

SIEM Lab Setup: AlienVault

October 12, 2020 By Raj Chandel

AlienVault OSSIM is an Open Source Security Information and Event Management (SIEM), which provides you with the feature-rich open source SIEM complete with event collection, normalization, and correlation. OSSIM is a unified platform which is providing the essential security capabilities like: –

- Asset discovery
- Vulnerability assessment
- Host Intrusion detection
- Network intrusion detection
- Behavioural monitoring
- SIEM event correlation
- Web UI Access
- Setup Network Monitoring
- Assets Discovery
- HIDS Deployment
- Log management
- OTX API integration

It is already loaded with the power of the AlienVault Open Threat Exchange (OTX). The open threat intelligence community provides community-generated threat intelligence and allows you to collaborate with them and also automates the process of updating your security infrastructure with threat data from any source.

AlienVault is very useful for monitoring your system security event or vulnerability and can help you to audit assessment security like PCI-DSS.



ALIEN VAULT OSSIM

So, without wasting more time or much theory let's begin the installation process. AlienVault OSSIM ISO can be easily found on the AlienVault OSSIM **product page**.

Table of Content

- Prerequisites
- Installation
- Setup log monitoring interface
- Web UI Access

Prerequisites

For the installation of AlienVault OSSIM, there are some minimum requirements as listed below.

- VMware or Virtual Box
- 2 NIC (Network interface card) E1000 compatible network cards

(You can have multiple NICs for Log Management or network monitoring)

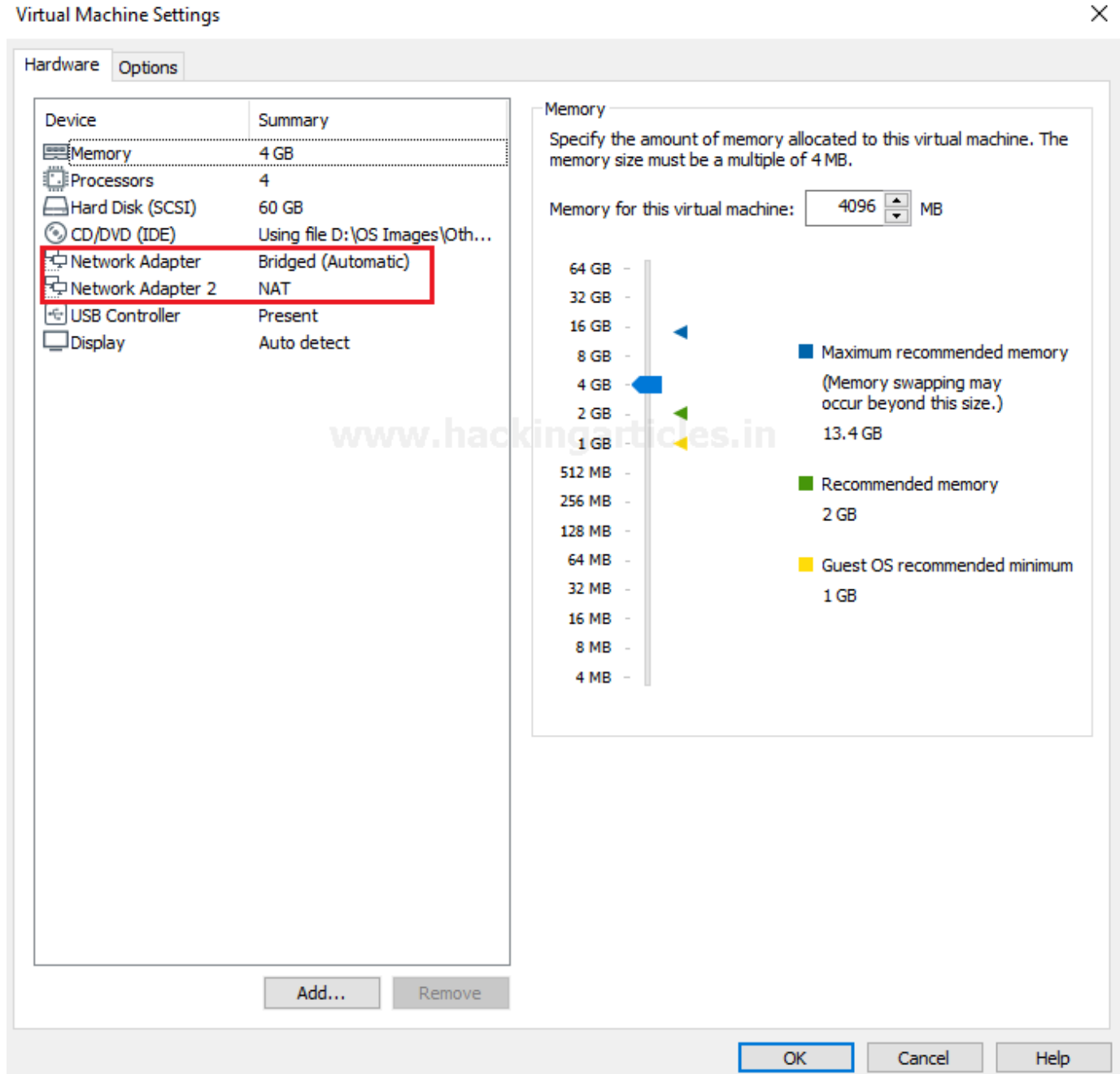
- 4 CPU cores
- 4-8GB RAM
- 60GB HDD

Installation

Once you've downloaded the AlienVault OSSIM ISO file, begin installation It on your virtual machine.

To install AlienVault OSSIM

- In your virtual machine, create a new VM instance using the AlienVault OSSIM ISO as the installation source.
- Complete the requirements of AlienVault as shown below.



Once you launch the new AlienVault instance, select Install AlienVault OSSIM 5.7.4 (64 Bit) and Hit Enter As shown below



ALIEN VAULT OSSIM

Install AlienVault OSSIM 5.7.4 (64 Bit)

Install AlienVault Sensor 5.7.4 (64 Bit)

Press [Tab] to edit options

#Install OSSIM

<http://www.alienvault.com>

The installation process takes you through a tour of setup options choose as per your requirements.

- Select language that you want to use



ALIEN VAULT OSSIM

Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

Chinese (Traditional)	-	中文(繁體)
Croatian	-	Hrvatski
Czech	-	Čeština
Danish	-	Dansk
Dutch	-	Nederlands
Dzongkha	-	ཇོ་མོ་གླང་མ་
English	-	English
Esperanto	-	Esperanto
Estonian	-	Eesti
Finnish	-	Suomi
French	-	Français
Galician	-	Galego
Georgian	-	ქართული
German	-	Deutsch

Screenshot

Go Back

Continue

Select your location



ALIEN VAULT OSSIM

Select your location

The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.

Country, territory or area:

India
Ireland
New Zealand
Nigeria
Philippines
Singapore
South Africa
United Kingdom
United States
Zambia
Zimbabwe
other

Screenshot

Go Back

Continue

Configure the network by Assigning

As we have 1 or more Network interface cards choose one for the primary network interface card for the management server. The IP address will be used to **access AlienVault OSSIM Web UI**. We are going to use eth0 for the management and the rest of the network is connected to eth1.



