Alien Vault Open Source SIEM Installation

OSSIM is an open source security information and event management system, integrating a selection of tools designed to aid network administrators in computer security, intrusion detection and prevention.

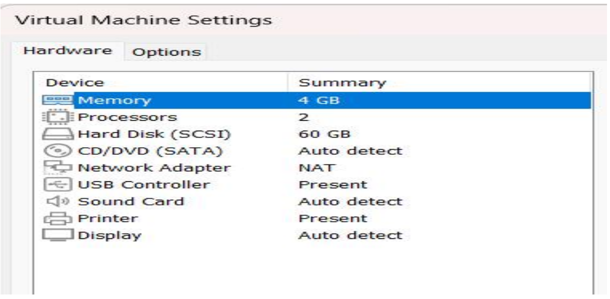
Please download the latest ISO image from the following link.

https://cdn-cybersecurity.att.com/downloads/AlienVault_OSSIM_64bits.iso

For an installation of AlienVault OSSIM, the minimum system requirements are as follows

2 CPU cores
4-8 GB RAM
50 GB HDD
E1000 compatible network cards

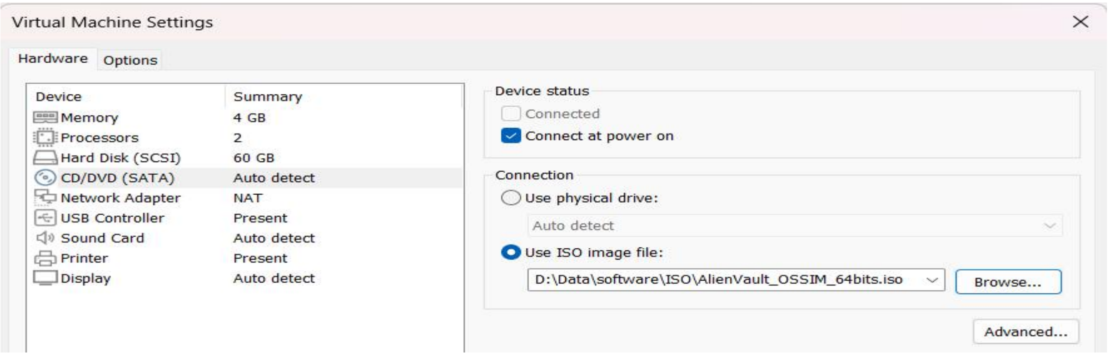
1. Create a Virtual machine with 2 CPU cores, 4 GB RAM, 60 GB HDD(Stored a s a single disk) and a network card in NAT mode as shown below. Select Ubuntu 64 bit in the OS.



Virtual Machine Settings

Device	Summary
Memory	4 GB
Processors	2
Hard Disk (SCSI)	60 GB
CD/DVD (SATA)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

2. Now in the above settings click CD/DVD. Click Use ISO Image file option. Click Browse button and select the path where you downloaded your Alien Vault OSSIM ISO image file.



Virtual Machine Settings

Device	Summary
Memory	4 GB
Processors	2
Hard Disk (SCSI)	60 GB
CD/DVD (SATA)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

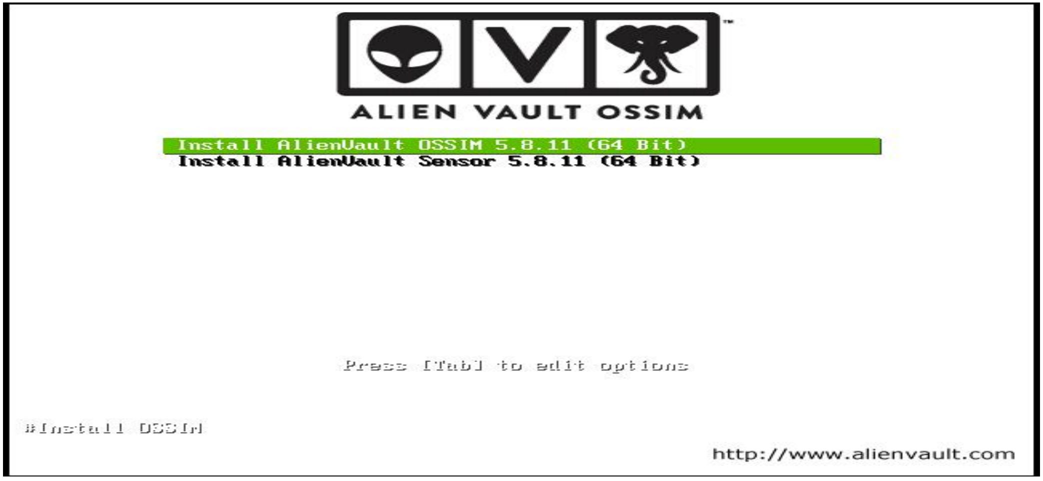
Device status
□ Connected
☑ Connect at power on

Connection
○ Use physical drive:
Auto detect
● Use ISO image file:
D:\Data\software\ISO\AlienVault_OSSIM_64bits.iso

Click OK

3. Start the VM to boot from the ISO.

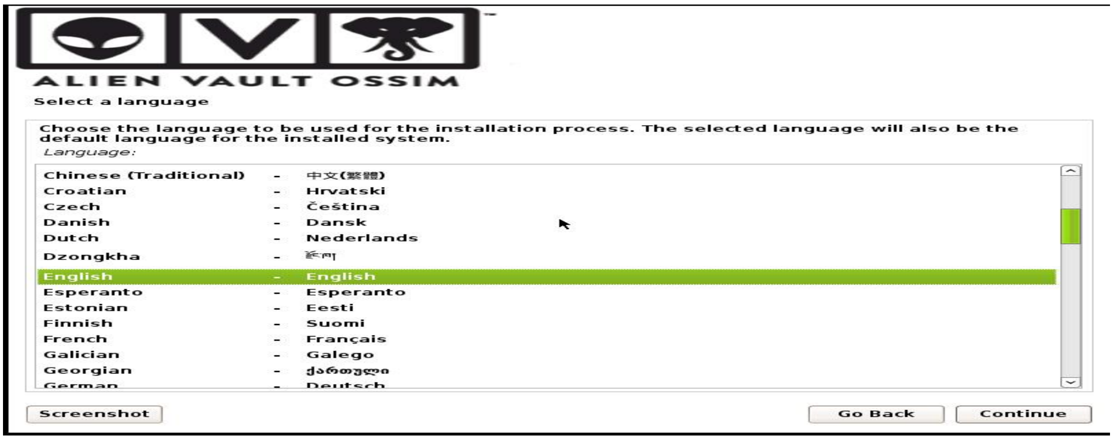
4. Once the machine starts, following page is displayed.



```
Install AlienVault OSSIM 5.8.11 (64 Bit)
Install AlienVault Sensor 5.8.11 (64 Bit)

Press [Tab] to edit options

#Install OSSIM
http://www.alienvault.com
```

Keep the first option selected to install AlienVault OSSIM. Press Enter.

