owlh_documentation Documentation

Release 0.17.x

owlh team

Oct 12, 2021

Contents

CHAPTER 1

Install OwlH

1.1 Install all-in-one system (AIO)

- how to deploy an all-in-one system

CHAPTER 2

OwlH Scenarios and main configurations

2.1 Basic deployment - All-in-one deployment

- how to deploy an all-in-one system

2.2 Software TAP Scenario

- How-to configure Software TAP Scenario

2.3 Wazuh Integration

- Configure OwlH as NIDS for Wazuh

CHAPTER 3

User Manual

3.1 Open Rules

- Suricata ruleset management - 3rd party and custom rulesets

CHAPTER 4

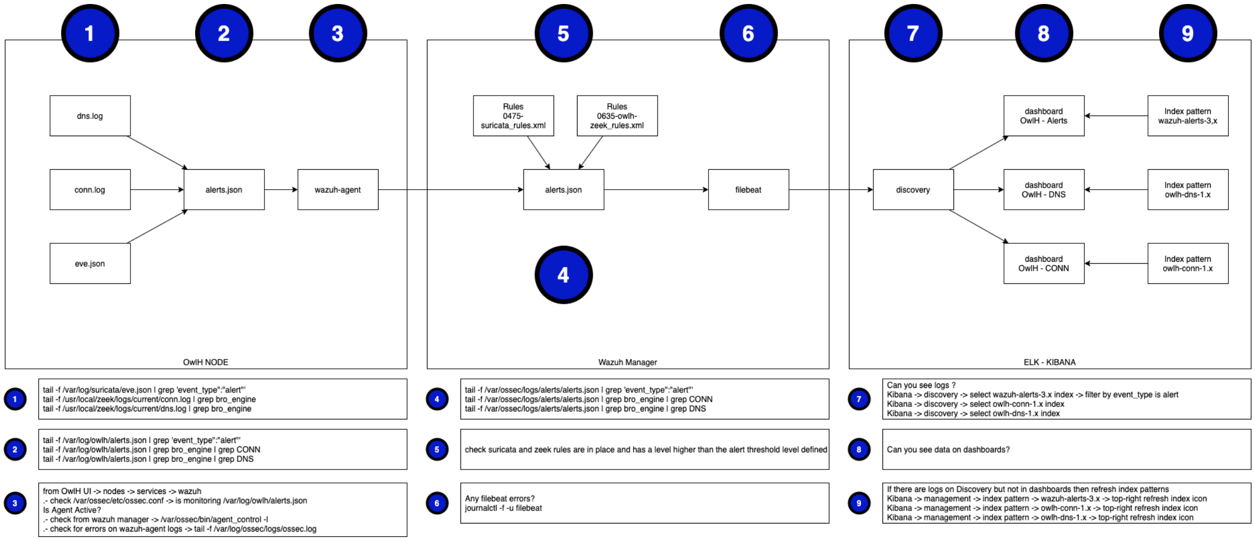
Troubleshooting

Warning: work in progress…

Note: If you are missing something in this documentation, please say hello in our slack #doc channel and let us know what is missing or should be good to have.

- join OwlH slack - OwlH Slack workspace

Check Flow Data diagram and checkpoints.



1

```
tail -f /var/log/suricata/eve.json | grep 'event_type":"alert"'
tail -f /usr/local/zeek/logs/current/conn.log | grep bro_engine
tail -f /usr/local/zeek/logs/current/dns.log | grep bro_engine
```

2

```
tail -f /var/log/owlh/alerts.json | grep 'event_type":"alert"'
tail -f /var/log/owlh/alerts.json | grep bro_engine | grep CONN
tail -f /var/log/owlh/alerts.json | grep bro_engine | grep DNS
```

3

from OwlH UI -> nodes -> services -> wazuh
.- check /var/ossec/etc/ossec.conf -> is monitoring /var/log/owlh/alerts.json
Is Agent Active?
.- check from wazuh manager -> /var/ossec/bin/agent_control -l
.- check for errors on wazuh-agent logs -> tail -f /var/log/ossec/logs/ossec.log

4

```
tail -f /var/ossec/logs/alerts/alerts.json | grep 'event_type":"alert"'
tail -f /var/ossec/logs/alerts/alerts.json | grep bro_engine | grep CONN
tail -f /var/ossec/logs/alerts/alerts.json | grep bro_engine | grep DNS
```

5

check suricata and zeek rules are in place and has a level higher than the alert threshold level defined

6

Any filebeat errors?
journalctl -f -u filebeat

7

Can you see logs ?
Kibana -> discovery -> select wazuh-alerts-3.x index -> filter by event_type is alert
Kibana -> discovery -> select owlh-conn-1.x index
Kibana -> discovery -> select owlh-dns-1.x index

8

Can you see data on dashboards?

