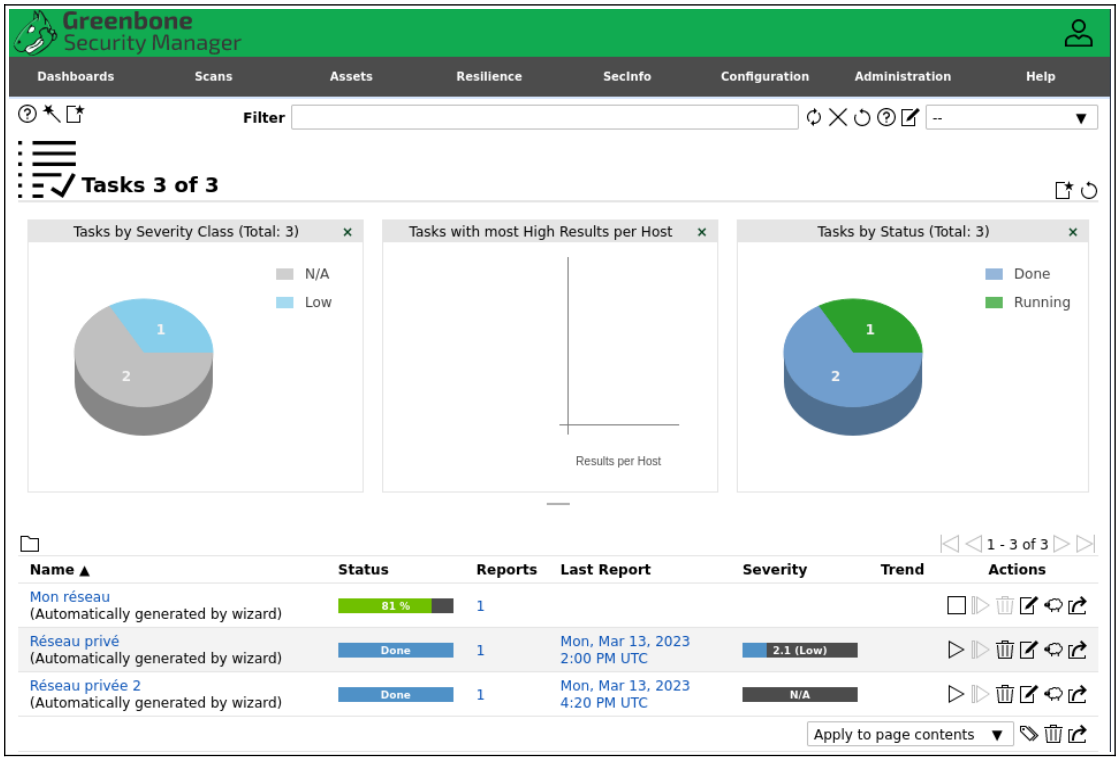
Vulnérabilités – GreenBone

Sommaire :