5. On the next screen, keep the language as English. Press Enter to continue.



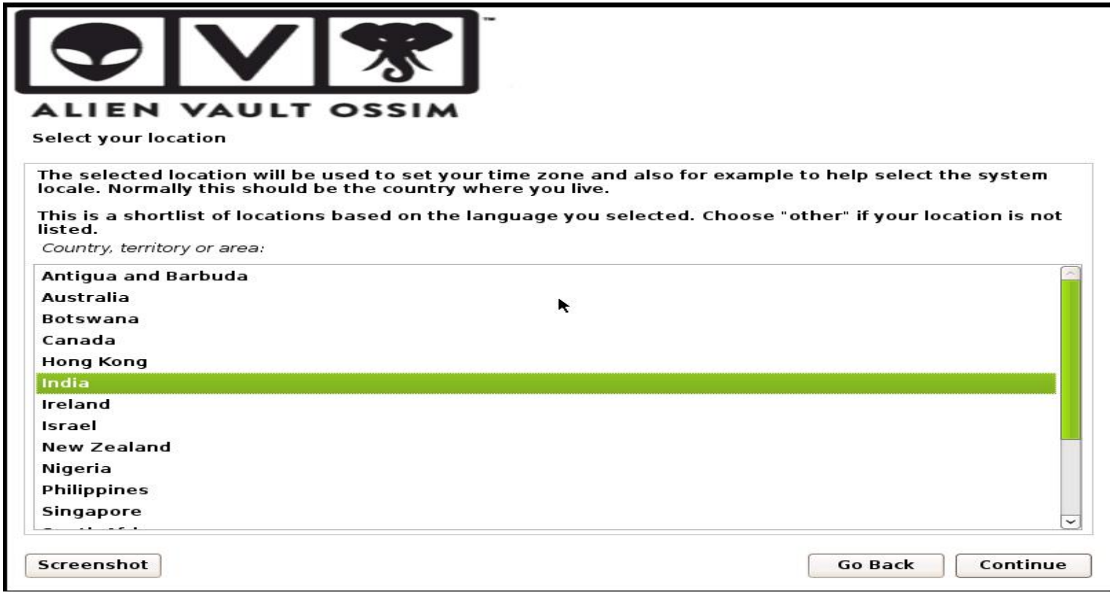
Select a language

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                -   རྫོང་ཁ
English                 -   English
Esperanto               -   Esperanto
Estonian                -   Eesti
Finnish                 -   Suomi
French                  -   Français
Galician                -   Galego
Georgian                -   ქართული
German                  -   Deutsch
```

6. On the following screen that is displayed, select your location.



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.

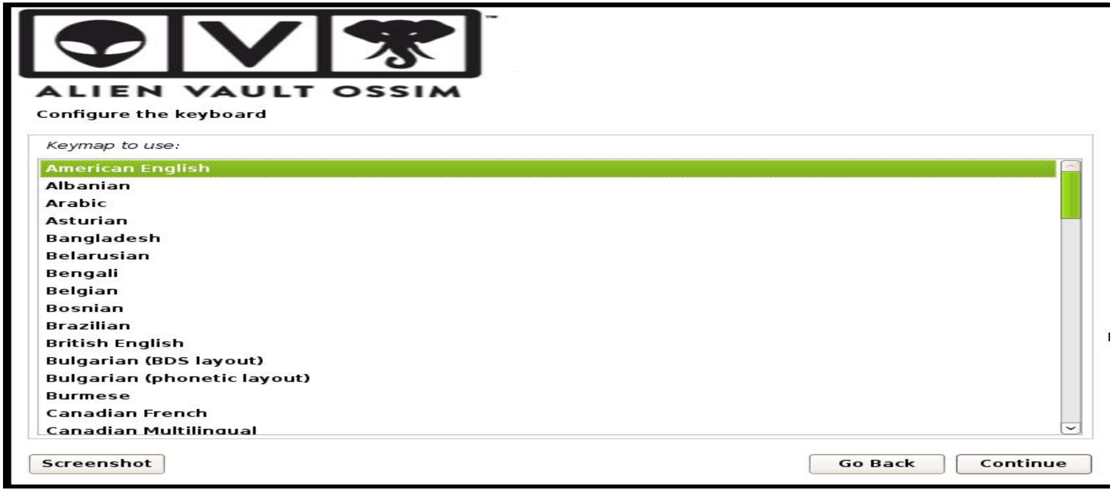
This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.

Country, territory or area:

```
Antigua and Barbuda
Australia
Botswana
Canada
Hong Kong
India
Ireland
Israel
New Zealand
Nigeria
Philippines
Singapore
```

Press Enter to continue.

7. On the following screen keep default keyboard map.



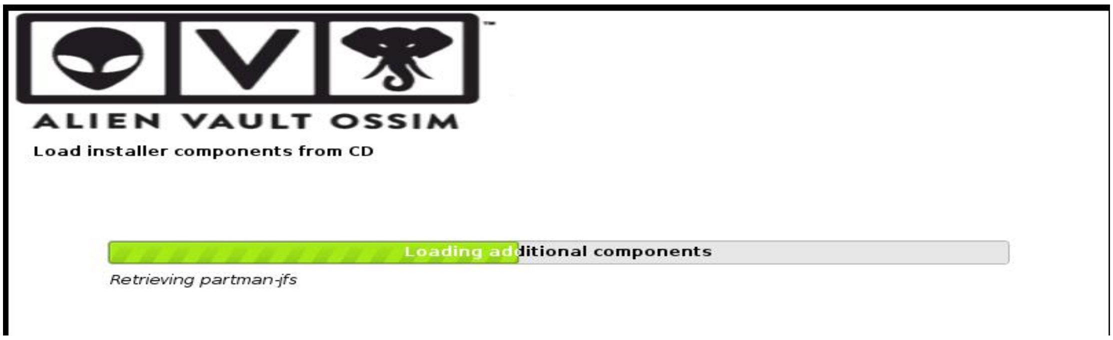
Configure the keyboard

Keymap to use:

American English
Albanian
Arabic
Asturian
Bangladesh
Belarusian
Bengali
Belgian
Bosnian
Brazilian
British English
Bulgarian (BDS layout)
Bulgarian (phonetic layout)
Burmese
Canadian French
Canadian Multilingual

Press Enter to continue.

8. It will load the installer components from the CD s shown below.

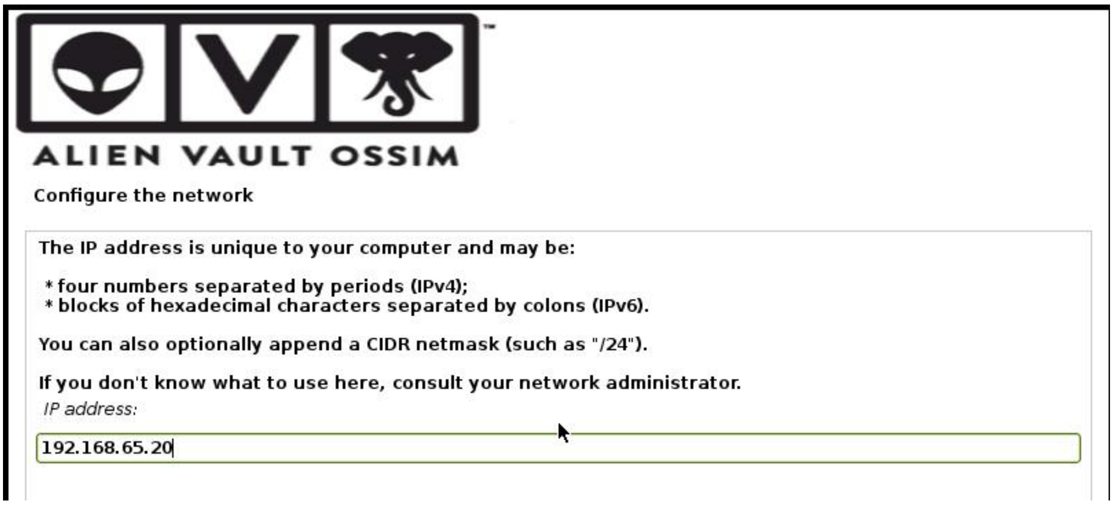


Load installer components from CD

Loading additional components

Retrieving partman-jfs

9. On the following screen type an IP address for this OSSIM machine. For this lab purpose make sure you provide an IP address in the range of your VMNet 8 adapter of VMWare player.



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).

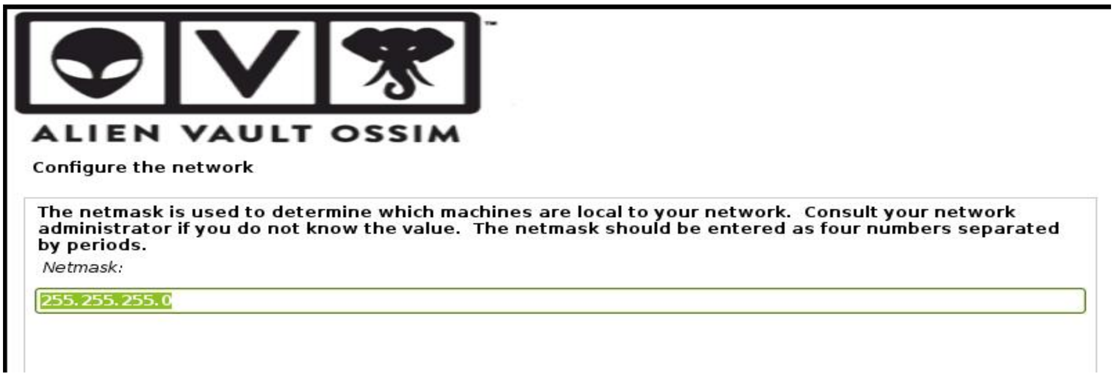
You can also optionally append a CIDR netmask (such as "/24").

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

IP address: 192.168.65.20

Press Enter to continue.

10. On the next screen keep the default subnet mask or change it to mach your network subnet mask.



ALIEN VAULT OSSIM

Configure the network

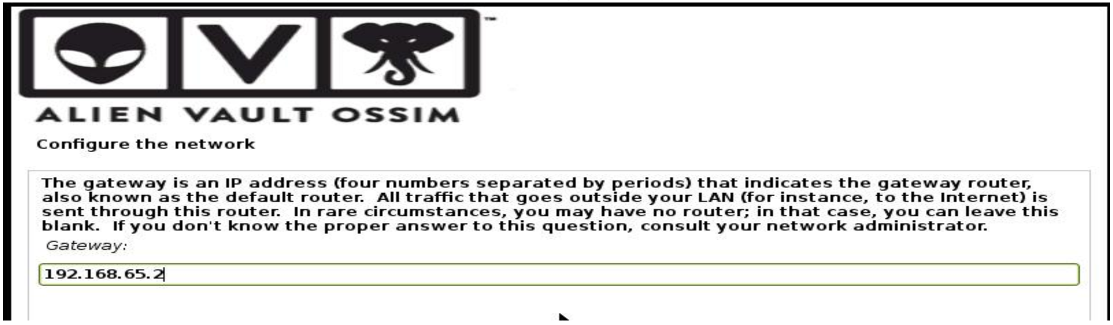
The netmask is used to determine which machines are local to your network. Consult your network administrator if you do not know the value. The netmask should be entered as four numbers separated by periods.

Netmask:

255.255.255.0

Press Enter to continue.

11. On the next screen provide the default gateway as shown below.



ALIEN VAULT OSSIM

Configure the network

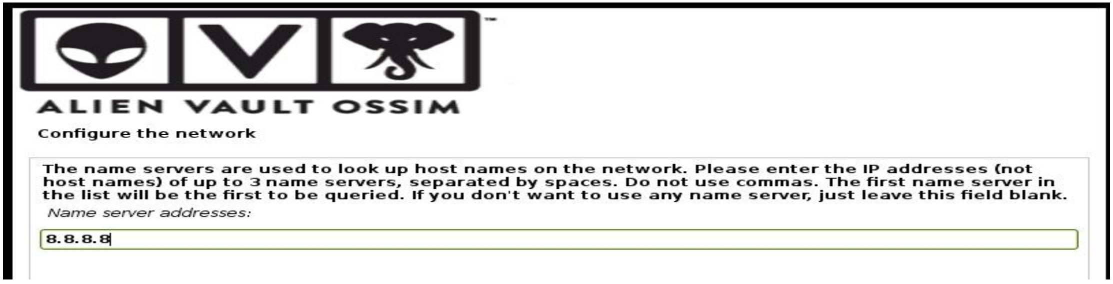
The gateway is an IP address (four numbers separated by periods) that indicates the gateway router, also known as the default router. All traffic that goes outside your LAN (for instance, to the Internet) is sent through this router. In rare circumstances, you may have no router; in that case, you can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

Gateway:

192.168.65.2

Press Enter to continue.

12. On the next screen provide a DNS Server.



ALIEN VAULT OSSIM

Configure the network

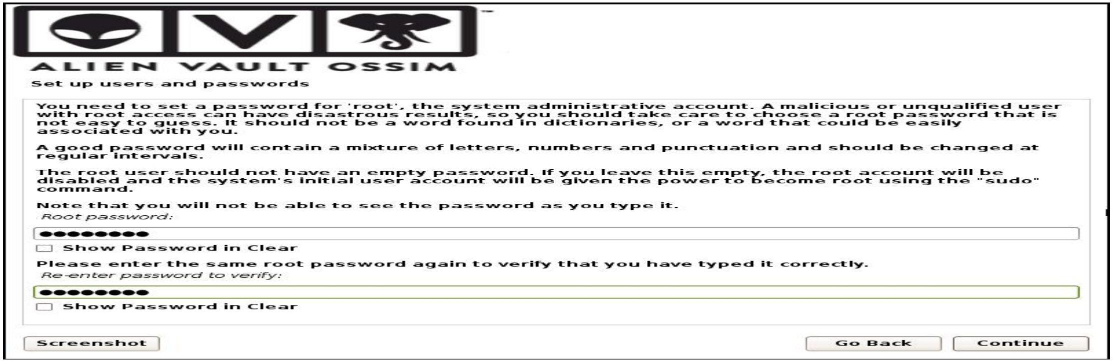
The name servers are used to look up host names on the network. Please enter the IP addresses (not host names) of up to 3 name servers, separated by spaces. Do not use commas. The first name server in the list will be the first to be queried. If you don't want to use any name server, just leave this field blank.

Name server addresses:

8.8.8.8

Press Enter to continue.

13. On the next screen provide a password for the root user.



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:

●●●●●●●●●

□ Show Password in Clear

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

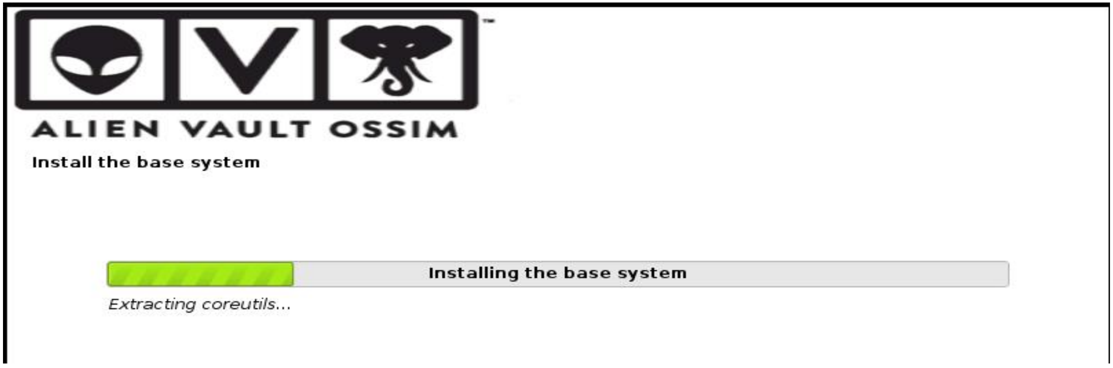
Re-enter password to verify:

●●●●●●●●●

□ Show Password in Clear

Press Enter to continue.

14. Now it will start installing the base system as shown below.



ALIEN VAULT OSSIM

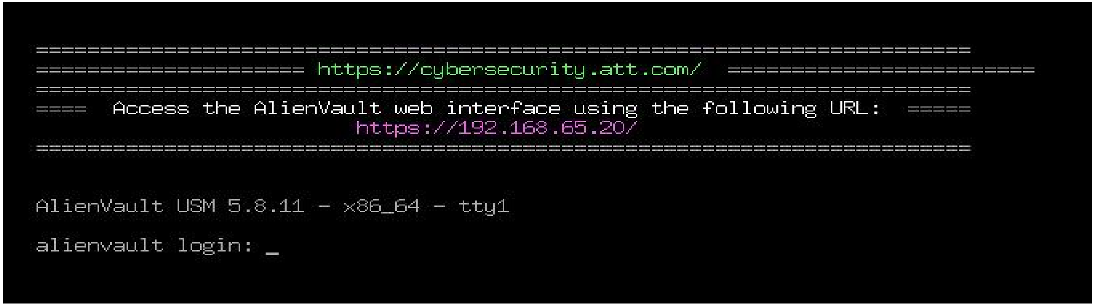
Install the base system

Installing the base system

Extracting coreutils...

It takes lot of time to complete this installation.

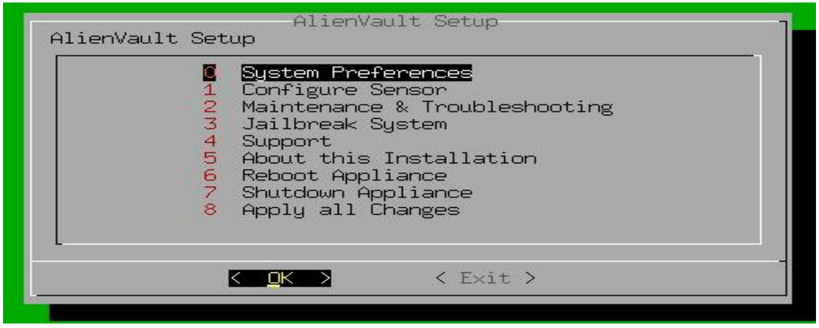
15. Once the installation is over, following sreen appears.



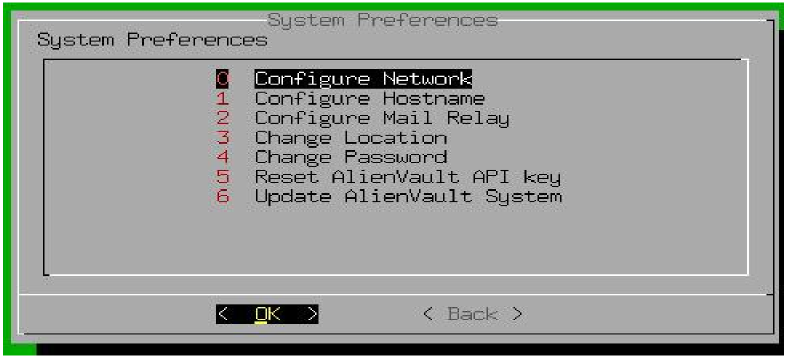
```
========================================================================
===================== https://cybersecurity.att.com/  ========================
========================================================================
====  Access the AlienVault web interface using the following URL:  =====
                        https://192.168.65.20/
========================================================================


AlienVault USM 5.8.11 - x86_64 - tty1

alienvault login: _
```

Provide username as **root** and password given during installation.

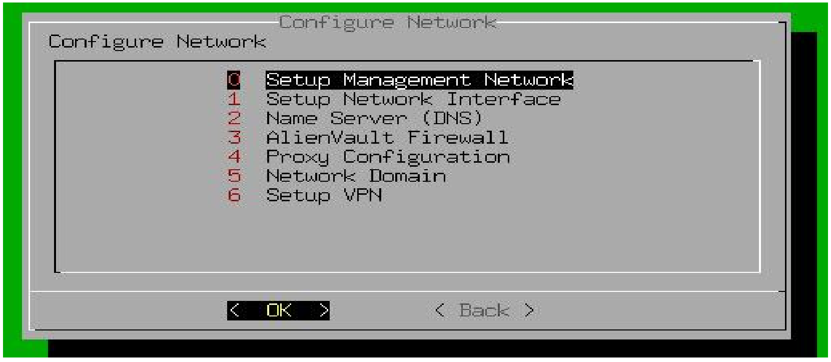
16. It takes some time to display the following screen.



17. Press Enter to go into the System Preference menu. Following options are displayed.



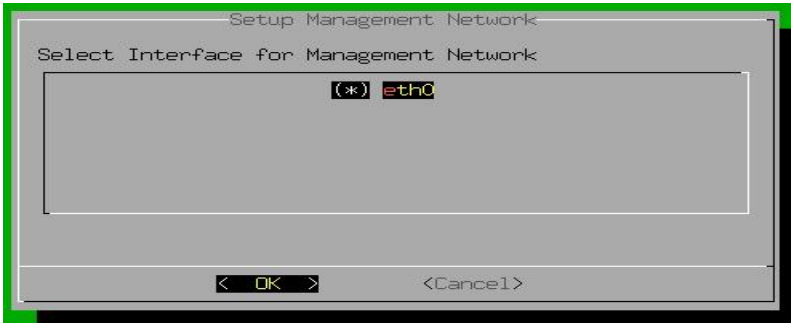
18. Press Enter to enter into Configure Network options. Following options are displayed.



