Déploiement d'un SIEM et enrichissement des données

Un SIEM (Security Information and Event Management) est une solution visant à corréler les logs de différentes sources et faciliter leur analyse en cas d'incident de sécurité.

Objectifs de l'enrichissement

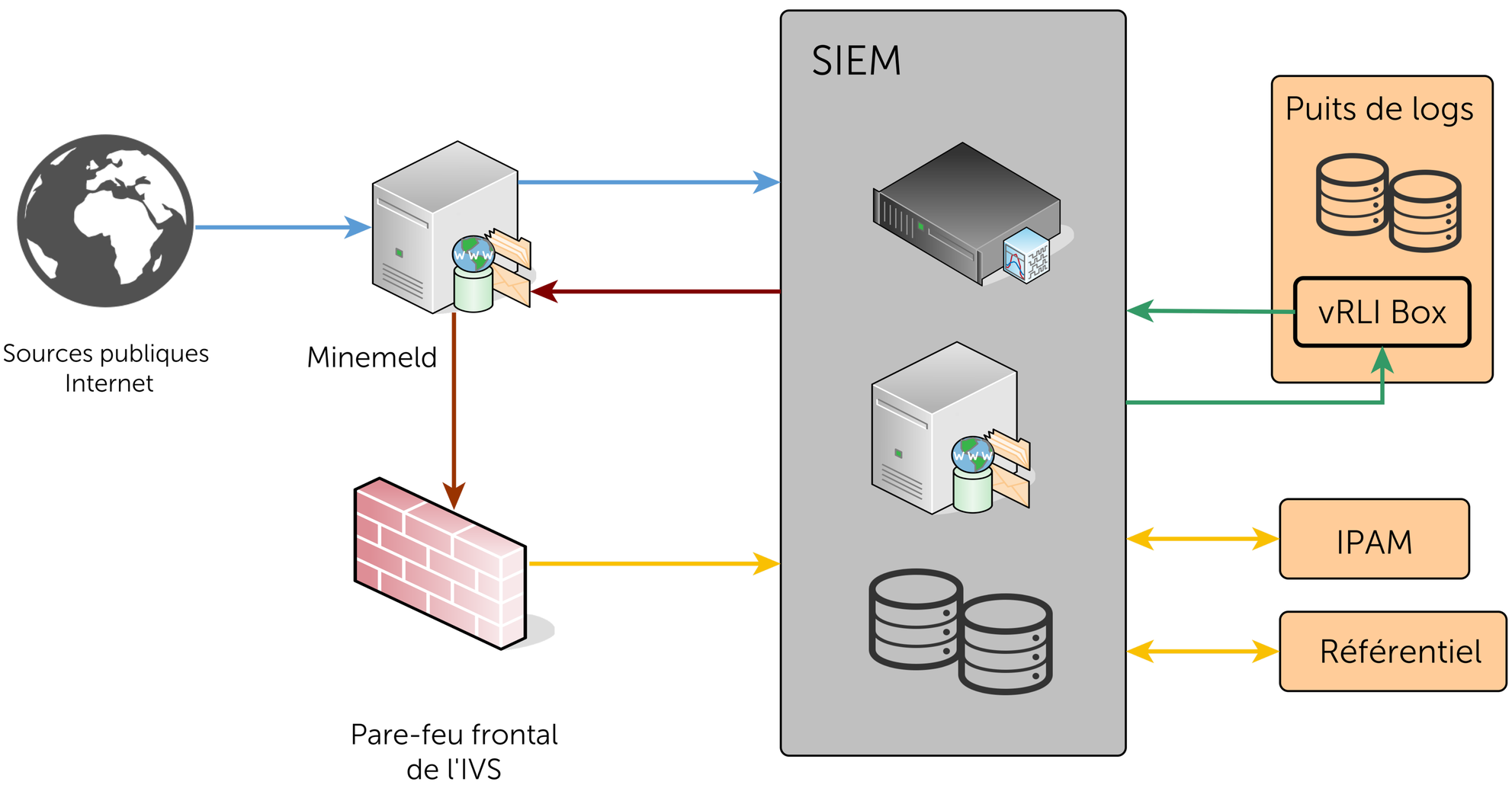
- automatiser une partie des tâches récurrentes des analystes
- augmenter le niveau de confiance dans les résultats fournis
- ajouter facilement de nouvelles sources de données

Interface avec les sources externes et Minemeld

L'outil open-source Minemeld est utilisé pour récupérer des listes d'IP et d'URL fournies par des services de réputation d'IP ou des CERT.
Les listes d'IP sont agrégées et classées selon le niveau de confiance qu'on peut avoir dans le service qui fournit l'information.

Interface avec les sources de données

Les capacités du SIEM sont modestes (< 500 évènements par seconde). Une interface a été développée avec le puits de logs pour faire une pré-sélection des évènements analysés par le SIEM.



Automatisation des actions

Le pare-feu récupère périodiquement sur Minemeld des listes d'IP à bloquer.
Pour être présentes dans ces listes, les IP doivent remplir de nombreux critères.

Interface avec les sources internes

Lorsque des évènements de sévérité élevée sont remontés ou corrélés par le SIEM, une vérification est faite pour savoir si la source de l'évènement fait partie de la communauté enseignement-recherche.
La réponse apportée varie en fonction des informations récoltées.

Automatisation de la réponse

1. Comparaison des IP suspectes avec des listes d'IP malveillantes
2. Si IP interne à RENATER, alerte aux équipes internes du GIP
3. Si IP de la communauté enseignement recherche, transmission au CERT
4. Si IP présente dans une source de confiance élevée, blocage automatique de l'IP
5. Sinon, analyse manuelle

Auteur : Thibaud Badouard

Si le sujet vous intéresse, n'hésitez pas à venir en discuter sur le stand Renater