Prise de notes : Sécurité

Généralités sur le cours

- quelques TDs / TPs autour de l'IAM ;
- Intervennant Capgemini ;
- Quizz à la fin simple mais qu'avec des pièges (médecine be like :'( ) -Léa ;
- Le quiz à la fin c'est 'facile', y'a surtout BCP de pièges. Donc faut faire gaffe (17-18 facile) -Pierre.
- on regarde dans ce cours quel technologie répond à quel besoin

Table des matières

Définitions

Mot	***Définition***
IAM	Identity and Access Management, gestion des identité des accès
Identité	ce qui fait l'unicité d'un objet/persone
Annuaire	Là où on enregistre les identités
UID	User ID
IAG (ou IGA)	Identity and Access Gouvernance
APIM	API Management (à part, on le compte pas vraiment)
AM	Acess Management
PAM	Privileged Acess Management
PKI	Public Key Management
CIAM	Customer IAM (le client et son IAM, genre un drive chez google quand on est pas dev là bas)
Workflow	Gere qui a accès à quoi, (ex: départ/arrivée collaborateur, passer une command, mutation, évolution ect...)
MFA	Multi-Factor Authentification
OIV	Organismes d'Importance Vital (par exemple hopitaux ou centrale nucléaire)
TPM	Puce pour chiffrer (ex : on y retrouve l'empreinte digitale)
on prem	On a nos propres serveurs
JML	Joiner Moover Leaver(le cycle de vie)
RBAC	Role Based Account Control (modèle de droit)
LDAP	Lightweight Direc tory Access Protocol: Consodilation de l'identité pour qu'elle soit cohérente dans le SI RH
Hab ou habilitation	le fait de valider ou pas (?)
ANSSI	Agence Nationale de Sécurité des Systèmes d'Information
SSO	Single Sign-On - authentification unique pour plusieurs apps
(X) SoD	Segregation of Duties (séparation des pouvs en gros, la personne qui valide les congés peut pas valide ses congés)
Fédération d'identité	Utiliser un compte X pour se connecter à X, Y, Z et autres (comme Google)
Off boarding	Enlever les droits quand les employé en ont plus besoin
SOC	Security Operations Center
ERP	Enterprise Resource Planning
CCM	Cloud Control Matrix: is a cybersecurity control framework for cloud computing (OpenSource)
KPI	Key Performance Indicators
SLA	Service Level Agreement
LDAP	Lightweight Directory Access Protocol

Mot	***Définition***
OID	Object IDentifier
Principe du moindre risque	c'est le principe du whitelist en IAM afin de limiter les risques: on fait en whitelist: de base t'as rien, et on te donne accès aux trucs dont t'as besoin
VOC	Vulnerability Operations Center
UCF	User Case Factory
CERT	Computer Emergency Response Team
CTI	Cyber Threat Intelligence
SWAT	Security Worldwide Assistance Team
TTPs	Tactics, Techniques and Procedures
MITRE ATT&CK	Matrix of TTPs
IoCs	Indicator of Compromises
MCO	Maintaining Operationnal Conditions

1. Introduction à IAM : end point security

1.1. Digital Identity (DI)

On retrouve dans la DI:

- IAM
- IAG
- PAM
- …

Une identité c'est nous, ce qui nous rend unique, On la prouve avec une carte d'identité. L'IAM c'est prouver comment c'est nous dans un système d'information.

Ensemble de procédures, orgas, techniques permettant de gérer une bonne utilisation des accès aux ressources d'un SI. On ne peux pas différencier les gens de l'ENSEEIHT entre eux selon l'école mais pas exemple on peut le faire selon le numéro INE ou le numéro de la carte vitale. Pas par le nom et le prénom car ce n'est pas unique (homonymes).