---

1 ./Recherches de vulnérabilités

- Scans > Tasks

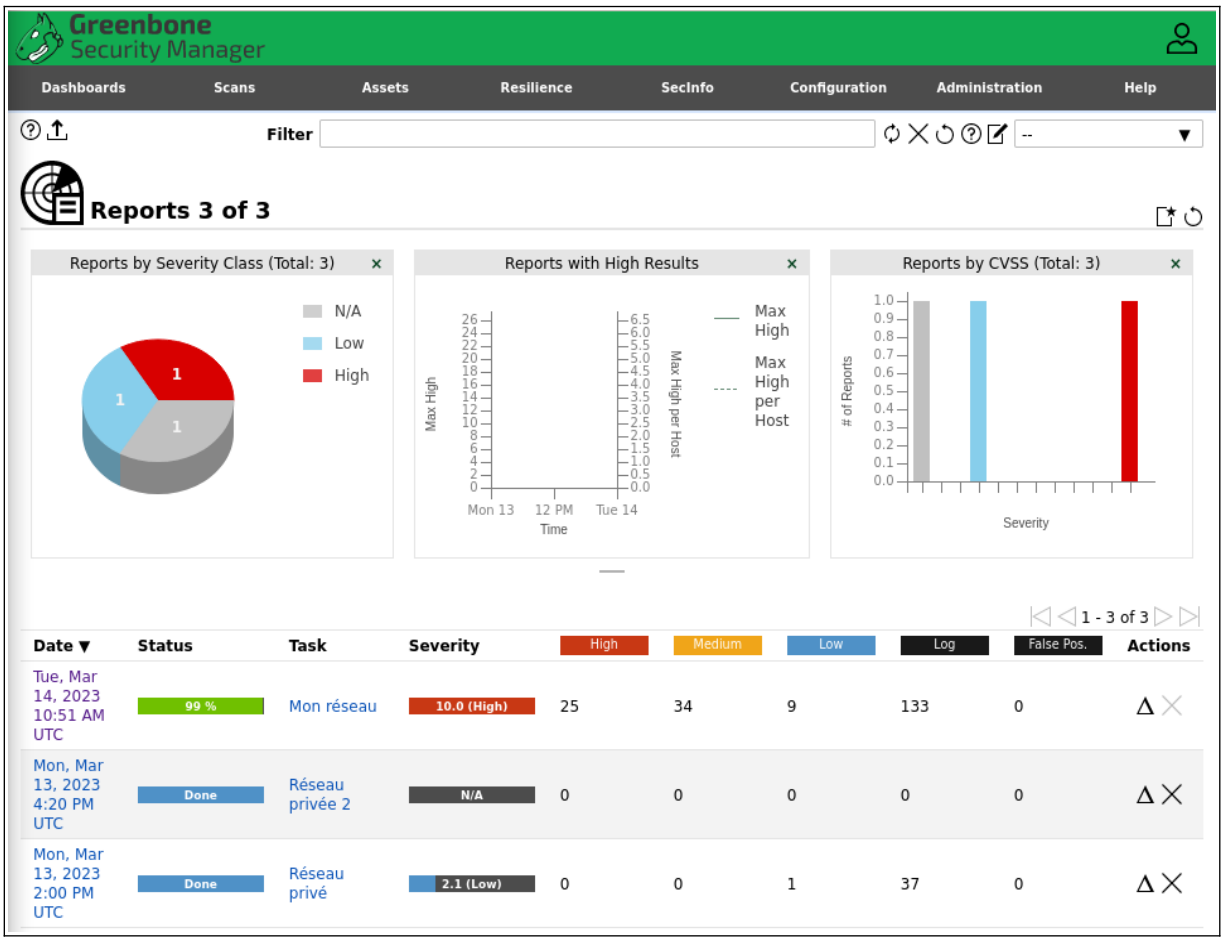


La catégorie **tasks** permet de **gérer les tâches** avec la colonne action ainsi que d'afficher l'**historique des scans** effectuées, les **résultats**, etc.
Cette fonctionnalité apporte donc à une entreprise et/ou un administrateur réseau de **répertorié les scans** déjà émis en les datant afin de **garder une chronologie des analyses** sur son réseau.

Indiquant différentes informations tel que :

