AIST 21 – Compte-rendu hebdomadaire

Compte-rendu Lundi 25/03/2024

Pour bien commencer la semaine, j'ai mis en place et configuré le module **Osquery**. Il s'agit d'outil open source qui permet d'interroger les systèmes d'exploitation pour obtenir des informations sur leur état et leur configuration. Intégré à **Wazuh**, il renforce la surveillance en offrant une visibilité approfondie sur les activités système, aidant ainsi à détecter les menaces et à renforcer la sécurité des infrastructures informatiques. Je rencontre malheureusement un problème de **PID** donc j'ai une erreur lors des alertes dans **Wazuh**, de plus la documentation officielle n'est pas claire sur la configuration : doit-on l'installer sur les hôtes surveillés ou sur le serveur en lui-même ? Je cherche à résoudre cette erreur, mais pour ne pas perdre trop de temps, j'ai testé la mise en place de la détection d'un mot clé dans un fichier ainsi que la détection d'un processus en cours. Enfin, puisqu'il est possible d'écrire des réglés personnalisées, j'ai pu écrire deux règles & décodeurs pour afficher la mémoire et le stockage restant et des alertes sont envoyées lorsqu'un certain seuil est atteint. Le soir même, j'ai tout documenté y compris les tests faits avant de partir en week-end du vendredi précédent notamment sur les tests de **YARA**, utilisé avec **Wazuh**, qui est un outil de détection de logiciels malveillants open source qui permet d'identifier et de classifier les menaces potentielles en analysant les fichiers à la recherche de modèles spécifiques. Intégré à **Wazuh**, il renforce la capacité de détection des menaces en permettant l'analyse automatique des fichiers nouvellement créés ou modifiés, optimisant ainsi la surveillance de la sécurité des systèmes. J'ai pu le tester avec une simulation **Xbash** et Mirai ainsi que **EICAR** et j'ai documenté lorsque j'ai configuré la collecte des journaux de **Windows Defender**.

Compte-rendu Mardi 26/03/2024 & Compte-rendu Mercredi 27/03/2024

Ces deux jours ont été dédiés aux différents tests de configurations de modules sur **Wazuh** afin de vérifier si d'éventuelles erreurs apparaissaient. J'ai retenté de réinstaller **Osquery** en vain :

- Le déploiement d'**Osquery** avec **Wazuh** rencontre plusieurs problèmes. La documentation manque de clarté quant à son emplacement d'installation, ce qui entraîne une confusion. De plus, des erreurs liées au **PID** empêchent la vérification du fichier **PID** et des conflits potentiels avec d'autres processus sont observés. Bien que la console **Osquery** fonctionne, l'intégration avec **Wazuh** génère des graphiques vides et des erreurs dans les logs. L'incertitude persiste quant à l'installation d'**Osquery** sur les hôtes supervisés, non spécifiée dans la documentation. Des révisions approfondies et des tests supplémentaires sont nécessaires pour résoudre ces problèmes, ainsi que l'exploration des ressources de support de **Wazuh**.
- J'ai réinstallé **Osquery** enfin d'après midi du mercredi et je me suis aperçu qu'il y avait des erreurs de lecture des packs de requêtes ont été signalées pour les packs "**it-compliance**", "**vuln-management**", "**hardware-monitoring**" et "**ossec-rootkit**". Ces erreurs indiquent des problèmes potentiels avec les chemins de configuration ou les autorisations d'accès aux fichiers de ces packs. Ensuite, il a été constaté que les fichiers de configuration des packs de requêtes avaient été déplacés vers un nouvel emplacement, ce qui a entraîné une incohérence avec les chemins spécifiés dans le fichier **osquery.conf**. Cela a nécessité une mise à jour de la configuration pour refléter les nouveaux emplacements des fichiers, ce qui a permis de régler ces erreurs.
- Enfin, malgré les tentatives d'arrêt manuel d'**osqueryd** à l'aide de la commande "**kill**", le processus a continué à être redémarré automatiquement, ce qui a généré l'erreur "**Pidfile check failed: Pidfile::Error::Busy**". Ceci suggère la présence d'un mécanisme de redémarrage automatique, potentiellement configuré dans des scripts système ou des services de supervision et lorsque le **kill** a enfin fonctionné (sur une durée limitée) l'erreur n'apparaît plus (encore une fois sur une durée limitée) et le statut du démon est sans erreurs, mais aucun graphique n'apparaît sur l'interface web **Wazuh**.
- J'ai donc fait part de ces erreurs à mon tuteur qui viendra m'aider, bien que j'ai suivis la documentation officielle de **Wazuh** et deux vidéos bien explicatives sans résoudre mon problème.

AIST 21 – Compte-rendu hebdomadaire

Compte-rendu Jeudi 28/03/2024

- J'ai configuré quelques règles pour améliorer la détection de virus ou autres acteurs malveillants avec **MITRE ATT&CK**.
- J'ai configuré la détection des événements sur docker, pour détecter les activités **Docker**, comme extraire une image **Docker**, démarrer une instance, exécuter d'autres commandes **Docker**, puis supprimer le conteneur.
- J'ai configuré **l'IDS Suricata** dans **Wazuh** permettant d'enrichir la détection des menaces en combinant les capacités d'inspection du trafic réseau de **Suricata** avec les fonctionnalités de surveillance et d'analyse de sécurité de **Wazuh**.
- J'ai pu configurer la détection d'un mot-clé dans un fichier à partir de règles et décodeurs **Wazuh**.
- Une alerte est envoyée lorsque ce mot clé serait absent ou supprimé du fichier surveillé par l'agent **Wazuh**.

Compte-rendu Vendredi 29/03/2024

- J'ai configuré **Wazuh** pour qu'il détecte des binaires suspects au moyen du module **Wazuh rootcheck** en altérant le binaire **/usr/bin/w**.
- J'ai configuré **Wazuh** pour pouvoir assurer la surveillance de l'exécution de commandes malveillantes avec **Auditd**.
- J'ai mis en place un **système** de détection et suppression des logiciels malveillants avec **VirusTotal**, ainsi que la mise en place de la surveillance d'un processus en cours d'exécution et ceux qui seraient non-autorisés à être exécutés.
- Enfin, avec d'autres règles et décodeurs, j'ai configuré des alertes pour indiquer lorsque l'espace disque d'un hôte atteint un certain seuil d'alerte d'espace restant et mis en place un système qui permet de vérifier si la sortie a changé

Compte-rendu général de cette semaine :

Cette semaine a été intense en efforts visant à renforcer la sécurité et la surveillance de notre système informatique. J'ai principalement travaillé sur la mise en place du module **Osquery** pour obtenir une meilleure visibilité des activités système. Malheureusement, des difficultés sont survenues, notamment des erreurs de configuration liées au PID et des incertitudes quant à l'emplacement optimal d'installation. Malgré ces défis, des progrès significatifs ont été accomplis, notamment avec la configuration de règles pour améliorer la détection de virus et des activités suspectes. De plus, des tentatives ont été faites pour intégrer **l'IDS Suricata** et pour mettre en place la détection de mots-clés dans les fichiers. En parallèle, des efforts ont été déployés pour configurer **Wazuh** afin de détecter des binaires suspects, surveiller l'exécution de commandes malveillantes et gérer l'espace disque restant sur les hôtes. Malgré les obstacles rencontrés, ces activités ont été essentielles pour renforcer la sécurité informatique, bien que des ajustements supplémentaires soient à prendre en compte pour résoudre les problèmes persistants particulièrement du module **Osquery**.