Endpoint Detection and Response (EDR)- Tools and resources Research.

1. **OSSEC** is open source Host base Intrusion **DETECTION** System and hence cannot be used in preventive mode. However, the alerts from OSSEC can be used as address any threats detected.

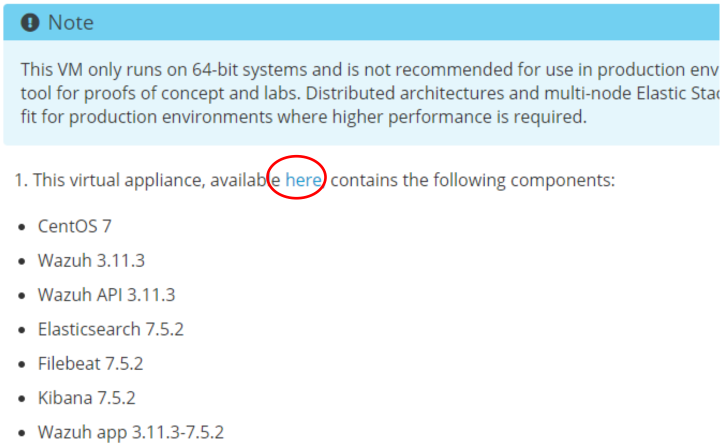
2. **WAZUH:**

   WAZUH is a free, open source and enterprise-ready security monitoring solution for threat detection, integrity monitoring, incident response and compliance. Looking at WAZUH in depth and testing the LAB below.

   a. Wazuh Documentation https://documentation.wazuh.com/3.11/index.html (go through to understand different features on how Wazuh can be used)

   b. After you open the web page from the above link → click installation guide and pick VM.

   c. Then click on the link on the corresponding page as shown below:



Note

This VM only runs on 64-bit systems and is not recommended for use in production env
tool for proofs of concept and labs. Distributed architectures and multi-node Elastic Stac
fit for production environments where higher performance is required.

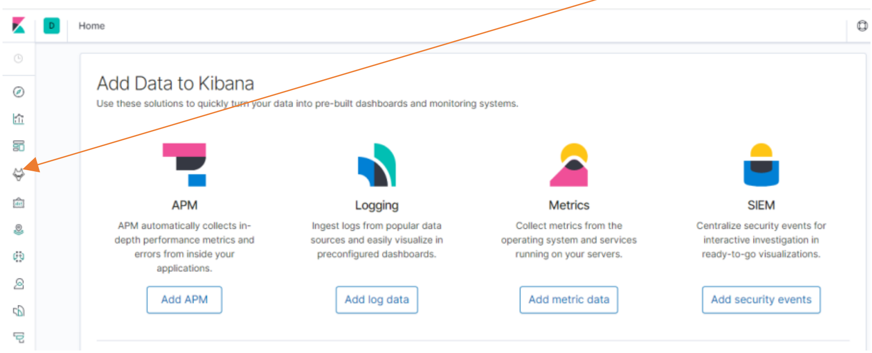
1. This virtual appliance, available here contains the following components:

- CentOS 7
- Wazuh 3.11.3
- Wazuh API 3.11.3
- Elasticsearch 7.5.2
- Filebeat 7.5.2
- Kibana 7.5.2
- Wazuh app 3.11.3-7.5.2

   d. This will download your OVA file and you can install this on Virtual Box. Start the virtual box and for login credential → **Username : root, Password: wazuh**

   e. Once logged in type if config or Ip address to get your IP. Make sure your VM is on the same subnet as your machine (use bridge network)

   f. Now take the Ip address and use https:// connection on your browser to connect to the Wazuh interface. (You may get a certificate issue → please select continue anyway)→ you should see a Kibana home page as shown below→ click on the Wazuh link as highlighted In the image



Add Data to Kibana

Use these solutions to quickly turn your data into pre-built dashboards and monitoring systems.

APM

APM automatically collects in-depth performance metrics and errors from inside your applications.

Add APM

Logging

Ingest logs from popular data sources and easily visualize in preconfigured dashboards.

Add log data

Metrics

Collect metrics from the operating system and services running on your servers.

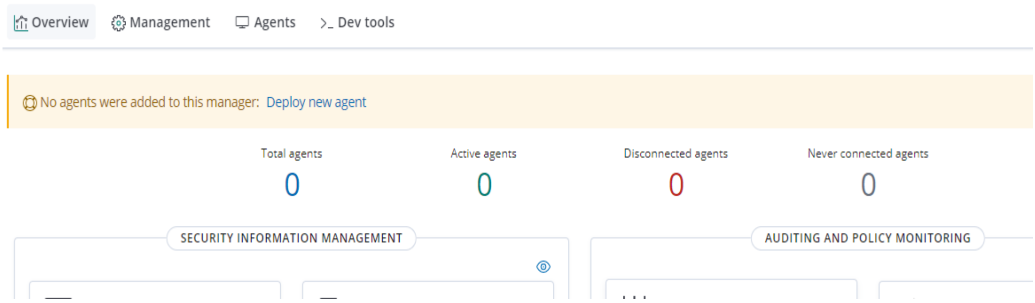
Add metric data

SIEM

Centralize security events for interactive investigation in ready-to-go visualizations.