4 (ou 5) grandes disciplines:

1. IAG : gestion des identités ;
2. AM ; Access Management ;
3. PAM ; Privileged Access Management;
4. PKI : gère le chiffrement entre 2 entités.
5. CIAM : Customer IAM (exemple: Google, Facebook ect…) (soumis à des contraintes comme RGPD par exemple)

l'IAM c'est :

- Authentifier ;
- Autoriser ;
- Gérer les users ;
- Centralisation des données.

C'est un enjeu de sécurité car:

- Espionnage ;
- Usurpation d'identité (peut aller jusqu'à la « fraude au président ») ;
- Vente (Black Market).

Ex : Airbus = plusieurs métiers avec différents rôles, on pourrait casser les chaînes de prod facilement.

Sécurité publique: modifier les dosages dans les usines indus/pharmaceutiques, ce qui peut être problématique/dangereux.

- Exemple : Si on usurpe le compte de maintenant du gars qui pèse la quantité des médoc et il change le grammage de 1 à 2 c'est un danger pour nous car on pourrait risquer de tuer des gens par exemple. (??? rien compris *Léa*)

Annuaire <=> grosse bdd.

sur PC pro **avant**, n'importe qui peut se connecter tant qu'il a le mdp et l'ID. Le PC pro interroge l'annuaire pour savoir s'il peut se connecter (comme les pc de l'ENSEEIHT où on peut se connecter à différents pc (réel)).

- Peut vite être le bordel quand on augmente en taille ;
- Et si c'est le bordel il est plus vulnérable car on ne peut pas tout surveiller ;
- On cherche plutôt à avoir un point d'entrée et un point de sortie unique.

IAM répond à quelque point de la RGPD car on sait qui a fait quoi.

Deux grandes exigences de sécu :
- NIS 2, pour les entreprise qui travaille avec des OIV ;
- DORA pour le bancaire. (Genre Dora l'exploratrice)

pass key : va remplacer les passwords.

Le pass key c'est **pas** toi qui met ton mdp au contraire du mdp.

IAM a pour but de complexifier le hack sans complexifier l'authentification pour l'utilisateur (on va pas mettre 15 mdps d'affilé).

1.2. IAG

C'est plus fonctionnel que technique.

fonctionnel: on s'intéresse aux intéractions entre acteurs afin de créer des règles, nomenclatures ect…

4 grands principes de l'IAG :

- Cycle de vie (JML)
- Habilitation
- unification (LDAP et RH)
- RBAC (Modèle de rôles/droits)

1.2.1. LMJ:

- Joiner: rejoints ;
  - Nouveaux employés
- Mover: changements verticaux/horizontaux dans une entreprise ;
  - Si vertical, il faut pas garder toutes les ressources (certaines faut garder) ;
- Leaver: quitter.
  - Employés partant, donc faut correctement leur enlever les droits aux ressources.

Mettre un verrou sur les droits en cas d'absence temporaire (ex: congé paternité/maternité, année sabatique, etc…)

1.2.2. RBAC

Modèle de droit : RBAC = on créer des rôles qui ont des droits et on les donnes ces rôles (ou les prêtes lul); ex: principe de discord (création de roles qui ont des accès ≠ en fonction du rôle)
- On essaie de les simplifier pour faciliter la gestion (? *Pierre*) ;
- On demande des droits (validé par supérieur ou tierce personne) avec un seul modèle d'habilitation (ex: secret défense).

Pour limiter la complexité temporelle, on ne va pas trop loin dans la délimitation des roles. Et en dessous d'un certain niveau (où c'est pas trop important/risqué), on essaie pas réellement de voir ce dont ils ont besoin pour donner les bons droits.

1.2.2.1. Droits métiers

- Représentation d besoins
- Manipulé par les utilisateurs finaux
- Faite par responsables métiers
- Modélisation simple et accessible

1.2.2.2. Droits applicatifs

- Modèle d'habilitation d'une application
- Utilisée pour l'alimentation …

1.2.3. Unification

Unification des identités.

