑ Quelques meilleures pratiques

- Mettre en place un processus de certification d'accès formel et documenté.
- Utiliser une combinaison de facteurs d'authentification pour valider l'identité des utilisateurs.
- Mettre à jour régulièrement les autorisations d'accès des utilisateurs.

❑ Quelques références

https://www.xpertics.ca/web/index.php/fr/servicesconseils-fr/gia/certif-acces

CAP2SEC
A consulting & InfoSec solutions firm

One-Time-Password (OTP)

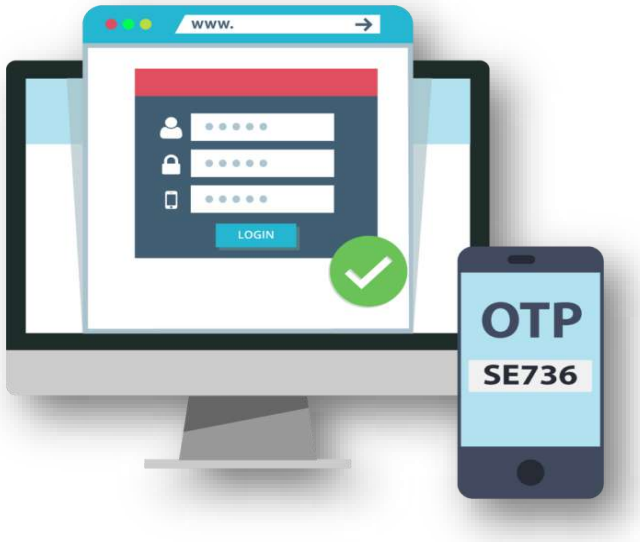
❑ Définition

Un mot de passe à usage unique (OTP) est une séquence de caractères numériques ou alphanumériques générée automatiquement qui permet d'authentifier un utilisateur pour une seule connexion ou transaction

❑ Contexte d'utilisation

Les OTP sont souvent utilisés dans les environnements suivants :

- Authentification en ligne
- Transactions bancaires



❑ Quelques meilleures pratiques

- Utiliser une méthode de génération d'OTP forte et fiable.
- Ne jamais partager un OTP avec quelqu'un d'autre.

❑ Quelques références

https://www.keepersecurity.com/blog/fr/2023/12/20/what-is-a-one-time-password-otp/#:~:text=Un%20mot%20de%20passe%20unique%20basé%20sur%20le%20temps%20est,pendant%2030%20à%2060%20secondes.

CAP2SEC
A consulting & InfoSec solutions firm

Session Management

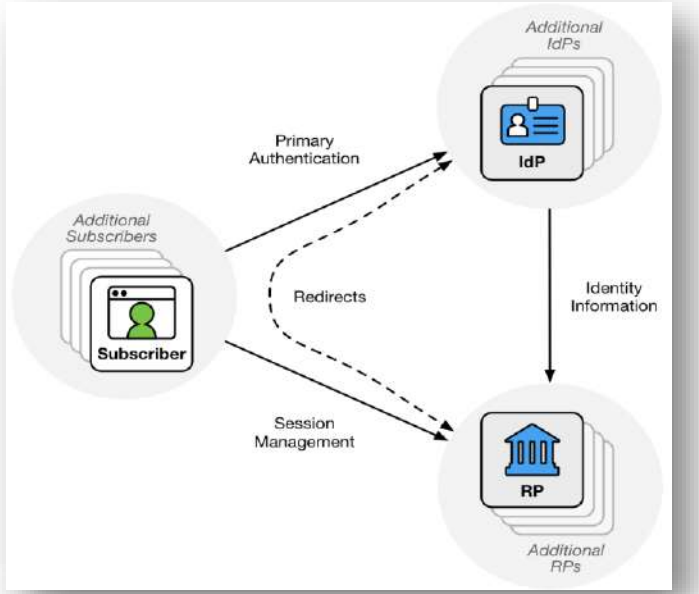
❑ Définition

Gestion des sessions est un processus de suivi et de contrôle des sessions utilisateur sur un système ou une application.

❑ Contexte d'utilisation

La gestion des sessions est utilisée dans une grande variété d'environnements, notamment :

- Sites Web et applications Web.
- Réseaux d'entreprise.



❑ Quelques meilleures pratiques

- Utiliser des mots de passe forts et une authentification multifacteur.
- Utiliser des jetons de session sécurisés.
- Invalider les sessions lorsqu'elles ne sont plus utilisées.

