Intégration de Wazuh à Slack puis à Zulip pour la gestion de notifications

I – Les outils

Wazuh :

Wazuh est une plateforme open source utilisée pour la prévention, la détection et la réponse aux menaces. Elle sécurise les environnements de travail sur site, virtualisés, conteneurisés et en cloud. **Wazuh** est largement utilisé par des milliers d'organisations à travers le monde, de la petite entreprise à la grande entreprise. La solution **Wazuh** se compose de plusieurs agents de sécurité des terminaux, déployés sur les systèmes surveillés, et d'un serveur de gestion, qui collecte et analyse les données recueillies par les agents.

Zulip :

Zulip est une puissante application open source conçue pour aider les équipes (qu'il s'agisse de projets open source ou d'entreprises) à collaborer efficacement. **Zulip** combine l'immédiateté du chat en temps réel avec un modèle de discussion par e-mail. Avec **Zulip**, il est possible de rattraper les conversations importantes tout en ignorant celles qui sont sans importance.

Slack :

Slack est une application de messagerie pour les entreprises qui connecte les personnes aux informations dont elles ont besoin. Elle transforme la communication des organisations en mettant en lien les personnes pour les faire collaborer comme une seule équipe unie.

II – Intégration de Wazuh à Slack

A – L'espace de travail

On commence déjà par créer un nouvel espace de travail en se rendant sur le site officiel de **Slack** et on clique sur « **Créer un espace de travail** », puis on remplit les différents champs requis.

Le champ « **Sur quoi travaille votre équipe en ce moment ?** » concerne la création du premier canal sur **Slack**.

B – L'application

À partir d'ici, on crée notre nouvelle application qui permettra d'intégrer **Wazuh** à **Slack**.

On clique sur la flèche à côté du nom de l'entreprise : 

Puis, on sélectionne « **Outils et paramètres** » ensuite « **Gérer les applications** » après sur « **Créer** » en haut à droite de la page où l'on est redirigé.

On clique ensuite sur « **Create New App** » puis sur « **From scratch** », on lui donne un nom et on sélectionne l'espace de travail qu'on a créé précédemment.

Enfin, on clique sur « **Incoming Webhooks** », puis on l'active, puis sur « **Add New Webhook to Workspace** » en bas de la page.

On peut au préalable créer un canal **#alertes** de la création de notre espace de travail, et on le sélectionne ici. (**#alertes** pour notre cas) puis on clique sur « **Permettre** ».

On récupère le lien dans la partie « **Webhook URL** ».

C – Configuration fichier ossec.conf

On se connecte à notre serveur **Wazuh** en ligne de commande puis on édite le fichier **ossec.conf** dans **/var/ossec/etc/**

On ajoute alors la configuration suivante dans la partie **<!-- Osquery integration -->**

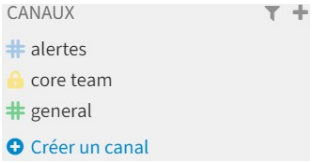
On redémarre l'agent avec **systemctl restart wazuh-manager**

Les alertes de **Wazuh** seront alors notifiées dans le canal #alertes de Slack

```
#ajout notif slack
  <integration>
    <name>slack</name>
    <hook_url>url</hook_url>
    <level>7</level>
   <alert_format>json</alert_format>
  </integration>
```

III – L'intégration avec Zulip

A – Le canal



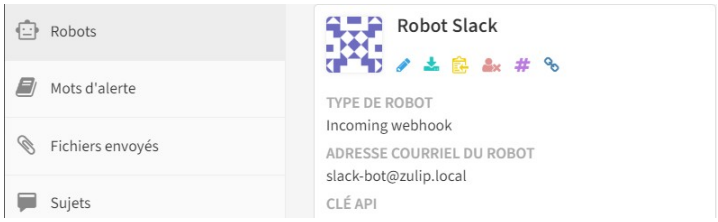
Après avoir créé un serveur Zulip, on s'identifie et on crée un canal ou seront publiées les alertes (notifications).

B – Le bot

Ensuite, on crée un bot avec le type « **Incoming Webook** », qui permet de publier les notifications dans le canal préalablement crée.

Pour cela, on clique sur son avatar en haut à gauche, puis dans la section de gauche sur « **Robots** », ensuite sur « **Ajouter un nouveau robot** ».

On rempli les informations, avec le type « **Incoming Webook** », son nom et éventuellement une adresse courriel pour le robot, puis sur « **Ajouter** ».



C – L'URL

À partir d'ici, on génère l'URL du bot.

Pour cela, on clique sur de notre bot. Puis, on choisit l'intégration (**slack-comatible-webhook**), notre canal sur lequel les notifications seront envoyées (**#alertes**).

On copie notre URL.

On se rend ici dans notre configuration **OSSEC** (**/var/ossec/etc/ossec.conf**) pour y ajouter l'intégration suivante :

```
#ajout notif zulip
  <integration>
    <name>slack-compatible-webhook</name>
    <hook_url>url_bot</hook_url>
    <level>7</level>
    <alert_format>json</alert_format>
  </integration>
```

Le bot publiera alors des messages de notifications dans le canal **#alertes** de **Zulip**.