ORDRE DU JOUR

- Contexte UM Active Directory
- Actions de renforcement de la sécurité en 3 axes :
  - Recommandations techniques
  - Recommandations fonctionnelles
  - Recommandations organisationnelles

Les principes d'un Active Directory

- Définition : service d'annuaire spécialisé et propriétaire dans les environnements de systèmes d'exploitation Windows
- Fonctions principales : authentification des utilisateurs, autorisation des accès aux ressources, stratégies de groupe

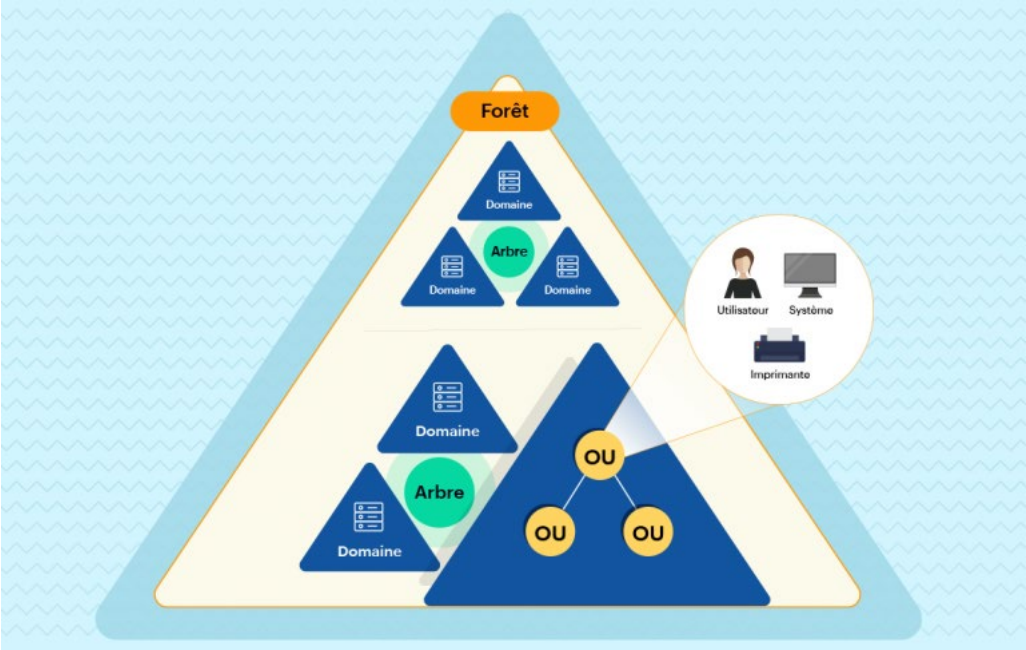
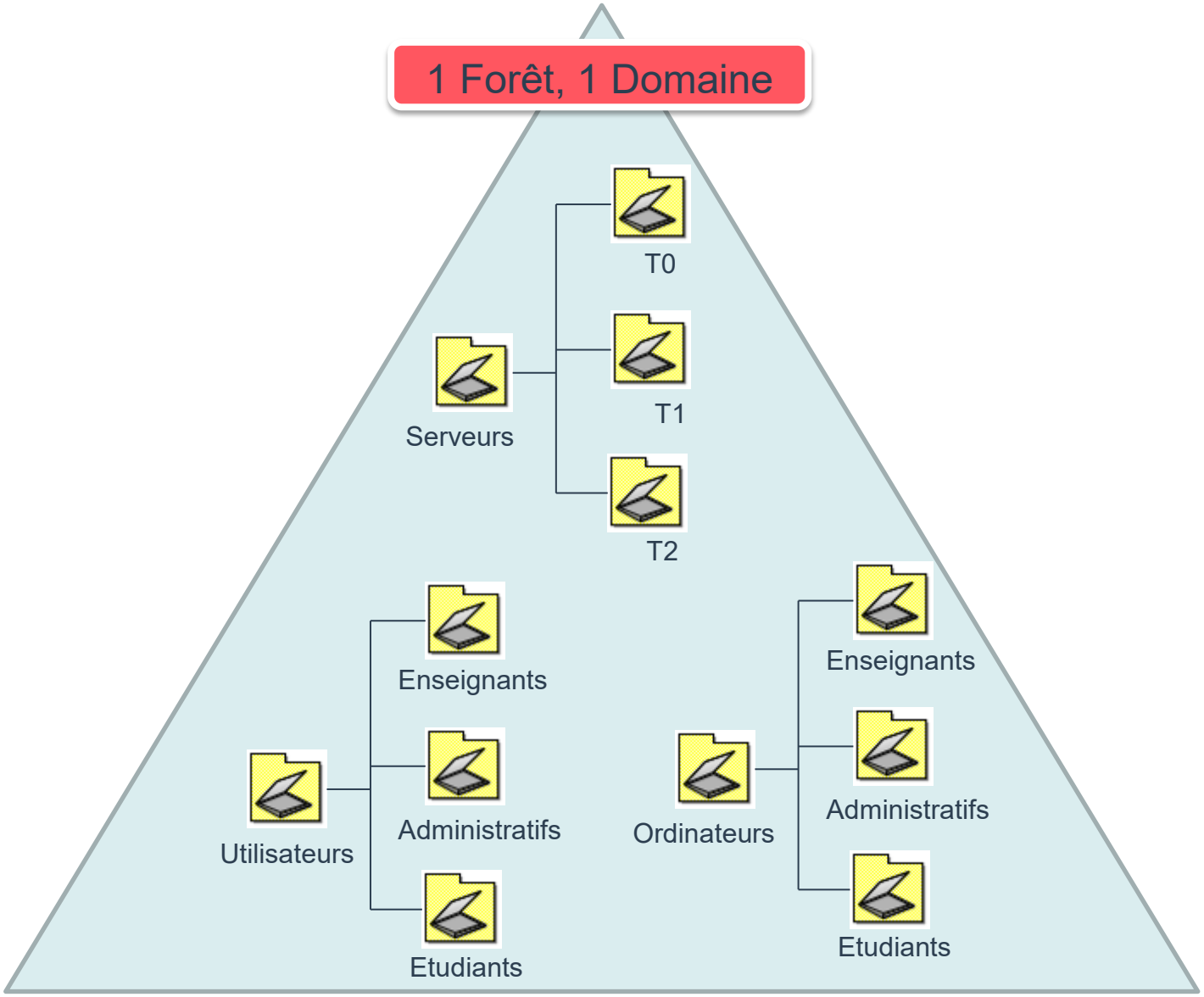


