DOUBLE

Benoit

SIO2

Introduction

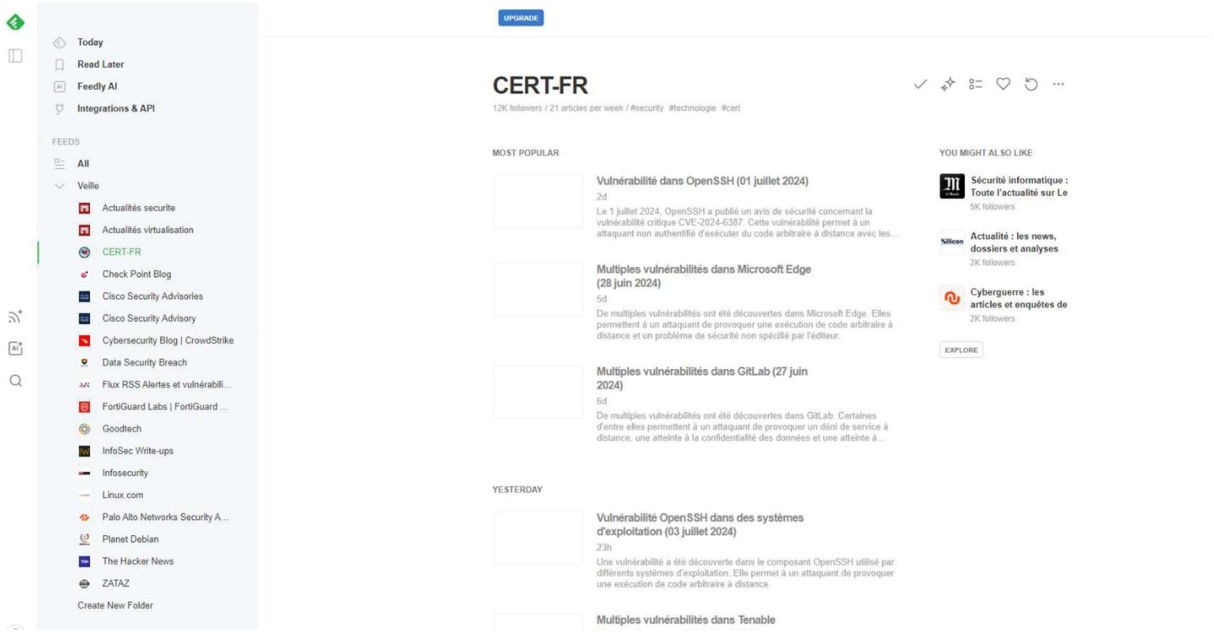
Au cours de mon stage au sein du service IT-Monitoring de Securitas, une de mes premières tâches a été de mettre en place un système de veille technologique. Cette mission avait pour objectif de suivre en temps réel les nouvelles vulnérabilités et menaces potentielles pouvant affecter les infrastructures de l'entreprise. Ce rapport détaille les outils utilisés, les processus mis en place, et les résultats obtenus.

1. Mise en Place de la Veille Technologique

1.1. Création d'un Compte Feedly

Pour centraliser et organiser les informations pertinentes, j'ai créé un compte sur Feedly, une plateforme de curation de contenu. Feedly permet de suivre des flux RSS de différentes sources, ce qui facilite la collecte et la gestion des informations.

- Abonnement à des Médias Pertinents : J'ai sélectionné et suivi des médias spécialisés en sécurité informatique, tels que Threatpost, Dark Reading, et les blogs de fournisseurs de solutions de sécurité comme Cisco et Palo Alto Networks.
- Organisation des Flux : Les flux d'informations ont été organisés par catégories (vulnérabilités, mises à jour de sécurité, analyses techniques, etc.) pour une consultation plus efficace.