Add security events

g. Click on deploy new agents as shown below:

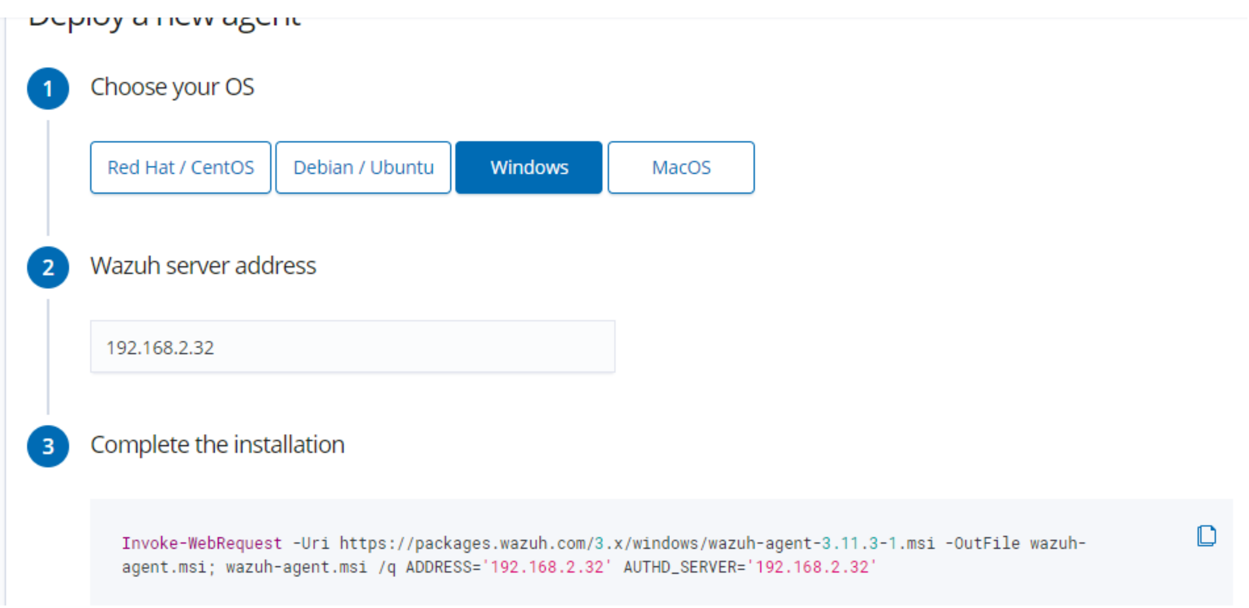

Overview
Management
Agents
>_ Dev tools

No agents were added to this manager: Deploy new agent

Total agents	Active agents	Disconnected agents	Never connected agents
0	0	0	0

SECURITY INFORMATION MANAGEMENT
AUDITING AND POLICY MONITORING

h. Then choose the OS and other details for the agent



Deploy a new agent

1 Choose your OS

Red Hat / CentOS | Debian / Ubuntu | Windows | MacOS

2 Wazuh server address

192.168.2.32

3 Complete the installation

```
Invoke-WebRequest -Uri https://packages.wazuh.com/3.x/windows/wazuh-agent-3.11.3-1.msi -OutFile wazuh-
agent.msi; wazuh-agent.msi /q ADDRESS='192.168.2.32' AUTHD_SERVER='192.168.2.32'
```

Copy the complete installation command and paste into your terminal. Should work.

i. If step h. does not work, we can use the package installation link to download the GUI for each system from the link below.

   https://documentation.wazuh.com/2.1/installation-guide/packages-list/index.html

   additional documentation for agent registration can be found here (https://documentation.wazuh.com/3.7/user-manual/registering/use-registration-service.html#password-authorization)

j. In order to manage agent and extract keys for the agent run the following commands on the manager VM

   /var/ossec/bin/manage-agents → select **A** to add agent → then enter all the details for the id → then enter **E** to extract keys → use that key on the windows agent to connect.

k. Use the following links below to perform file integrity monitoring and other Wazhu features

   https://www.youtube.com/watch?v=BgYra9rNrD0

   https://www.youtube.com/watch?v=TlkiIdgZAvM

   https://www.youtube.com/watch?v=WpfpxRY3Ufk

Preventing and Detecting ransomware - Wazhu Lab

1. Ransomware test script is attached:

   ransomware test script.txt

2. On the agent that needs to be monitored setup a test directory and add that directory path to ossec.conf file as shown below:

   ```
   mkdir -p /home/danish/test → /var/ossec/etc/ossec.conf
                                          ↓
                                      <syscheck>
                                      <directories check_all="yes"
                                      whodata="yes">/home/danish/test</directories>
                                      </syscheck>
   ```

3. Now restart agent and run python script:

   ```
   systemctl restart wazuh-agent→ python3 wazuh-ransomware-poc.py prepare
   ```

4. List directories:

   ```
   ls -lRh /home/danish/test → you should be able to see new directories
   ```

   these files also show under the Wazuh UI as alerts or logs of files been created

5. Setting up the attack: run the command below

   ```
   python3 wazuh-ransomware-poc.py attack
   ```

6. Wazuh will now show 2 log types- file being created and files being deleted

   Wazuh is able to detect the events generated by a ransomware attack, but it still can be difficult for a person to know when the attack is going on. That is why it helps to automatically trigger alerts when this situation is detected. For this purpose, we use the Alerting feature of Open Distro (the free and open source alternative to Elastic Watchers).

7. Using the alert and triggering functions (**say trigger if count is > x files**) setup the alert. **This can help identify ransomware attacks during an active attack and help prevent complete damage.**

8. Setup a active response which is a script that runs when a specific kind of alert is triggered. This can be configured in the ossec.conf file under the server /var/ossec/etc/ossec.conf

   Here is the documentation for active response and custom rules

   https://documentation.wazuh.com/3.10/user-manual/capabilities/active-response/how-it-works.html#active-response-configuration

   https://documentation.wazuh.com/3.10/user-manual/capabilities/active-response/remediation-configuration.html