Schéma Active Directory



Actions des administrateurs dans l'AD

- Comptes privilégiés – ajout / désactivation / pwd
- Comptes de services – ajout / désactivation / pwd
- Groupes de sécurité – ajout / suppression membres
- GPO (300) – Création / suppression

PAS de création manuelle de compte utilisateur

Maitrise de la gestion du cycle de vie des comptes (ajout / modification / désactivation / changement pwd) par l'ENT

ACTIONS TECHNIQUES - DOMAIN CONTROLER

- Segmentation réseau - Isoler les DC dans un VLAN dédié
  - Filtrer les flux avec les autres réseaux

Ports	Usage	Type de traffic
TCP / UDP 389	Récupération et réplication de données d'annuaire, authentification utilisateurs et comptes de services / machines, GPO, relations d'approbation, etc.	LDAP
TCP 636	Récupération et réplication de données d'annuaire, authentification utilisateurs et comptes de services / machines, GPO, relations d'approbation, etc.	LDAP SSL
TCP 3268	Récupération et réplication de données d'annuaire, authentification utilisateurs et comptes de services / machines, GPO, relations d'approbation, etc.	LDAP GC
TCP 3269	Récupération et réplication de données d'annuaire, authentification utilisateurs et comptes de services / machines, GPO, relations d'approbation, etc.	LDAP GC SSL
TCP / UDP 88	Authentification utilisateurs et comptes de services / machines, relations d'approbation inter forêts, etc.	Kerberos
TCP / UDP 53	Résolution de nom d'hôtes, authentification utilisateurs et comptes de services / machine, etc.	DNS
TCP / UDP 445	Réplication de données, authentification utilisateurs et comptes de services / machines, GPO, relations d'approbation, etc.	SMB, CIFS, SMBv2, etc.
TCP 25	Réplication de données	SMTP
TCP 135	Réplication de données	RPC, EPM
UDP 137	Authentification utilisateurs et comptes de services / machines	NetLogon, NetBIOS Name resolution
TCP 139	Authentification utilisateurs et comptes de services / machines, réplication	DFSN, NetLogon, NetBIOS, etc.
TCP 5722	Réplication de fichiers	RPC, DFSR (SYSVOL)
UDP 123	Synchronisation d'horloge	Windows Time
TCP / UDP 464	Authentification utilisateurs et comptes de services / machines, relations d'approbation inter forêts, etc.	Kerberos change / set password
UDP 138	DFS, GPO	DFSN, NetLogon, NetBIOS, etc.
UDP 67 / 2535	DHCP	DHCP, MADCAP
TCP dynamique	Réplication, authentification utilisateurs et comptes de services / machines, GPO, relations d'approbation, etc.	RPC, DCOM, EPM,DRSUAPI, NetLogonR, SamR, FRS
UDP dynamique	GPO	DCOM, RPC, EPM

