

AlienVault Kurulumu

AlienVault Unified Security Management (USM) gelişmiş tehditlere karşı etkili bir biçimde savunma yapabilmek için geliştirilmiş bütünleşik bir güvenlik yönetim sistemidir. AlienVault; Server, Sensor ve Logger olmak üzere üç temel bileşenden oluşur. Bu bileşenler tek başına kullanılabildiği gibi hepsi bir arada bütünleşik bir sistem olarakta kullanılabilmektedir. Bu temel bileşenler gerçek zamanlı olarak akıllı tehdit algılama, log kolerasyonu gibi özellikler sağlar.

AlienVault'u oluşturan bu temel bileşenler;

Server: Sensörler tarafından gelen bilgileri toplar ve ilişkilendirir. Ayrıca bu bilgilerin tek bir ekrandan yönetim ve raporlanmasını sağlar. Güvenlik otomasyonu özelliği sayesinde gelen tehditlere karşı hızlıca yanıt verilmesini sağlar. Ortak yönetim sayesinde ağ güvenliğinin maliyet ve karmaşıklığınız azaltır. Akıllı tehdit algılama özelliği ile sürekli güvenlik zaafiyeti araştırma gereksinimini ortadan kaldırır.

Sensor: Ağınızda bulunan logları toplamak ve eksiksiz görüntülenebilmesi için sağladığı güvenlik özellikleri vardır. Bunlar Asset Discovery (Varlık Keşfi), Vulnerability Assessment (Zaafiyet Değerlendirme), Intrusion Detection (Saldırı Tespiti), Behavioral Monitoring (Davranışsal İzleme) ve SIEM şeklindedir.

Logger: Adli makamların olay araştırmalarında ihtiyaç duyduğu loglar, yasalara uygun şekilde dijital imza ile uzun süreli depolama ve ölçeklendirilebilir şekilde yapılabilir. Loglar 5te1 oranında sıkıştırılarak saklanır. Entegre log arama özelliği sayesinde aranılan loglar kısa sürede bulunabilir.

Kurulumdan sonra 5 adımdan oluşan yapılandırma işlemini gerçekleştirerek birkaç dakika içerisinde AlienVault'u kullanmaya başlayabilirsiniz.

1. Ağa Bağlanma: Yani USM ağa bağlanır ve trafiği inceleyerek ağ hakkında bilgi toplar.
2. Ağı Tarama: USM bağlı olduğu ağda bulduğu cihazları, servisleri, ve güvenlik açıklıklarını tarar.
3. Sistem & Network İzleme: USM 'in testip etmiş olduğu tehdit ve kötü niyetli davranışları tespit eder ve grafik halinde sunar.
4. Log Toplama: Loglar toplanır.
5. Analiz Etme ve Çözüm: Tehdit içeren olaylar analiz edilerek çözüm üretilir.

Virtual Machine Requirements	USM All-in-One		USM Standard		
	All Models	Remote Sensor	Server	Logger	Sensor
Total Cores	8	4	8		
RAM (GB)	16	8	24		
Storage (TB) Compressed / Uncompressed	5.0 / 1.0		6.0 / 1.2	9.0 / 1.8	6.0 / 1.2
Virtualization Environment	VMware ESXi4.0+		VMware ESXi4.0+		