- Nom
- Status
- Niveau de gravité
- Date

- Scans > Reports

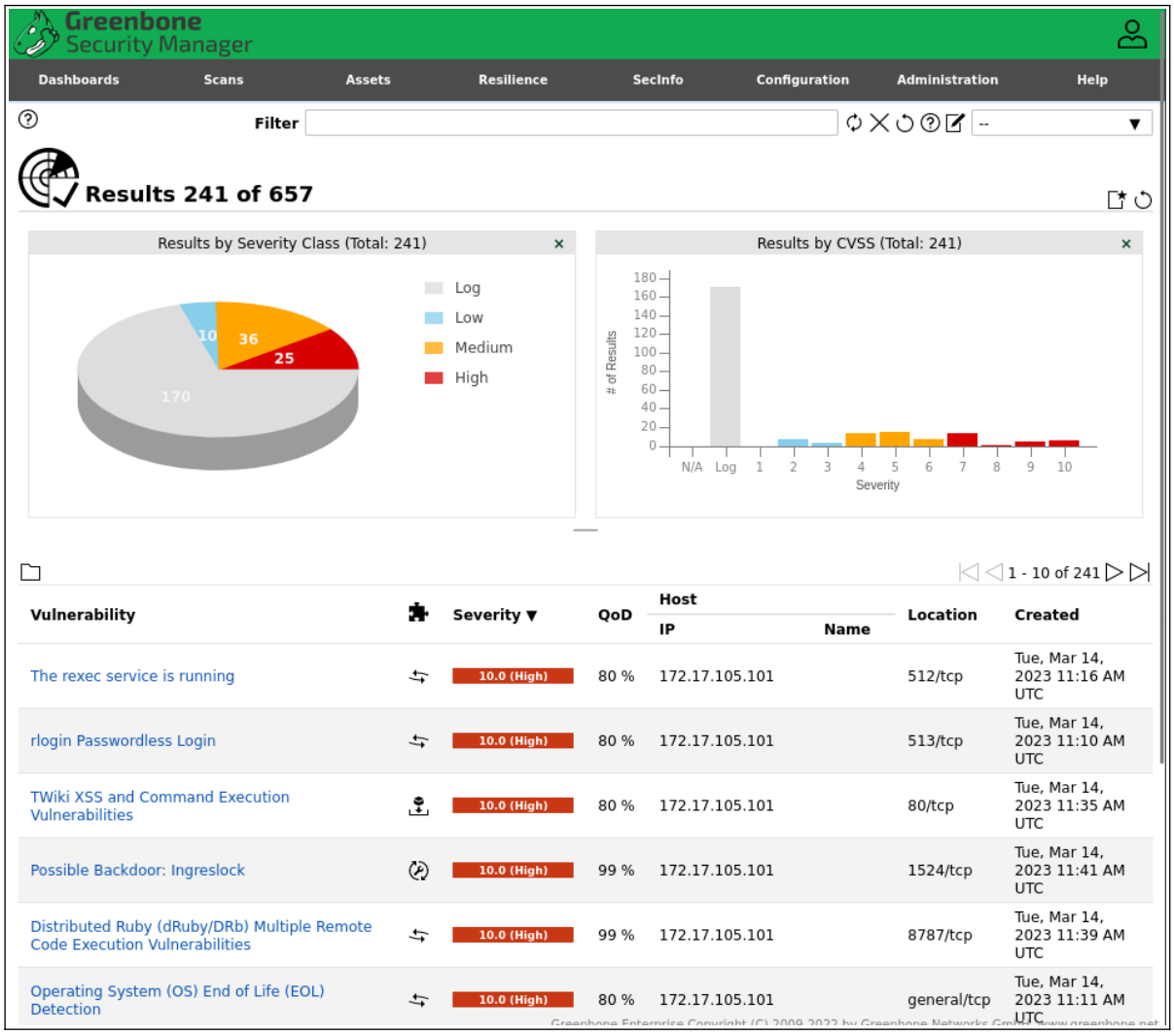


La catégorie **reports** paraît similaire, mais celle-ci offre plus de détails sur les **niveaux de gravité** rencontré concernant les **failles**, par ailleurs un indication du nombre de logs produit par le scan est affiché.
Une entreprise et/ou un administrateur réseau peut donc élaborer un **classement des failles de sécurité** lui permettant de produire un **graphe** classant les soucis rencontrés en fonction de leur **gravité ainsi que la vraisemblance** de ces derniers.

Le niveau de gravité d'une faille est déterminé par trois sections distinctes :