```
Configure Network
Configure Network

        0  Setup Management Network
        1  Setup Network Interface
        2  Name Server (DNS)
        3  AlienVault Firewall
        4  Proxy Configuration
        5  Network Domain
        6  Setup VPN

        <  OK  >          < Back >
```

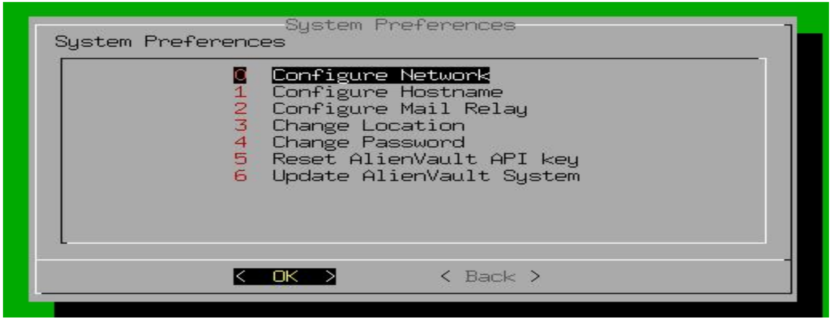
Press Enter to enter into Setup Management Nework option.

19. Make sure the interface is selected (* is displayed).



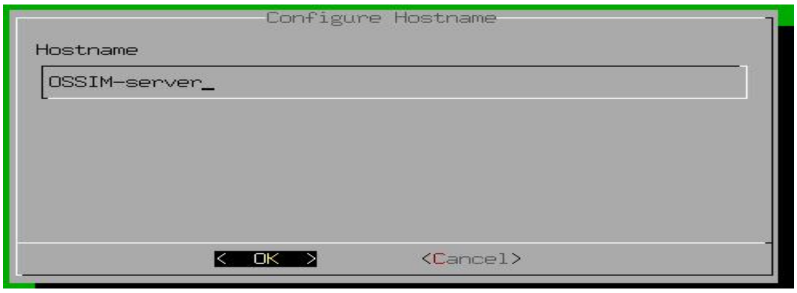
```
Setup Management Network
Select Interface for Management Network

        (*) eth0

        <  OK  >          <Cancel>
```

20. If you press Enter, it will ask you to set IP address, Subnet mask and Default gateway. However as it is already set during installation, press cancel. Press Cancel till you reac to following screen.



```
System Preferences
System Preferences

        0  Configure Network
        1  Configure Hostname
        2  Configure Mail Relay
        3  Change Location
        4  Change Password
        5  Reset AlienVault API key
        6  Update AlienVault System

        <  OK  >          < Back >
```

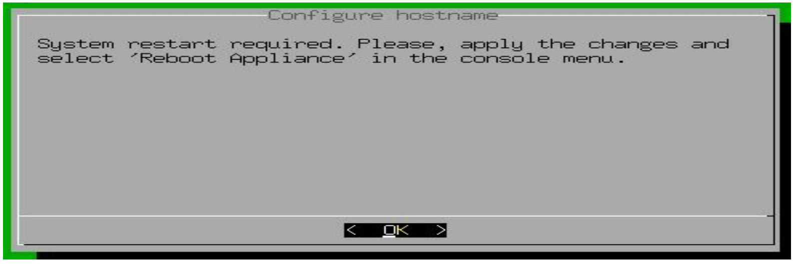
21. Select **Configure Hostname** and press Enter.



```
Configure Hostname
Hostname
OSSIM-server_

        <  OK  >          <Cancel>
```

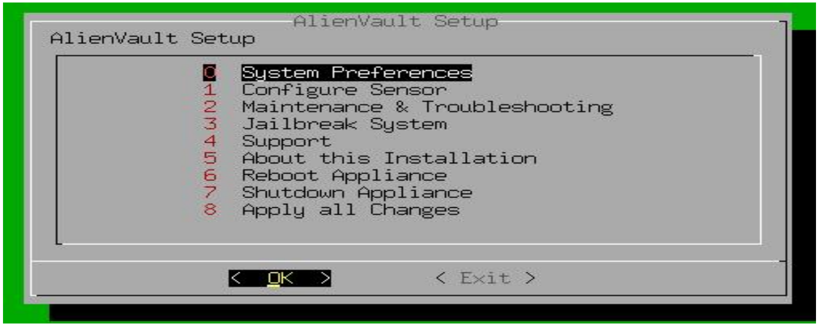
Type a Hostname for your OSSIM server and press Enter.

22. Following screen is displayed.



```
Configure hostname

System restart required. Please, apply the changes and
select 'Reboot Appliance' in the console menu.

                    < OK >
```

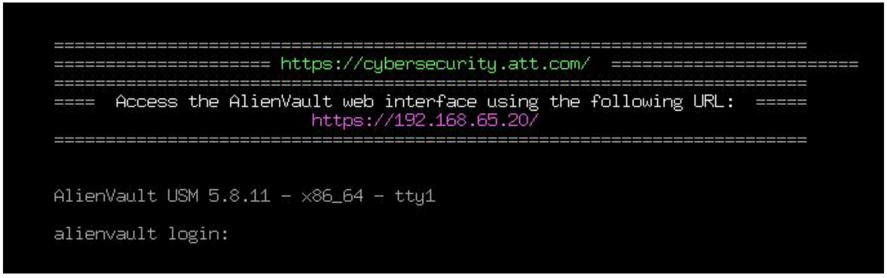
Press Enter. Press back to come to the following screen.



```
                 AlienVault Setup
AlienVault Setup

          0  System Preferences
          1  Configure Sensor
          2  Maintenance & Troubleshooting
          3  Jailbreak System
          4  Support
          5  About this Installation
          6  Reboot Appliance
          7  Shutdown Appliance
          8  Apply all Changes

       < OK >            < Exit >
```

23. Select **Reboot appliance** option and press Enter. Press Yes.

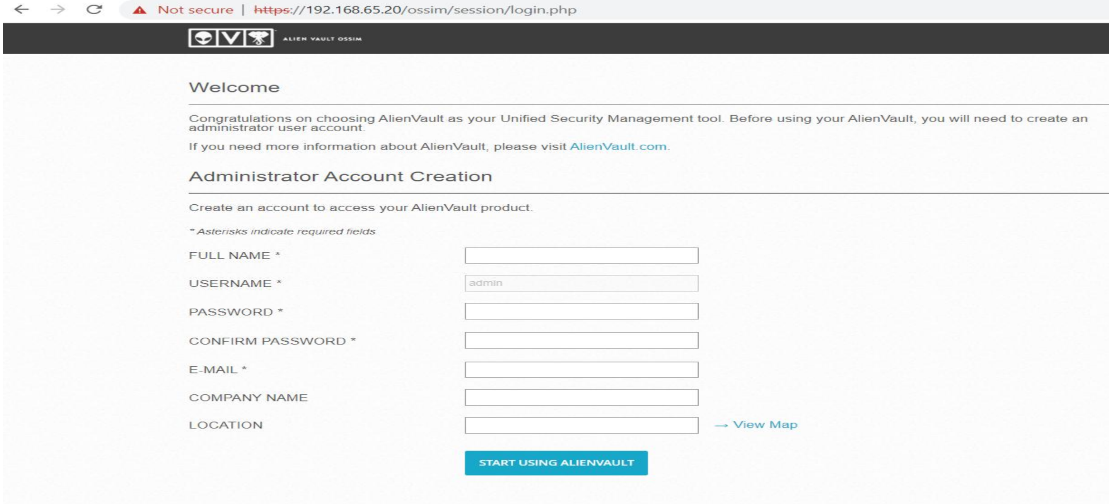
Once the system reboots, following screen is displayed.