Ex: dans LDAP je m'appelle MARTIN Nolann, mais dans le SI RH je peux avoir un « bug » et m'appeler MARTIN Nohlan. *Nolann* beaucoup de Nolann quand même non ? peut etre donc *Nono*

erreur de frappe entre LDAP et SI RH (par ex: passage de Nolann à Nohlan), ça peut aussi être « normal » car mariages/divorces ou changement de sexe/genre.

1. Le principe est de savoir QUI A RAISON (en général: celui qui crée ⇒ LDAP pour @mail et service RH pour nom/prénom)
2. Donc on fusionne les infos qu'on croit.

Identifiants Comme des associations nom/prénom peuvent être communes, on va associer aux entrées de la base, un identifiant.

2 types d'identifiants:

- Utilisateur : connu et utilisé par l'utilisateur (souvent) *ex: pseudo*
- Technique : ID unique par individu et peu souvent utilisé *ex: num carte vitale ou INE*

Finalité (ETL) Un logiciel qui compare les attributs des différentes bases, les combine en fonction de celles qu'il croit, et ensuite il propage les infos combinées.

- La question de la rapidité de synchronisation est importante car faire automatiquement peut créer des problèmes où tu lock out une personne de ses accès.

1.2.4. Workflow

Workflow (provisionning mais avec actions de l'user) Il y a 2 workflow de base:

- Automatique: comme sur moodle quand on cherche l'accès à nos cours: on demande, on a.
- Manuelles : automatique mais il faut une validation d'un intervenant.
  - On peut faire varier le nombre d'intervenants mais, éviter de mettre trop d'intervenants car ça peut GRANDEMENT retarder l'attribution des rôles.

1.2.5. Habilitation:

en gros: séparation des pouvoirs

Différents niveaux en fonction du role de l'individu, qui lui donne ou non accès à des ressources.

On utilise aujourd'hui beaucoup l'IA. Pour aider à gérer les comptes.

Exemple: Airbus a ∼5k applications, ∼100k users, donc avec 1 compte/app/personne on arrive VITE dans des trucs **TRÈS Compliqués** à gérer.

1.2.6. Certification

Si jamais on a pas supprimé des droits, donc faut un jour le faire migrer sur un truc « safe » => un compte pas utilisé est un danger (peut être hack sans qu'on le sache).

Si la certification(de l'ANSSI) passe pas on peut avoir plusieurs problèmes:

- Pas de label donc pas de contrat avec certaines entreprises ;
- Sanctions financières ;

- etc…

Identifier ≠ Authentifier :
- Identifier : dire « c'est toi », on te fais confiance ;
- Authentifier : prouver que c'est bien toi, pas que shallah c'est moi.

ex: via le mail de l'école: on peut identifier des gens (savoir qu'ils existent) mais on peut pas se connecter à leur place.

1.3. PAM

(leader du marché: cyberark)

un PAM est un compte qui as suffisamment de droits pour compromettre tout ou partie du service.(ex: `sudo rm -rf ./*`)

bastion = place forte (médiéval) point de sécurisation important.

revoir le fonctionnement

les comptes à privilèges vont passer par un bastion pour accéder à qql chose et il ne peut passer nulle part ailleurs. (ex: pour rentrer dans un festival on passe par la sécu qui s'assure de l'autorisation d'accès)

L'ANSSI préconise également une rotation des mots de passe des PAM tout les 180 jours (faut les apprendre ou gestionnaire de mdp).

VPN: passer d'un point A à un point B sans qu'on te voit.

dans un bastion on met en place une session sécurisée, chiffrée et pas aliénable.

Protocoles de gestion de session à distance:
- Linux: SSH ;
- Windows: RDP.

