Step-by-Step guide to setting up Elastic Security Stack with Fleet Server and Cortex XSOAR or TheHive SOAR on the latest edition of Ubuntu Server

This guide assumes that you have basic knowledge of Linux administration and security concepts.

**Prerequisites:**

1. **Ubuntu Server**: Latest edition installed.
2. **Root or Sudo Privileges**: Access to a user with administrative privileges.
3. **Basic Network Configuration**: Ensure that your server has network connectivity and DNS resolution.

**Step 1: Update and Upgrade Ubuntu**

sudo apt update

sudo apt upgrade -y

**Step 2: Install Java (Required for Elastic Stack)**

Elastic Stack requires Java. Install OpenJDK 11 (or a supported version):

sudo apt install openjdk-11-jdk -y

**Step 3: Install Elastic Stack (Elasticsearch, Kibana, and Fleet Server)**

**3.1. Add Elastic APT Repository**

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

sudo sh -c 'echo "deb https://artifacts.elastic.co/packages/8.x/apt stable main" > /etc/apt/sources.list.d/elastic-8.x.list'

**3.2. Install Elasticsearch**

sudo apt update

sudo apt install elasticsearch -y

**3.3. Configure Elasticsearch**

Edit the Elasticsearch configuration file:

sudo nano /etc/elasticsearch/elasticsearch.yml

**Set the following parameters:**

network.host: 0.0.0.0

http.port: 9200

**Enable and start the Elasticsearch service:**

sudo systemctl enable elasticsearch

sudo systemctl start elasticsearch

**Verify Elasticsearch is running:**

curl -X GET "localhost:9200/"

**3.4. Install Kibana**

sudo apt install kibana -y

**3.5. Configure Kibana**

Edit the Kibana configuration file:

sudo nano /etc/kibana/kibana.yml

**Set the following parameters:**

server.host: "0.0.0.0"

elasticsearch.hosts: ["http://localhost:9200"]

**Enable and start the Kibana service:**

sudo systemctl enable kibana

sudo systemctl start kibana

**Verify Kibana is running:**

curl -X GET "localhost:5601/"

**3.6. Install Fleet Server**

Fleet Server is part of the Elastic Agent. First, download and install Elastic Agent:

wget https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.x.x-linux-x86\_64.tar.gz

tar xzvf elastic-agent-8.x.x-linux-x86\_64.tar.gz

cd elastic-agent-8.x.x-linux-x86\_64

sudo ./elastic-agent install

**3.7. Configure Fleet Server**

Follow the instructions provided by the Fleet Server to enroll the agent:

sudo elastic-agent enroll -f <ENROLLMENT-URL> -s <SECRET>

**Make sure Fleet Server is running:**

sudo systemctl enable elastic-agent

sudo systemctl start elastic-agent

**Step 4: Install Cortex XSOAR**

**4.1. Download and Install Cortex XSOAR Alternative is TheHive**

Cortex XSOAR is typically installed as a virtual machine or in a container. Refer to the official Cortex XSOAR documentation for detailed installation instructions. You may use the official images provided by Palo Alto Networks or deploy using their installation script.

**4.2. Configure Cortex XSOAR**

1. Follow the installation guide provided by Palo Alto Networks.
2. Ensure that Cortex XSOAR can communicate with Elastic Stack for data ingestion and response actions.

**Step 5: Integrate Elastic Security with Cortex XSOAR**

**5.1. Configure Elastic Security Integration in Cortex XSOAR**

1. Log in to Cortex XSOAR.
2. Go to the **Settings** and navigate to **Integrations**.
3. Search for and configure the **Elastic Security** integration.
4. Provide the necessary connection details to integrate with your Elastic Stack.

**5.2. Create and Test Playbooks**

1. Create playbooks in Cortex XSOAR to automate response actions based on alerts from Elastic Security.
2. Test the integration by generating sample alerts in Elastic Security and ensuring that Cortex XSOAR responds appropriately.

**Step 6: Verify and Monitor**

1. **Verify Integration**: Ensure that Elastic Security alerts are being ingested and processed by Cortex XSOAR.
2. **Monitor Logs**: Check the logs of both Elastic Stack and Cortex XSOAR for any errors or issues.
3. **Regular Updates**: Keep both Elastic Stack and Cortex XSOAR updated to their latest versions for security and feature enhancements.
4. **Step 4: Install TheHive**

**4.1. Add TheHive APT Repository**

sudo apt install software-properties-common

sudo add-apt-repository ppa:thehive-project/ppa

sudo apt update

**4.2. Install TheHive**

sudo apt install thehive -y

**4.3. Configure TheHive**

Edit the TheHive configuration file:

sudo nano /etc/thehive/application.conf

**Set the following parameters:**

play.server.http.port = 9000

**Configure the database settings and other parameters as required.**

**Enable and start TheHive service:**

sudo systemctl enable thehive

sudo systemctl start thehive

**Verify TheHive is running by accessing it via the web browser:**

**http://<YOUR\_SERVER\_IP>:9000**

**Step 5: Integrate Elastic Security with TheHive**

**5.1. Configure Elastic Security Integration in TheHive**

1. Log in to TheHive.
2. Go to Administration > Connector and create a new connector.
3. Select Elastic Security as the type of connector and configure the necessary details to integrate with your Elastic Stack.

**5.2. Configure Elastic Security to Send Alerts to TheHive**

1. In Kibana, navigate to Security > Rules and create or modify a rule to send alerts to TheHive.
2. Configure the alerting mechanism, such as webhook or direct integration, to forward alerts from Elastic Security to TheHive.

**5.3. Create and Test Playbooks**

1. Create cases and alerts in TheHive based on incoming alerts from Elastic Security.
2. Test the integration by generating sample alerts in Elastic Security and ensuring that TheHive receives and processes them appropriately.

**Step 6: Verify and Monitor**

1. Verify Integration: Ensure that alerts from Elastic Security are correctly ingested and processed by TheHive.
2. Monitor Logs: Check the logs of both Elastic Stack and TheHive for any errors or issues.
3. Regular Updates: Keep both Elastic Stack and TheHive updated to their latest versions for security and feature enhancements.

**Conclusion**

You now have a setup of Elastic Security Stack with Fleet Server and TheHive. This setup will allow you to leverage Elastic Stack’s powerful data analysis and TheHive’s incident management capabilities. Fine-tune the configurations and integrate additional tools as needed for your environment. If you encounter any issues, consult the official documentation for Elastic Stack and TheHive or seek support from their respective communities.

**Note:** Cortex XSOAR is acquired by Palo Alto and is now part of its ecosystem but there is a community edition still available.

**Conclusion**

You now have a basic setup of Elastic Security Stack with Fleet Server and Cortex XSOAR. Make sure to fine-tune the configurations and integrate additional security tools as needed for your specific environment. If you encounter any issues, refer to the official documentation or seek support from Elastic and Cortex XSOAR communities.