AIST 21 – Compte-rendu hebdomadaire

Compte-rendu Lundi 04/03/2024

Aujourd'hui, je me suis penché sur les différentes intégrations notamment avec le logiciel de communication **Zulip** utilisé par l'organisme. Après de nombreuses recherches de documentations ou forum comme **Github**, il n'est pas facile voir pas possible à l'heure actuelle d'intégré **Wazuh** à **Zulip**.

Pour l'instant l'envoie de notifications sur **Slack** fonctionne.
Cependant, il aurait été intéressant que les notifications soient envoyées sur **Zulip**.

Compte-rendu Mardi 05/03/2024

Ce jour-ci, j'ai testé une installation de **Zulip sur Linux**.

Compte-rendu Mercredi 06/03/2024

Après avoir installé **Zulip** sur une VM la veille, j'ai essayé de regarder les configurations afin de trouver une solution pour intégrer **Zulip** avec **Wazuh**.

J'ai essayé alors de créer un **bot** sur **Zulip** qui permet d'écouter dans le canal **#alertes** de **Slack** ou les notifications **Wazuh** sont envoyés afin de les publier dans le canal #alertes de **Zulip** grâce à cette **intégration.**

Compte-rendu Jeudi 07/03/2024

Toujours la même activité, trouver un moyen pour lier **Wazuh** avec **Zulip.**

J'ai essayé d'installer un serveur **Zabbix sur Ubuntu 22.04.4** qui peut être intégré à **Zulip**, puis j'ai essayé de le lier avec **Wazuh** afin de faire remonter les alertes de **Zabbix** dans **Wazuh**, en vain puisqu'aucune documentation n'est possible et seul un dépôt **Github** avec des scripts susceptibles de fonctionner, incomplets pas à jours et qui finalement ne fonctionne pas.

Compte-rendu Vendredi 08/03/2024

Toujours la même activité, trouver un moyen pour lier **Wazuh** avec **Zulip.**

De manière simple, on souhaite envoyer les alertes **Zabbix** vers **Wazuh**.
De même, j'ai essayé de trouver de la documentation pour faire remonter les alertes de **Wazuh** dans **Zulip**.

UPDATE : J'ai généré l'URL du bot sortant (**incoming webhook**) que j'ai créé pour qu'il puisse écrire un message dans le canal **#alertes** de **Zulip**.

Il suffisait que je mette ce lien-là dans le fichier **ossec.conf** de **Wazuh**, suivant la même syntaxe d'intégration qu'avec **Slack**.

Compte-rendu général de cette semaine :

Cette semaine a été dédiée à l'amélioration des systèmes de communication et de surveillance au sein de l'organisme. Des efforts considérables ont été déployés pour intégrer **Wazuh** avec le logiciel de communication **Zulip**.
Malgré des recherches approfondies et des tentatives d'installation sur **Linux**, les résultats n'ont pas été concluants dans l'immédiat. Des expérimentations ont également été menées pour connecter **Zulip** avec **Wazuh**, impliquant la création d'un bot pour transmettre les notifications entre les deux systèmes. Parallèlement, des essais infructueux ont été réalisés pour lier un serveur **Zabbix** à **Zulip** et à **Wazuh** afin de remonter les alertes **Zabbix**.
Malheureusement, l'absence de documentation adéquate a entravé ces efforts. Néanmoins, une avancée positive a été réalisée avec la génération d'une URL pour un bot sortant sur **Zulip**, ouvrant ainsi la possibilité d'écrire des messages dans le canal approprié. En résumé, malgré les défis rencontrés, des progrès ont été accomplis dans l'objectif d'améliorer l'intégration et la gestion des alertes au sein de l'organisme.