ACTIONS TECHNIQUES - DOMAIN CONTROLER

- Activer le pare-feu local des serveurs sur tous les profils
- Automatiser la mise à jour des systèmes avec le service WSUS ou autoriser un flux sur le site update.microsoft.com – gestion des reboot
- Activer l'anti-virus Defender
- Architecture PKI à 2 niveaux
- Bloquer l'usage des Browsers Internet
- Ajouter les comptes T0 dédiés dans le groupe « Protected Users »
- Définir une stratégie de mot de passe renforcée pour les T0
- Mettre en œuvre une politique de sauvegarde de l'AD
  - Job Veeam Backup toutes les nuits
  - Externalisation des backups dans un coffre
- Désactiver le service Spooler
- Utiliser les PAW (Protected Access Workstation) pour administrer les DC*

* https://learn.microsoft.com/fr-fr/security/compass/privileged-access-devices

ACTIONS TECHNIQUES GENERALES

- Segmentation réseau : Isoler les réseaux serveurs et postes utilisateurs
  - Filtrer les flux entre ces réseaux (voir matrice des flux MS)
- Déployer des OS supportés
  - Windows Server 2012R2 - Arrêt des mises à jour sécurité le 10/10/2023*
- Activer le pare-feu local des serveurs
- Automatiser la mise à jour des systèmes avec le service WSUS
- Mise en œuvre de LAPS
- Utiliser des scripts Powershell signés par la PKI
- OS du parc utilisateurs à jour

* - https://endoflife.date/windows-server

ACTIONS FONCTIONNELLES

- **Journalisation :**
  - Définir une taille des journaux des évènements conforme aux recommandations
- **Activer les fonctionnalités d'audit :**
  - Opérations réussies et échec
- Exporter les journaux dans un outil de centralisation de logs
- Anti-virus à jour sur tous les postes et serveurs Windows
- Niveau fonctionnel de la forêt le plus élevé possible (W2016)
- Définir une architecture logique de l'annuaire
  - Adaptée au modèle d'administration et à la délégation de droits
- Définir une convention de nommage (groupes, GPO)

ACTIONS ORGANISATIONNELLES

- **RH - Gestion des administrateurs de l'AD**
  - Nombre limité mais suffisant pour assurer la continuité de service
  - Compte dédié à l'administration avec moindre privilège (délégation de droits)
  - Gestion du cycle de vie des comptes
  - Sensibilisation à la sécurité
  - Niveau d'expertise suffisant
  - Ne pas utiliser les comptes d'administrations intégrés

- **Gestion des comptes utilisateurs**
  - Intégré dans les processus métiers
  - Définir les règles de création et de désactivation
  - Appliquer le principe du moindre droit et privilège

DEFINITION DU MODELE D'ADMINISTRATION PAR NIVEAU

Afin d'empêcher les élévations de privilèges par rebonds successifs, il est recommandé **de segmenter les niveaux d'administration** et de forcer une utilisation par niveau des comptes de domaine.

