Mise en place de la détection brute force fail2ban dans Wazuh

Last updated by | Leslie Lemaire | 18 juin 2025 at 19:10 UTC+2

📋 Détection de fichiers avec Wazuh – FIM `/etc` + Fail2Ban

Ce fichier documente un type de détection réalisée avec Wazuh sur un agent Debian 12 (`Zimbra`) :

- La **détection d'intrusion via Fail2Ban** à travers les logs syslog

---

🔐 1. Détection Fail2Ban (via journaux syslog)

📥 Principe

Wazuh peut détecter les bannissements appliqués par Fail2Ban en analysant `/var/log/auth.log` ou `journald` .

🔍 Requêtes utiles dans `Discover`

```
data.syslog_program: "fail2ban"
```

ou

```
message: "Ban" OR message: "Unban"
```

🖼️ Exemple d'événement attendu

- `Ban 192.168.0.42`
- `Unban 10.4.0.32`
- `NOTICE [sshd] 192.168.1.100 already banned`

🧠 Remarques

- Les événements Fail2Ban ne s'affichent **pas** dans `File Integrity Monitoring` , mais uniquement dans `Discover` ou des dashboards personnalisés.
- Le module FIM ne détecte **que les changements sur disque**, pas les logs ou événements système.

🔐 2. Détection des bannissements Fail2Ban

🎯 Objectif

Superviser les bannissements déclenchés par Fail2Ban et les faire remonter dans Wazuh via le module `logcollector`.

🛠️ Configuration `ossec.conf` (sur l'agent Wazuh)

🔹 Si les logs sont dans `/var/log/auth.log` :

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/auth.log</location>
</localfile>
```

🔹 Si Fail2Ban utilise `journald` (Debian 11/12 par défaut) :

```
<localfile>
  <log_format>syslog</log_format>
  <command>journalctl -f -n 0 -u fail2ban</command>
</localfile>
```

🔍 Requêtes de vérification dans l'interface Wazuh

Dans **Explore > Discover**, utiliser :

```
data.syslog_program: "fail2ban"
```

ou

```
message: "Ban" OR message: "Unban"
```

📌 Événements attendus

Exemples de messages que tu peux retrouver :

- `Ban 192.168.1.10`
- `Unban 10.4.0.42`
- `NOTICE [sshd] 192.168.0.55 already banned`

🧠 Remarques importantes

- Fail2Ban ne génère pas de règles `syscheck`, donc les événements n'apparaissent **pas** dans le menu `File Integrity Monitoring`.
- Il est recommandé d'activer une règle personnalisée dans Wazuh pour alerter sur les bannissements critiques.