- High
- Medium
- Low

- Scans > Results

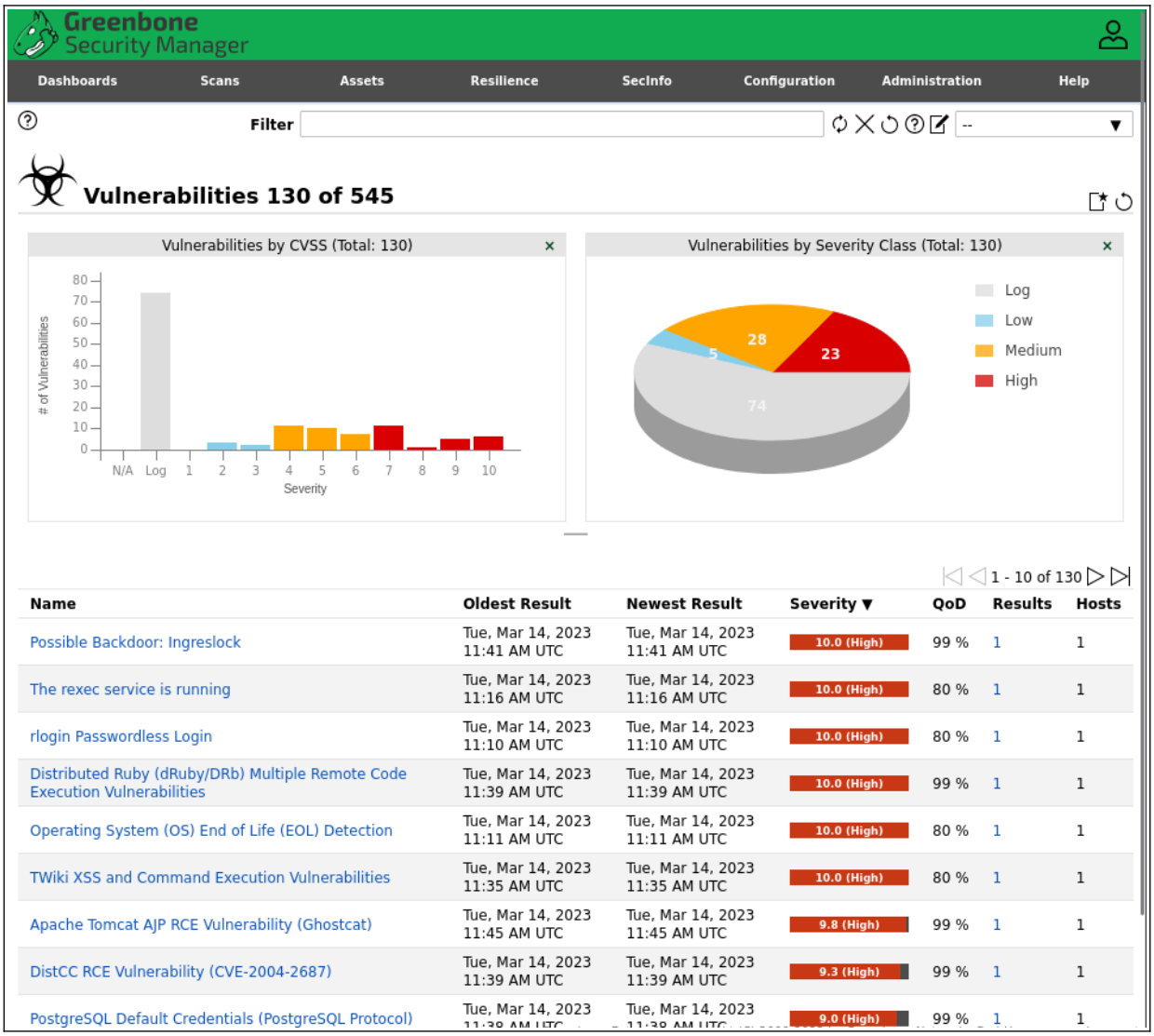


La catégorie **results** détaille l'ensemble des services et protocoles scannés sur vos machines en informant sur le **niveau de vulnérabilités**.
Ainsi, cette fonctionnalité guide l'administrateur en indiquant approximativement le **chemin** sur lequel vous orientez si vous souhaitez **investiguer** sur la faille ou bien **sécurisé** celle-ci.

Des colonnes informatives sont disponibles tel que :

- QoD (Pourcentage de fiabilité sur le scan effectué)
- Host IP
- Location (localisation de la possible faille)

- Scans > Vulnerabilities



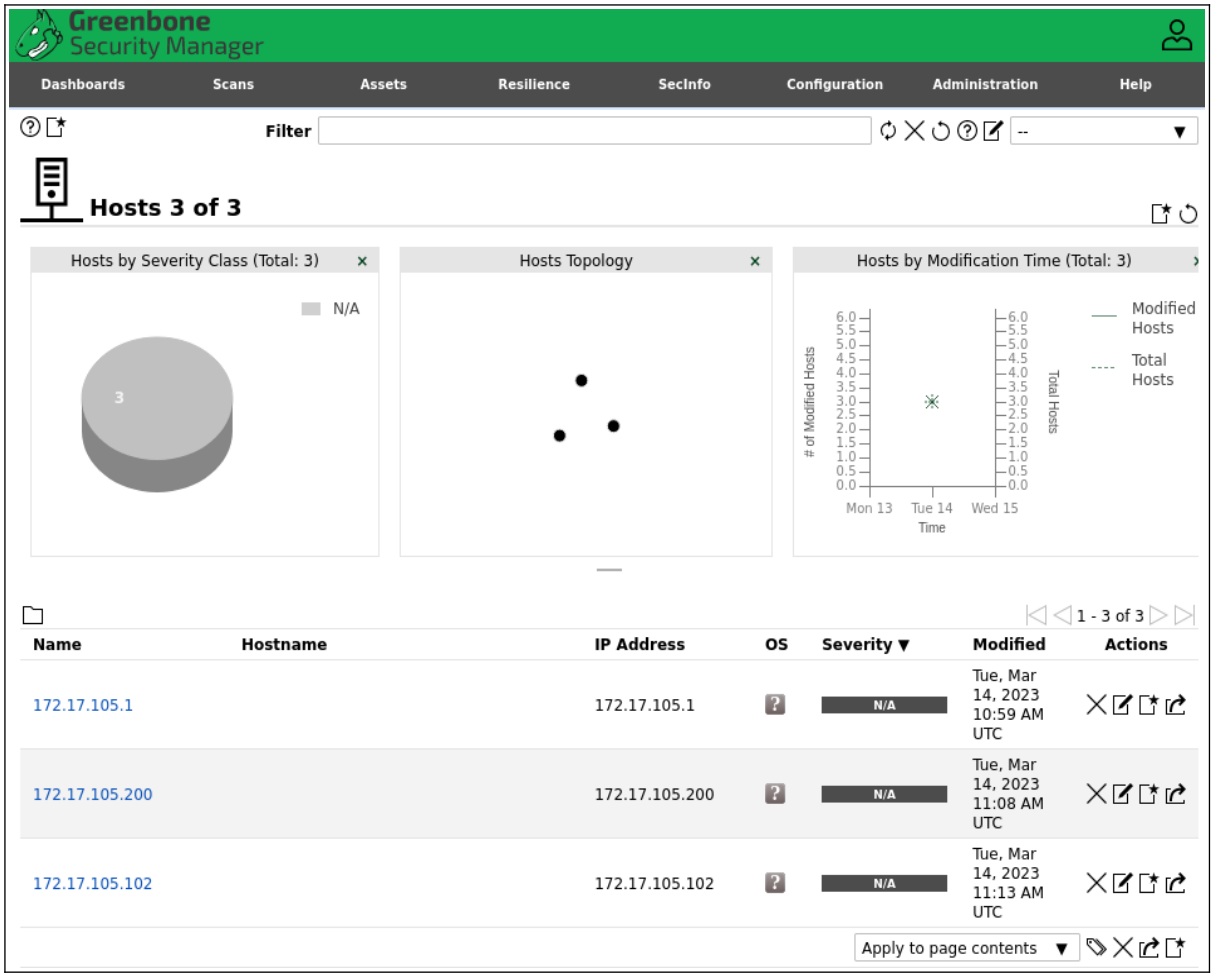
La catégorie **vulnerabilities** n'affiche que l'ensemble des possibles **vulnérabilités présentes sur l'ensemble d'un réseau** indiquant le nom complet de ces dernières. L'administrateur peut donc déterminer quels sont les **domaines touchés par une défaillance de sécurité**, en classant par ordre décroissant le **niveau d'importance**.