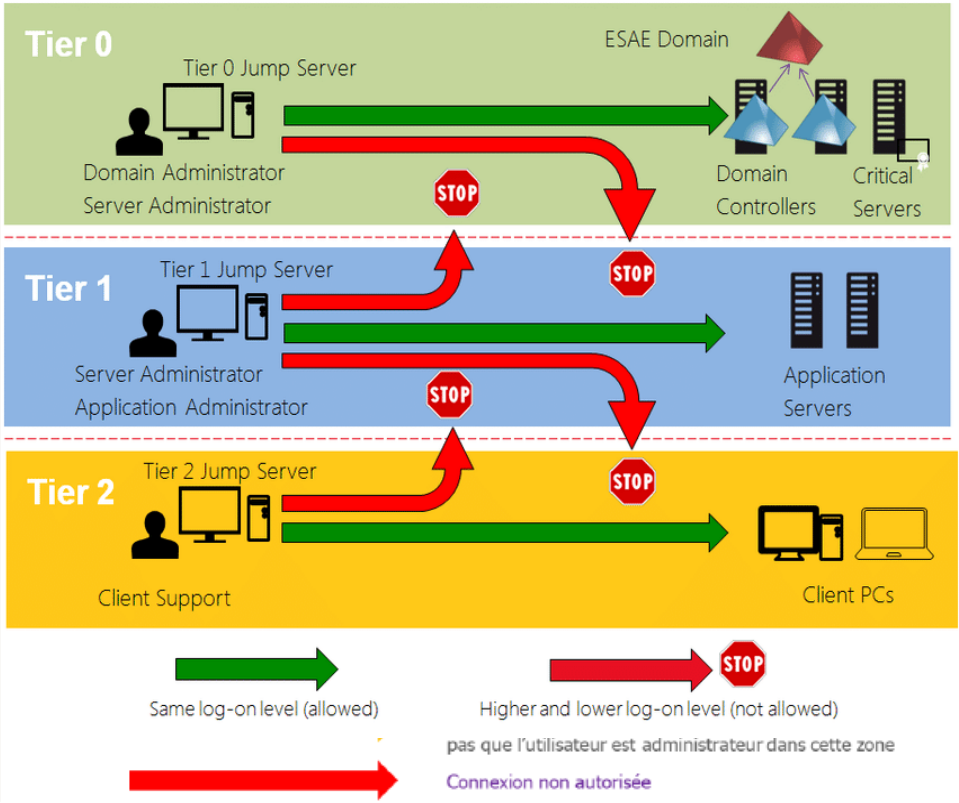
Les principes suivants sont notamment à respecter :

/ Les comptes d'administrateurs du domaine doivent être utiliser uniquement pour les tâches d'administration du domaine.

/ Les comptes administrateurs des serveurs hébergeant les données métier doivent être dédiés à l'administration de ces serveurs.

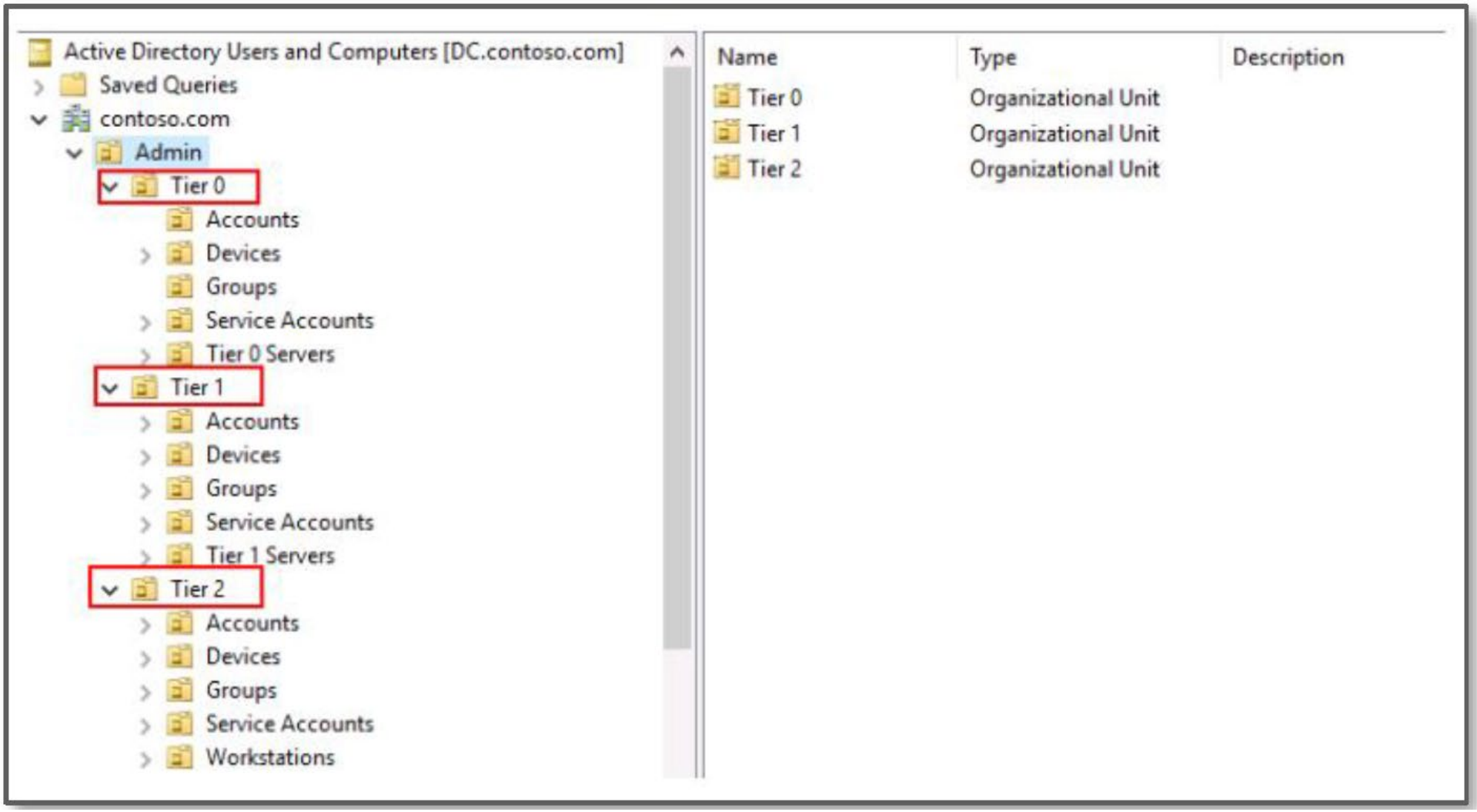
/ Les comptes administrateurs des postes sont limités exclusivement aux postes de travail.

