Du 04 mars au 05 avril 2024

Présentation stage 2024 - 3S-Sécurité

Tuteurs : Sébastien CLERGET & Nicolas DUSSERT

07/04/2024

Céréna HOSTAINS 2BTS SIO

SOMMAIRE

I. Présentation de 3S-Sécurité

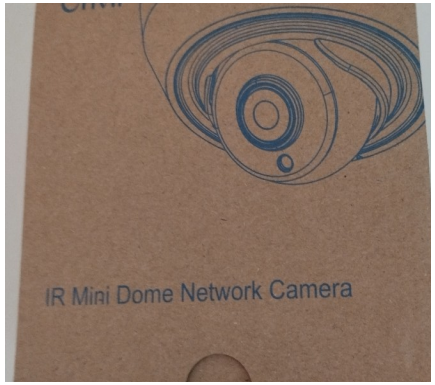
- 3S-Sécurité (Chenôve)
- Société par actions simplifiée
- Activités : Sécurité informatique et numérique
- Équipe : 1 développeur, 3 techniciens réseau et sécurité, 1 commercial, équipe 3R et 3-nuage.
- Missions : Cybersécurité défensive (firewall, proxy, reverse-proxy...), offensive (audit,...)

II. Partie informatique

- Linux, Windows et Mac OS
- Outils de virtualisation : VMware, Proxmox
- 15 serveurs : Linux, Centos, Debian pour la prod, les tests, les clients, les sites web...
- 2 pare-feu : StromShield, Pfsense
- Anti-virus : Windows Defender, Trend micro

III. Missions

- Mises à jours **Stormshield** (HA, DUO → proxy AD, standard)
- Visites client : mise en place de serveurs (2) et caméras (10 / 50) **Camtrace** (CHLC et Regroupement scolaire à Saint-Augustin)



STORMSHIELD

CamTrace

III. Missions

- Mise en place de **Grafana / Loki / Promtail** :
- Dashboard / Logs interfacés
- Permet d’explorer, filtrer et consulter des logs
- Stocke les logs critiques
- Stocke les index et métadonnées des logs
- Compatibilité **syslog**
- Installation Dockerisée
- Tests : remonter des logs + serveur web apache (debian) + supervision + alertes

III. Missions

- Mise en place et configuration de **Wazuh** et **Wazuh agent** :
- Plateforme de sécurité gratuite et open source
- **SIEM**
- **Protège** les données contre les menaces de sécurité
- **Analyse** des données de journaux
- **Détection** des intrusions et des logiciels malveillants
- **Surveillance** de l'intégrité des fichiers
- **Détection** des vulnérabilités
- **Évaluation** de la configuration

wazuh.

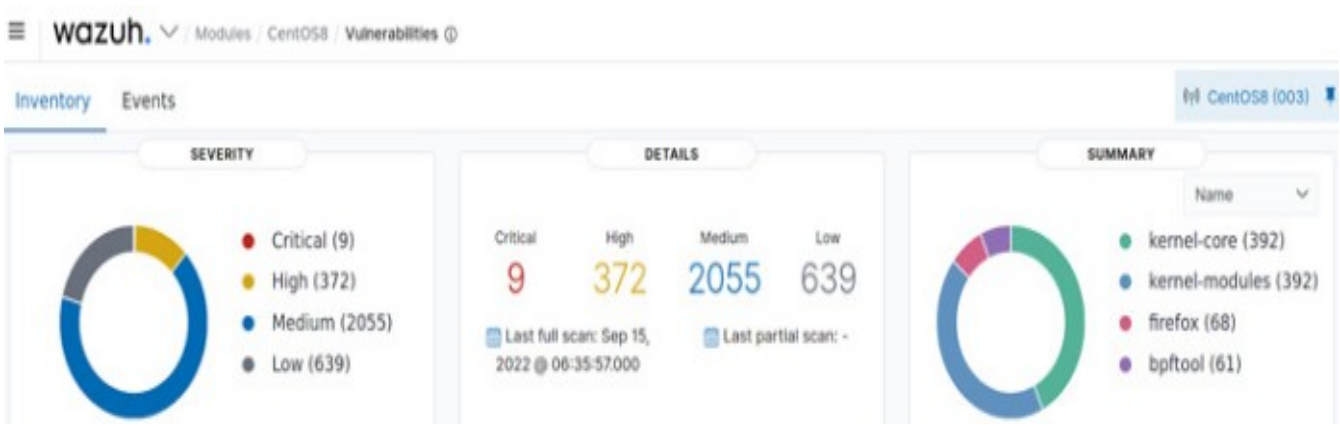
III. Missions

- Installation dockerisée → debian 12.5
- 1-25 agents :