1.2. Surveillance Quotidienne

Chaque jour, je vérifiais les nouvelles publications sur Feedly pour détecter les vulnérabilités et les menaces récentes. Ce processus consistait en :

- Identification des Vulnérabilités : Lecture des articles et rapports pour repérer les nouvelles vulnérabilités signalées.
- Vérification des CVE : Les CVE (Common Vulnerabilities and Exposures) sont des identifiants uniques attribués aux vulnérabilités de sécurité. Je vérifiais les CVE pour obtenir des détails

1.3. Vérification de l'Impact sur l'Infrastructure

Une fois les vulnérabilités identifiées, il était crucial de déterminer si elles affectaient les systèmes en place chez Securitas. Pour cela, j'utilisais deux outils principaux dont j'ai installé les agents (annexes p 19) :

1.3.1. OCS Inventory

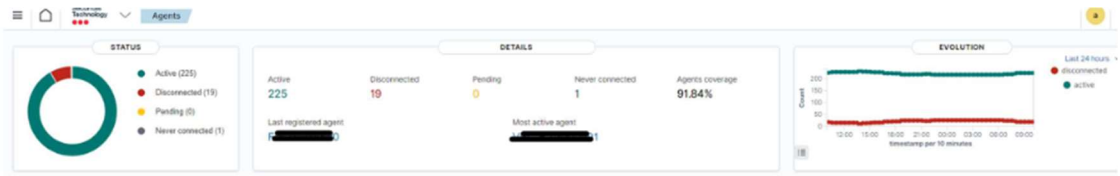
OCS Inventory (Open Computer and Software Inventory) est un outil de gestion d'inventaire qui permet de recenser les équipements matériels et logiciels présents sur le réseau.

- Consultation de l'Inventaire : J'utilisais OCS Inventory pour vérifier si le hardware ou le software mentionné dans les rapports de vulnérabilités était présent dans notre infrastructure.
- Évaluation de l'Exposition : Basé sur les résultats de l'inventaire, j'évaluais l'exposition de notre infrastructure aux nouvelles vulnérabilités.

1.3.2. Wazuh

Wazuh est un outil SIEM (une solution de sécurité qui permet aux organisations de détecter les menaces avant qu'elles ne perturbent leurs activités).

- Installation des Agents : J'ai installé les agents Wazuh sur les machines pour collecter et analyser les données de sécurité.
- Surveillance Continue : Wazuh permettait de surveiller en continu les événements de sécurité et de détecter les comportements anormaux ou les indicateurs de compromission.

- 

générer des alertes en cas de détection de vulnérabilités ou d'incidents de sécurité.

2. Processus de Veille et Réponse aux Vulnérabilités

2.1. Identification des Vulnérabilités

Chaque jour, après avoir parcouru les flux Feedly, je compilais une liste des nouvelles vulnérabilités découvertes. Les vulnérabilités critiques et celles potentiellement exploitables étaient notées en priorité.

2.2. Vérification de l'Impact

Pour chaque vulnérabilité identifiée, je procédais comme suit :

- Recherche dans OCS Inventory : Vérification de la présence des logiciels ou matériels vulnérables.
- Analyse avec Wazuh : Utilisation de Wazuh pour détecter toute activité suspecte ou indicateurs de compromission liés à la vulnérabilité.

2.3. Actions Correctives

Si une vulnérabilité affectait l'infrastructure de Securitas, des actions correctives étaient planifiées :

- Mises à Jour et Correctifs : Application des correctifs de sécurité fournis par les éditeurs de logiciels ou les fabricants de matériel.
- Configurations de Sécurité : Modification des configurations de sécurité pour atténuer les risques.
- Alertes et Notifications : Communication avec les équipes concernées pour les informer des vulnérabilités et des mesures prises.

Conclusion

Le travail de veille technologique a été une composante essentielle de mon stage, permettant d'assurer la sécurité continue des infrastructures de Securitas. Grâce à l'utilisation de Feedly, OCS Inventory et Wazuh, j'ai pu identifier rapidement les vulnérabilités, évaluer leur impact et prendre les mesures nécessaires pour les corriger. Cette expérience m'a permis de développer des compétences précieuses en matière de surveillance de la sécurité et de réponse aux incidents.