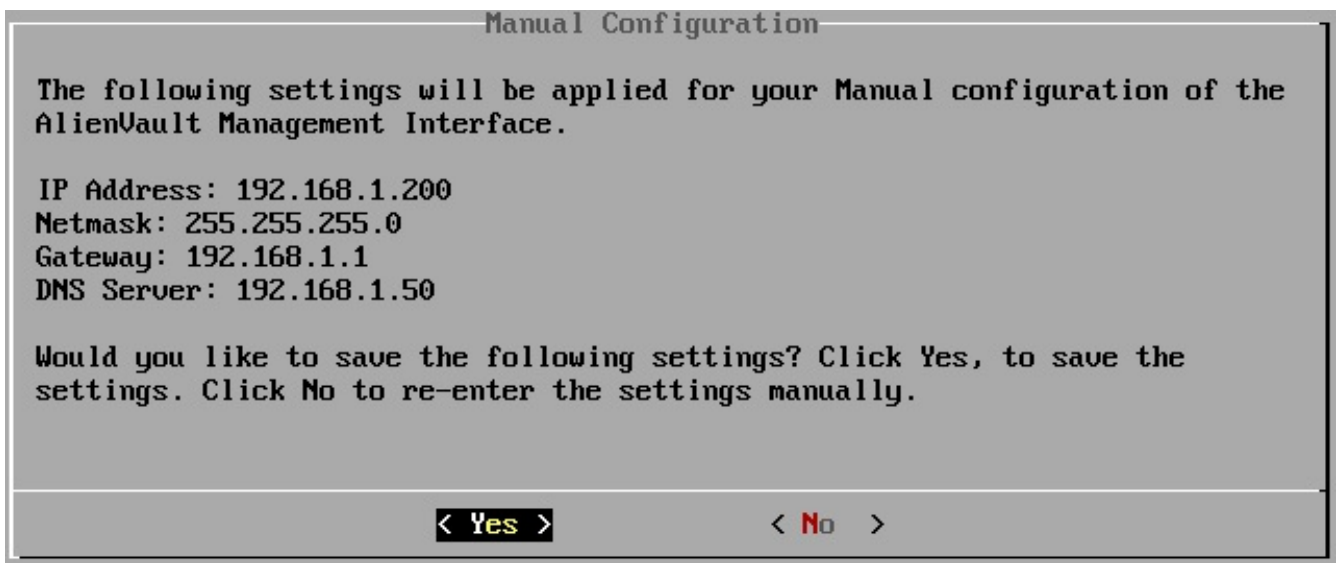
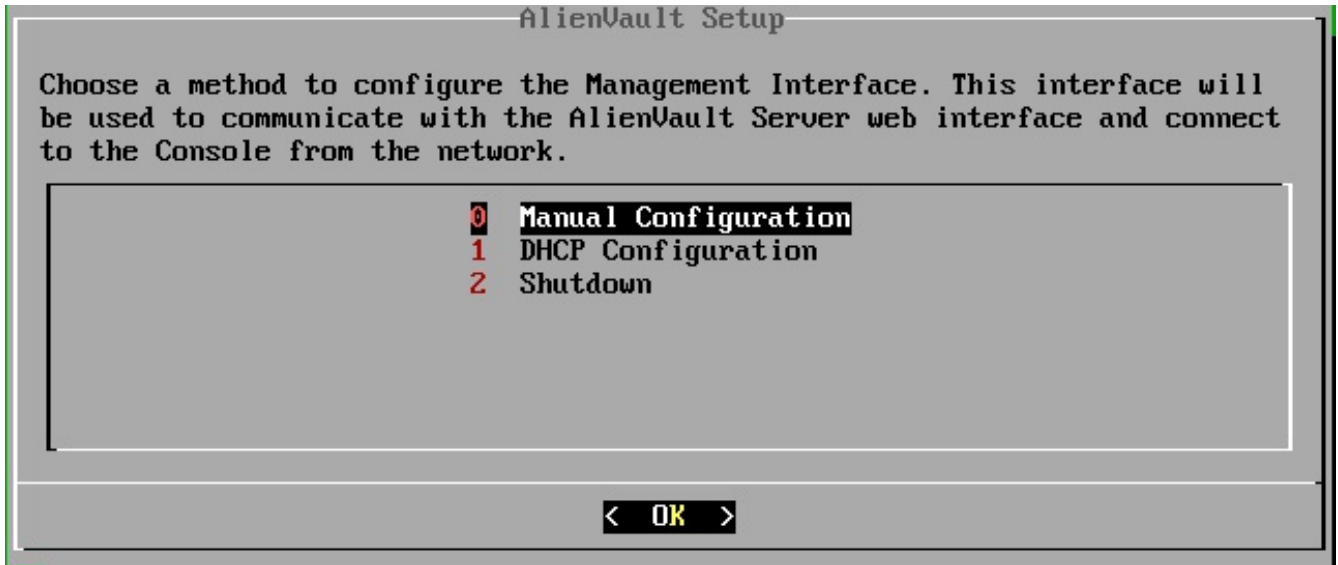
AlienVault USM Sistem Gereksinimleri

Sistem gereksinimlerini sağlayan bir alt tapı hazırlanarak kurulum işlemi aşağıdaki adımlar takip edilerek gerçekleştirilebilir.

30 günlük ücretsiz deneme sürümünü şu adresten indirebilirsiniz.

AlienVault USM Kurulumu

-Sistemi başlatınız. AlienVault kurulum ekranı açılacaktır. İlk olarak network yapılandırma türünü seçiniz. Burada manuel seçim yapılmış olup IP adres, Netmask, Gateway, DNS gibi bilgiler girilmiştir. İlgili ayarları kendi ağınıza göre yapınız.



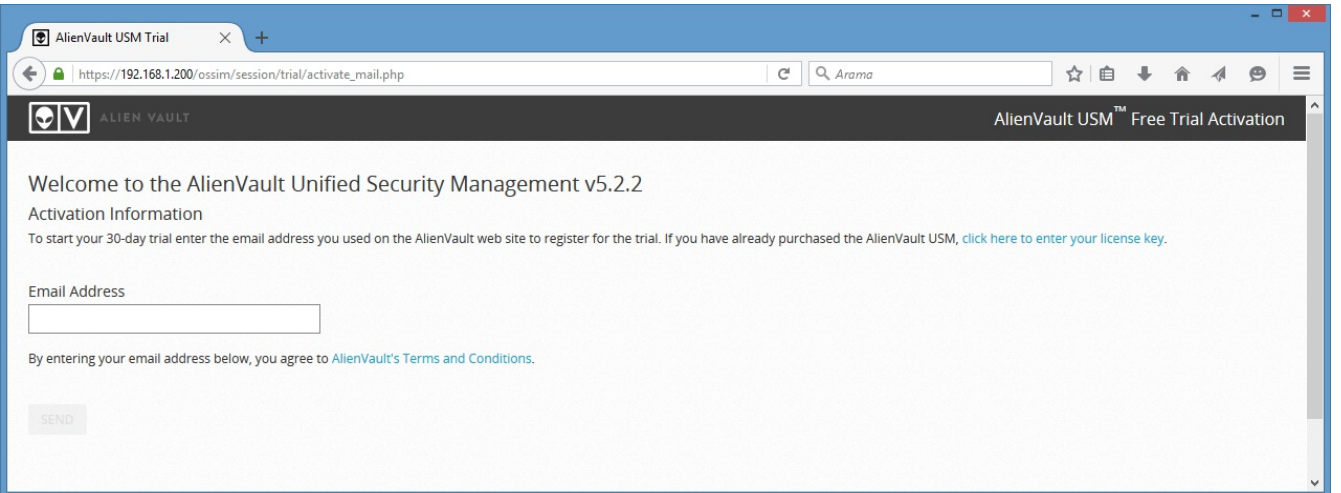
- Kurulum işlemi tamamlanırken bekleyiniz.
- Kurulum işlemi tamamlandıktan sonra kullanıcı bilgilerinin yer aldığı ekran açılacaktır. İlk olarak bu ekranda yer alan bilgiler ile sisteme giriş yaparak root parolanızı değiştiriniz.

```
=====
===== http://www.alienvault.com =====
=====
==== Access the AlienVault web interface using the following URL: ====
===== https://192.168.1.200/ =====
=====
== ### First time instructions ###
== 1. Enter USERNAME:root and PASSWORD:kerlryuw to access.
== 2. You will be prompted to change this password in the first run *only*
== 3. Enjoy!

AlienVault USM 5.2.2 - x86_64 - tty1

VirtualUSMA11InOne login: _
```