Configure the network

Your system has multiple network interfaces. Choose the one to use as the primary network interface during the installation. If possible, the first connected network interface found has been selected.

Primary network interface:

eth0: Intel Corporation 82545EM Gigabit Ethernet Controller (Copper)

eth1: Intel Corporation 82545EM Gigabit Ethernet Controller (Copper)

Screenshot

Go Back

Continue

Assign a Unique IP address to the server as shown below. If you don't know what to use here, consult your network administrator.



ALIEN VAULT OSSIM

Configure the network

The IP address is unique to your computer and may be:

- * four numbers separated by periods (IPv4);
- * blocks of hexadecimal characters separated by colons (IPv6).

You can also optionally append a CIDR netmask (such as "/24").

If you don't know what to use here, consult your network administrator.

IP address:

Screenshot

Go Back

Continue

Assign the Netmask of the assigned unique IP address



ALIEN VAULT OSSIM

Configure the network

The netmask is used to determine which machines are local to your network. Consult your network administrator if you do not know the value. The netmask should be entered as four numbers separated by periods.

Netmask:

Screenshot

Go Back

Continue

Provide the Gateway: That indicates the gateway router, as known as the default router. All traffic goes outside your LAN is sent through this router.



ALIEN VAULT OSSIM

Configure the network hackingarticles.in

The gateway is an IP address (four numbers separated by periods) that indicates the gateway router, also known as the default router. All traffic that goes outside your LAN (for instance, to the Internet) is sent through this router. In rare circumstances, you may have no router; in that case, you can leave this blank. If you don't know the proper answer to this question, consult your network administrator.

Gateway:

Screenshot

Go Back

Continue

Then the installation process takes you to set up a root password this will be used for the root login account in the AlienVault OSSIM login console.



ALIEN VAULT OSSIM

Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

Note that you will not be able to see the password as you type it.

Root password:

••••

Please enter the same root password again to verify that you have typed it correctly.

Re-enter password to verify:

••••

Screenshot

Go Back

Continue

Then on the next prompt set up your time zone as the final step.

And then it will install the base system. It takes quite long depends on your system speed as usually, it takes 10-15 to finish the installation till then go get served you with a coffee ☕.



ALIEN VAULT OSSIM

Install the base system

www.hackingarticles.in

Installing the base system

Preparing to configure linux-base (amd64)

You can now login to the AlienVault OSSIM console with the root user and enter the password that you designated in the setup process.

```
=====
===== http://www.alienvault.com =====
=====
==== Access the AlienVault web interface using the following URL: ====
===== https://192.168.1.70/ =====
=====

AlienVault USM 5.7.4 - x86_64 - tty1
alienvault login: _
```

Login with credentials of the root account.

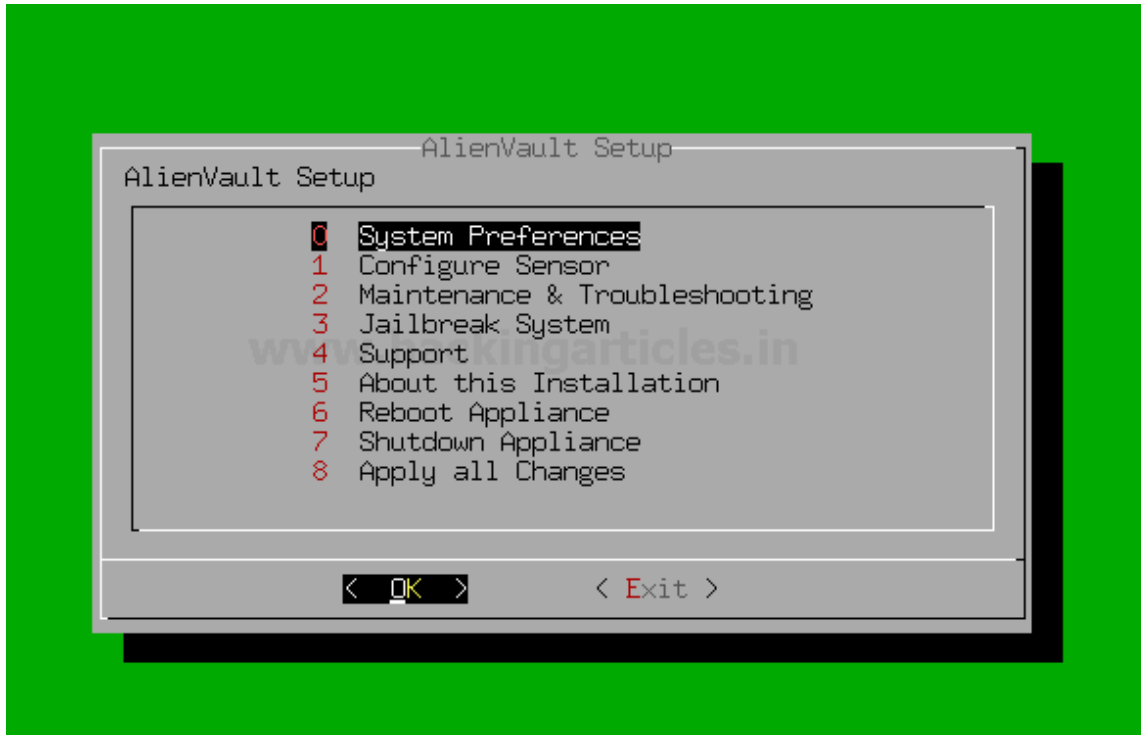
Setup log monitoring interface

After successfully login, you must configure the log management interface.

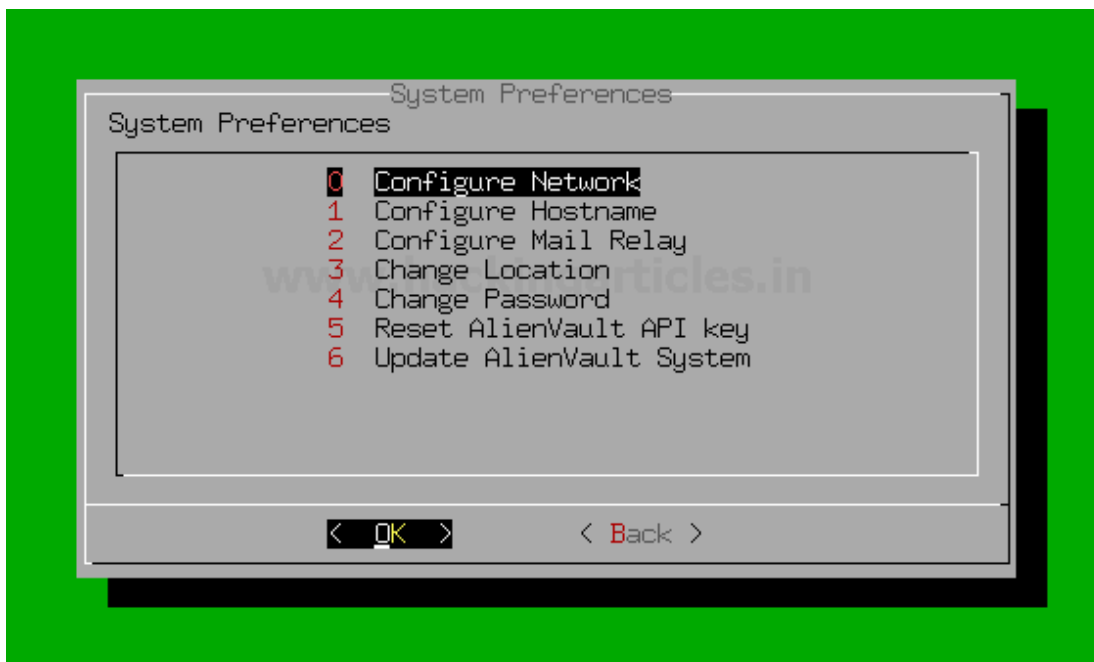
To set up a network interface for log management and scanning follow the steps as described below.

