

Wazuh, XDR ve SIEM özelliklerini birleştiren ücretsiz ve açık kaynaklı bir güvenlik platformudur. Şirket içi, sanallaştırılmış, kapsayıcılı ve bulut tabanlı ortamlarda iş yüklerini korur. Çözüm, tek bir evrensel aracı ve üç merkezi bileşenden oluşur: Wazuh sunucusu, Wazuh dizin oluşturucu ve Wazuh panosu.

Wazuh, kuruluşların ve bireylerin veri varlıklarını güvenlik tehditlerine karşı korumalarına yardımcı olur. Küçük işletmelerden büyük işletmelere kadar dünya çapında binlerce kuruluş tarafından yaygın olarak kullanılmaktadır.

**Wazuh Server:** Wazuh sunucusu, Wazuh ajanlarından alınan verileri analiz etmekten, tehditler veya anomalilikler tespit edildiğinde uyarıları tetiklemekten sorumludur. Ayrıca, araçların yapılandırmasını uzaktan yönetmek ve durumlarını izlemek için kullanılır.

**Elastic Stack:** Elastic stack günlük yönetimi için Elasticsearch, Kibana, Filebeat ve diğerleri dahil olmak üzere popüler açık kaynak projelerinin birleşik bir paketidir. Wazuh sunucusu tarafından oluşturulan uyarıları indeksler ve depolar. Ayrıca Wazuh ve Kibana\* arasındaki entegrasyon, veri görselleştirme ve analizi için bir kullanıcı arayüzü sağlar. Bu arayüz aynı zamanda Wazuh konfigürasyonunu yönetmek ve durumunu izlemek için de kullanılır.

Wazuh ile alakalı bileşenleri üç tane temel bileşeni vardır:

**Filebeat:** Olayları ve uyarıları Elasticsearch'e göndermek için Wazuh sunucusunda kullanılır. Wazuh analiz motorunun çıktısını okur ve olayları şifreli bir kanal aracılığıyla gerçek zamanlı olarak gönderir.

**Elasticsearch:** Yüksek düzeyde ölçeklenebilir, tam metin arama ve analiz motorudur. Elasticsearch dağıtılmıştır, yani veri endeksleri parçalara bölünür ve her parçanın sıfır veya daha fazla kopyası olabilir. Wazuh, uyarı verileri, ham olaylar ve durum izleme bilgileri için farklı endeksler kullanır.

**Kibana:** Veri madenciliği, analiz ve görselleştirme için esnek ve sezgisel bir web arayüzüdür. Bir Elasticsearch kümesinde dizine alınmış içeriğin üstünde çalışır. Wazuh web kullanıcı arayüzü Kibana'ya eklenmiş şekilde tamamen yerleştirilmiştir. Güvenlik olayları, yasal uyumluluk (örn. PCI DSS, GDPR, CIS, HIPAA, NIST 800-53), tespit edilen güvenlik açığı bulunan uygulamalar, dosya bütünlüğü izleme verileri, yapılandırma değerlendirme sonuçları, bulut altyapısı izleme olayları için kullanıma hazır panoları içerir.

**Wazuh Dashboard:** Bu merkezi bileşen, verilerin madenciliği, analizi ve görselleştirilmesi için esnek ve sezgisel bir web arayüzüdür. Kullanıma hazır panolar sağlayarak kullanıcı arayüzünde sorunsuz bir şekilde gezinmenizi sağlar. Kullanıcılar, güvenlik olaylarını hızla görselleştirebilir, güvenlik açığı bulunan uygulamaları tespit edebilir, dosya bütünlüğü izleme verilerini, yapılandırma değerlendirme sonuçlarını, bulut altyapısı izleme olaylarını ve PCI DSS, GDPR, CIS, HIPAA ve NIST 800-53 standartları gibi yasal uyumlulukları tespit edebilir.

**Wazuh Indexer:** Wazuh dizin oluşturucu, yüksek düzeyde ölçeklenebilir, tam metin arama ve analiz motorudur. Bu Wazuh merkezi bileşeni, Wazuh sunucusu tarafından oluşturulan uyarıları indeksler ve depolar ve neredeyse gerçek zamanlı veri arama ve analitik yetenekleri sağlar.