- Web tarayıcısı üzerinden belirlediğiniz IP adresine erişim sağlayınız. Aktivasyon işlemi için eposta adresini yazarak devam ediniz. Ve işlemi “FINISH” diyerek tamamlayınız.



AlienVault USM Trial

https://192.168.1.200/ossim/session/trial/activate_mail.php

ALIEN VAULT

AlienVault USM™ Free Trial Activation

Welcome to the AlienVault Unified Security Management v5.2.2

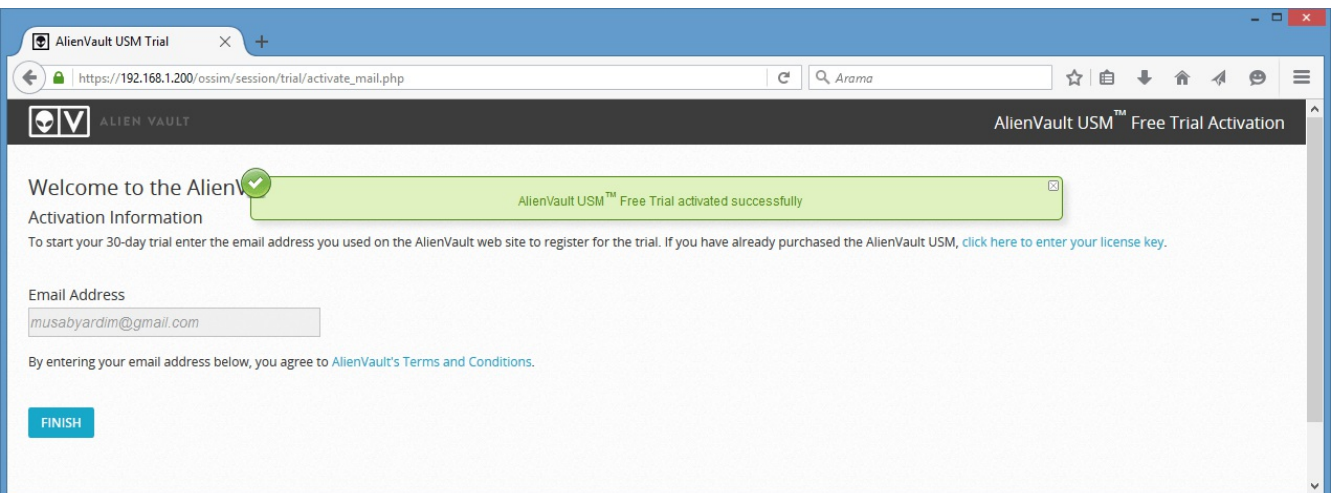
Activation Information

To start your 30-day trial enter the email address you used on the AlienVault web site to register for the trial. If you have already purchased the AlienVault USM, [click here to enter your license key](#).

Email Address

By entering your email address below, you agree to [AlienVault's Terms and Conditions](#).

SEND



AlienVault USM Trial

https://192.168.1.200/ossim/session/trial/activate_mail.php

ALIEN VAULT

AlienVault USM™ Free Trial Activation

Welcome to the AlienVault

Activation Information

To start your 30-day trial enter the email address you used on the AlienVault web site to register for the trial. If you have already purchased the AlienVault USM, [click here to enter your license key](#).

Email Address

By entering your email address below, you agree to [AlienVault's Terms and Conditions](#).

FINISH

- AlienVault için yetkili kullanıcı hesap bilgilerini yazınız.

AlienVault USM [VirtualUS... X +

https://192.168.1.200/ossim/session/login.php

ALIEN VAULT

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](https://www.alienvault.com).

Administrator Account Creation

Create an account to access your AlienVault product.