Click on **System Preferences > Configure Network > Setup Network Interface > eth1 > IP address > netmask.**

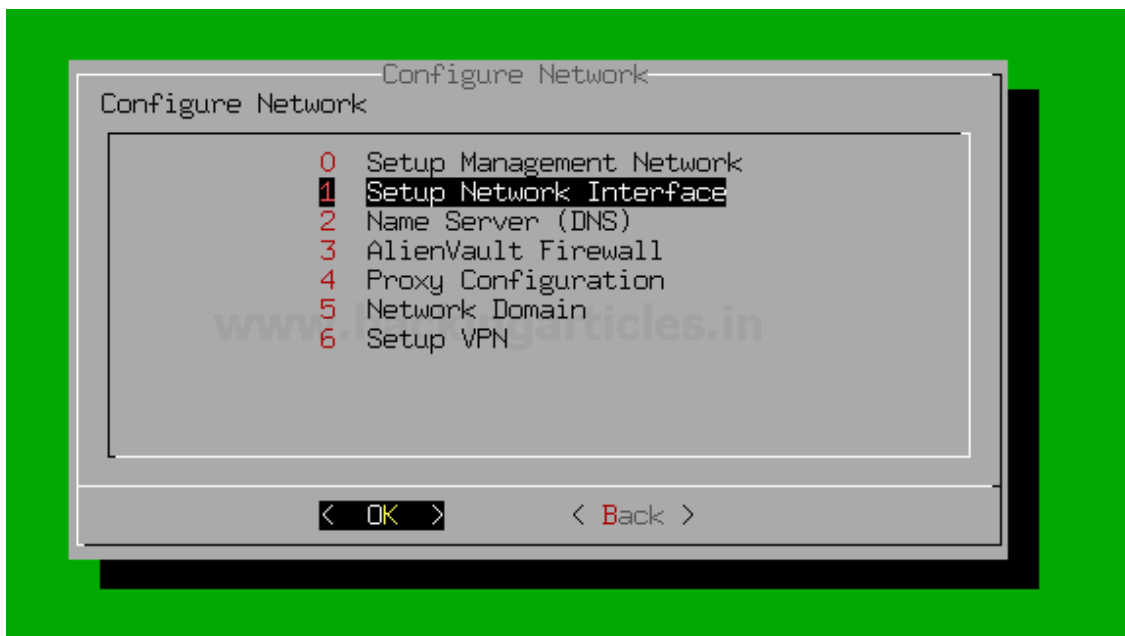
Go to System Preferences



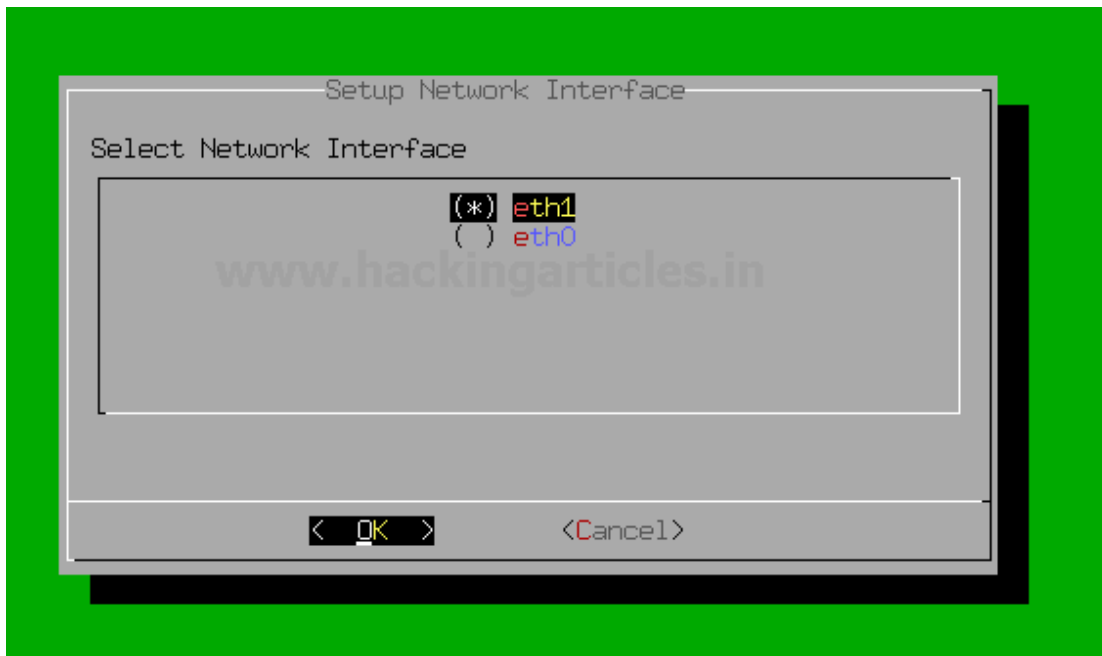
Select Configure Network



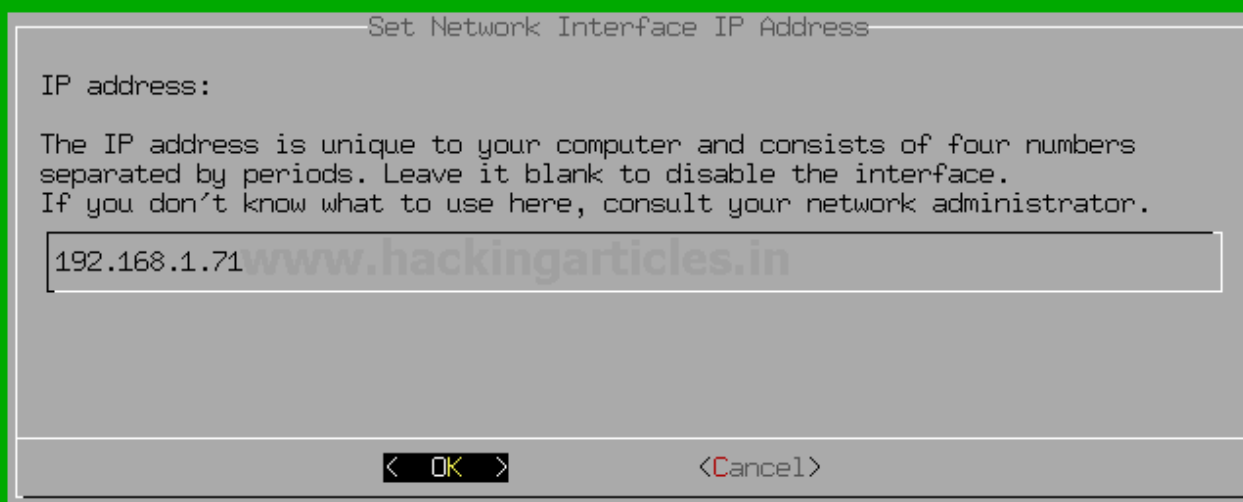
Select Network Interface



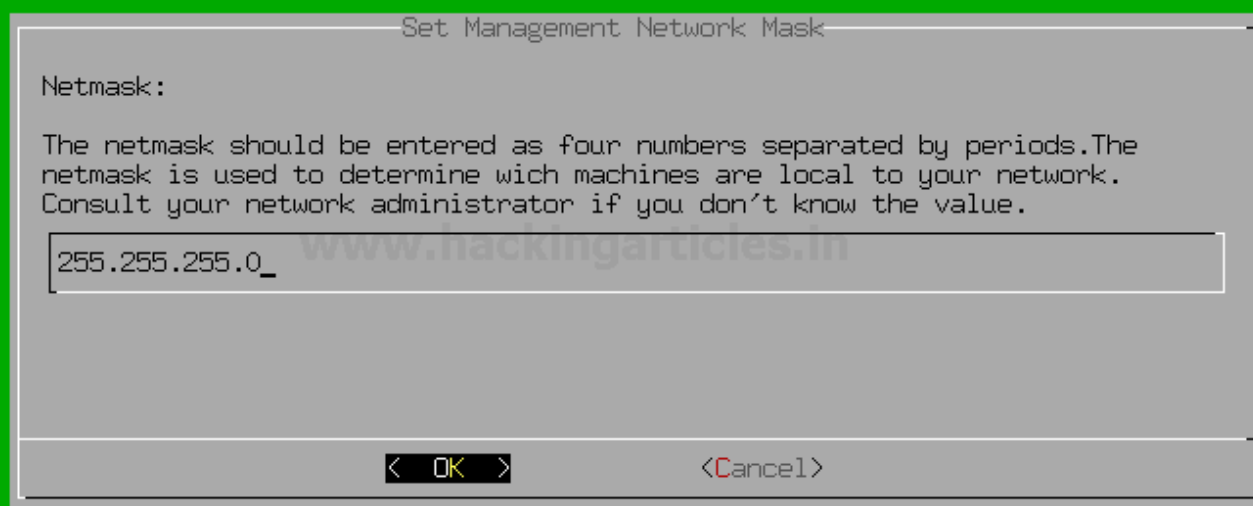