Différentes informations accompagne le détaille des vulnérabilités :

- Oldest Result
- Newest Result
- QoD
- Hosts (nombre d'hosts possédant ce service/protocole et possiblement touchés par une faille de sécurité)

2 ./Gestion des actifs

- Assets > Hosts

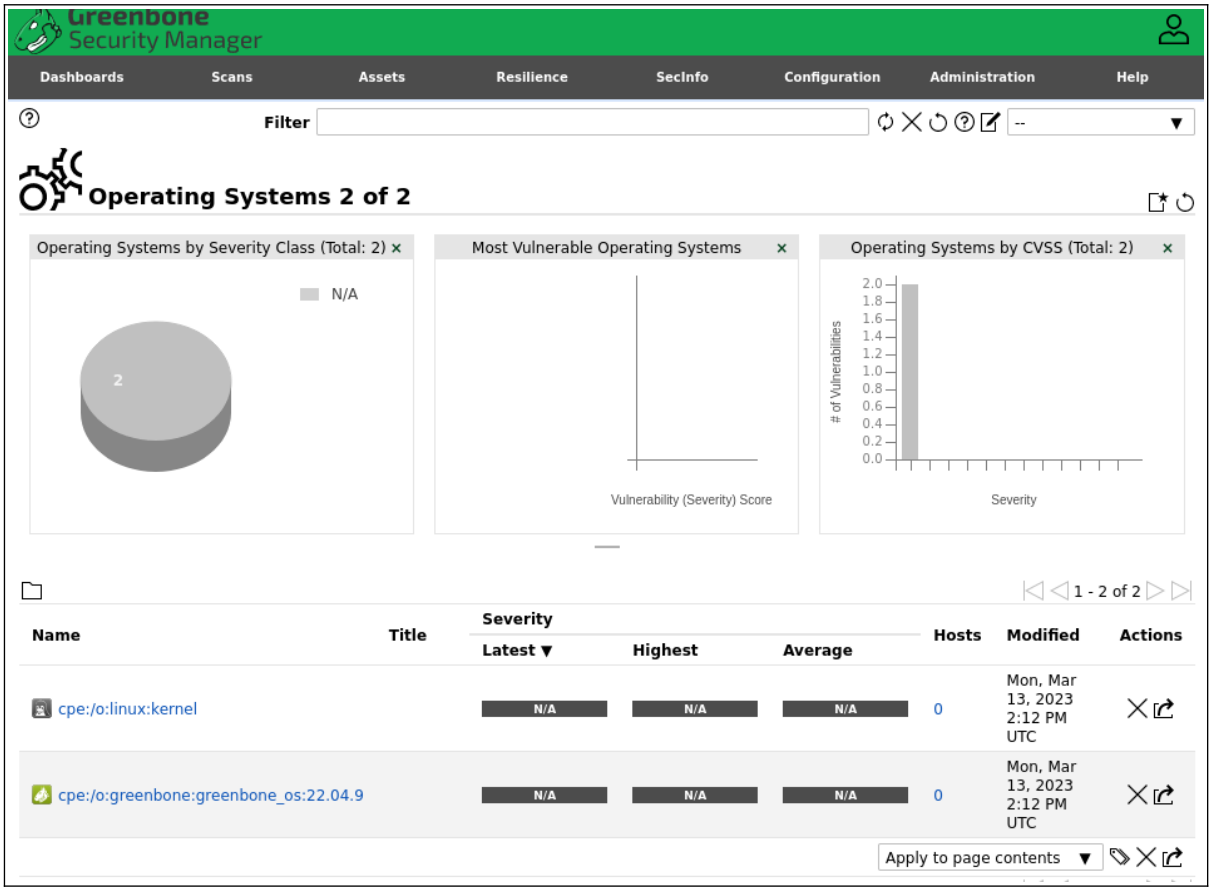


La catégorie **assets** permet de répertorier les **machines présentes sur le réseau** analysé ainsi que les **connexions entre elles**. En indiquant, les **adresses ip** ainsi que **l'OS** présent sur la machine concerné.