❑ Quelques références

https://www.oneidentity.com/fr-fr/what-is-privileged-session-management/

CAP2SEC
A consulting & InfoSec solutions firm

Token Management

❑ Définition

Gestion des jetons est le processus de création, de distribution et de validation de jetons de sécurité.

❑ Contexte d'utilisation

La gestion des jetons est souvent utilisée dans les environnements suivants :

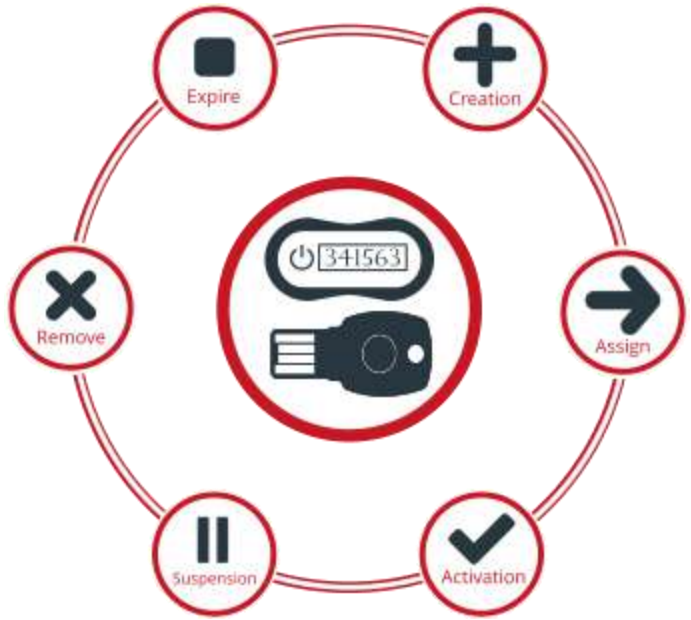
- Sites Web et applications Web.
- API.

❑ Quelques meilleures pratiques

- Utiliser des jetons forts et uniques.
- Stocker les jetons de manière sécurisée.
- Invalider les jetons lorsqu'ils ne sont plus utilisés.

❑ Quelques références

https://www.okta.com/fr/identity-101/what-is-token-based-authentication/#:~:text=L%27authentification%20forte%20par%20jeton%20s%27appuie%20sur%20un%20protocole,jeton%20lui%20a%20été%20accordé.



CAP2SEC
A consulting & InfoSec solutions firm

Identity Store

❑ Définition

Magasin d'identités est un référentiel centralisé contenant les informations d'identité des utilisateurs.

❑ Contexte d'utilisation

Les magasins d'identités sont souvent utilisés dans les environnements suivants :

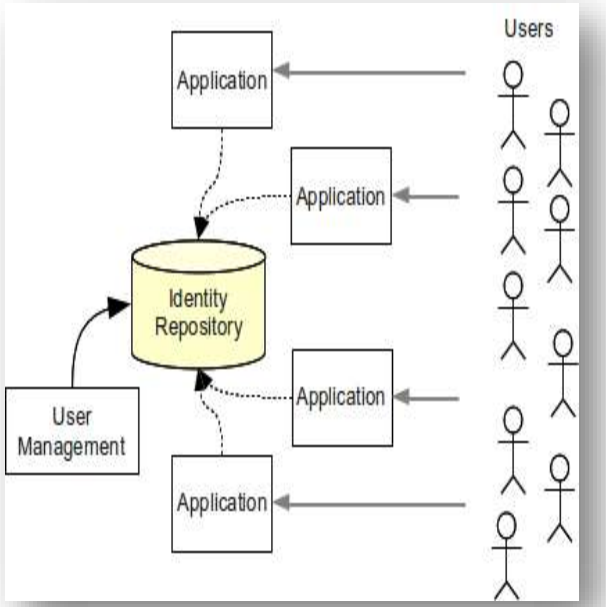
- Grandes entreprises et organisations
- Pour centraliser la gestion des identités des utilisateurs

❑ Quelques meilleures pratiques

- Utiliser un magasin d'identités sécurisé et fiable.
- Mettre en place des contrôles d'accès stricts pour le magasin d'identités.
- Surveiller l'activité du magasin d'identités pour détecter les accès non autorisés.

❑ Quelques références

https://www.microsoft.com/fr-ca/security/business/security-101/what-is-identity-access-management-iam#:~:text=Qu%27est-ce%20qu%27,ont%20accès%20aux%20ressources%20appropriées.



CAP2SEC
A consulting & InfoSec solutions firm

Directory Federation

❑ Définition

Fédération d'annuaires est un système permettant aux organisations de partager des informations d'identité des utilisateurs entre elles.