Le schéma ci-contre illustre le principe d'une administration structurée par niveau.



- Création d'une arborescence d'unités organisationnelles
- Application de stratégies de groupes (GPO)

CIBLE D'UN MODELE D'ADMINISTRATION EN 3 TIERS



AUDIT

- **Audit régulier**
  - Utiliser des outils d'audit : Oradad, Ping Castle, BloodHound
  - Faire une revue régulière des comptes à privilèges

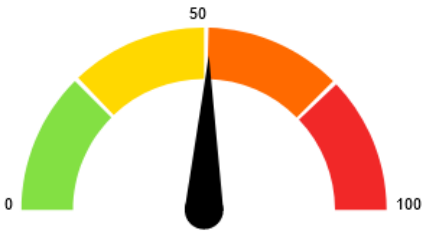
PING CASTLE – Modèle de risques

Stale Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	ACL Check	Old trust protocol	Backup
Network topography	Admin control	SID Filtering	Certificate take over
Object configuration	Irreversible change	SIDHistory	Golden ticket
Obsolete OS	Privilege control	Trust impermeability	Local group vulnerability
Old authentication protocols		Trust inactive	Network sniffing
Provisioning			Pass-the-credential
Replication			Password retrieval
Unfinished migration			Reconnaissance
Vulnerability management			Temporary admins
			Weak password

Legend:
- score is 0 - no risk identified but some improvements detected
- score between 1 and 10 - a few actions have been identified
- score between 10 and 30 - rules should be looked with attention
- score higher than 30 - major risks identified