Select eth1 for log management and scanning.



Assign a unique IP address to set up a network management interface.



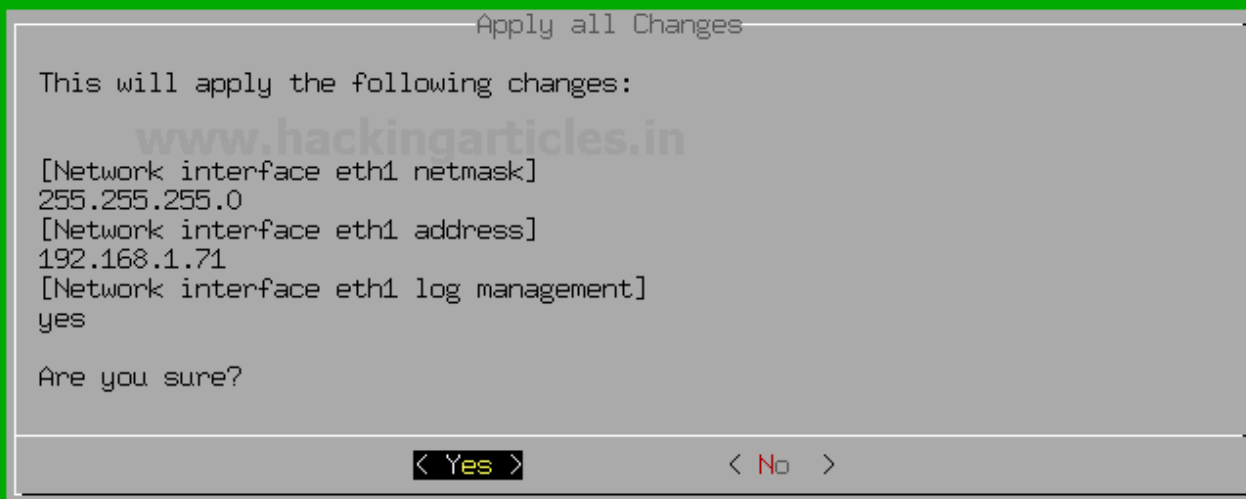
Assign the netmask of the designated IP address.



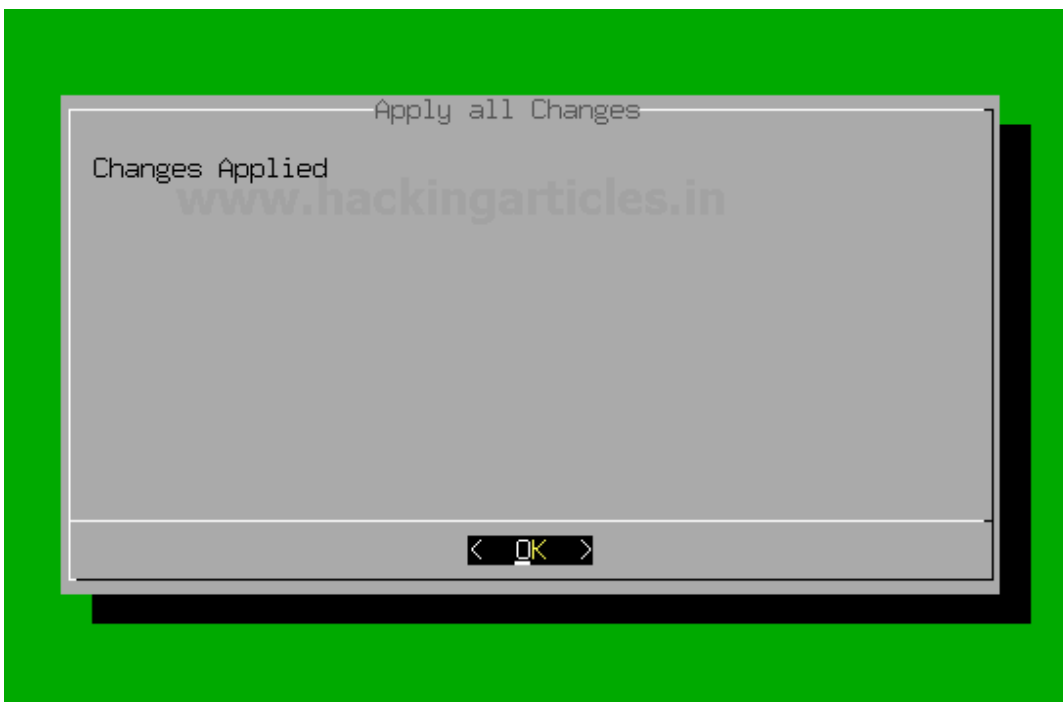
And then come back to the AlienVault setup by selecting back and back and then select Apply all Changes as shown below.