❑ Contexte d'utilisation

La fédération d'annuaires est souvent utilisée dans les environnements suivants :

- Grandes entreprises et organisations avec plusieurs filiales.
- Partenariats entre entreprises.



❑ Quelques meilleures pratiques

- Utiliser une solution de fédération d'annuaires sécurisée et fiable.
- Mettre en place des contrôles d'accès stricts pour les annuaires fédérés.
- Surveiller l'activité des annuaires fédérés pour détecter les accès non autorisés.
- Mettre à jour régulièrement les informations d'identité des utilisateurs.

❑ Quelques références

https://jumpcloud.com/fr/blog/what-is-adfs#:~:text=ADFS%20permet%20aux%20organisations%20d,au-delà%20des%20frontières%20organisationnelles.

CAP2SEC
A consulting & InfoSec solutions firm

Provisioning

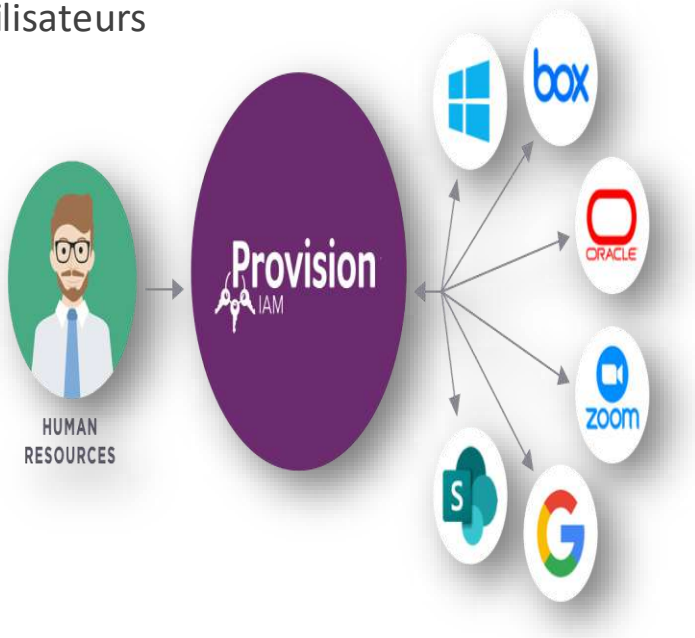
❑ Définition

Provisionnement est un processus de création et de configuration des comptes d'utilisateurs et des ressources associées.

❑ Contexte d'utilisation

Le provisioning est souvent utilisé dans les environnements suivants :

- Grandes entreprises et organisations.
- Pour automatiser la gestion des comptes d'utilisateurs.



❑ Quelque meilleures pratiques

- Utiliser un outil de provisioning automatisé.
- Mettre en place un processus de provisioning formel et documenté.
- Définir des rôles et des permissions clairs pour les utilisateurs.

❑ Quelques références

https://www.redhat.com/fr/topics/automation/what-is-provisioning#:~:text=Le%20provisionnement%20des%20utilisateurs%20est,domaine%20de%20responsabilité%20des%20utilisateurs.

CAP2SEC
A consulting & InfoSec solutions firm

Deprovisioning

❑ Définition

Déprovisionnement est un processus de suppression des comptes d'utilisateurs et des ressources associées.

❑ Contexte d'utilisation

Le déprovisioning est souvent utilisé dans les environnements suivants :

- Grandes entreprises et organisations.
- Pour automatiser la gestion des comptes d'utilisateurs.



❑ Quelques meilleures pratiques

- Mettre en place un processus de déprovisionnement formel et documenté.
- Définir des rôles et des permissions clairs pour les utilisateurs responsables du déprovisionnement.
- Effectuer des audits réguliers du processus de déprovisionnement.

❑ Quelques références

https://www.redhat.com/fr/topics/automation/what-is-provisioning#:~:text=Le%20provisionnement%20des%20utilisateurs%20est,domaine%20de%20responsabilité%20des%20utilisateurs.

CAP2SEC
A consulting & InfoSec solutions firm

Self-service

❑ Définition

Self-service est un processus permettant aux utilisateurs de gérer leurs propres comptes et ressources informatiques.

❑ Contexte d'utilisation

Le self-service est souvent utilisé dans les environnements suivants :

- Grandes entreprises et organisations.



❑ Quelques meilleures pratiques

- Mettre en place un portail self-service facile à utiliser et accessible.
- Proposer une documentation complète et des tutoriels.
- Mettre en place des contrôles de sécurité stricts pour le portail self-service.
- Surveiller l'activité du portail self-service pour détecter les utilisations abusives.