**Wazuh Agent:** Wazuh aracı çoklu platformdur ve kullanıcının izlemek istediği ana bilgisayarlarda çalışır. Wazuh yöneticisi ile iletişim kurar, şifreli ve kimliği doğrulanmış bir kanal aracılığıyla neredeyse gerçek zamanlı olarak veri gönderir. Aracı, performanslarını etkilemeden çok çeşitli farklı

uç noktaları izleme ihtiyacı göz önünde bulundurularak geliştirilmiştir. Ortalama 35 MB RAM gerektirir. Bu nedenle, en popüler işletim sistemlerinde desteklenir.

Wazuh aracı, sisteminizin güvenliğini artırmak için temel özellikler sağlar.

Log collector	Command execution
File integrity monitoring (FIM)	Security configuration assessment (SCA)
System inventory	Malware detection
Active response	Container security
Cloud security	

## WAZUH KURULUMU

Wazuh aracını indirebilmenin birçok alternatif yolu bulunmaktadır. Bu yollardan birincisi ve kendi sayfasında öne çıkarılan kurulum; <https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html> sayfasından adım adım ilerleyerek indirme işlemini tamamlamaktır.

Bu yönteme alternatif olarak şunlar gösterilebilir:

**Docker'da Dağıtım:** Docker, yazılım kapsayıcılarında uygulamalar oluşturmak, teslim etmek ve çalıştırmak için açık bir platformdur. Docker kapsayıcıları, çalıştırmak için gereken her şey dahil olmak üzere yazılımı paketler: kod, çalışma zamanı, sistem araçları, sistem kitaplıklarını ve ayarlar. Docker, uygulamaları altyapıdan ayırmayı sağlar. Bu, kapsayıcının çalıştığı ortamdan bağımsız olarak uygulamanın her zaman aynı şekilde çalışacağını garanti eder. Kapsayıcılar bulutta veya şirket içinde çalışabilir. Wazuh'u, wazuh/wazuh-manager, wazuh/wazuh-indexer ve wazuh/wazuh-dashboard gibi Docker görüntülerini kullanarak kurabilirsiniz. Tüm bu Wazuh Docker görüntülerini Docker hub'ında bulunur.

**Paketlerden Kurulum:** Wazuh yönetici ve aracı, paketlerden kuruluma alternatif olarak kaynaklar aracılığıyla kurulabilir.

**Amazon Makine Görüntüleri (AMI):** Wazuh, önceden oluşturulmuş bir Amazon Machine Image (AMI) sağlar. AMI, Amazon Elastic Compute Cloud (Amazon EC2) içinde sanal bir bilgi işlem ortamı oluşturmak için kullanıma hazır, önceden yapılandırılmış bir şablondur.

Bu alternatif yolların yanı sıra biz bu projede diğer bir alternatif yol olan OVA 4.2 versiyonun kurulumunu tercih ettik.

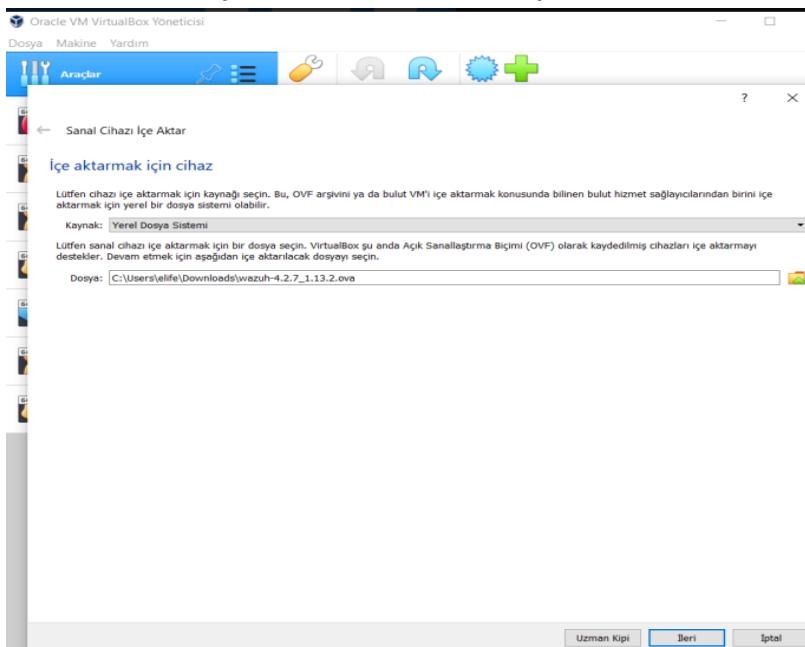
**Sanal Makine (OVA):** Wazuh, VirtualBox veya diğer OVA uyumlu sanallaştırma sistemlerini kullanarak doğrudan içe aktarabileceğiniz önceden oluşturulmuş bir sanal makine görüntüsü (OVA) sağlar. Bu VM'nin yalnızca 64 bit sistemlerde çalıştığını ve ürünün yüksek kullanılabilirliğini ve ölçeklenebilirliğini sağlamadığını dikkate alın.

