

TOSA certification

Présentation par :

Marvin , Guy , Alan , Jason

Comment réagir en cas d'attaques

Le temps joue contre nous



Plan d'Intervention

Type? Moment?

Chaque type de menace demande un type de réponse

Pour chaque moment de l'ataque, existe une stratégie plus adéquat

Plan d'Intervention

Qui?

Il faut prévoir une liste des personnes à qui appeler

CISO - Chief Information Security Officer

CTO - Chief Technology Officer

Département Juridique

Assurance

Autorités compétentes

Plan d'Intervention

Quand?

Le temp est court

Il faut prioriser les actions qui peuvent réduire les dégâts

Plan d'Intervention

Quoi?

Les premier démarche

Déconnecter les câbles

Isoler les ordinateurs affecté

Arrêter la production

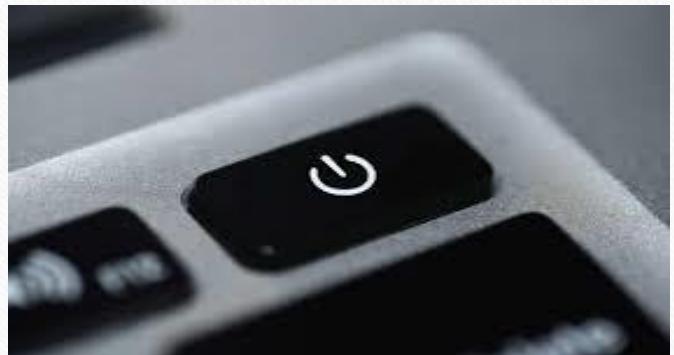
Analyser les dégâts

Observer le comportement

Rôles et responsabilités



- Ne pas éteindre
- ne pas désinstaller de logiciels
- Ne pas réinstaller d'OS
- Ne pas mettre à jour l'antivirus
- N'y touchez plus
- Prévenir d'autres organismes
- Appeler la police



Authentification multifactorielle

Ce qu'il faut savoir sur l'AMF :

- L'Authentification multifactorielle (AMF) part du principe qu'aucun facteur n'est parfait.
- Chacun de ces facteurs a ses points forts et ses points faibles.
- Il existe 3 familles d'authentification : **Simple , Fort , Unique**

Les différentes familles de l'authentification multifactorielle.

L'authentification simple

Ne repose que sur un seul facteur

L'authentification unique

permet une seule authentification permettant d'accéder à plusieurs applications informatiques.

L'authentification forte

Elle repose sur deux facteurs ou plus.

Quelques exemples d'authentification

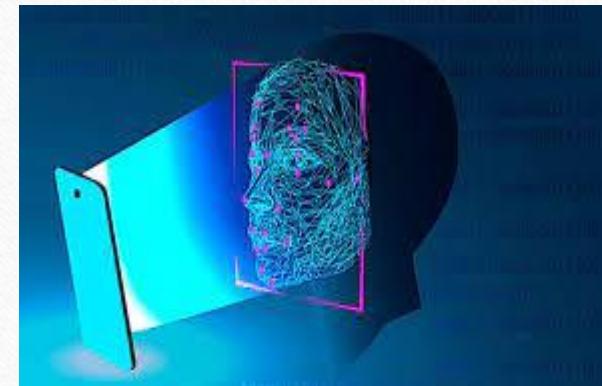
1) Balayage d'empreinte digitale



2) Balayage de la rétine



3) Reconnaissance faciale ou vocal



l'authentification adaptative multifactorielle

Pourquoi mettre en place la MFA ?

L'Authentification utilise des règles et des informations sur l'utilisateur pour déterminer les facteurs à appliquer.

Les entreprises utilisent la MFA.

Quelles informations sont recueillies pour mettre en place la MFA

1. Le nombre de tentatives de connexion échouées
2. L'emplacement géographique de l'utilisateur
3. La géo-vélocité ou la distance physique entre des tentatives de connexion consécutives
4. L'appareil utilisé pour la connexion
5. Le jour et l'heure de la tentative de connexion
6. Le système d'exploitation
7. L'adresse IP source
8. Le rôle de l'utilisateur

Authentification à l'aide d'un objet physique

Exemples d'objets physique permettant une authentification :

- Clé USB, clé RFID, carte à puce



Utilités des objets physique :

L'utilisateur garde son objet physique avec lui, et donc hors ligne, il ne peut être intercepté sur les réseaux.



Identité numérique

- Ensemble des traces laissées par un individu
- Identité calculée, déclarative et agissante.
- Utilité de l'IDN :
 - - visibilité
 - - partage de connaissances, opinions

Identité numérique : questions

- Velléités de suppression de l'anonymat par certains acteurs
- Quelle place à la liberté d'expression dans l'anonymat ou pas ?