Alertes de sécurité par les logs : renversons la situation

Dominique FOURNIER

26/05/2025

Sommaire

- Recommandation CNIL / SIEM
- Structuration des analyses
- Rapports journaliers
- Déploiement Graylog ou LogDom
- Nouvelles règles

Recommandation CNIL

- Centralisation des logs pour un an
- Analyser les données de ces logs

Outil d'analyse : le SIEM *Security Information and Event Management*

Alertes

Une alerte :

- Détection d'un *pattern* dans un log
- Notification de l'informaticien

Connaissez-vous tous les logs intéressants de votre infrastructure ?

Filtrage des non-évènements

Proposition :

- Définir les *patterns* des logs inutiles

  => Tout log inconnu alertera l'informaticien pour analyse

Mais un log inutile pour un serveur sera utile pour un autre : rationalisation

Structuration des analyses

Pour chaque équipement, définir la liste des services

Pour chaque service actif, définir les schémas normaux

Équipement	Service	Schéma
Serveur 1	SSH	SSH Public
	Postfix	Postfix envoi seul
Serveur 2	SSH	SSH Interne
	Postfix	Postfix public
		Postfix envoi seul

Rapports journaliers

- Rapport des logs inconnus envoyé journalièrement aux informaticiens
- Ordonné par serveur, au lieu d'être trié par heure

```
    HOST : serveur1.domaine.tld
sshd: error: kex_exchange_identification: banner line contains invalid characters
sshd: banner exchange: Connection from AA.BBB.CCC.DDD port 62484: invalid format
(systemd): pam_unix(systemd-user:session): session opened for user root(uid=0) by (uid=0)

    HOST : serveur2.domaine.tld
systemd: Queued start job for default target default.target.
mariadbd: 2024-11-23  1:59:06 26454 [Warning] Aborted connection 26454 to db: 'gitea' user: 'gitea'
 host: 'localhost' (Got an error reading communication packets)
```

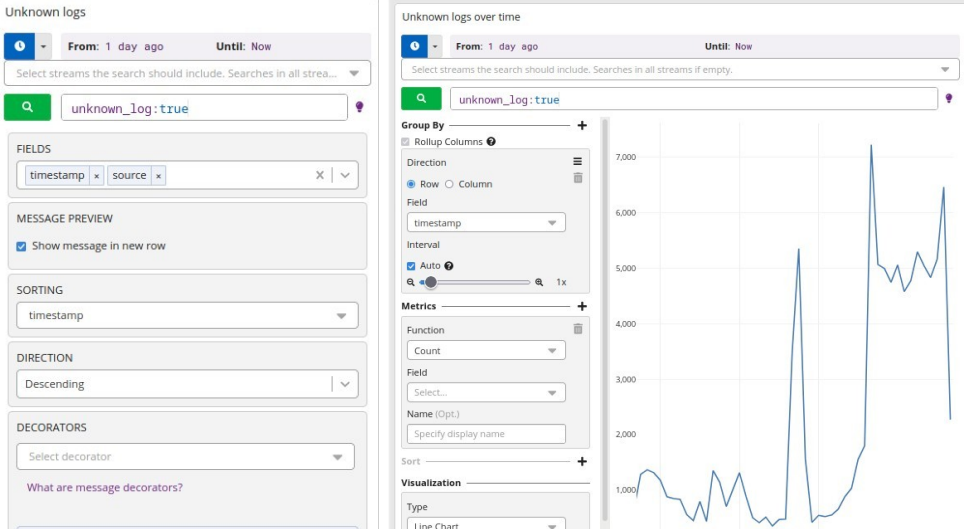
Déploiement Graylog

1. Installer GrayLog
2. Paramétrer les Flux *(Streams)* pour filtrer serveur par serveur ou par groupe de serveurs
3. Créer un pipeline prenant en entrée un ou plusieurs flux et ayant la liste des services autorisés avec leurs schémas normaux associés
4. Créer des schémas normaux spécifiques à l'infrastructure