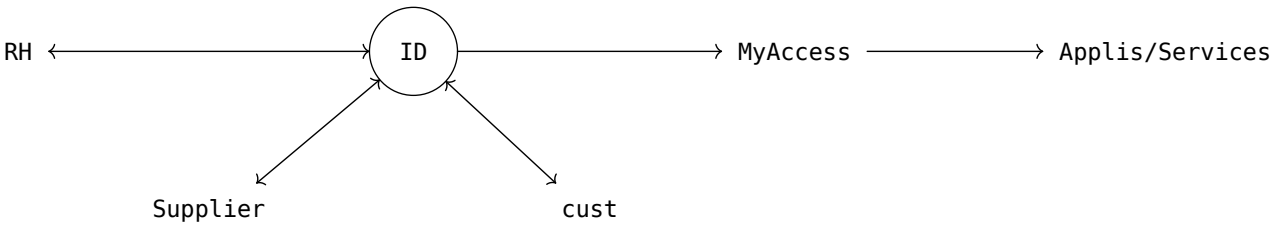
Mais elles ont leurs limites pour les PAM.

une application pour gérer un bastion c'est 7 serveurs.

on enregistre les sessions pour pouvoir les remonter (ex : pour une enquête judiciaire).

1.4. IAM (Identity Access Management)

ensemble de procédures, organisation et moyens techs qui gère les IDs des utilisateurs et leurs accès. Il y a toujours les mêmes données:
- Utilisateurs (clients, fournisseurs, employés ect…) (Populations)
- Services (Applications)
- Fournisseur d'ID (Annuaire)
- niveau de droits (Habilitations)



1.4.1. Annuaires:

BdD centralisées utilisées pour stocker et gérer ls infos d'id des users, ainsi que leurs droits et accès aux rss.

les + connus:
1. Microsoft Active directory
2. Microsoft Entra ID (Anciennement Azure AD)
3. OpenLDAP (il faut mettre la description)

3 composantes essentiels pour l'intégrité :

Monitoring	**Audit**	**Reporting**
• detecte intrusions • identifier abus privilèges • assure dispo/perf des services	• Fourni piste pour les enquêtes • Vérifier efficacité des contrôles + identifier les lacunes • Satisfaire exigences réglementaires/conformités	• Informer de l'état de la sécurité • Identifier les lacunes • Documenter les incidents de sécu

1.4.2. CIAM

Gère + contrôle les accès des clients aux services, parce que les ressources sont pas du tout les mêmes.

(en terme d'éthique: *demandez à boeing, en ce moment c'est pas la joie*)

1.4.3. PKI/CLM (Public Key Infrastructure/ Certificate Lifecycle Management)

PKI: éléments délivrant des certificats numériques pour faire des chiffrements.

CLM: gestion du cycle de vie des certificats numériques depuis création jusqu'à expiration/ révocation. Gère les rotations de certificats sur $\neq$ clés publiques.

2. Cours sur le Cloud Security Course (CSC contre son camp)

« 50 ans depuis 7 années » Le prof

🍟 😨

ouvrir un compte sur AWS, OVH, Azure, (GCP)

2.1. Intro sur le cloud

Définition 1: Cloud
Accéder à un service à distance qui ne nous appartient pas via Internet

Jeff le Bzezoz il a créer une énorme infra pour pouvoir gérer les commandes le jour du black friday. Mais le reste de l'année… bah y'a clairement pas les mêmes demandes. Donc les ressources sont pas utilisées.

Ils ont donc décidé de laisser les ressources accessibles via un API. Leur 1er client: NASA.

- AWS (Amazon Web Services) est le plus gros fournisseur de cloud worldwide.

On a accès au cloud via internet donc un réseau publique donc pas secure du tout.

Le plus gros avantage pour les entreprise est le **CAPEX (CAPital EXpenses) vs OPEX (OPerative EXpenses)**

✨ 🎀 **Citation inspirante** 🎀 ✨ **:**
Le cloud c'est comme quand on va au supermarché en bas, on y va pour acheter une bouteille d'eau et on ressort avec le sandwich, les chocolats..

🌷 🌺 *Laubreux Sébastien* 🦋 *12 mars 2025* 🌺 🌷

MCO : Maintien aux Conditions Opérationnelles.

