

## FICHE 5 – SIEM WAZUH – RÉPONSE AUX INCIDENTS

Lien officiel de l'installation :

<https://documentation.wazuh.com/current/user-manual/capabilities/active-response/index.html>

### SOMMAIRE

A. Module – réponses aux incidents.....	1
B. Configuration d'une réponse aux incidents.....	1
B.1 Vérification de la disponibilité de la commande.....	2
B.2 Création d'une réponse active.....	2

### A. MODULE – RÉPONSES AUX INCIDENTS

Un incident de sécurité désigne tout événement ou activité indésirable qui met en danger ou menace la confidentialité, l'intégrité ou la disponibilité des actifs numériques, des réseaux, des données ou des ressources. Ces incidents comprennent les accès non autorisés, les violations de données, les infections par des logiciels malveillants, les attaques par déni de service et toute autre activité qui compromet la sécurité de l'environnement informatique d'une organisation.

L'objectif de la réponse aux incidents est de gérer efficacement un incident de sécurité et de rétablir les opérations normales le plus rapidement possible. **À mesure que les ressources numériques des organisations augmentent en permanence, la gestion manuelle des incidents devient de plus en plus difficile, d'où la nécessité de l'automatisation.**

La réponse automatisée aux incidents implique des actions automatiques prises en réponse aux incidents de sécurité. Ces actions peuvent inclure l'isolement des points de terminaison compromis, le blocage des adresses IP malveillantes, la mise en quarantaine des appareils infectés ou la désactivation des comptes d'utilisateurs compromis. **En automatisant la réponse aux incidents, les équipes de cybersécurité réduisent le temps de réponse aux menaces détectées, préviennent ou minimisent l'impact des incidents et gèrent efficacement un grand volume d'événements de sécurité.**

Le module Wazuh Active Response permet aux utilisateurs d'exécuter des actions automatisées lorsque des incidents sont détectés sur les terminaux. Cela améliore les processus de réponse aux incidents d'une organisation, permettant aux équipes de sécurité de prendre des mesures immédiates et automatisées pour contrer les menaces détectées.

L'un des avantages du module Wazuh Active Response est son adaptabilité. Wazuh permet aux équipes de sécurité de créer des actions de réponse active personnalisées dans n'importe quel langage de programmation, en les adaptant à leurs besoins spécifiques. Cela garantit que lorsqu'une menace est détectée, la réponse peut être personnalisée pour s'adapter aux exigences de l'organisation.

### B. CONFIGURATION D'UNE RÉPONSE AUX INCIDENTS

Wazuh dispose de programmes, scripts et binaires déjà installés pouvant être activés au besoin des situations.

Vous pouvez en retrouver la liste :

```
/var/ossec/active-response/bin# ls
default-firewall-drop  firewall-d-drop  host-deny          ipfw kaspersky.pypf
restart-wazuh          wazuh-slack      disable-account    firewall-drop     ip-
customblock kaspersky      npf                restart.sh         route-null
```

Exemple d'activation d'une réponse à une attaque par force brute sur le service SSH d'un poste.

## B.1 VÉRIFICATION DE LA DISPONIBILITÉ DE LA COMMANDE

Pour cela vous devez vérifier le contenu du fichier « ossec.conf ».

Vous pouvez atteindre ce fichier de deux façons :

- sur l'interface du serveur Wazuh : **Gestion du serveur / paramètres / Configuration d'édition.**



- sur le serveur Wazuh : **/var/ossec/etc/ossec.conf**

Nous devons vérifier que la commande liée à une demande de blocage d'adresse IP suite à une attaque par force brute soit disponible dans le fichier « ossec.conf » :

```
<command>
<name>firewall-drop</name>
<executable>firewall-drop</executable>
<timeout_allowed>yes</timeout_allowed>
</command>
```

Nous constatons dans cet exemple que la commande est bien disponible et appellera le binaire « **firewall-drop** ».

## B.2 CRÉATION D'UNE RÉPONSE ACTIVE

La création d'une réponse dans ce même fichier « ossec.conf » va permettre d'automatiser le lancement du binaire associé dès que le « **rules** » (la règle) indiqué sera observé sur le point d'extrémité.

Voici la partie de script à rajouter pour notre cas :

```
<active-response>
<command>firewall-drop</command>
<location>local</location>
<rules_id>5763</rules_id>
<timeout>180</timeout>
</active-response>
```

Une réponse active sera déclenchée dès que la règle 5763 sera observée par le serveur Wazuh. L'IP de l'attaquant sera bloquée pendant 180 secondes.

Pour visualiser les règles :












```
/var/ossec/ruleset/rules# ls
0010-rules_config.xml  0285-systemd_rules.xml  0565-ms_ipsec_rules.xml
0015-ossec_rules.xml   0290-firewalld_rules.xml 0570-sca_rules.xml
0016-wazuh_rules.xml   0295-mysql_rules.xml    0575-win-base_rules.xml
...
/var/ossec/ruleset/rules# nano 0095-sshd_rules.xml
```

```
GNU nano 6.2                                0095-sshd_rules.xml

<rule id="5763" level="10" frequency="8" timeframe="120" ignore="60">
  <if_matched_sid>5760</if_matched_sid>
  <same_source_ip/>
  <description>sshd: brute force trying to get access to the system. Authentication failed ATTENTION.</description>
  <mitre>
    <id>T1110</id>
  </mitre>
  <group>authentication_failures,gdpr_IV_35.7.d,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_SI.4,nist_800_53_AU.14,nist_
</rule>
</group>
```

Nous retrouvons ici la règle précisant que nous sommes face à une attaque par force brute sur le service SSH au niveau de multiples essais d'authentification.

Voici une réponse qui serait apportée dans le cas d'une attaque par force brute sur le service SSH après l'activation de la réponse :

	Feb 17, 2025 @ 16:56:13.5...	CubDHCP	Host Blocked by firewall-drop Active Response	3	651
	Feb 17, 2025 @ 16:56:13.5...	CubDHCP	sshd: authentication failed.	5	5760
	Feb 17, 2025 @ 16:56:13.5...	CubDHCP	sshd: authentication failed.	5	5760
	Feb 17, 2025 @ 16:56:11.5...	CubDHCP	sshd: authentication failed.	5	5760
	Feb 17, 2025 @ 16:56:11.5...	CubDHCP	sshd: authentication failed.	5	5760
	Feb 17, 2025 @ 16:56:11.5...	CubDHCP	sshd: authentication failed.	5	5760
	Feb 17, 2025 @ 16:56:11.5...	CubDHCP	sshd: authentication failed.	5	5760
	Feb 17, 2025 @ 16:56:11.5...	CubDHCP	PAM: Multiple failed logins in a small period of time.	10	5551
	Feb 17, 2025 @ 16:56:11.5...	CubDHCP	sshd: authentication failed.	5	5760
	Feb 17, 2025 @ 16:56:11.5...	CubDHCP	sshd: authentication failed.	5	5760
	Feb 17, 2025 @ 16:56:11.5...	CubDHCP	sshd: brute force trying to get access to the system. Authentication failed ATTENTION.	10	5763

L'adresse IP de l'attaquant est bloquée pendant les 180 secondes définies dans le fichier « ossec.conf ».