** Asterisks indicate required fields*

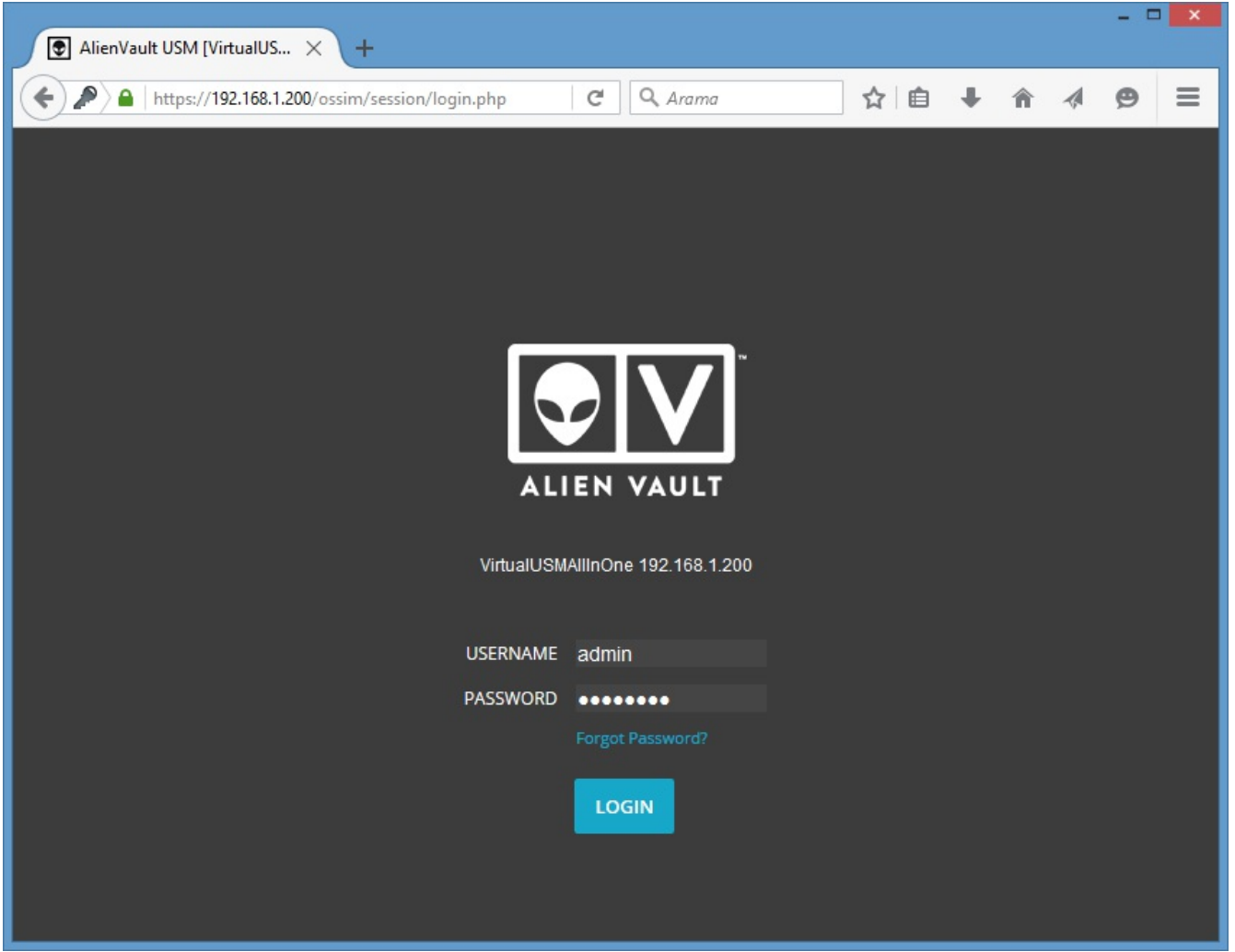
FULL NAME *	Musab Yardım
USERNAME *	admin
PASSWORD *	medium
CONFIRM PASSWORD *	medium
E-MAIL *	musabyardim@gmail.com
COMPANY NAME	MSB
LOCATION	Türkiye → View Map

☐ Share anonymous usage statistics and system information with AlienVault to help us make USM better. [Learn More](#)