Alexy a que 20 minutes de retard 🎉 comme toujours 🗿 He remembered you exist but not for too long lmao

ca

Azure et AWS ont des problèmatiques liés aux IAs ⇒ beaucoup d'entreprises incorporent des IAs dans leurs procéssus.

- Cela pose des problèmes de sécurité car ça part dans Internet, et dans les modèles d'entrainement de IAs, donc ça devient publique ;
- Azure et AWS ont mis en place des serveurs à eux qu'ils installent directement dans les locaux des entreprises pour stocker les données sensible des entreprises.

3 grands modèles de cloud :

- IaaS (Infrastructure as a Service) : je fais tout de A à Z;
- PaaS (Plateform as a Service);
- SaaS (Software as a Service) : google Drive, (Applis Web 😭) .

Qui est responsable de quoi en fonction du modèle:

- IAM : user
- Data : User
- Apps : IaaS/Paas (User) SaaS (Cloud Service Provider)
- …

2.1.1. Enjeux:

- Impacts financiers: perte de clients;
- Réputation : on te voit mal;
- Juridiques et règlementaires : genre free y'a 6 mois;
- Impacts organisationnels : Pointer du doigt les autres.

✨ 🎀 **Citation inspirante** 🎀 ✨ **:**
Lorsque l'entreprise se fait attaquer, dans notre jargon on dit se faire poutrer

🌷 🌺 *Sébastien Labreux* 🦋 *12 mars 2025* 🌺 🌷

NIST equivalent de l'ANSSI mais pour les US.

Dans la sécu y'a les « geek » et y'a ceux qui font de la gouvernance (ceux qui créent les règles à suivre/protocoles ect…), genre du droit etc…

lire le doc pour connaitre tout les gestes à appliquer pour mettre en place un cloud

On doit protéger plein d'aspects suseptibles d'être attaqués:

1. Governance : Que les protocoles soient efficaces ;
2. IAM : mauvais accès à X, ect… ;
3. Crypto/Encryption : Que les infos soient bien cryptés ;
4. Données : duh ;
5. Infrastructure : Avoir une infra robuste face à des potentielles attaques ;
6. Workload (DDoS) ;
7. Shift-left App Security : ???;
8. Continuité de business + résilience : en cas d'attaque, il faut pouvoir continuer à opérer pour éviter des trop grosses pertes d'argent ;
9. Visibilité + detection : Faut pouvoir avoir une vision de tout et détecter les anomalies (par exemple: si un compte accède à des répositories qu'il avait jamais consulté + téléchargement ect…) : le scan est automatisé (+ calcul de % d'anomalie), et le SOC a les warnings en Real Time;
10. Security Icident Managment and response.

2.2. DevSecOps

On ne peut plus parler de DevOps simplement. On parle toujours de DevSecOps.

On peut pas parler de cloud sans parler de DevSecOps. La méthode Agile est indispensable pour accélérer le processus.

Le Sec est là pour fusionner les Dev et les Ops.

Aujourd'hui on fait surtout du PaaS

2.2.1. Dev

L'équipe qui fait le service.

On planifie, on code, on test et on livre aux Ops, et ils récupèrent les éventuels retours.

Il faut faire un code avec un minimum de sécurité.

2.2.2. Ops

L'équipe qui Maintient le service.

On délivre, on déploie (via scripts), on opère, on surveille, et on transfert les éventuels retours.

Si on voit un problème sur un script ou autre. On ne débranche JAMAIS dès le début, on doit récupérer les logs, isoler, prendre des screens ect… Et seulement après on peut débrancher les serveurs.

- Important pour pouvoir porter plainte, analyser, essayer de combler les brèches.

Comment gérer les smartphones des collaborateurs pour éviter que le téléphone (Google, Apple ou autre), ou si jamais il est hacké, récupère des données? ect…

2.2.3. Zero Trust:

- On fait pas confiance aux collaborateurs: 50% des attaques viennent interne à l'entreprise.
- On s'assure que c'est bien la personne à qui appartient le compte:
  - MFA
  - Demander une vérification tout les X temps (avec une variation aléatoire)

2.2.4. Wiz :

Service d'analyse de « failles » des comptes cloud (AWS, Azure, ect…):

Car un oubli de configuration fait que les données envoyées sur le cloud sont accessibles à tous.