Renseignements disponibles sur l'infrastructure :

- Adress IP
- Schéma du réseau
- Connexion des machines
- OS
- Nom

- Assets > Operating Systems

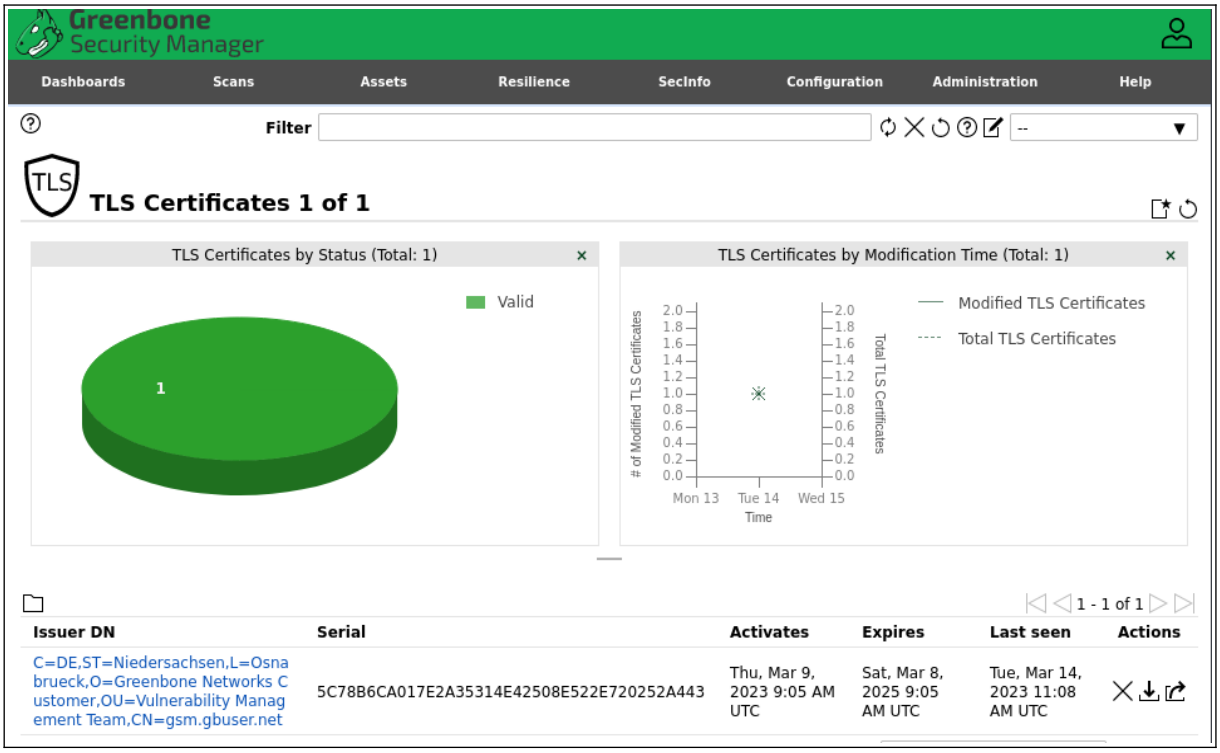


La catégorie **operating systems**, permet de visualiser les **systèmes d'exploitations** fournissant une vue différente sur les **données stockées**. Alors que la vue des hôtes est centrée sur les hôtes individuels, cette vue se concentre sur les systèmes d'exploitation **utilisés**.

Informations complémentaires disponibles :