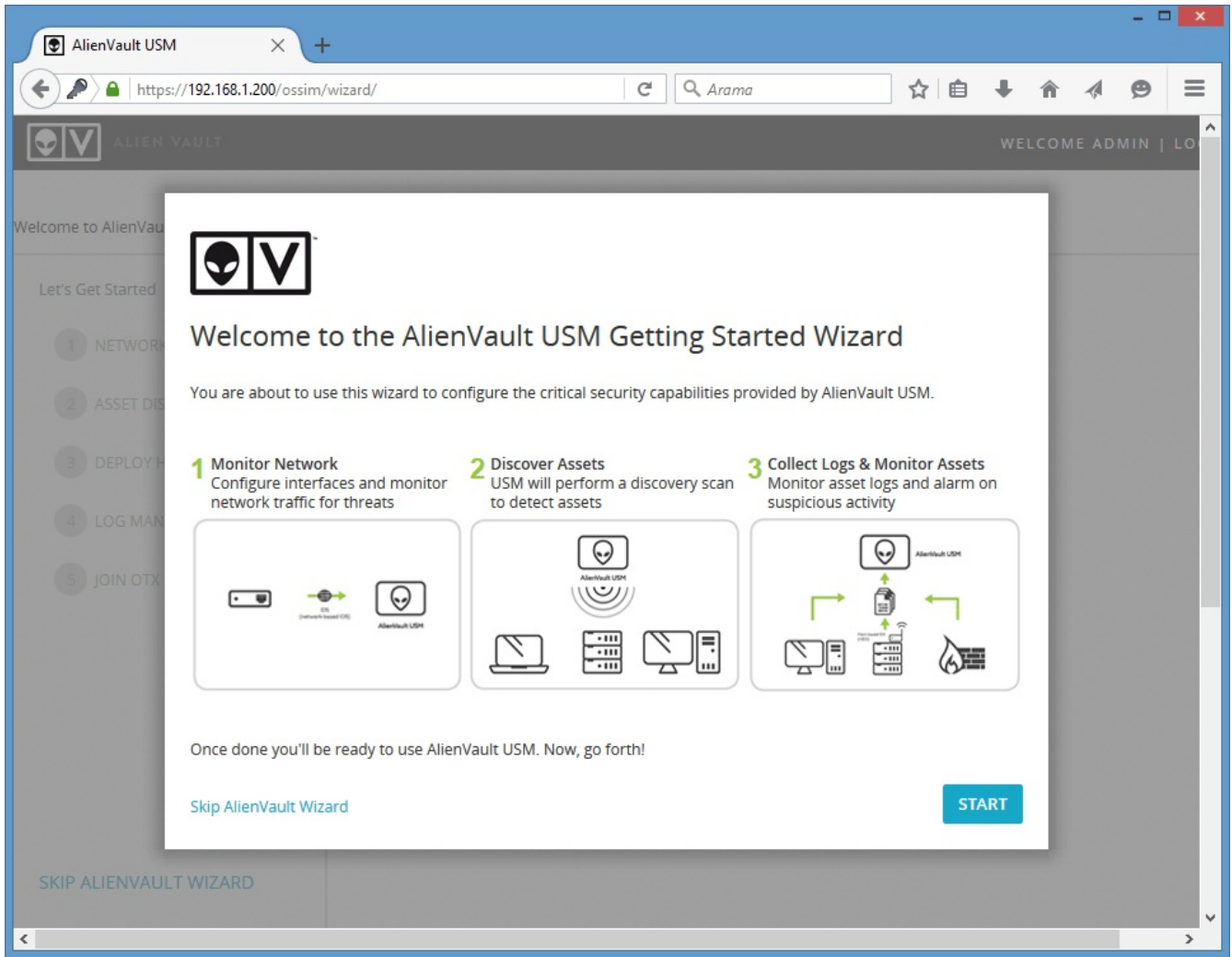
[START USING ALIENVAULT](#)

maps-api-ssl.google.com bekleniyor...

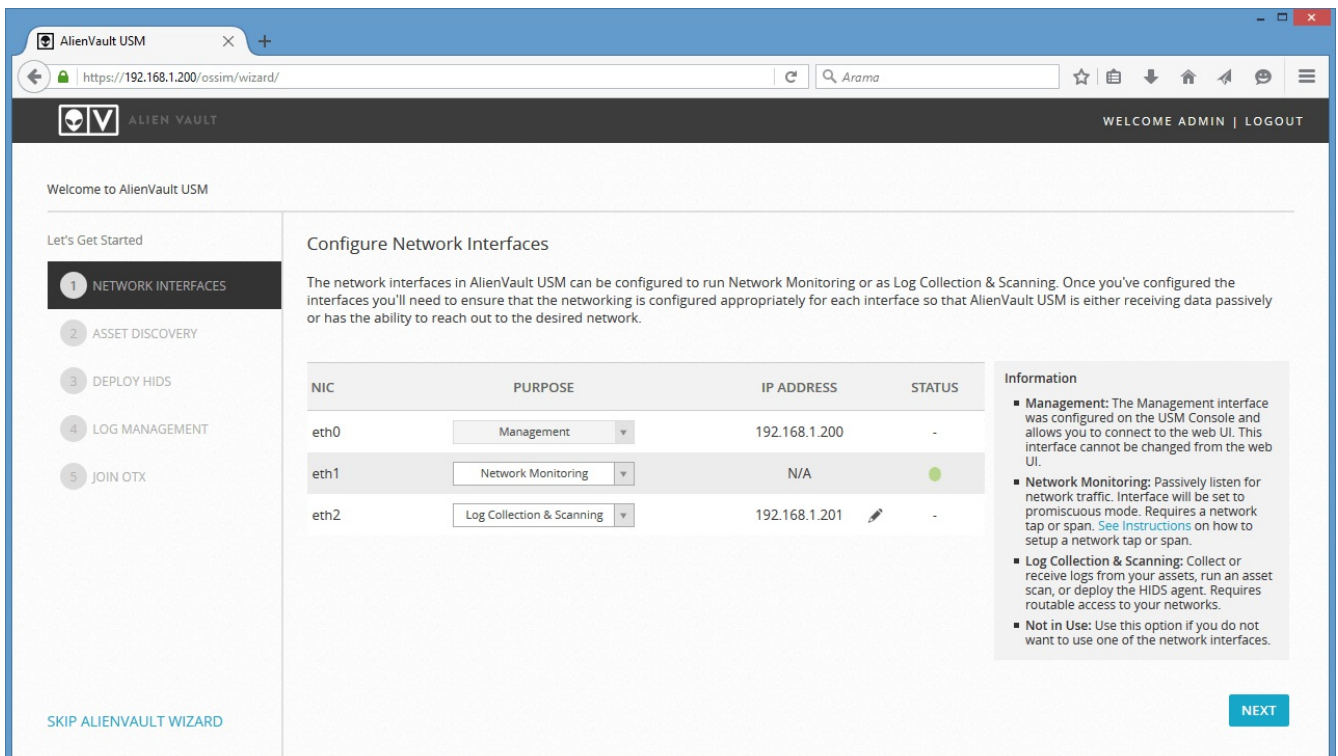
- AlienVault 'a erişim sağlayabilirsiniz. Kullanıcı bilgilerinizi yazarak giriş yapınız.