3. Les Annuaires

On trouve les annuaires dans les entreprise, dans les gros réseaux. Les annuaires sont comparables à des bases de données centralisées.

Le LDAP permet de faire les authentifications et les autorisations.

3.1. Différence avec BDD

- Les 2 stockent des données et on doit s'authentifier.
- On s'authentifie pour avoir accès aux données de l'annuaire.
- Sur un annuaire, les données sont hyper indexés : BEAUCOUP plus de consultations pour lire qu'écrire
- Ils sont faits de manière hiérarchique
- Ils sont compacts.
- peuvent étendre recherche sur d'autres annuaires et organiser les résultats
- réalisent des BIND (vérification du bon login/MDP pr une connexion) + gestion authentification + gestion des droits

Objectif des annuaires c'est que ça aille le plus vite possible.

3.2. Protocol LDAP (Lightweight Directory Access Protocol)

Format pour importer/exporter des données dans des annuaires avec des fichiers texte.

- En Java via JNDI

le design d'un annuaire est format hiérarchique. L'annuaire est composé de :

- Classes ;
- Entrées ;
- Attributs ;
- Valeurs (format dépends de l'attribut).

3.2.1. Vocabulaire de base :

Classes:

composé de:

- Nom
- OID (Object ID)
- Attributs obligatoires
- Attributs optionnels
- type (structurel, auxiliaire, abstrait)

Entrées : peut définir une personne,un groupe, une unité… La distinction se fait par le biais de classes.

DIT (Directory Information Tree)

définit structure/arborescence de l'annuaire

Données LDAP sont struct arborescence hiérarchique.

3.2.1.1. Les classes

Une classe est défini par un nom qui l'identifie, un OID

Possibilité d'héritage : création de classes filles pour ajouter des attributs supplémentaires.

Il y a des attributs prédéfinis, qui sont paramétrables.

Si un des attributs est limité en terme de taille (par ex 52 charactères), on peut les modifier pour passer par exemple à 256 caractères.

3.2.1.2. Les attributs

il peut être mono ou multivalué (avec une lettre, une $*$ ou si il faut un nom précis).

Il y a des attributs fonctionnels (cn) et d'autres techniques (uid).

3.2.1.3. Une entrée

Il y a beaucoup d'entrées possibles, elles peuvent définir une personne, un groupe, une entité organisationnelle etc ...

Même les classes passent par des entrées.

3.2.2. Filtres LDAP

Servent à faire des recherches. Les recherches sont composées d'un attribut, d'un opérateur de comparaison et d'une valeur.

On mets dans la forme (&(cond 1)(cond 2)) pour **ET** et similairement: (|(cond 1)(cond 2)) pour **OU**. On mets à la negative en mettant **!** avant la condition.

3.2.3. Debug/logs

On regarde le paramètre **olcLogLevel** dans la section **cn=config**.

3.2.4. Indexation

Permets les recherches plus rapides. Indexes calculés à chaque modif/création $\Rightarrow$ plus il y a d'indexes, plus l'ecriture est lente.

3.2.5. ACL (Access Control List)

gère les droits d'accès des entrées de l'annuaires.

Il y a différents niveaux de droits. Chaque niveau supérieur inclu les inférieurs.

3.2.6. Vocab en plus:

- **LDIF** : Format d'import/export d'un annuaire (en fichier texte)
- **OID** : ID universels, représentés sous forme d'entiers.
- **Bind** : Permets de vérifier couple login/mdp est valide
- **DN** Distinguished name
- **RDN** Attribut de l'arborescence
- **base DN** défini racine de l'annuaire
- **GPO**: Group Policy Object. Appliquer des paramètres de sécu sur utilisateurs ou ordinateurs. *ex: forcer le changement de mdp tout les 180 jours*

Les PGO font soit en fonction de

1. l'utilisateur, quel que soit le poste.
2. Ordinateur, quel que soit l'utilisateur.