Verify the changes that you have done if correct then select yes.



Now you have successfully set up the Network interface for the log management !!!



Hmm ? !! you have successfully installed and set upped AlienVault in VMware.

Web UI Access

The AlienVault OSSIM Appliance Web User Interface provides Access to all the tools and capabilities that OSSIM Appliance makes available for managing the security of your organization's network and computer as well as all devices connected in a network.

From the OSSIM Appliance Web UI, you can view all essential information about network devices, user activity, monitor endpoints, applications, and network traffic in your environment.


As you monitor information coming in from the network devices or endpoints, you can go about defining and refining policies and correlation directives to fine-tune the behaviour of your OSSIM Appliance system to alert you of potential security issues and vulnerabilities.

By completing the installation process, you can access the Web UI and setup your **admin account**.

To access Web UI, open up your favourite browser and visit

`https://192.168.1.70`

← → ↻ ⚠ Not secure | 192.168.1.70/ossim/session/login.php

 ALIEN VAULT OSSIM

Welcome

Congratulations on choosing AlienVault as your Unified Security Management tool. Before using the administrator user account.

If you need more information about AlienVault, please visit AlienVault.com.

Administrator Account Creation

Create an account to access your AlienVault product.

** Asterisks indicate required fields*

FULL NAME *

USERNAME *

PASSWORD *
medium

CONFIRM PASSWORD *
medium

E-MAIL *

COMPANY NAME

LOCATION [View Map](#)

Further, the following windows appear after the completion of the administrator account.

Default login credentials of AlienVault OSSIM serve are

Username: – admin

Password: – that you designated in the previous step.

Use login credentials to access OSSIM Web UI.



ALIEN VAULT OSSIM

alienvault 192.168.1.70

USERNAME admin

PASSWORD

[Forgot Password?](#)

LOGIN

After successful login to OSSIM Web UI appear for further settings



Welcome to the AlienVault OSSIM Getting Started Wizard

You are about to use this wizard to configure the critical security capabilities provided by AlienVault OSSIM.

1 Monitor Network

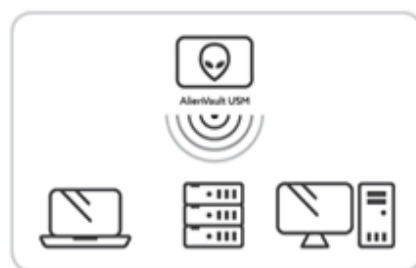
Configure interfaces and monitor network traffic for threats



2

Discover Assets

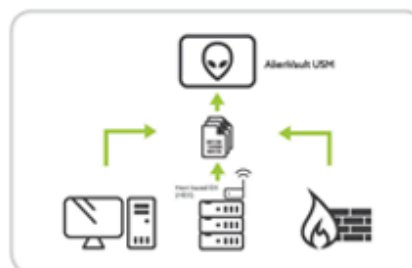
OSSIM will perform a discovery scan to detect assets



3

Collect Logs & Monitor Assets

Monitor asset logs and alarm on suspicious activity



Once done you'll be ready to use AlienVault OSSIM. Now, go forth!

[Skip AlienVault Wizard](#)

START

It shows you 3 options for the further configurations

1. Monitor network: – configure your network interfaces for the Management and Log collection and scanning.
2. Discover Assets: – Automatically discover your network devices, applications, endpoints in the network of your organization.
3. Collect Logs & monitor Assets: – Monitor Asset logs and alarm on suspicious activity.

Click on the start button for the further configuration of OSSIM Server

After clicking on the start button another window will prompt for the network configuration.

We configured network interfaces for the management and Log collection and management as shown below.

eth0: – Management

eth1: – Log Collection & Monitoring

← → ↻ ⚠ Not secure | 192.168.1.70/ossim/wizard/

ALIEN VAULT OSSIM

Welcome to AlienVault OSSIM

Let's Get Started

- 1 **NETWORK INTERFACES**
- 2 ASSET DISCOVERY
- 3 DEPLOY HIDS
- 4 LOG MANAGEMENT
- 5 JOIN OTX

Configure Network Interfaces

The network interfaces in AlienVault OSSIM can be configured to run Network Monitoring Scanning. Once you've configured the interfaces you'll need to ensure that the network is appropriately configured for each interface so that AlienVault OSSIM is either receiving data passed out to the desired network.

NIC	PURPOSE	IP ADDRESS	STATUS
eth0	Management	192.168.1.70	-
eth1	Log Collection & Scanning	192.168.1.71	-

Assets Discovery

In the 2nd step, OSSIM Server will automatically perform Assets Discovery in the network.

Types of ASSETS in the OSSIM Server are

- Windows

- Linux
- Network devices

WELCOME ADMIN | LOGOUT

Velcome to AlienVault OSSIM

Let's Get Started

- 1 NETWORK INTERFACES
- 2 ASSET DISCOVERY
- 3 DEPLOY HIDS
- 4 LOG MANAGEMENT
- 5 JOIN OTX

Scan & Add Assets

In order to begin monitoring your environment we must first find the assets in your network. There are three (3) ways you can add assets to monitor: you can scan your network using network ranges, import a CSV of assets in your network, or you can add assets manually.

Add Asset Manually

Hostname IP Select an Asset Type + ADD

SCAN NETWORKS **IMPORT FROM CSV**

Search

HOSTNAME	IP	TYPE
alienvault	192.168.1.70	Linux
Host-192-168-1-3	192.168.1.3	Windows
Host-192-168-1-8	192.168.1.8	Linux
Host-192-168-1-9	192.168.1.9	Linux

SHOWING 1 TO 4 OF 4 ASSETS

FIRST PREVIOUS 1 NEXT LAST

As you can see it automatically discover some of the Network Assets that are alive in the network.

HIDS Deployment

In the 3rd step, we will Deploy HIDS (Host intrusion detection system) on Windows, Linux devices to perform Rootkit Detection, File integrity, monitoring, and collection of Event logs.

Enter log in details of the discovered Assets such as username or password for the Deployment of HIDS as shown below.