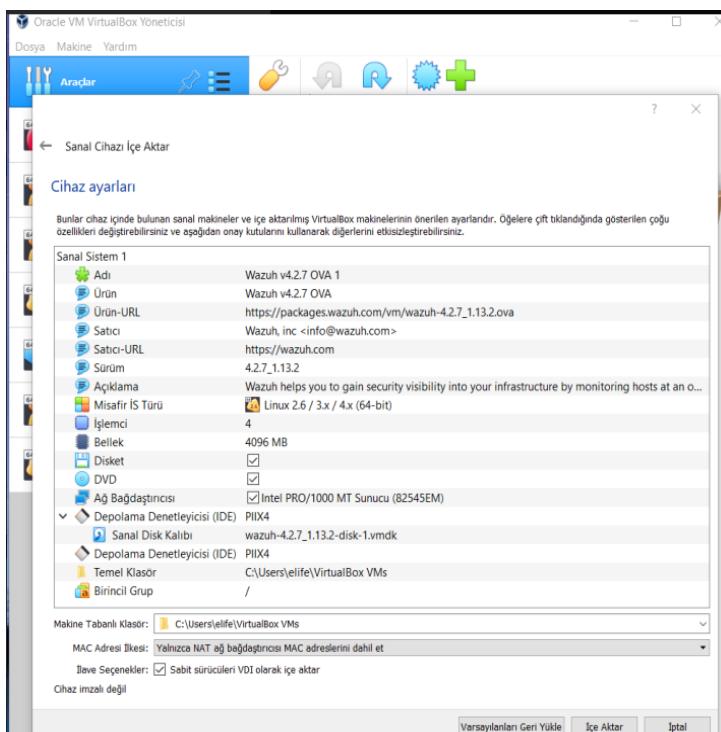
**OVA** aşağıdaki bileşenleri içermektedir:

- CentOS 7
- Wazuh manager: 4.2.7
- Open Distro for Elasticsearch: 1.13.2
- Filebeat-OSS: 7.10.2
- Kibana: 7.10.2
- Wazuh Kibana plugin: 4.2.7-7.10.2

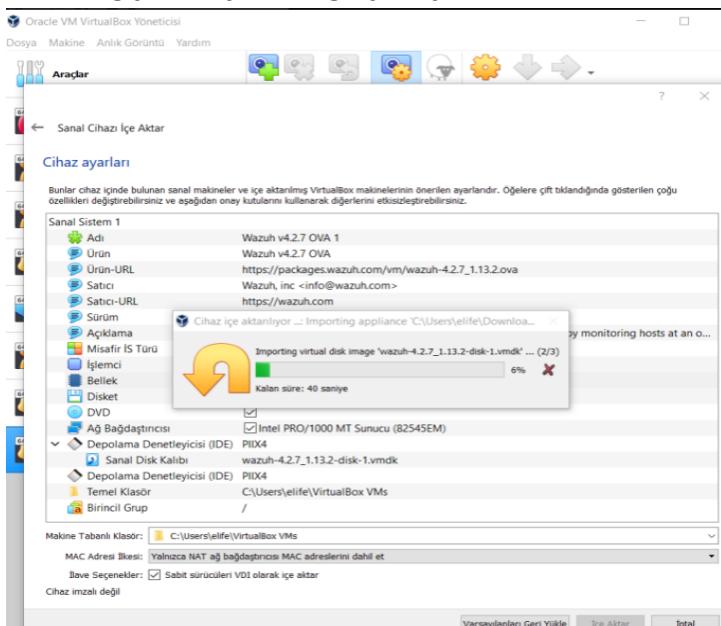
Projemizde yukarıda bahsedilen OVA indirildikten sonra kurulum için şu aşamaları izledik:

**1. İndirilen OVA dosyası VirtualBox üzerine import edilir.**

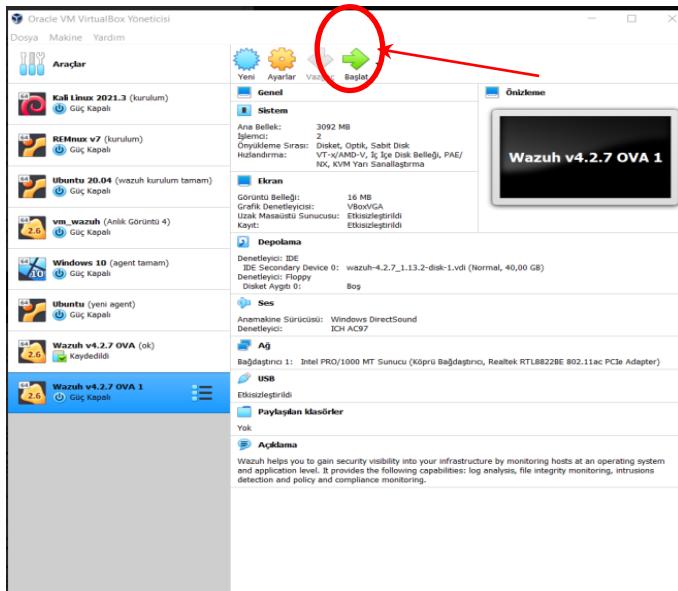




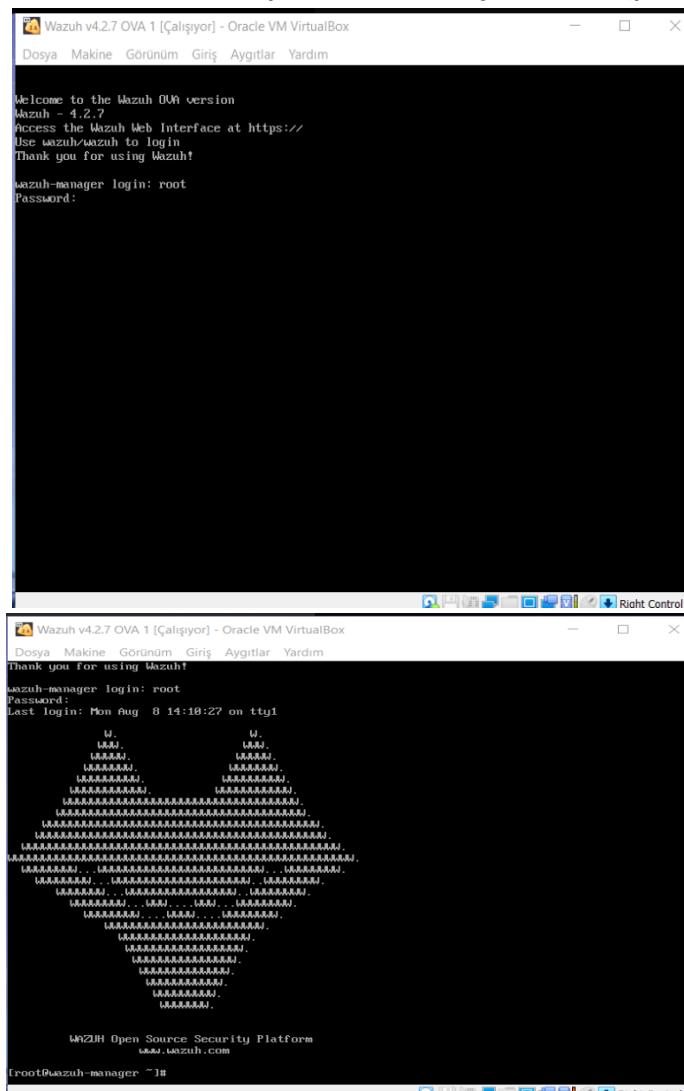
**Kurulum aşamasında varsayılan değerler değiştirilebilir.İçe aktarma işlemi yapıldıktan sonra değiştirme işlemleri gerçekleştirilemez.**