4. Cycle de vie des Projets IAM

Pourquoi pas de sens de dire « projet IAM » car un « projet » IAM vis dans le SI pendant un long moment en évolution permanente… donc on va parler de programme IAM.

Un **projet** a un début et une fin. Au contraire, un programme évolue.

Et dans un SI, il est constament en évolution par rapport à de nouveaux logiciels, nouvelles techniques, technologies etc…

4.1. 2 modes de forfait:

On peut vendre un projet suivant 2 manières:

- Forfait ;
- AT/ Régie.

Elles sont différent.

Forfait

- Engagement de **résultat** ;
- projet cadré d'un POV ;
- cycle en V ou Agilité .
  - On préfère le cycle en V car en IAM, il y a trop d'interlocuteurs donc l'agile est défavorisé dans ces cas .

AT/ Régie

- engagement de moyens.

Phases d'un projet

1. RFP : request for proposal, identification d'un besoin ;
2. Phase d'avant-vente (négocitation) ;
3. Design + Réalisation du projet ;
4. Usage quotidien, incidents, ajuster le code .

En IAM le contexte client va tout influencer (exemple un en aéronautique et un en pharmacie ne demandent pas du tout les même choses)

Tout se joue au moment du design :

- bcp de réunions ;
- bcp de discussions .

4.2. PAM

En sécurité, un compte à privilège, est un compte qui peut mettre en péril le SI.

Pourquoi les protéger?

Plus rapide de récupérer des infos, ou d'en détruire.

APT Gros groupes d'attaquants (souvent rattachés aux pays (US, Israel, Corée du Nord, Chine, Russie etc…))

C'est pas anormal d'avoir + de comptes privilégié que d'employés. En effet, c'est dû à l'utilisation de nombreux logiciels/services. Et la possession de ces comptes est concentré sur une toute petite population d'employés.

La PAM permets de:

- atténuer les risques de sécurité en s'assurant que les accès sont limités à ceux nécessaires pour le travail
- Réduction d la surface d'attaque globale
- Diminution des coûts opérationnels + complexité
- Amélioration de l visibilité + connaissance du contexte (film de l'écran + logs)
- Améliore conformité réglementaire .

4.2.1. Compte local vs compte d'entreprise

Un compte local est un compte enregistré en dur sur l'ordinateur.

4.2.2. Compte de domaine

Si tu l'as, t'es Dieu.

4.2.3. Compte de service

4.2.4. Compte d'équipes

1 compte pour une équipe

À BANNIR: On peut pas savoir qui a fait quoi.

4.2.5. Compte à privilèges Non Interactif et Non personnels

Compte Machine 2 Machine, faut bien les proteger aussi car vu qu'ils sont M2M, personne va aller vérifier tout les matins.

4.3. Solution de PAM

- coffre fort où on sépare les comptes en zones/roles.
- Accès que via Bastion sécurisé
  - AUCUNE connexion latérale
- mdp changés régulièrement et automatiquement
- accès au bastion via portail web: permets connexion à distance et connexion indirecte

4.4. Architecture multi-tiers

Afin de ségréguer les risques, on divise le SI en plusieurs tiers en fonction du risque si la machine est hackée.

- Tier 0: Contrôleur de données, Public Key Infrastructure ;
- Tier 1: serveur Web + base de données ;
- Tier 2: poste de travail, tablette, téléphone etc ....

5. IAG ou IGA (et non pas viagé) (Re du cours d'avant)

C'est plus fonctionnel que technique.

fonctionnel: on s'intéresse aux intéractions entre acteurs afin de créer des règles, nomenclatures ect…

5.1. Unification

Dans les SI, il y a plusieurs sources d'identité :

- Annuaires ;
- RH ;
- ...