```
=========================================================================
==================== https://cybersecurity.att.com/ =======================
=========================================================================
====  Access the AlienVault web interface using the following URL:  =====
                        https://192.168.65.20/
=========================================================================


AlienVault USM 5.8.11 - x86_64 - tty1

alienvault login:
```

Further configuration is using the web console. Thus open the browser on your main Windows machine or any other VM and type the URL shown in the above screen.

24. Once you open the link, following page is displayed in the browser.



Not secure | ~~https~~://192.168.65.20/ossim/session/login.php

Welcome

Congratulations on choosing AlienVault as your Unified Security Management tool. Before using your AlienVault, you will need to create an administrator user account.

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

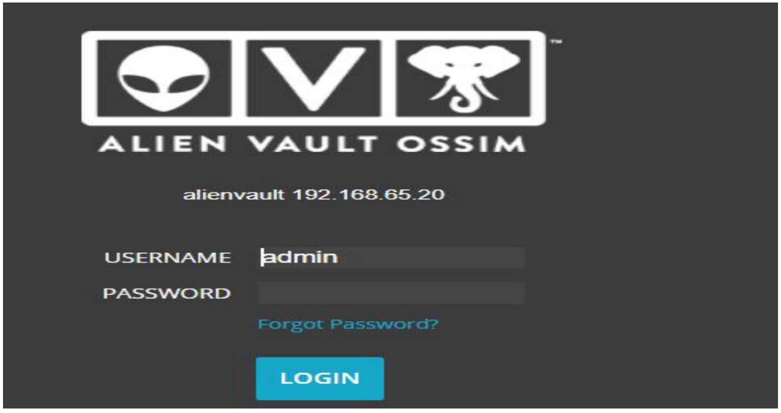
Administrator Account Creation

Create an account to access your AlienVault product.

** Asterisks indicate required fields*

FULL NAME *	
USERNAME *	admin
PASSWORD *	
CONFIRM PASSWORD *	
E-MAIL *	
COMPANY NAME	
LOCATION	→ View Map

Provide details. Click Start using AlienVault. It will create an admin user. Following screen is displayed.



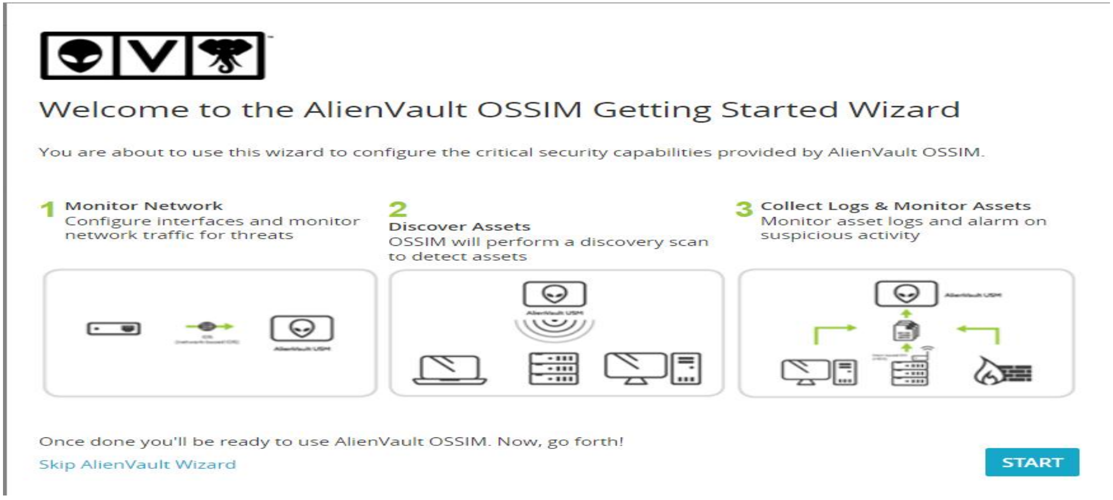
ALIEN VAULT OSSIM

alienvault 192.168.65.20

USERNAME admin

PASSWORD

Once you login, following screen is displayed.



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

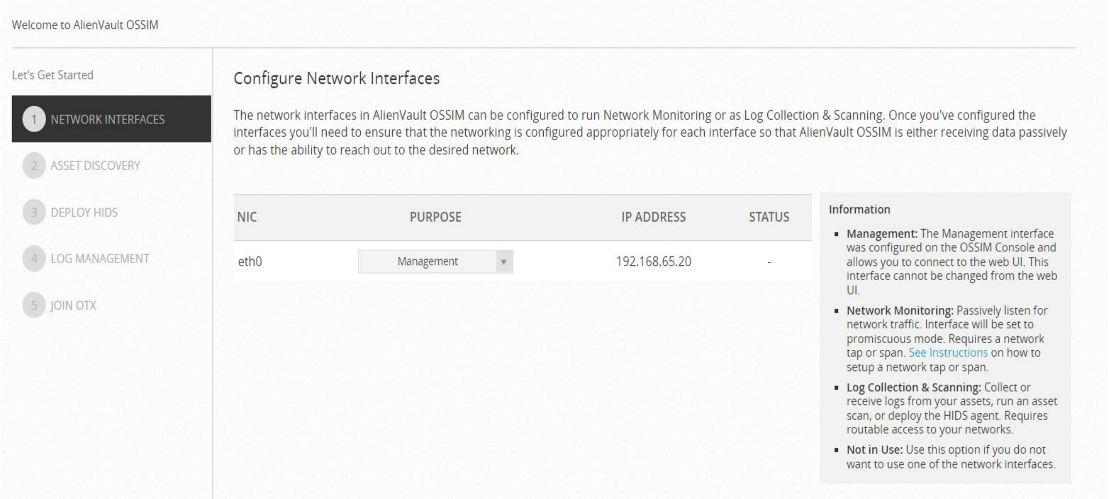
2 Discover Assets
OSSIM will perform a discovery scan to detect assets

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!

Click START.

Following screen is displayed.



Welcome to AlienVault OSSIM

Configure Network Interfaces

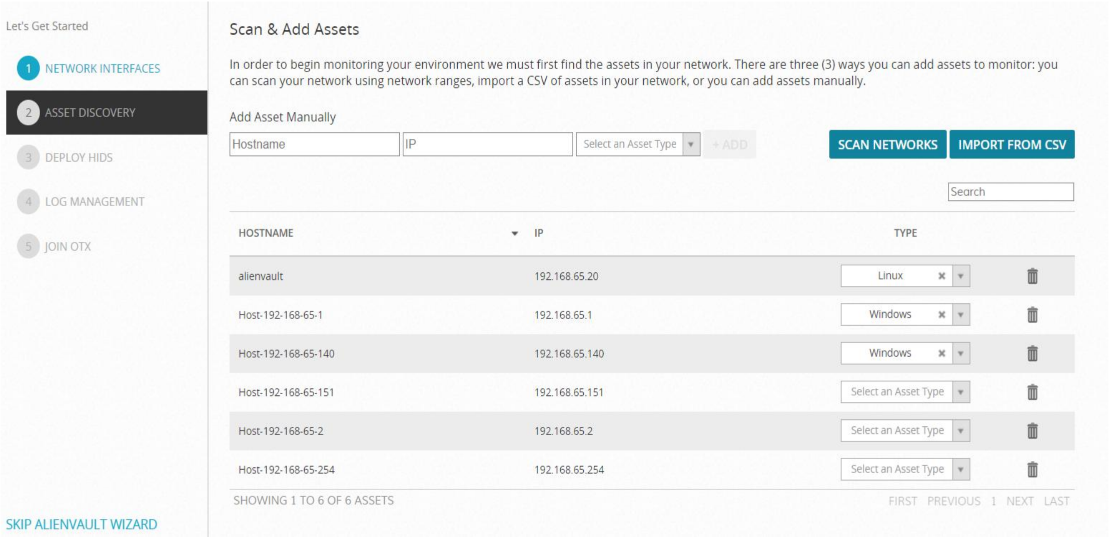
The network interfaces in AlienVault OSSIM can be configured to run Network Monitoring or as Log Collection & Scanning. Once you've configured the interfaces you'll need to ensure that the networking is configured appropriately for each interface so that AlienVault OSSIM is either receiving data passively or has the ability to reach out to the desired network.

NIC	PURPOSE	IP ADDRESS	STATUS
eth0	Management	192.168.65.20	-

Information

- **Management:** The Management interface was configured on the OSSIM Console and allows you to connect to the web UI. This interface cannot be changed from the web UI.
- **Network Monitoring:** Passively listen for network traffic. Interface will be set to promiscuous mode. Requires a network tap or span. See Instructions on how to setup a network tap or span.
- **Log Collection & Scanning:** Collect or receive logs from your assets, run an asset scan, or deploy the HIDS agent. Requires routable access to your networks.
- **Not in Use:** Use this option if you do not want to use one of the network interfaces.