❑ Quelques références

https://www.netiq.com/fr-fr/documentation/identity-manager-46/setup/data/b19fq48e.html

CAP2SEC
A consulting & InfoSec solutions firm

Delegation

❑ Définition

Délégation est un processus de confier une tâche ou une responsabilité à une autre personne.

❑ Contexte d'utilisation

La délégation est souvent utilisée dans les environnements suivants :

- Grandes entreprises et organisations.
- Projets complexes avec plusieurs équipes impliquées.



❑ Quelques meilleures pratiques

- Définir clairement la tâche et les objectifs.
- Choisir la bonne personne pour la tâche.
- Fournir les ressources et les informations nécessaires.
- Suivre l'avancement de la tâche et apporter un soutien si nécessaire.

❑ Quelques références

https://learn.microsoft.com/fr-fr/windows-server/identity/ad-fs/design/when-to-use-identity-delegation

CAP2SEC
A consulting & InfoSec solutions firm

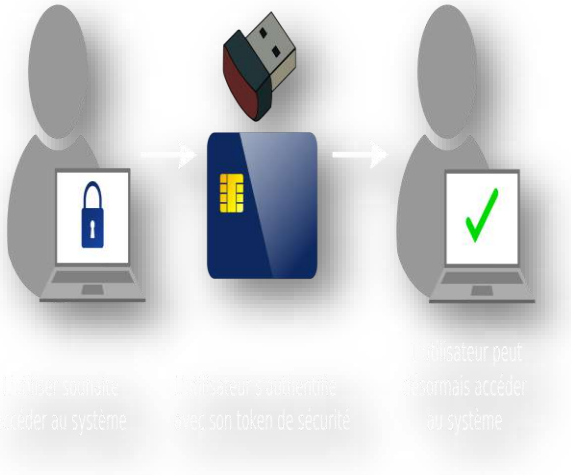
Token (jeton)

❑ Définition

Un token est un processus qui vise à sécuriser les actifs en les protégeant contre les accès non autorisés ou les potentielles fraudes.

❑ Contexte d'utilisation

Les tokens sont souvent utilisés dans les architectures distribuées, telles que les applications monopages, les applications mobiles natives et les API Web. Ils permettent d'authentifier et d'autoriser les utilisateurs de manière sécurisée sans avoir à stocker des informations sensibles comme les mots de passe côté client.



❑ Quelques meilleures pratiques

- Utiliser le protocole HTTPS
- Stocker les jetons en toute sécurité

❑ Quelques références

Token Best Practices (auth0.com)

CAP2SEC
A consulting & InfoSec solutions firm

Cookie (Témoin)

❑ Définition

Les cookies sont de minuscules fichiers de données utilisés pour suivre vos activités et informations en ligne lorsque vous naviguez sur un site Web.

❑ Contexte d'utilisation

Les cookies sont largement utilisés dans le développement web pour diverses fonctionnalités, notamment :

- Gestion de session
- Personnalisation de l'expérience utilisateur



❑ Quelques meilleures pratiques

- Utiliser le protocole HTTPS
- Stocker les cookies en toute sécurité et en toute confidentialité

❑ Quelques références

Token Best Practices (auth0.com)

CAP2SEC
A consulting & InfoSec solutions firm

Conclusion

la gestion des identités et des accès (GIA) est un domaine crucial pour la sécurité informatique. Elle permet de garantir que seuls les utilisateurs autorisés ont accès aux ressources et aux données de l'organisation.

CAP2SEC
A consulting & InfoSec solutions firm

Conclusion

Nous avons abordé plusieurs concepts et terminologies clés de la GIA, tels que :

- **L'authentification:** le processus de vérification de l'identité d'un utilisateur.
- **L'autorisation:** le processus de détermination des ressources et des données accessibles à un utilisateur.
- **Le provisioning:** le processus de création et de configuration des comptes d'utilisateurs.
- **Le déprovisionnement:** le processus de suppression des comptes d'utilisateurs et des ressources associées.
- **Le self-service:** le processus permettant aux utilisateurs de gérer leurs propres comptes et ressources informatiques.
- **La délégation:** le processus de confier une tâche ou une responsabilité à une autre personne.

Il est important de comprendre ces concepts et terminologies pour mettre en place une stratégie GIA efficace.

CAP2SEC
A consulting & InfoSec solutions firm

Questions et discussions

Nous invitons maintenant les participants à poser des questions ou à entamer des discussions sur le processus de normalisation et ses avantages pour notre entreprise.