- Açılış ekranında başlangıç sihirbazı ile ilk yapılandırmanızı gerçekleştirebilirsiniz. “START” diyerek sihirbazı başlatınız.



- Network yapılandırmanızı gerçekleştiriniz.



- AlienVault bulunduğunuz networkü tarayarak aktif sunucuları listeler. Bu listede izlemek istemediğiniz sunucular varsa o sunucuları kaldırarak devam ediniz.

AlienVault USM

https://192.168.1.200/ossim/wizard/

WELCOME ADMIN | LOGOUT

Welcome to AlienVault USM

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
Host-192-168-1-1	192.168.1.1	Linux
Host-192-168-1-101	192.168.1.101	Linux
Host-192-168-1-11	192.168.1.11	Windows
Host-192-168-1-254	192.168.1.254	Linux
Host-192-168-1-3	192.168.1.3	Select an Asset Type
Host-192-168-1-6	192.168.1.6	Select an Asset Type
VirtualUSMAllInOne	192.168.1.200	Linux

SHOWING 1 TO 7 OF 7 ASSETS

FIRST PREVIOUS 1 NEXT LAST

SKIP ALIENVAULT WIZARD

BACK

NEXT

- İzlemek istediğiniz Linux/Windows sistemlere Host Intrusion Detection System (HIDS) kurulumunun yapılabilmesi için kullanıcı bilgilerinizi yazarak "DEPLOY" butonuna basınız. Bu işlemi Linux ve Windows sistemleriniz için ayrı ayrı gerçekleştirmeniz gerekmektedir. (Bu yazıda 1 Linux ve 1 Windows eklenmiştir.)

AlienVault USM

https://192.168.1.200/ossim/wizard/

WELCOME ADMIN | LOGOUT

Welcome to AlienVault USM

Let's Get Started

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

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.

WINDOWS (1) UNIX / LINUX (4)

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

SSH Username
root

SSH Password

DEPLOY

Deploy to the following hosts:

- Local_192_168_1_0_24
 - ☐ Host-192-168-1-254
 - ☐ Host-192-168-1-1
 - ☒ Host-192-168-1-101
 - ☐ VirtualUSMAAllinOne

SKIP ALIENVAULT WIZARD BACK NEXT

AlienVault USM

https://192.168.1.200/ossim/wizard/

WELCOME ADMIN | LOGOUT

Welcome to AlienVault USM

Let's Get Started

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

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.

WINDOWS (1) UNIX / LINUX (4)

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
musab

Password

Domain (Optional)

DEPLOY

Deploy to the following hosts:

- Local_192_168_1_0_24
 - ☒ Host-192-168-1-11

SKIP ALIENVAULT WIZARD BACK NEXT

-İşlemin tamamlanması için devam ediniz.