- Nom de l'OS
- Niveau de sévérité
- Nombre d'hosts
- Date de modification

- Assets > TLS Certificates



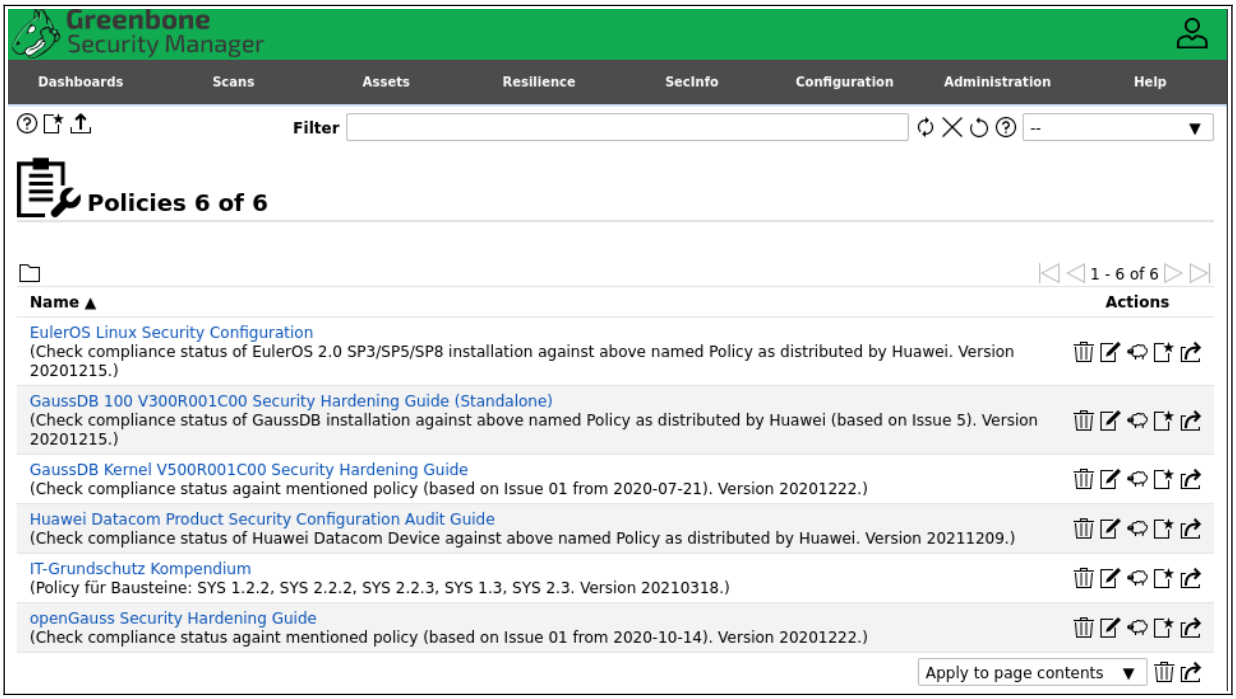
Dans la catégorie **TLS Certificates**, tous les certificats TLS existants peuvent être affichés. Vous pouvez cliquez sur le **nom d'un certificat TLS** pour **afficher les détails** du certificat TLS.

Informations complémentaires disponibles :