## 2. Wazuh OVA çalıştırılır.



## 3. Açılan pencerede login yapabilmek için wazuh-manager login kısmına "root" , Password kısmına ise "wazuh" yazılır ve enter tuşuna basılır.(password yazılrıken ekranda görünmez)



4. Sistem açıldıktan sonra “`systemctl status kibana`”, “`systemctl status wazuh-manager`”, “`systemctl status elasticsearch`” yazılarak kibana, wazuh-manager ve elasticsearch ün aktif bir şekilde çalışıyor olması gerekmektedir.  
 Eger durum aktif degil ise örneğin “`systemctl start elasticsearch`” yazılıp tekrar elasticsearch ün durumunun kontrol edilmesi gerekmektedir.

```

Wazuh v4.2.7 OVA 1 [Çalışıyor] - Oracle VM VirtualBox
Dosya Makine Görümlü Giriş Aygıtlar Yardım

WAZUH Open-Source Security Platform
www.wazuh.com

root@wazuh-manager:~# systemctl start wazuh-manager
root@wazuh-manager:~# systemctl status wazuh-manager
● wazuh-manager.service - Wazuh Manager
   Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-08-08 11:23:41 UTC; 7s ago
     Docs: https://www.wazuh.com
    Process: 826 ExecStart=/usr/bin/wazuh-control start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/wazuh-manager.service
           ├─1452 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
           ├─1494 /var/ossec/bin/wazuh-authd
           ├─1518 /var/ossec/bin/wazuh-db
           ├─1534 /var/ossec/bin/wazuh-execd
           ├─1551 /var/ossec/bin/wazuh-analysisd
           ├─1561 /var/ossec/bin/wazuh-syscheckd
           ├─1611 /var/ossec/bin/wazuh-remoted...
           ├─1643 /var/ossec/bin/wazuh-logcollector
           ├─1663 /var/ossec/bin/wazuh-monitord
           ├─1685 /var/ossec/bin/wazuh-modulesd
           └─1842 /usr/bin/python /usr/bin/yum check-update

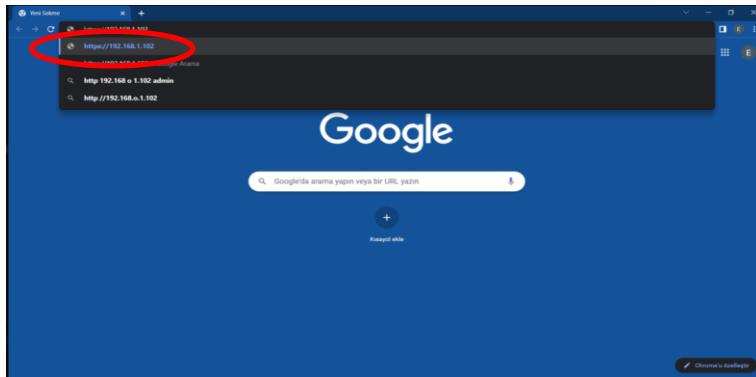
Aug 08 11:29:29 wazuh-manager env[826]: Started wazuh-authd...
Aug 08 11:29:30 wazuh-manager env[826]: Started wazuh-db...
Aug 08 11:29:31 wazuh-manager env[826]: Started wazuh-execd...
Aug 08 11:29:32 wazuh-manager env[826]: Started wazuh-analysisd...
Aug 08 11:29:33 wazuh-manager env[826]: Started wazuh-syscheckd...
Aug 08 11:29:34 wazuh-manager env[826]: Started wazuh-remoted...
Aug 08 11:29:36 wazuh-manager env[826]: Started wazuh-logcollector
Aug 08 11:29:37 wazuh-manager env[826]: Started wazuh-monitord...
Aug 08 11:29:38 wazuh-manager env[826]: Started wazuh-modulesd...
Aug 08 11:29:48 wazuh-manager env[826]: Completed.
root@wazuh-manager:~# 

[root@wazuh-manager ~]# systemctl start elasticsearch
[root@wazuh-manager ~]# systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/etc/systemd/system/elasticsearch.service; enabled; vendor preset: disabled)
   Drop-In: /etc/systemd/system/elasticsearch.service.d
             └─elasticsearch.conf
     Active: active (running) since Mon 2022-08-08 11:29:47 UTC; 1min 28s ago
       Docs: https://www.elastic.co
      Main PID: 828 (java)
     CGroup: /system.slice/elasticsearch.service
             └─828 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl...
```