  Processeurs: **4** vCPU

  Mémoire: **8** Gio RAM

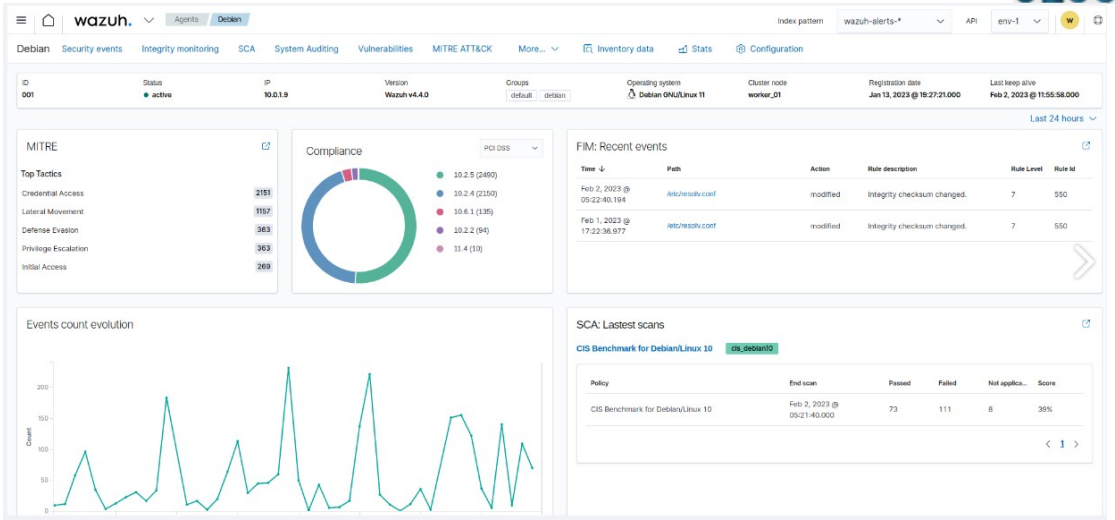
  Stockage: **50** Go
- Norme GDPR



III. Missions

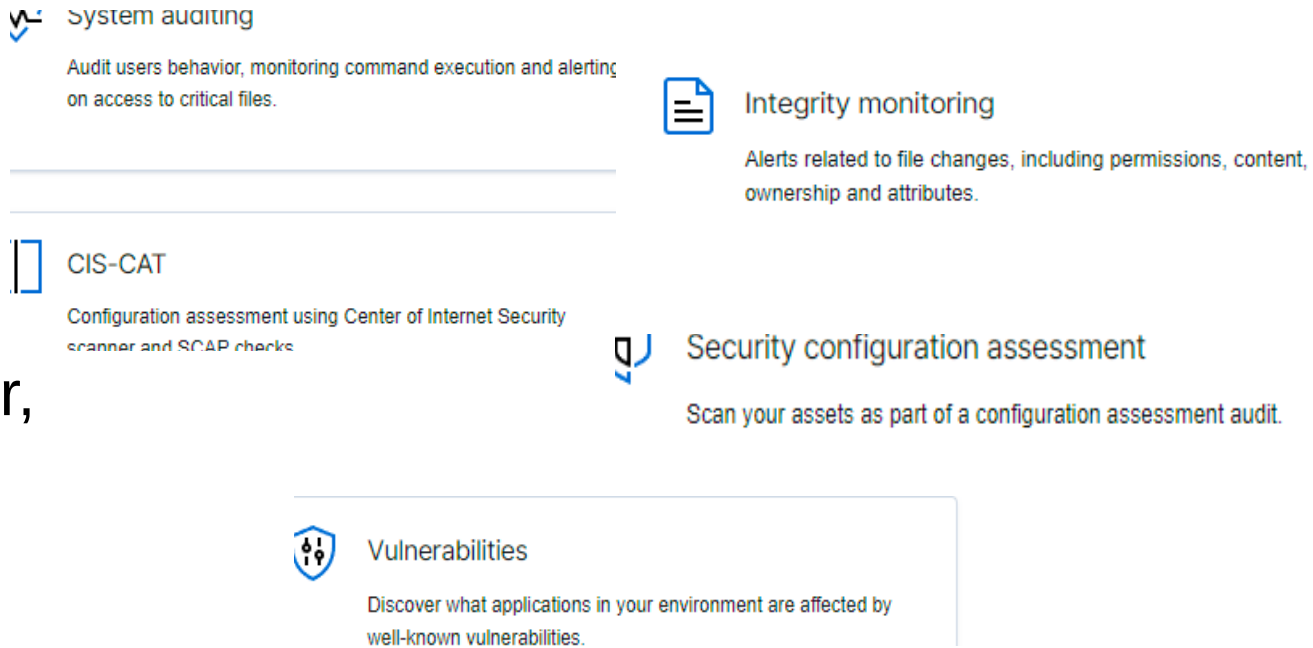
- Paramétrage :

  - Seuil d’alerte,
  - Activation des archives Wazuh
  - Wazuh-statistics-*
  - Configuration de sortie Syslog
  - Configuration des alertes e-mail
  - Changement du logo Wazuh
  - Modification mot de passe des utilisateurs Wazuh
  - Visualisation des événements sur le tableau de bord