PING CASTLE – Exemple rapport

Stale Objects



Stale Objects : 51 /100

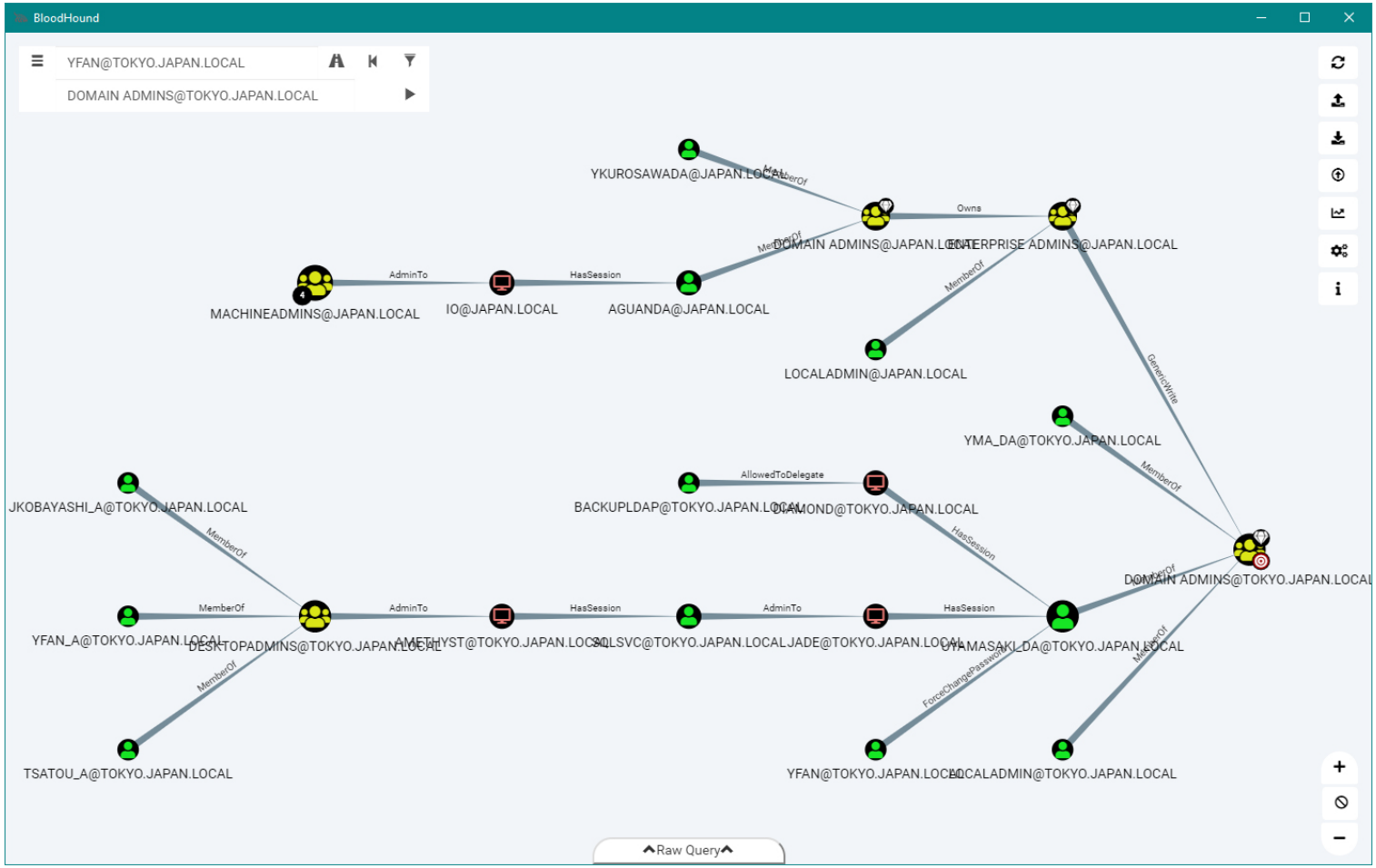
It is about operations related to user or computer objects

Stale Objects rule details [6 rules matched on a total of 41]

Presence of Des Enabled account = 7	+ 15 Point(s)
Relatively high number of inactive user accounts: 27% (more than 25% of all users)	+ 10 Point(s)
Relatively high number of inactive computer accounts: 20% (more than 20% of all computers)	+ 10 Point(s)
Presence of non-supported version of Windows 10 = 8	+ 10 Point(s)
Presence of Windows 7 = 18	+ 5 Point(s)
Number of accounts which has never-expiring passwords: 141	+ 1 Point(s)

BLOODHOUND

Outil de recherche des chemins d'attaque dans un AD



Références

- Notes techniques ANSSI :
  - https://www.ssi.gouv.fr/administration/bonnes-pratiques/poste-de-travail-et-serveurs/
- Articles JRES :
  - JRES 2019 – « Active Directory en milieu universitaire : une approche par la sécurité »
  - JRES 2017 – « Audit de l'AD : Contrôle des bonnes pratiques »
- Documentation Microsoft :
  - https://learn.microsoft.com/fr-fr/security/compass/privileged-access-access-model
- Outils d'audit :
  - Service ADS ORADAD - https://club.ssi.gouv.fr
  - PING CASTLE - https://www.pingcastle.com
  - BLOODHOUND - https://bloodhound.readthedocs.io/en/latest/index.html

PERSPECTIVES

- Mise en œuvre de la double authentification
- Séparation en plusieurs forêts – **Seule la forêt est une limite de sécurité**
- Implémentation de Privileged Access Management (PAM)
- …