Donc il peut y avoir des anomalies entre les sources. Il faut donc déterminer qui on croit.

- On se mets au mileu des sources, et on croit celle qui a créer l'info. **Peut ne concerner que une des données dans la bdd** (si nom, prénom, @mail,adresse physique, etc…).

Je mets dans la partie du haut.

👍

6. SOC/CERT/CTI careers and activities

Slides en anglais

6.1. Représentation Générale

3 centres majeurs et leurs but:

- CTI : Rechercher pour Anticiper
- SOC : Know to Detect
- CERT : Contextualize to React
  - Peuvent idenifier un groupe via la note de ransom (les groupes de hackers ont pas 5O formats de notes de rançon)

6.2. Careers on SOC:

- SOC Manager

6.2.1. Detection :

Soc Analyst N1 :

DO	DON'T DO
Shifts of 24/7 (Surtout 3x8)	Qualifies Incidents
Handles initial tirage of incidents	Conducts in-depth investigations
Monitors security alerts	Presents findings directly to the customer

Soc Analyst N2 :

DO	DON'T DO	MAYBE
Qualifies incidents detected by level 1 analysts	24/7 shifts (except in worldwide companies that don't stop)	create detection rules
Conducts in-depth investigations		
In contact with customer		

User case Factory :

DO
Creates detection rules
Demonstrates

SOC Analyst N3 :

DO
Gestion des évènements Critiques
Train and moniter lower level SOC Analysts
Security Audit: Perform security audits to assess the effectiveness of proection measures
Participation in simulations: participates in incident response simulation to test and improve procedures.

6.2.2. Reaction

DO	**DON'T DO**	**MAYBE**

CTI … VOC PenTest

6.2.3. Anticipation

CTI Analyst

6.2.4. Support

Engagement Manager

- N'a pas de rôle technique, uniquement du « humain ».

System And Network Administrator.

- Répare les pannes du réseau
- S'occupe de l'évolution du réseau (nouveaux PCs, serveurs et autre)
- Maintient les serveurs
- Implantation de sécurité
- Backup et restauration (peut contrer un ransomware en bonne partie)
- MAJs et Patchs

Approche 3,2,1

- Au moins **3** mois de sauvegarde
- sur **2** serveurs différents
- dont **1** offline

Ingé de Maintien en Condition d'Opérations

DO	**DON'T DO**	**MAYBE**

7. Exercice : Logs

Who ? with a macintoch (MAC) in mozilla from beijing

What ? Récupération d'image, de données, etc…

When ? 26 janvier 2025

Where ? Jafsoft/

Why ?

Forme:

<user> [date + time + fuseau horaire] '<Request>'<status> <Byte size> '<URL>'

Who: fcrawler.locksmart.com (robot de Google) puis ppp931

What: récupère des contacts, et l'autre récupère des Images, en gros: récupérer des infos

Where: 123.123.123.123 (Beijin) (3 où mais on a qu'un qu'on peut retracer)

When: 26 Jan 2025 minuit

Why:

1) fcrawler récupère à …h les contacts à l'adresse fastwebcrawler. Voulait obtenir les contacts de ashen@looksmart.net 2)

8. Exercice pratique

8.1. Ex1

Who : Le groupe TA505/Clop (russophone) What : Un rançongiciel sans chiffrement When : Depuis 2019. Clop a l'habitude d'attaquer pendant les vacances 😂 Where : Le logiciel est déployé partout hors de l'ancienne Union Soviétique. Why : Pour faire de la thune nan ?

8.2. Ex2

When: depuis 2013, mais découvert le 24 November 2021 et patché en décembre 2021

Where: EVERYWHERE (includes: AWS, Minecraft, Steam, Tencent)

Why: y'aura toujours des failles? Ou sinon tout ce qui implique l'extraction de données

Who: vulnérabilité en Java

What: push Java code on Servers and computers

9. Poubelle