Click Next. It will start Asset Discovery. It scans the network and displays the hosts discovered as shown below.



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.

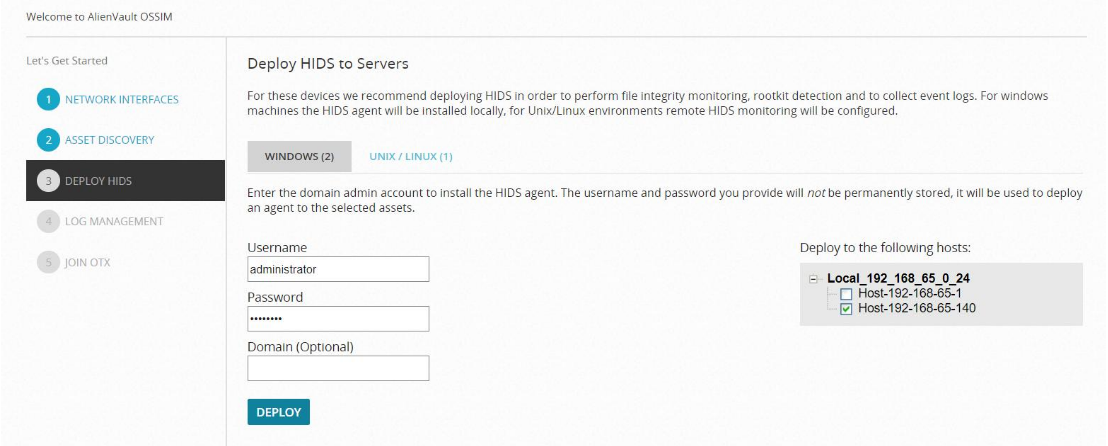
Add Asset Manually

HOSTNAME	IP	TYPE
alienvault	192.168.65.20	Linux
Host-192-168-65-1	192.168.65.1	Windows
Host-192-168-65-140	192.168.65.140	Windows
Host-192-168-65-151	192.168.65.151	Select an Asset Type
Host-192-168-65-2	192.168.65.2	Select an Asset Type
Host-192-168-65-254	192.168.65.254	Select an Asset Type

SHOWING 1 TO 6 OF 6 ASSETS

You can add hosts manually if the hosts are not discovered. If you want to scan network click SCAN NETWORKS option. You can add hosts later also.
Once you get all your hosts, Click Next .

The following page allows you to deploy HIDS on the Windows machines. For Linux machines remote HIDS monitoring will be configured. On Windows tab, expand Network address displayed. Provide Username and password and click deploy.



Deploy HIDS to Servers

For these devices we recommend deploying HIDS in order to perform file integrity monitoring, rootkit 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.

Enter the domain admin account to install the HIDS agent. The username and password you provide will *not* be permanently stored, it will be used to deploy an agent to the selected assets.

Username: administrator

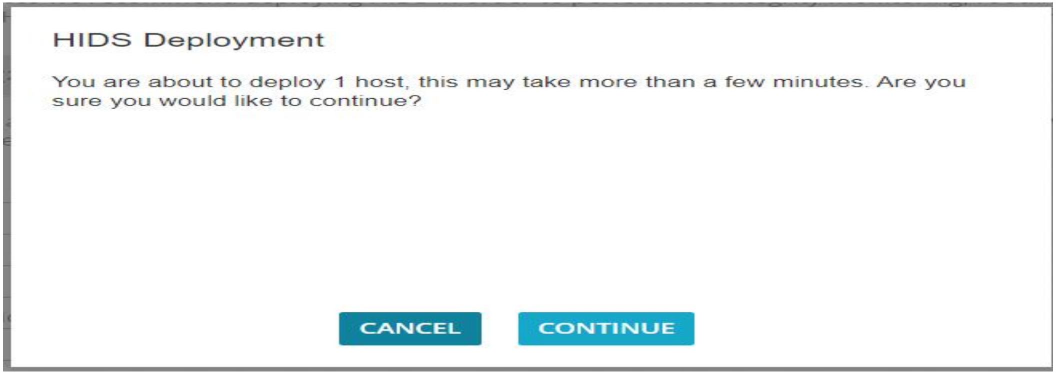
Password: ••••••••

Domain (Optional):

Deploy to the following hosts:

Local_192_168_65_0_24
- □ Host-192-168-65-1
- ☑ Host-192-168-65-140

Following screen is displayed.

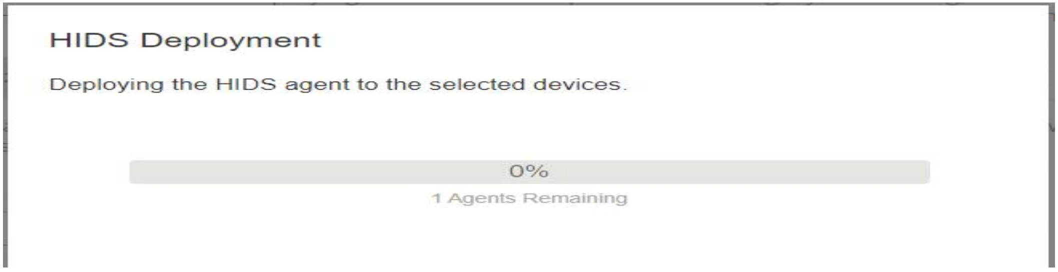


HIDS Deployment

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

Click Continue.

It starts deploying the HIDS.

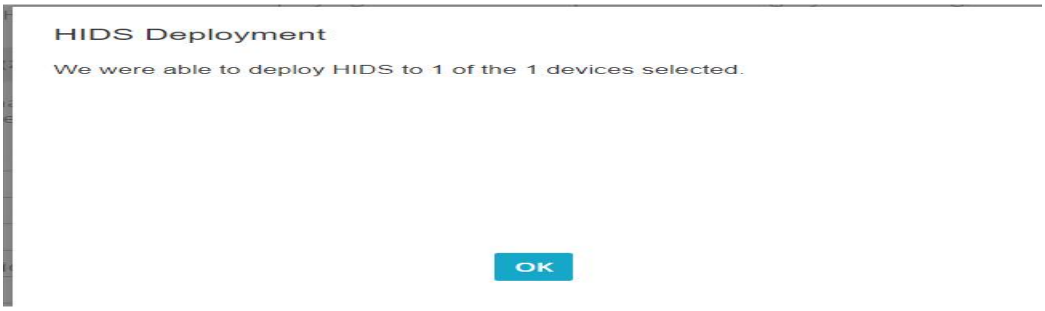


HIDS Deployment

Deploying the HIDS agent to the selected devices.

0%

1 Agents Remaining

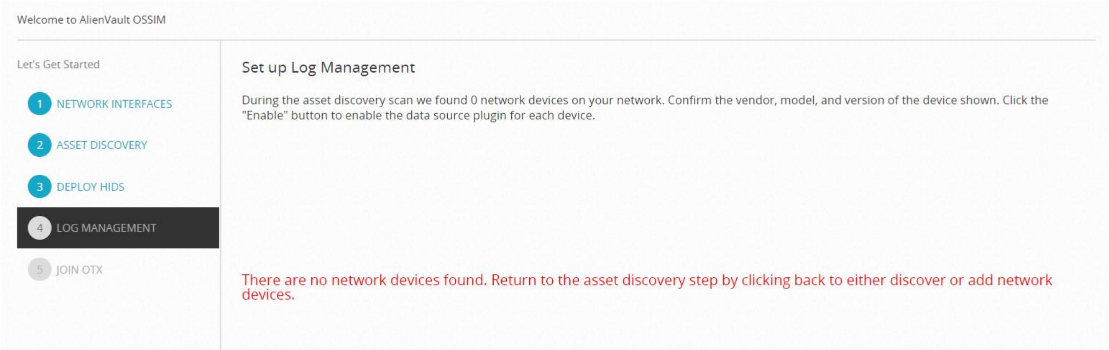


HIDS Deployment

We were able to deploy HIDS to 1 of the 1 devices selected.

However it may fail. Thus it is always good to install the HIDS agent on the client machines manually.

Click OK. Click NEXT.
On Log Management screen, you may get following error.



Welcome to AlienVault OSSIM

Let's Get Started

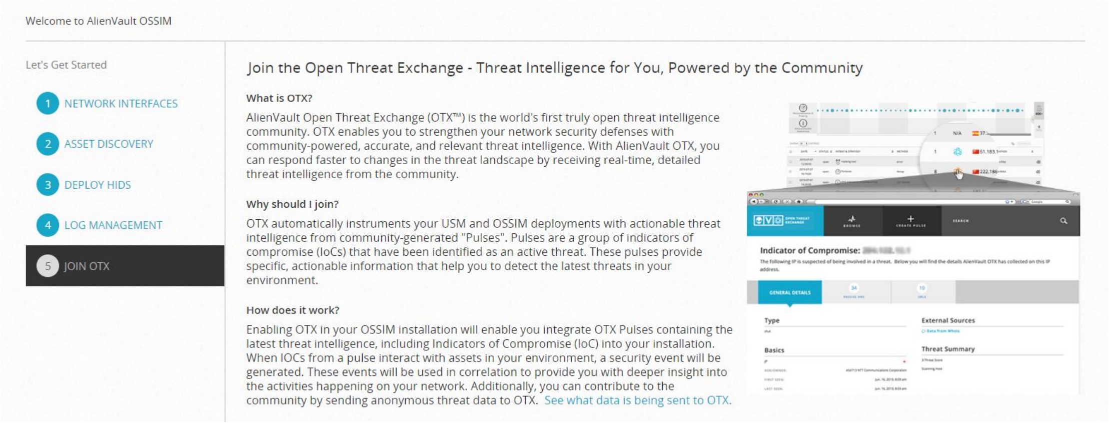
1 NETWORK INTERFACES
2 ASSET DISCOVERY
3 DEPLOY HIDS
4 LOG MANAGEMENT
5 JOIN OTX

Set up Log Management

During the asset discovery scan we found 0 network devices on your network. Confirm the vendor, model, and version of the device shown. Click the "Enable" button to enable the data source plugin for each device.

There are no network devices found. Return to the asset discovery step by clicking back to either discover or add network devices.

Click SKIP THIS STEP.
On the following screen you can participate in the Open Threat Exchange community.



Welcome to AlienVault OSSIM

Let's Get Started

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

Join the Open Threat Exchange - Threat Intelligence for You, Powered by the Community

