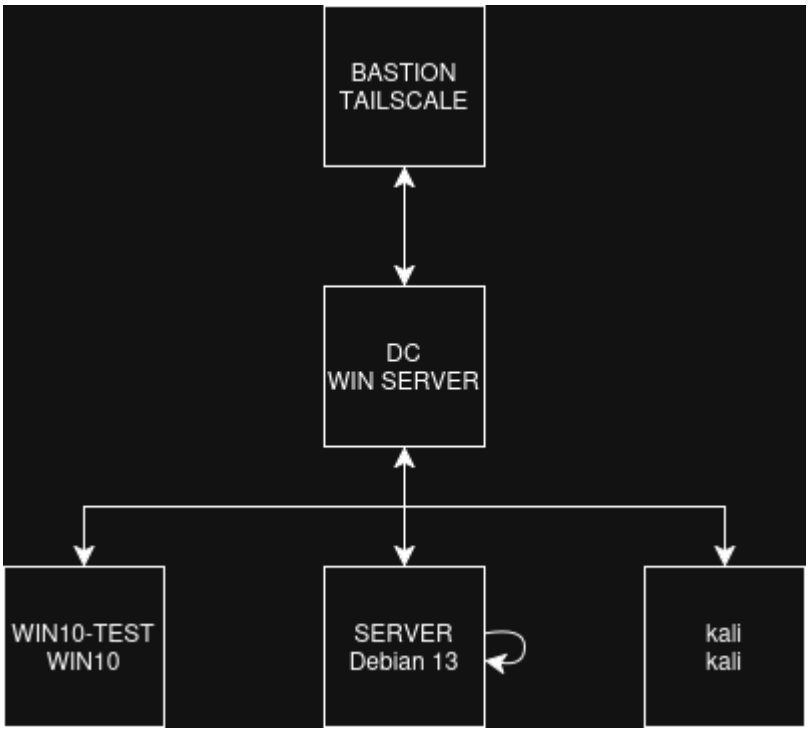
SOC : Compte Rendu BUILD

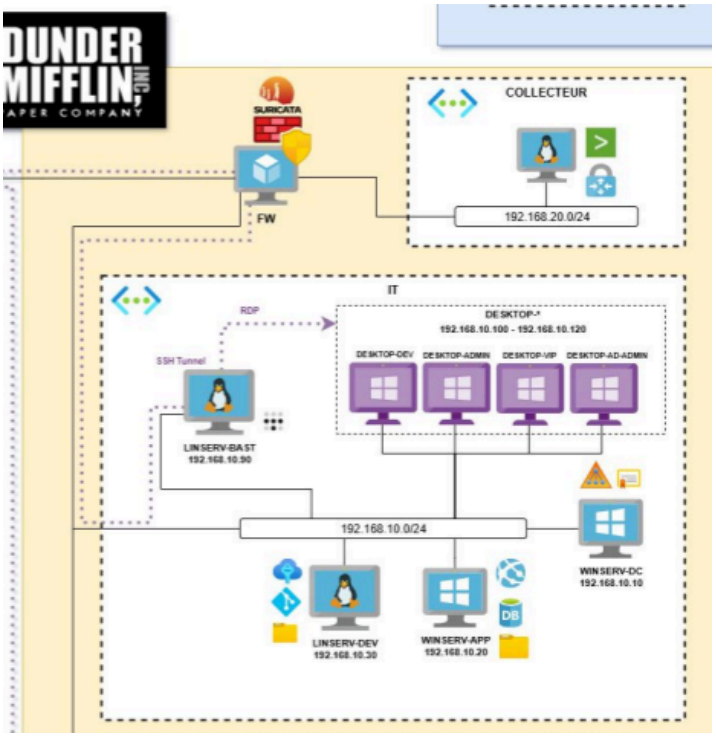
BARATIN - Paul; DOUCET - Thélio; DUGUEY - Martin; NAIT NADIR - Salma

1) infrastructure build

infrastructure du build



infrastructure du client



nous simulons l'infrastructure de dunder mifflin à l'aide des VM ci-dessus. Les VMs sont hébergés sur des machines différentes et interconnectés entre elles via Tailscale. La machine kali ne fait pas partie de l'infrastructure et sert à simuler des attaques.

2) architecture projet

```
projet-SOC/
│
├── backup/
│   ├── savedsearches.conf
│
├── detection/
│   ├── enumeration-linux
│   ├── kerberoasting
│   ├── password-looting
│   ├── README.md
│   └── ……..
│
├── documentation/
│   ├── diagramme_architecture.png
│   ├── fichereflex.md
│   ├── matrice-communication.md
│   ├── regles.md
│   ├── sourcesettypesdedonnées.md
│   └── …….
│
└── README.md
```

Le dossier backup contient les sauvegardes du projet.
Le dossier détection contient les règles de détection splunk.
Le dossier documentation contient tous les documents importants au projet.

3) règles implémentées

sont implémenté les règles suivantes:

- Active Directory :
    - Kerberoasting
    - AS-REPRoasting
    - Password Spraying
- Windows:
    - Création d'une tâche planifiée suspecte
    - Création d'un service suspect
    - Création ou modification de clé RUN
    - Dump LSASS
- Linux:

    - Multiples commandes d’énumération
    - Activité de password looting
- Réseau :
    - Scan de port (horizontal / vertical)

Nos alertes sont envoyées par n8n à IRIS.