Select the desired host from the list to provide login credentials

For the Deployment of **Windows Asset** select Windows

Let's Get Started

1 NETWORK INTERFACES

2 ASSET DISCOVERY

3 DEPLOY HIDS

4 LOG MANAGEMENT

5 JOIN OTX

SKIP ALIENVAULT WIZARD

Deploy HIDS to Servers

For these devices we recommend deploying HIDS in order to perform file integrity monitoring, intrusion detection and to collect event logs. For windows machines the HIDS agent will be installed locally, for Unix/Linux environments remote HIDS monitoring will be configured.

WINDOWS (1)

UNIX / LINUX (3)

Enter the domain admin account to install the HIDS agent. The username and password you provide will be permanently stored, it will be used to deploy an agent to the selected assets.

Username

raj

Password

...

Domain (Optional)

DEPLOY

Deploy to the following hosts:

Local_192_168_1_0_24

☒ Host-192-168-1-3

Same as well for the **Linux Asset** as shown below

2 ASSET DISCOVERY

3 DEPLOY HIDS

4 LOG MANAGEMENT

5 JOIN OTX

WINDOWS (1)

UNIX / LINUX (3)

Unix hosts will be remotely monitored. The username and password will be stored and used to periodically access the selected assets.

SSH Username

raj

SSH Password

...

DEPLOY

Deploy to the following hosts:

Local_192_168_1_0_24

☐ alienvault

☒ Host-192-168-1-9

☒ Host-192-168-1-8

Further, then click the Deploy button for the Deployment of HIDS then click on the continue button to start the process of deployment.

HIDS Deployment

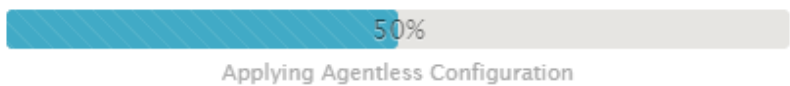
You are about to deploy 1 host, this may take more than a few minutes. Are you sure you would like to continue?



This process will take a few minutes as shown below.

HIDS Deployment

Deploying the HIDS agent to the selected devices.



Now the question is till the completion of the deployment process what you are going to do...?? ?

The answer is quite simple

Till then relax or chill with some music....

Log Management

Those devices that were selected as “network devices” on the asset discovery screen OSSIM will ask you to capture their logs so what we need to do is simply select their Logs Vendor/Model and version and then select Enable.

If you don’t have network devices, then don’t need to worry simply skip this step.

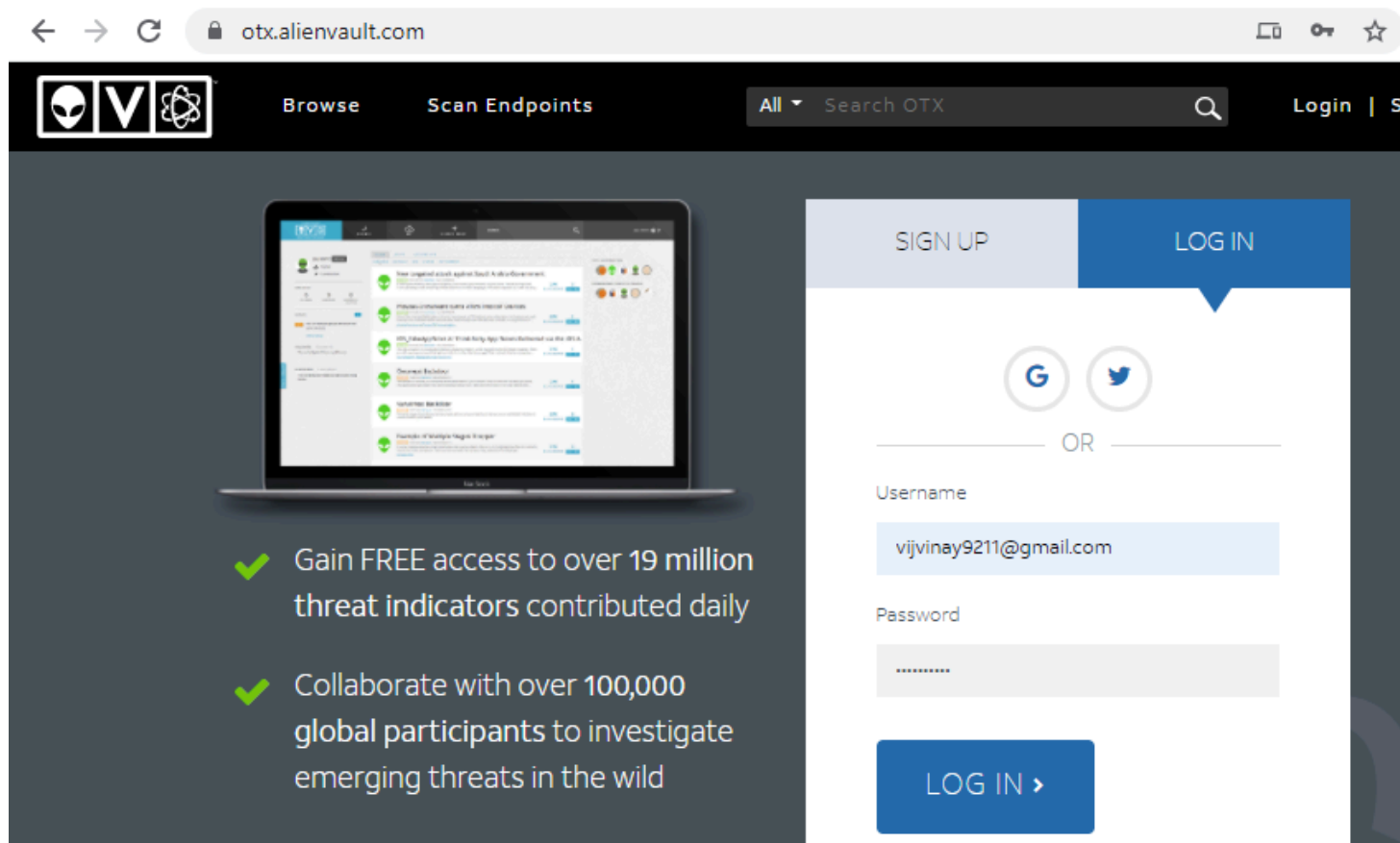
OTX API Integration

On the next window, it will ask for OTX (Open Threat Exchange) registration Token.

Registration is still free, and it is required for automatically indicating or updating the latest threat signatures.

For the registration of OTX visit on: –

<https://otx.alienvault.com/>



After creating account login to AlienVault OTX console and locate to the API integration and then copy OTX API Key as shown below

otx.alienvault.com/api

Dashboard Browse Scan Endpoints Create Pulse Submit Sample API Integration

All Search OTX

The OTX DirectConnect API allows you to easily synchronize the Threat Intelligence available in OTX to the tools you use to monitor your environment. Using the DirectConnect agents you can integrate with your infrastructure to detect threats targeting your environment. If there is no pre-built agent for the products you are using, leverage the DirectConnect SDK (available in Java and Python) to develop your own integration for the community.