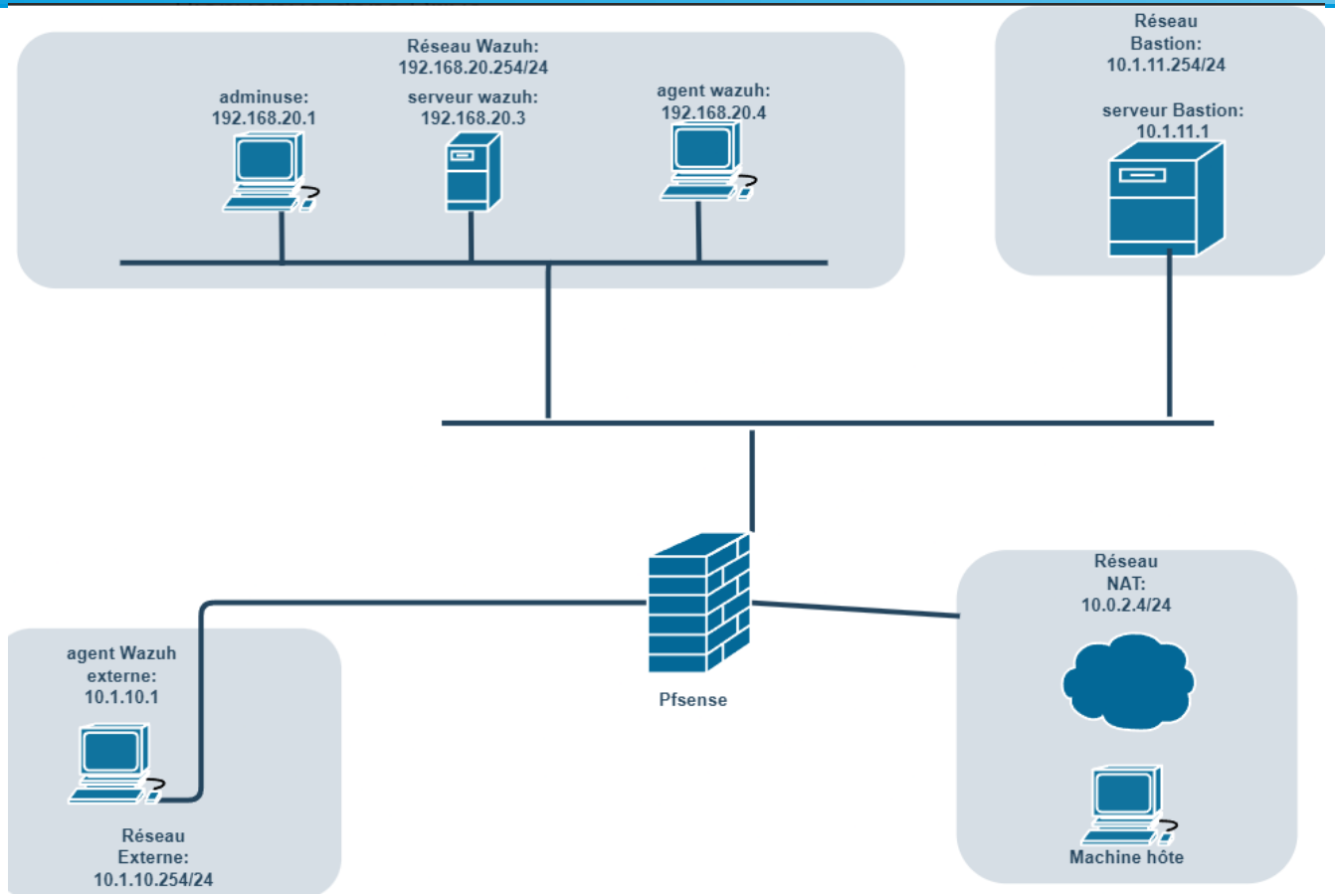


III. Missions

- Configurations complémentaires :
  - Healthcheck,
  - CIS-CAT,
  - Osquery integration,
  - System inventory,
  - Vulnerability-detector,
  - SCA.



III. Missions



III. Missions

- Mise en place d'un pare-feu **Pfsense (image ISO)**
- Paramétrage de **4 interfaces** pour **4 sous-réseaux**
- **Règles de filtrages** pour le **SSH** et le **bastion**
- **Restrictions** des accès aux agents (seulement Wazuh)

Ports	Protocoles	Besoins
1514	TCP	connexion du service Wazuh agent
1515	TCP	service d'inscription de l'agent
514	UDP	collecte les logs des agents Wazuh
55000	TCP	API RESTful serveur*
9200	TCP	visualisation client de l'interface Wazuh
443	TCP	interface web Wazuh utilisateur

III. Missions

- Mise en place d’un bastion (**The Bastion OVH**)
- Accès **SSH** plus sécurisé
- Docker
- **Clé** → ed25519 norme
- Rôle : accès sécurisé pour aller de l’utilisateur au serveur Wazuh
- Mise en place de la **TOTP** (en cours)
- Mise en place de règles de pare-feu avec les bons ports

IV. Bilan du stage

- État d'achèvement des missions confiées
- Évolutions futures
- Ce qu'a apporté mon travail à l'entreprise
- Ce que m’a apporté le stage
- Difficultés rencontrées