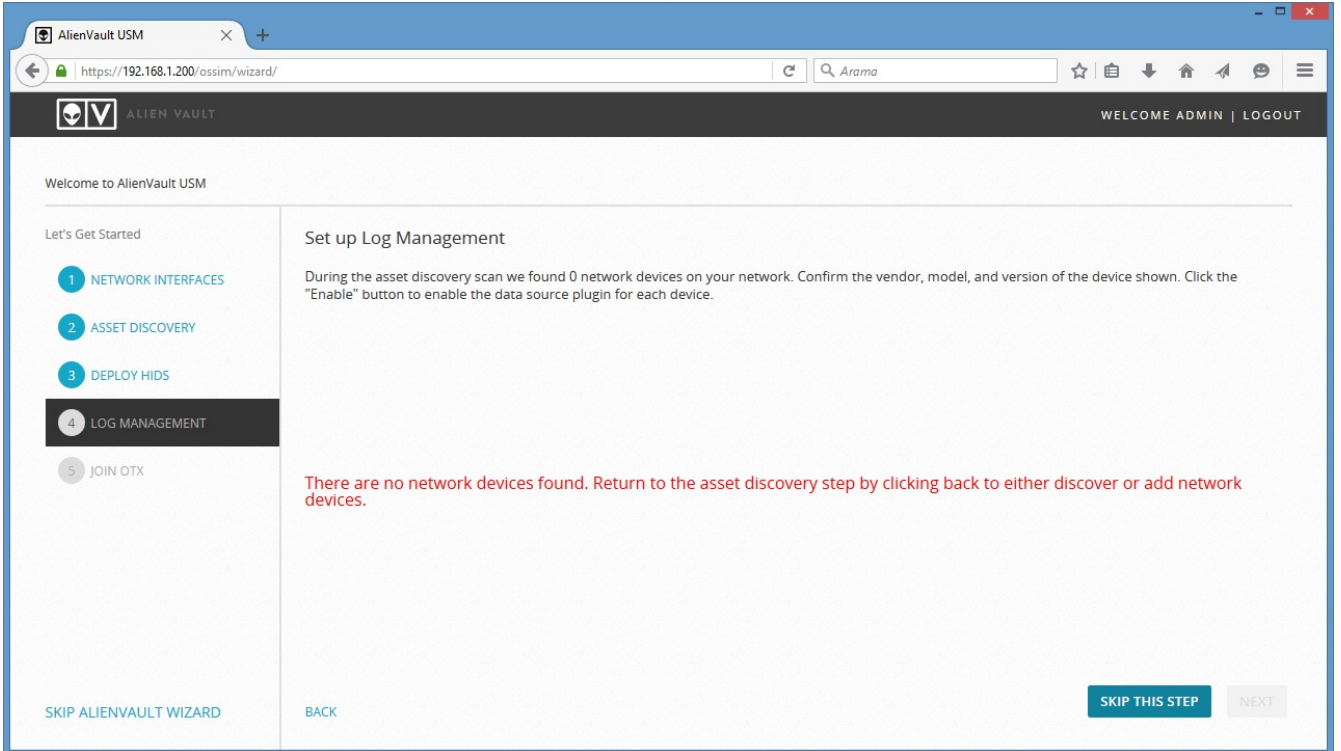
HIDS Deployment

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

CANCEL

CONTINUE

- Bulunduğuz ağıdaki network cihazlarına ait logları takip etmek isterseniz bu ekranda listelenecek olan aygıtlarınızı ekleyebilir veya bu adımı atlayabilirsiniz.



- Varsa OTX hesabınızı ekleyebilirsiniz.

AlienVault USM

https://192.168.1.200/ossim/wizard/

Arama

WELCOME ADMIN | LOGOUT

Welcome to AlienVault USM

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 USM 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.](#)

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.

Enter OTX key

Indicator of Compromise: 192.168.1.100

The following IP is suspected of being involved in a threat. Below you will find the details AlienVault OTX has collected on this IP address.

GENERAL DETAILS

THREAT DATA

IOCs

Type

mal

Basics

IP	192.168.1.100
EXTERNAL	ALIENVAULT COMMUNITARIAN CORPORATION
IP	192.168.1.100
LAST DATA	jan 16 2018 8:00 AM

External Sources

[View from where](#)

Threat Summary

Threat type	Malware
Threat name	Sample file

SKIP ALIENVAULT WIZARD

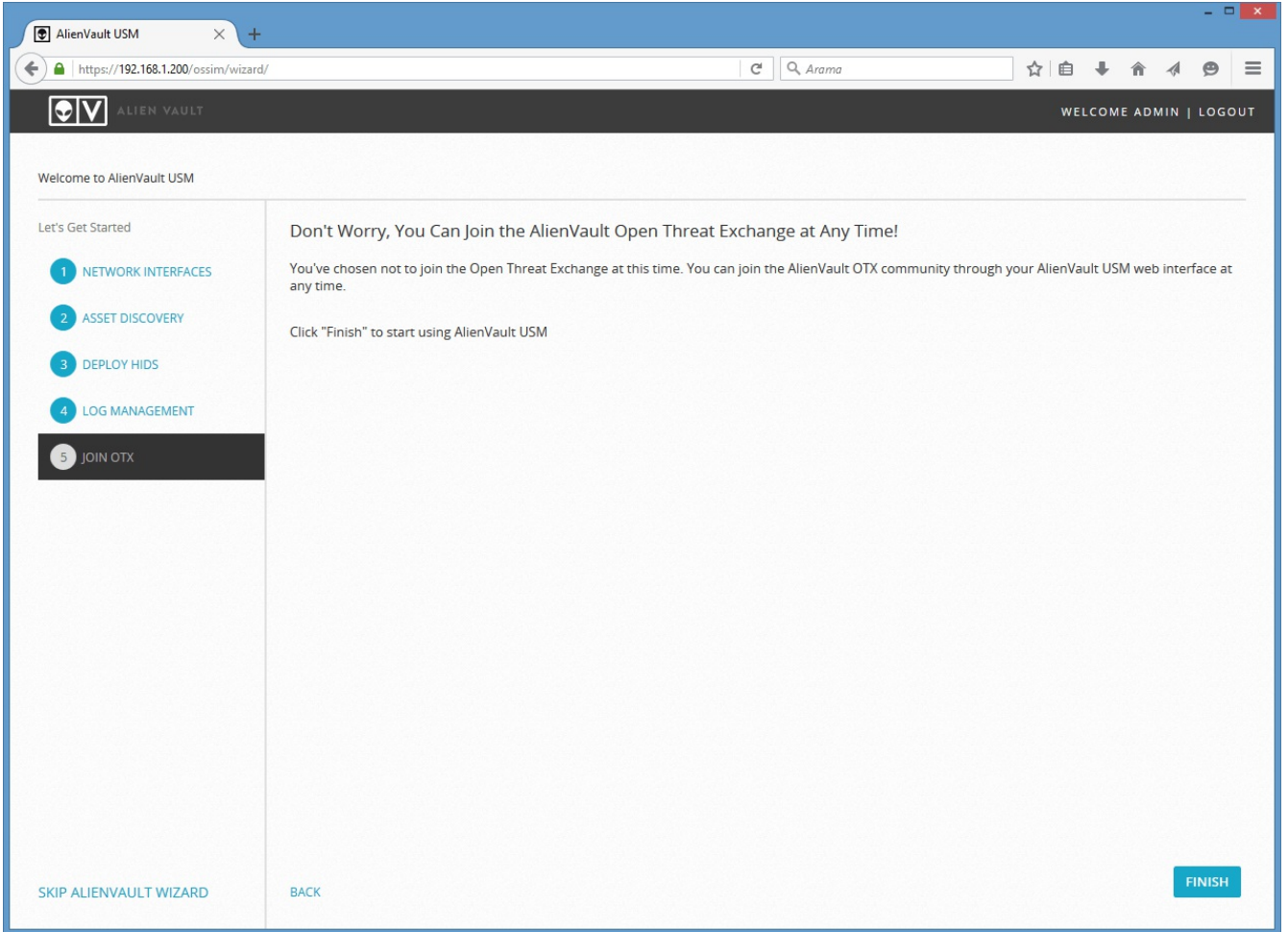
BACK

SKIP THIS STEP

NEXT

- FINISH butonuna basarak sihirbazı kapatabilirsiniz.