Astuce : Dans la configuration, il faut que le "Pipeline Processor" soit après le "Message Filter Chain"

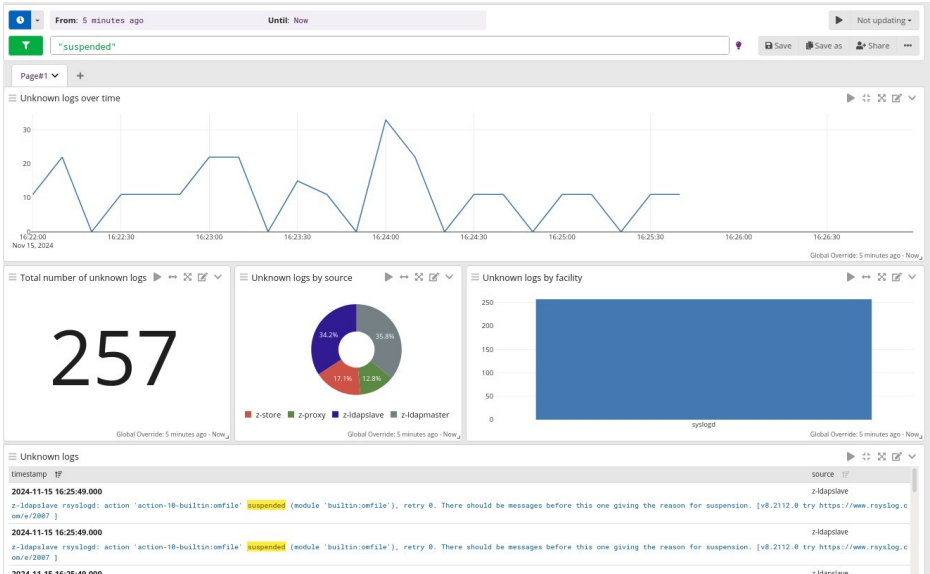
Création du Tableau de Bord (1/2)

Il faut maintenant définir un tableau de bord pour tous les logs inconnus



sari
Le Réseau des informaticiens du Sillon Alpin

Création du Tableau de Bord (2/2)



Le Réseau des informaticiens du Sillon Alpin

Déploiement LogDom

Graylog est très lourd en RAM et disque
La version légère est LogDom, écrit en PHP :

1. Installer le PHP
2. Cloner le repository
3. Définir la liste des serveurs et leurs services autorisés avec les schémas normaux associés
4. Créer des schémas normaux spécifiques à l'infrastructure dans le fichier CSV

Création de schémas normaux

Un schéma *(Pipeline)* Graylog est de la forme :

```
rule "TEST"
when
  has_field("message")
then
    set_fields(grok(
    "%{START:unknown_log;boolean}%{HOSTNAME:hostname} Texte du log",
    to_string($message.message), true));

    //set_field("TEST", true);
end
```

Démarrage rapide

- Plus de 100 services sont déjà disponibles dans le repository Git https://gitlab.in2p3.fr/dominique.fournier/LogDom
- Déploiement immédiat sur les infrastructures

Apache, Postfix, Sympa, MariaDB, LemonLDAP, Rspamd en sont quelques exemples.

Conclusion

- Supprimer les logs normaux : apparition des logs inconnus
- Logs inconnus signalés en alerte => traités par l'informaticien

Traitements possibles :

1. Corriger le problème à la source : le log disparaît
2. Mettre en place d'une règle d'exception dans le SIEM : le log disparaît
3. Conserver l'erreur pour traitement ultérieur

Conclusion

Objectifs atteints :

- Détection immédiate de nouveaux logs et action corrective pro-active
- Détection d'alertes de sécurité
- Amélioration de la qualité de notre infrastructure

Bonus : Déclenchement d'une alerte temps réel pour tout nouveau log

Évolution : Faire tendre le nombre de lignes du rapport vers zéro

Action !

Démonstration

Merci

Vos questions ?