9

If there are logs on Discovery but not in dashboards then refresh index patterns
Kibana -> management -> index pattern -> wazuh-alerts-3.x -> top-right refresh index icon
Kibana -> management -> index pattern -> owlh-conn-1.x -> top-right refresh index icon
Kibana -> management -> index pattern -> owlh-dns-1.x -> top-right refresh index icon

4.1 OwlH Node

Suricata doesn't create alerts

4.2 OwlH Master

4.3 OwlH UI

4.4 OwlH Dashboards on Kibana

Can't see any alert on owlh-alert dashboard

Maybe Saved Queries are using a different index pattern than the one you are using:

- Open Saved queries OwlH Alert, OwlH Conn and OwlH DNS.
- OwlH Alert should be using wazuh-alerts-3.x, wazuh-alerts-4.x or wazuh-alerts-* depending on your Wazuh version. if you are running wazuh 3.x use wazuh-alerts-3.x. if running wazuh 4.x choose wazuh-alerts-*.
- Save, you should see now events in discovery, if any then your dashboard should work now.

If your OwlH Alerts dashboard isn't showing anything maybe is because your wazuh-alerts index pattern needs to be updated.

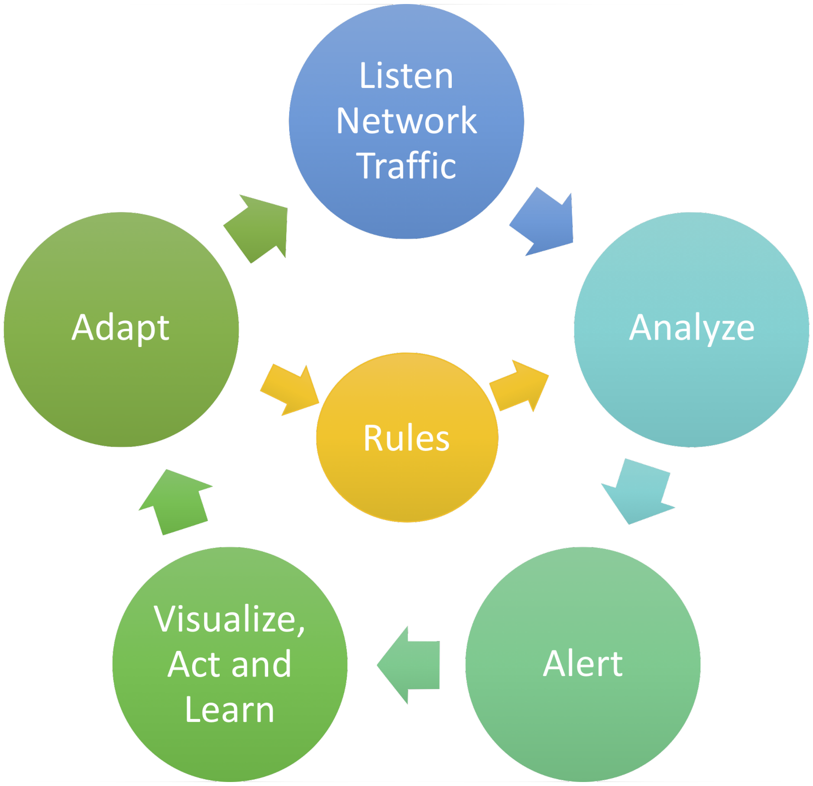
- detect if you need to refresh index patter by searching on discovery for event_type. open any event found and look for alert symbol. If you can see alert symbol then you need to refresh your index pattern
- go kibana -> management -> index pattern -> wazuh-alerts pattern -> reload wazuh index pattern
- go back to discovery, verify alert symbol is gone.
- open OwlH Alerts dashboard, you should see alerts now

CHAPTER 5

About OwlH

Current - v0.17.x

This picture will summarize the process we are working in.



5.1 If you need help

- email our support team - support@owlh.net
- join OwlH slack - OwlH Slack workspace
- ask for professional support and services - prohelp@owlh.net

OwlH - current v0.17.x

documentation last updated - Oct 12, 2021

- email our support team - support@owlh.net
- join OwlH slack - OwlH Slack workspace

documentation last updated - Oct 12, 2021