11/13



- AlienVault'a erişim için "EXPLORE ALIENVAULT USM" linkine tıklayınız.

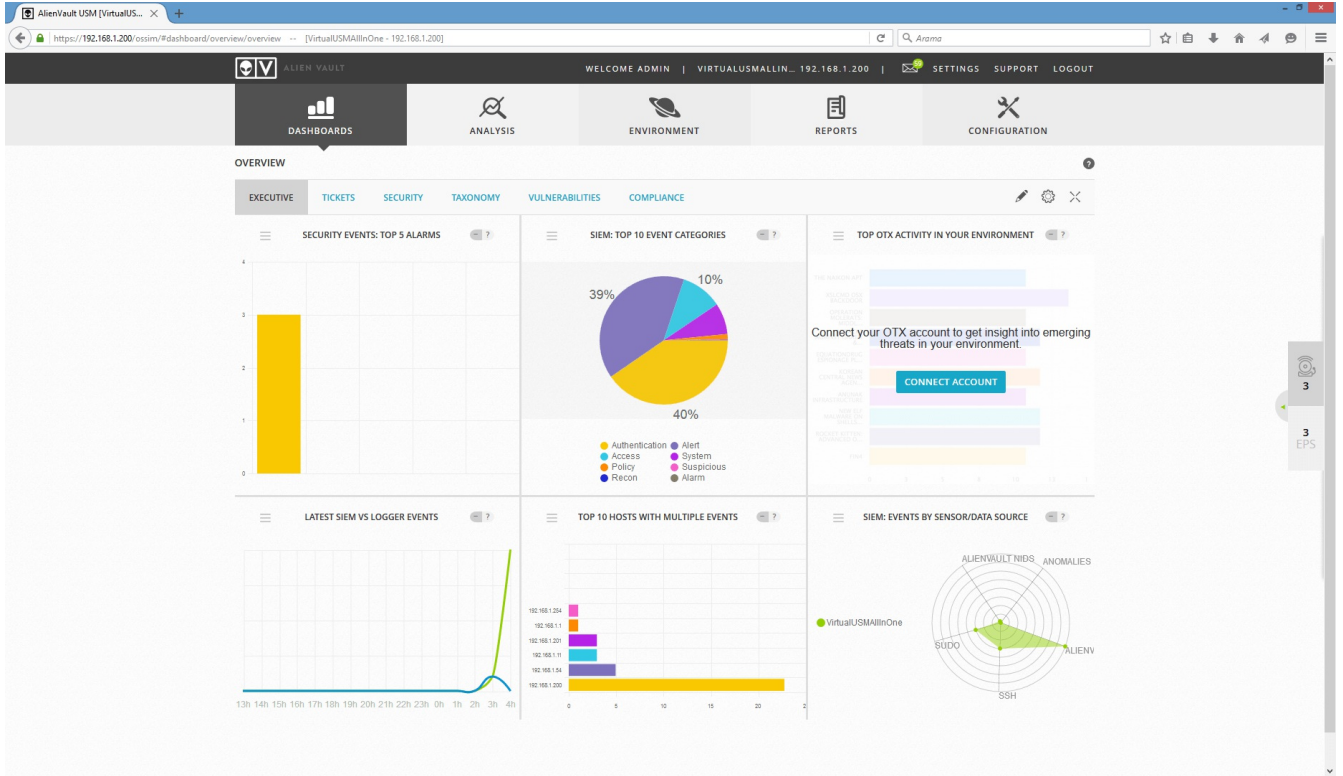
Congratulations!

Data is now coming into AlienVault. AlienVault has generated a few alarms. You can either view the alarms or explore AlienVault USM

[EXPLORE ALIENVAULT USM](#)

[SEE ALARMS](#)

- AlienVault Dashboard ekranı açılacaktır.



- Kurulum işlemi tamamlandıktan sonra sisteme eklediğiniz Linux ve Windows sunuculara HIDS'in sorunsuz yüklendiğiniz kontrol ediniz. Environment >> Detection >> Agents bölümünden kontrol edebilirsiniz.

OVERVIEW

AGENTS

AGENTLESS

EDIT RULES

CONFIG

HIDS CONTROL

AGENT CONTROL

SYSCHECKS

AGENT.CONF

Search

AGENT INFORMATION

ADD AGENT

ID	AGENT NAME	ASSET	IP/CIDR	CURRENT IP	CURRENT USER	STATUS	ACTIONS
000	VirtualUSMAllinOne (server)	VirtualUSMAllinOne	127.0.0.1	127.0.0.1	-	Active/local	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>
001	Host-192-168-1-11	Host-192-168-1-11	0.0.0.0/0	192.168.1.11	-	Active	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>
2	Host-192-168-1-101	Host-192-168-1-101	192.168.1.101	192.168.1.101	-	Active	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>

SHOWING 1 TO 3 OF 3 AGENTS

FIRSTPREVIOUS1NEXTLAST

- Bazı durumlarda HIDS'in kurulumunda problem olabilir. Bu gibi durumlarda HIDS'i sizin yüklemeniz gerekebilir.