- Nom distinctif
- Numéro de série
- Date d'activation
- Date d'expiration

3 ./Résilience

- Resilience > Compliance Policies

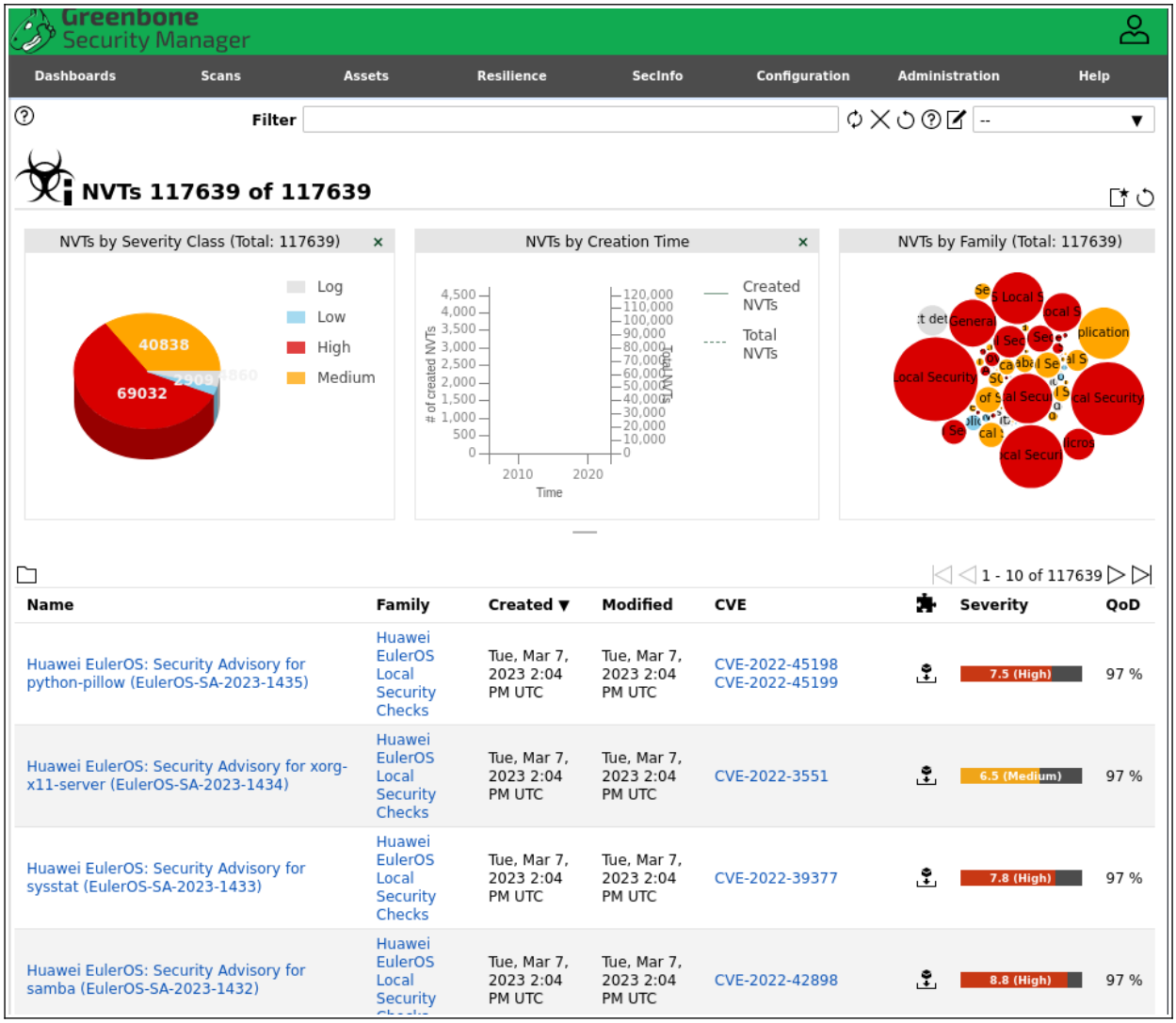


Dans la catégorie **Policies**, les **stratégies de conformité** sont utilisées par les **entreprises**, les **organisations** ou les autorités pour vérifier si tous les produits, applications, systèmes d'exploitation et autres composants utilisés **répondent à certaines spécifications**.

Informations complémentaires disponibles :

Nom complet des polices présentes sur greenbone, celles-ci peuvent être modifiés, cloner ou encore supprimés.

4 ./SecInfo



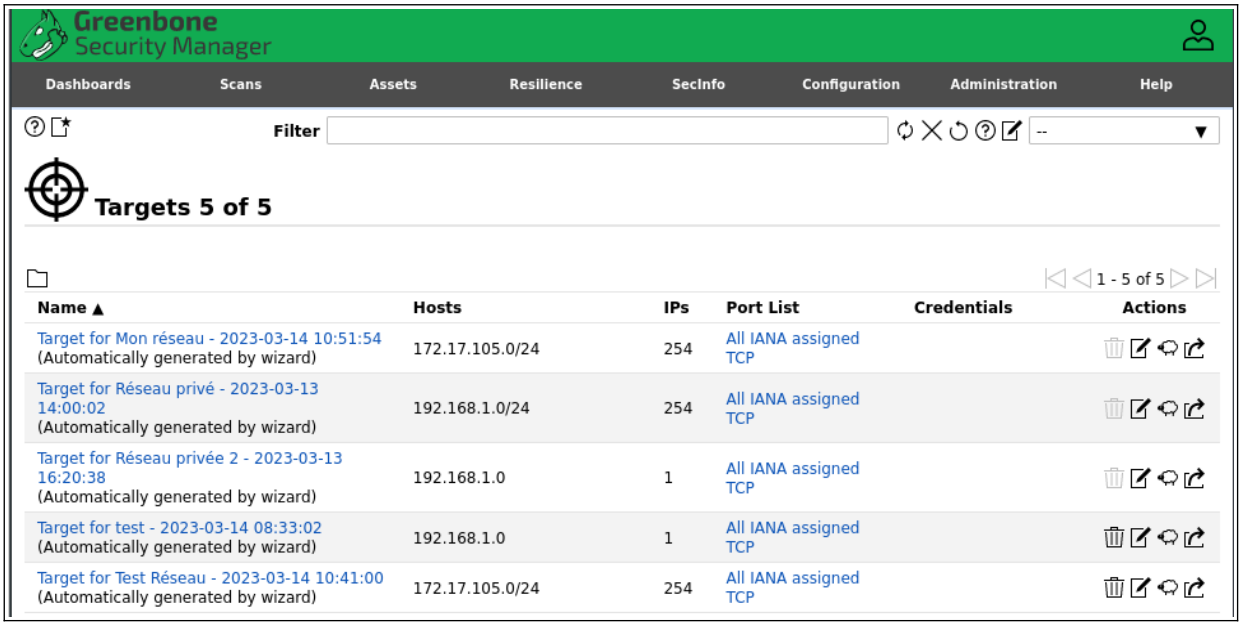
La gestion **SecInfo** fournit un accès **centralisé** à un large éventail d'informations de sécurité informatique. NVT autrement dit **Network vulnerability tests** répertoriant l'ensemble des vulnérabilités rencontrées.

Informations complémentaires disponibles :

- Nom
- Famille
- Date de création
- Date de modification
- Sévérité

5 ./Gestion des cibles

- Configuration > targets



Dans la catégorie **Targets**, toutes les cibles rencontrées lors des différentes analyses sont présentes ici afin d'obtenir un **historique des machines déjà analysées**. Greenbone liste donc via un **journal de log les hosts déjà ciblés** lors d'un scan.

Informations complémentaires disponibles :

- Nom
- Hosts (adresse IP)
- Ips
- Port list

6 ./Définition des identifiants

- Configuration > credentials