What is OTX?

AlienVault Open Threat Exchange (OTX™) is the world's first truly open threat intelligence community. OTX enables you to strengthen your network security defenses with community-powered, accurate, and relevant threat intelligence. With AlienVault OTX, you can respond faster to changes in the threat landscape by receiving real-time, detailed threat intelligence from the community.

Why should I join?

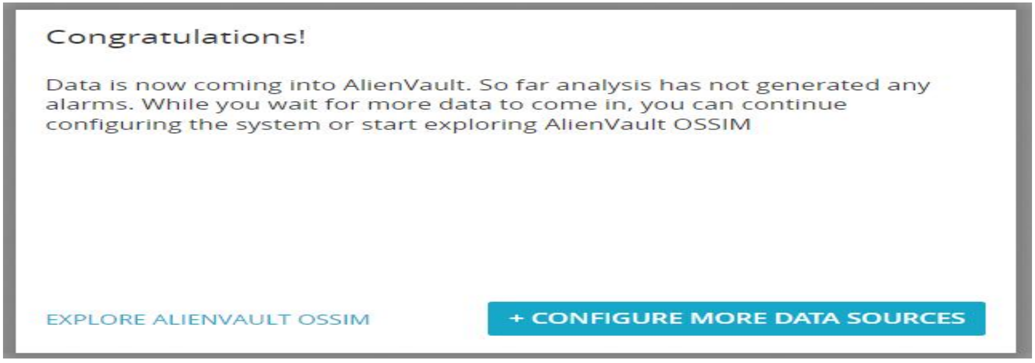
OTX automatically instruments your USM and OSSIM deployments with actionable threat intelligence from community-generated "Pulses". Pulses are a group of indicators of compromise (IoCs) that have been identified as an active threat. These pulses provide specific, actionable information that help you to detect the latest threats in your environment.

How does it work?

Enabling OTX in your OSSIM installation will enable you integrate OTX Pulses containing the latest threat intelligence, including Indicators of Compromise (IoC) into your installation. When IOCs from a pulse interact with assets in your environment, a security event will be generated. These events will be used in correlation to provide you with deeper insight into the activities happening 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.

Click SKIP THIS STEP if you do not want to participate.
Finally Click FINISH.

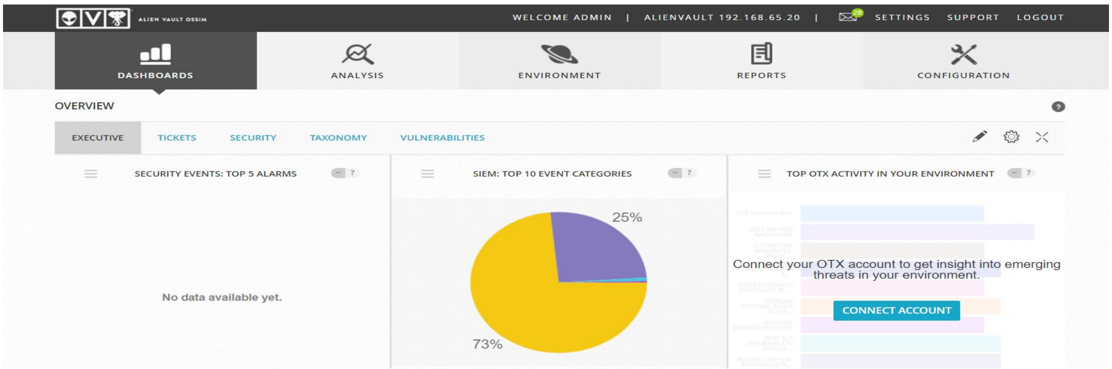
Following screen is displayed.



Congratulations!

Data is now coming into AlienVault. So far analysis has not generated any alarms. While you wait for more data to come in, you can continue configuring the system or start exploring AlienVault OSSIM

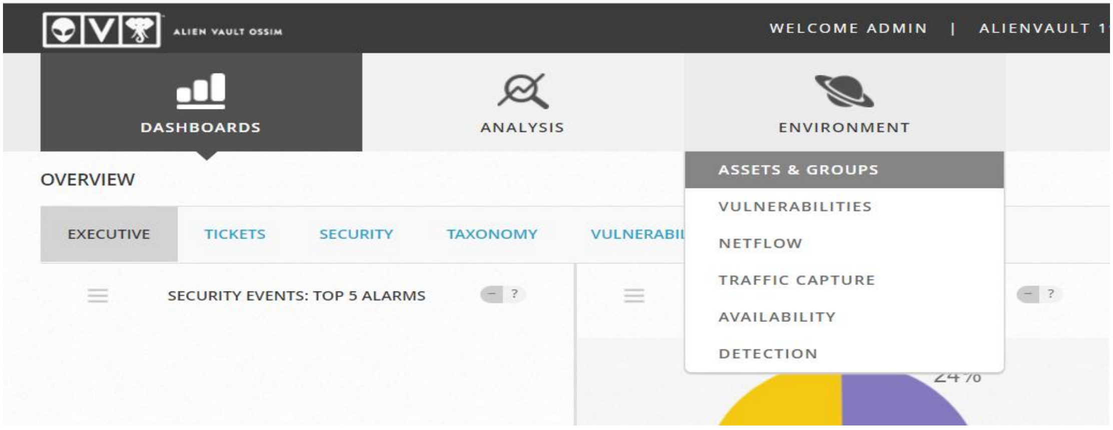
Click Explore AlienVault OSSIM.
You will reach to the following console.



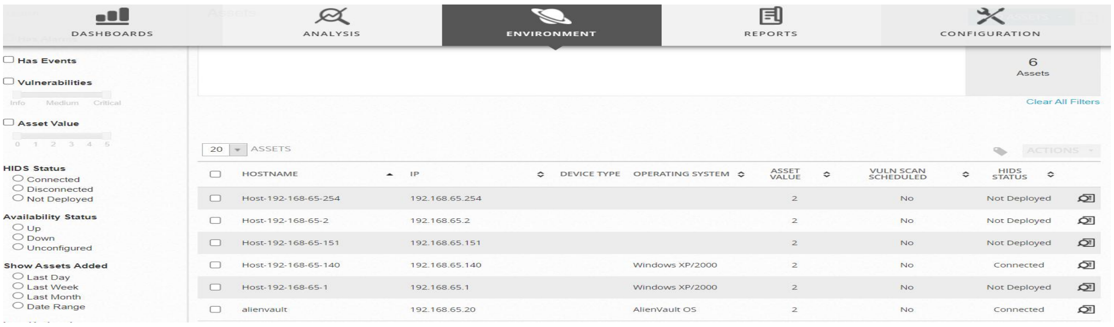
No data available yet.

Connect your OTX account to get insight into emerging threats in your environment.

Now click ENVIRONMENT tab and click Assets and Group as shown below.

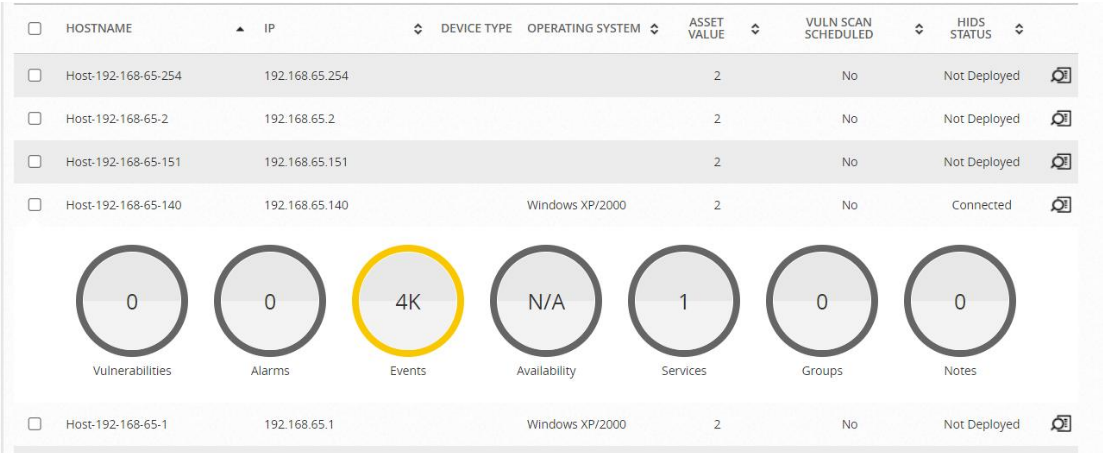


This will display following page. It will display hosts within your network and their HIDS status.



□	HOSTNAME	IP	DEVICE TYPE	OPERATING SYSTEM	ASSET VALUE	VULN SCAN SCHEDULED	HIDS STATUS
□	Host-192-168-65-254	192.168.65.254			2	No	Not Deployed
□	Host-192-168-65-2	192.168.65.2			2	No	Not Deployed
□	Host-192-168-65-151	192.168.65.151			2	No	Not Deployed
□	Host-192-168-65-140	192.168.65.140		Windows XP/2000	2	No	Connected
□	Host-192-168-65-1	192.168.65.1		Windows XP/2000	2	No	Not Deployed
□	alienvault	192.168.65.20		AlienVault OS	2	No	Connected

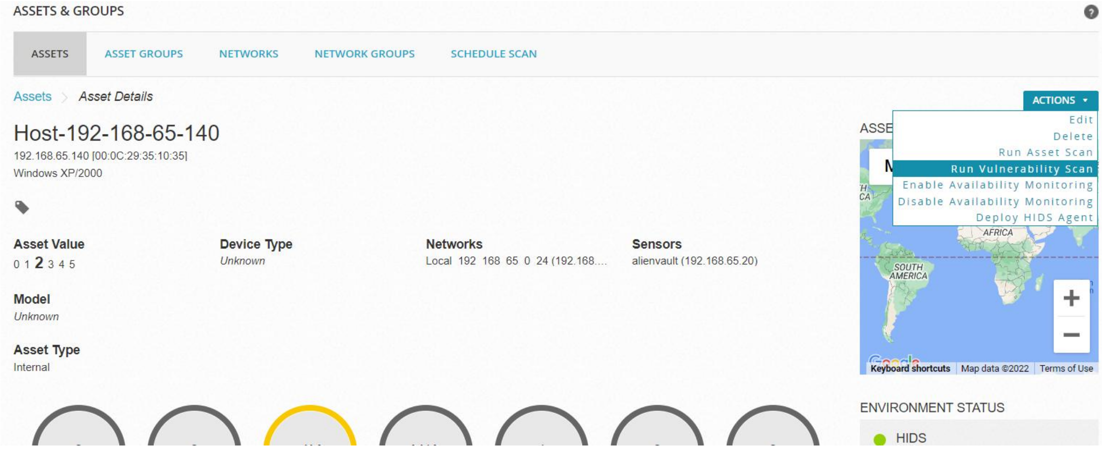
Click on any host and it will display details about that host as shown below.



□	HOSTNAME	IP	DEVICE TYPE	OPERATING SYSTEM	ASSET VALUE	VULN SCAN SCHEDULED	HIDS STATUS
□	Host-192-168-65-254	192.168.65.254			2	No	Not Deployed
□	Host-192-168-65-2	192.168.65.2			2	No	Not Deployed
□	Host-192-168-65-151	192.168.65.151			2	No	Not Deployed