Resources Docs TAXII Example API Uses

DirectConnect Agents

AlienVault OSSIM™ AlienVault USM™

DirectConnect API Usage

Your OTX Key: 48da0...
Using API: ✓
Client: otx ossimv5.8.5
Product:

Then after coming back to OSSIM Web UI and paste the copied “OTX key” in the place of “Enter token” as shown below

← → ↻ ⚠ Not secure | 192.168.1.70/ossim/wizard/

ALIEN VAULT OSSIM

Welcome to AlienVault OSSIM

on your network. Additionally, you can contribute to the community by sending anonymous threat data to OTX. [See what data is being sent to OTX.](#)

To get the community-powered threat intelligence from OTX into your installation, sign up for an OTX Account. Once your email address has been verified, you will receive an OTX key to connect.

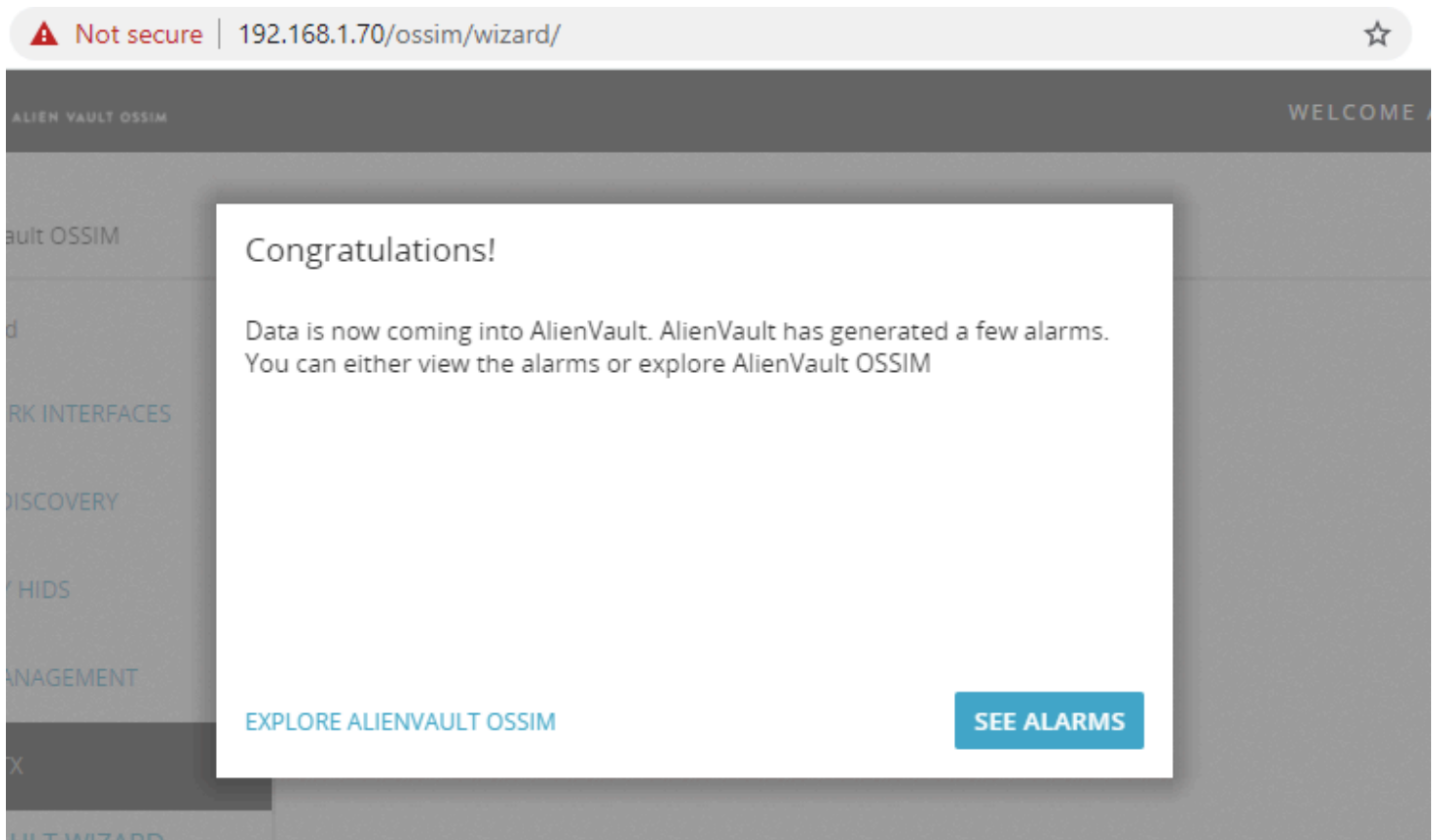
SIGN UP NOW

Enter your OTX key below to connect your account.

48da0b7f08cd5d79fe38207f41f81666193e8467af2f3bb2a7835974a68aca02

[SKIP ALIENVAULT WIZARD](#) [BACK](#)

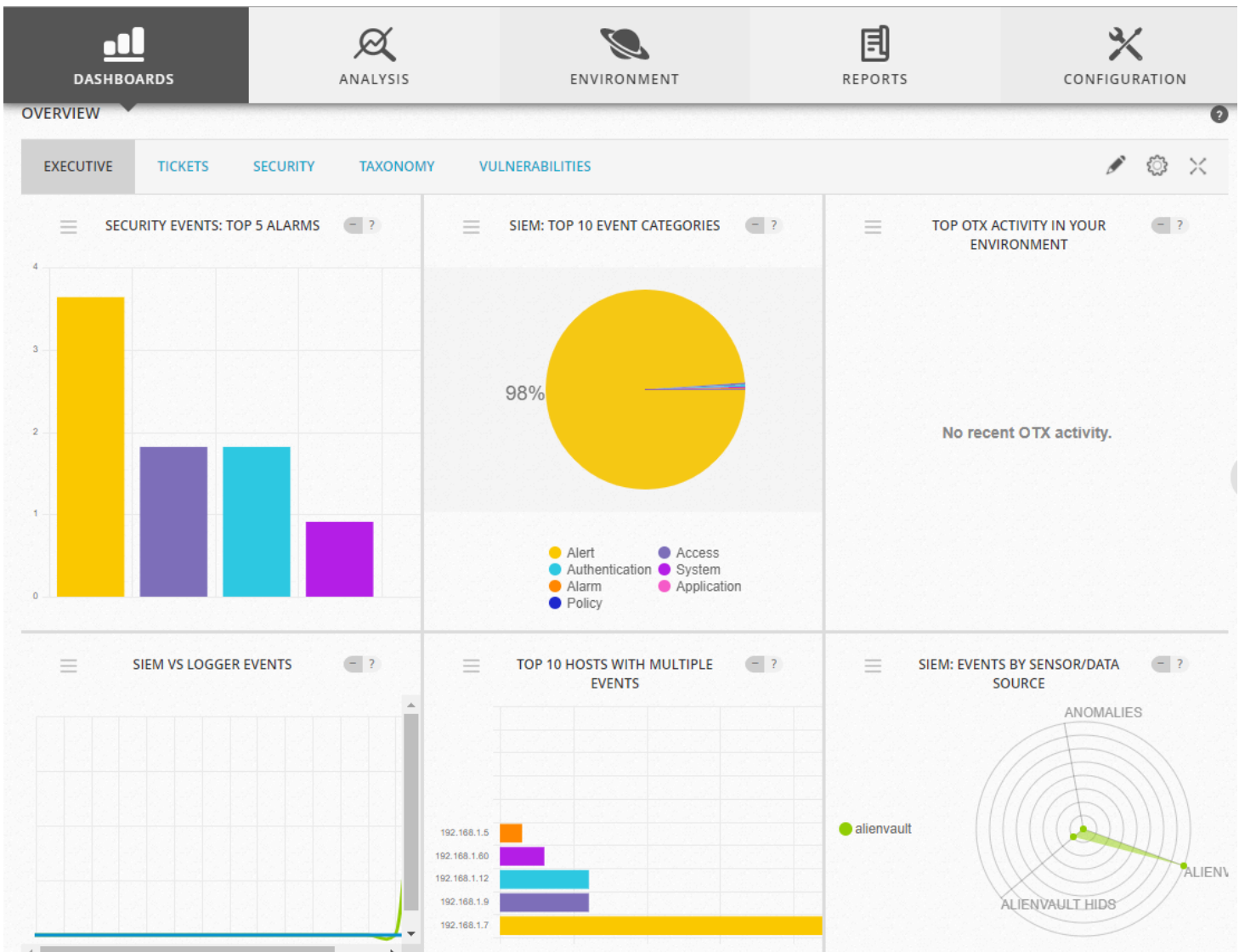
And then click “**Finish**” or “Skip” to bypass this step and then Finish configuration wizard