□	Host-192-168-65-140	192.168.65.140		Windows XP/2000	2	No	Connected
□	Host-192-168-65-1	192.168.65.1		Windows XP/2000	2	No	Not Deployed

Vulnerabilities	Alarms	Events	Availability	Services	Groups	Notes
0	0	4K	N/A	1	0	0

Click on the Magnifier icon in front of host. Following screen is displayed.



Host-192-168-65-140
192.168.65.140 [00:0C:29:35:10:35]
Windows XP/2000

Asset Value
0 1 2 3 4 5

Device Type
Unknown

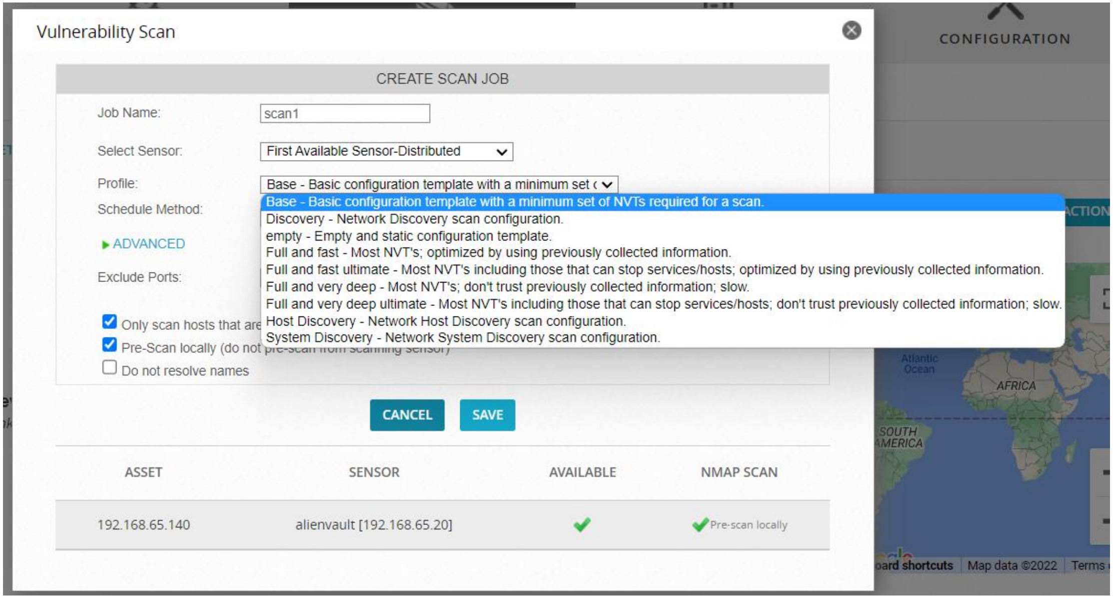
Networks
Local 192 168 65 0 24 (192.168....

Sensors
alienvault (192.168.65.20)

Model
Unknown

Asset Type
Internal

Click the ACTIONS button and click RUN VULNERABILITY SCAN.
On the new window that opens, Provide a job name,Select required profile.



Vulnerability Scan

CREATE SCAN JOB

Job Name: scan1

Select Sensor: First Available Sensor-Distributed

Profile: Base - Basic configuration template with a minimum set c

Schedule Method:

▸ ADVANCED

Exclude Ports:

- Base - Basic configuration template with a minimum set of NVTs required for a scan.
- Discovery - Network Discovery scan configuration.
- empty - Empty and static configuration template.
- Full and fast - Most NVT's; optimized by using previously collected information.
- Full and fast ultimate - Most NVT's including those that can stop services/hosts; optimized by using previously collected information.
- Full and very deep - Most NVT's; don't trust previously collected information; slow.
- Full and very deep ultimate - Most NVT's including those that can stop services/hosts; don't trust previously collected information; slow.
- Host Discovery - Network Host Discovery scan configuration.
- System Discovery - Network System Discovery scan configuration.

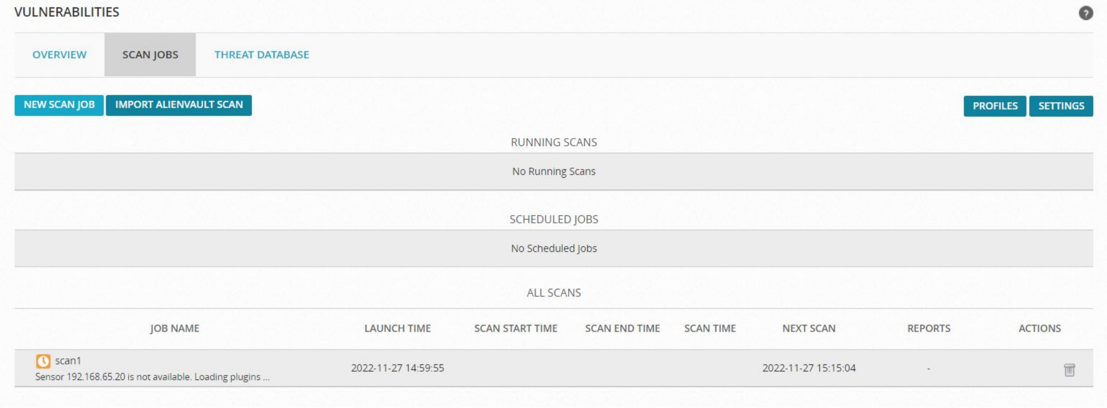
☑ Only scan hosts that are
☑ Pre-Scan locally (do not pre-scan from scanning sensor)
□ Do not resolve names

CANCEL SAVE

ASSET	SENSOR	AVAILABLE	NMAP SCAN
192.168.65.140	alienvault [192.168.65.20]	✓	✓ Pre-scan locally

Keep all other settings to default. Click Save.
Click Schedule Scan option on the same page.
Click Vulnerability Scans.

Following page shows the details.



RUNNING SCANS

No Running Scans

SCHEDULED JOBS

No Scheduled Jobs

ALL SCANS

JOB NAME	LAUNCH TIME	SCAN START TIME	SCAN END TIME	SCAN TIME	NEXT SCAN	REPORTS	ACTIONS
scan1 Sensor 192.168.65.20 is not available. Loading plugins ...	2022-11-27 14:59:55				2022-11-27 15:15:04	-	

Please follow steps mention below to add a Linux host to Alien Vault OSSIM.

https://cybersecurity.att.com/documentation/usm-appliance/ids-configuration/deploying-alienvault-hids.htm

Following link provides details to add a Windows host to Alien Vault OSSIM.

https://cybersecurity.att.com/documentation/usm-appliance/ids-configuration/deploying-alienvault-hids.htm

A complete online guide for Alien Vault OSSIM can be found on the link given below.

https://cybersecurity.att.com/documentation/usm-appliance-deployment-guide.htm?tocpath=Documentation%7CUSM%20Appliance%E2%84%A2%7CDeployment%20Guide%7C 0