Congratulations !!! you have successfully configured You AlienVault Web UI ?

As we can we see it generated some Alarms we can explore them by Selecting Explore AlienVault OSSIM

Let's browse through OSSIM Dashboard.



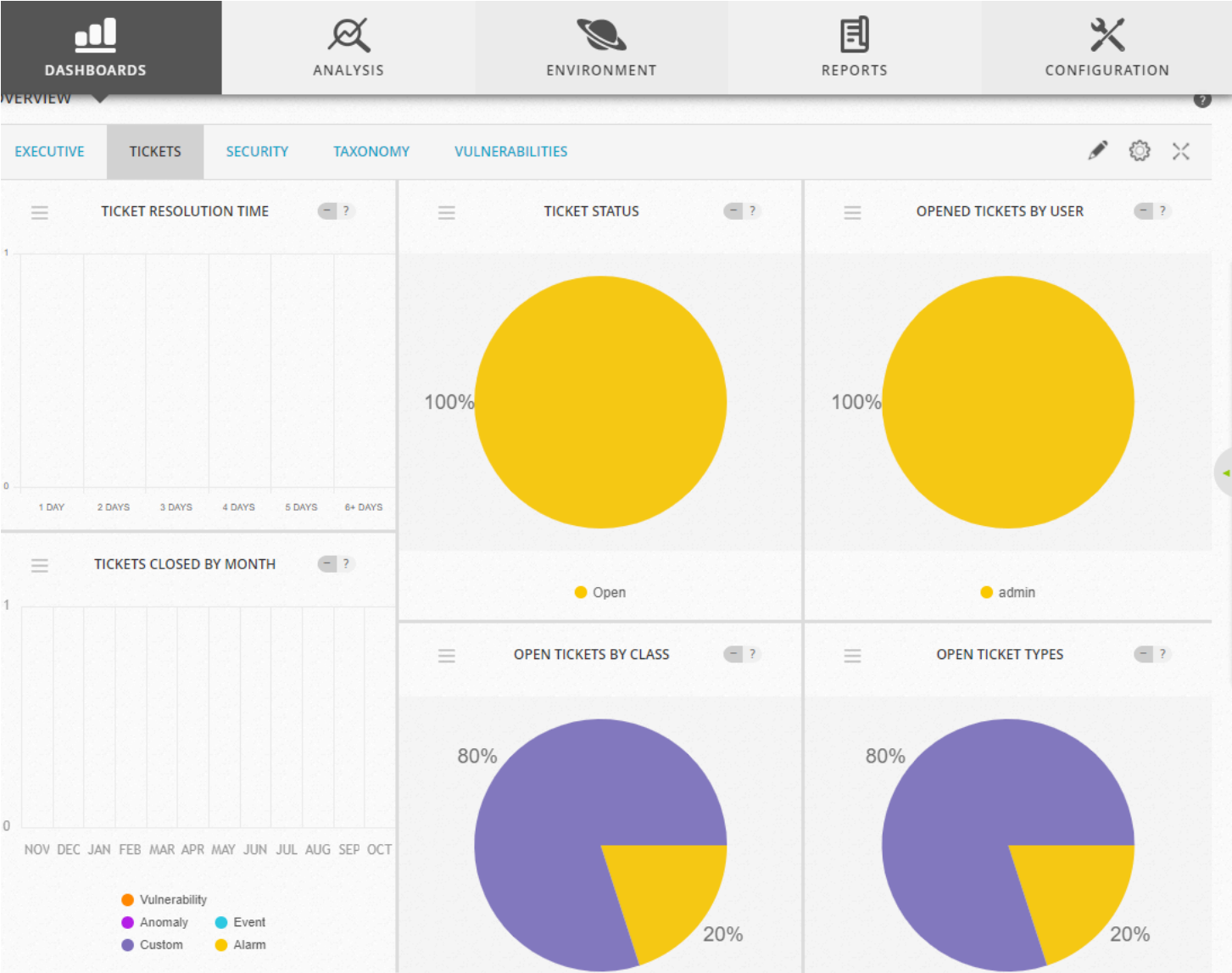
By default, the Web UI displays a collection of high-level graphs and charts summarizing the activity of your network.

From this main Dashboard, you can choose different menu options or click other selectable links and buttons.

Primary menu — Provides access to the main functions or operations of USM Appliance. These include:

- **Dashboards** — display of all network security charts, tables, and graphs; deployment status and global of the USM Appliance system, network, and devices; and OTX threat and pulse visualizations.
- **Analysis** — Display providing search, sorting, filtered selection, and display of Alarms, Security Events (SIEM), Raw Logs, and Tickets.
- **Environment** — Provides display and management of Assets & Groups, Vulnerabilities, NetFlow data, Traffic Capture, Availability, and Detection.
- **Reports** — Provides display and management of various built-in and custom reports selectable by categories such as alarms, assets, compliance, raw logs, security operations, tickets, and user activities.
- **Configuration** — Provides options to view and manage deployed OSSIM Appliance components; Administration options let you manage users, system configuration, and backup and restore settings.

Secondary menu (or submenu) — For each primary menu selection, there are typically additional secondary or submenu options specific to a particular topic that are displayed when you click the primary selection, for example, **Dashboard > overview > Tickets**.



Hold tight! this is not enough.....

Have patience ?