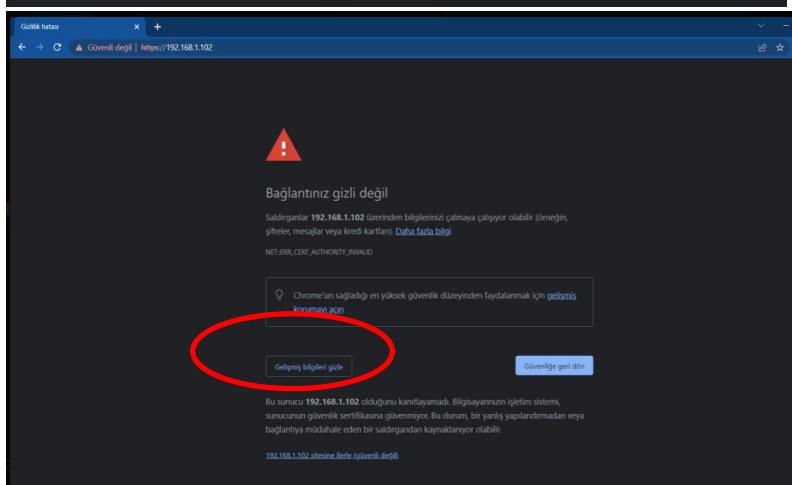
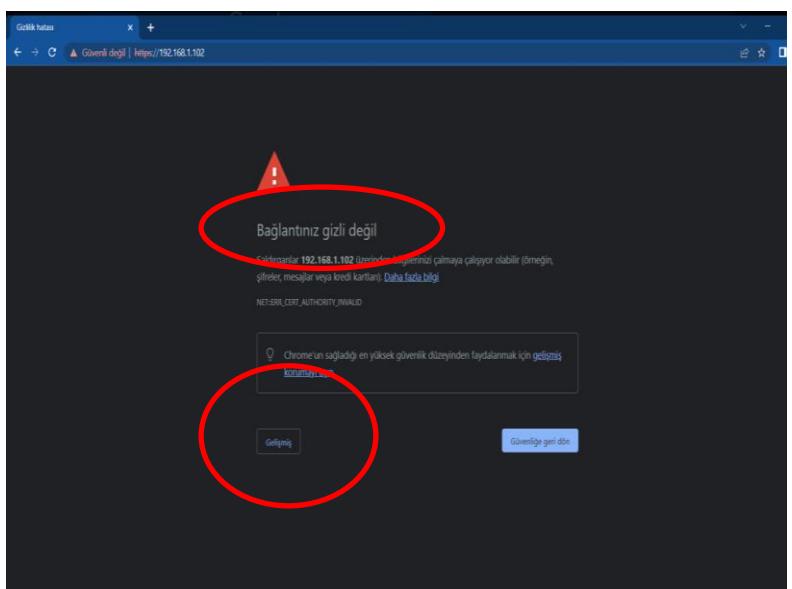
5. Wazuh arayüzüne ulaşabilmesi için “ip addr” yazılarak bi rip adresi alınır ve bu ip adresi tarayıcıya [https://alinan\\_ip\\_adresi](https://alinan_ip_adresi) şeklinde yazılır.

```

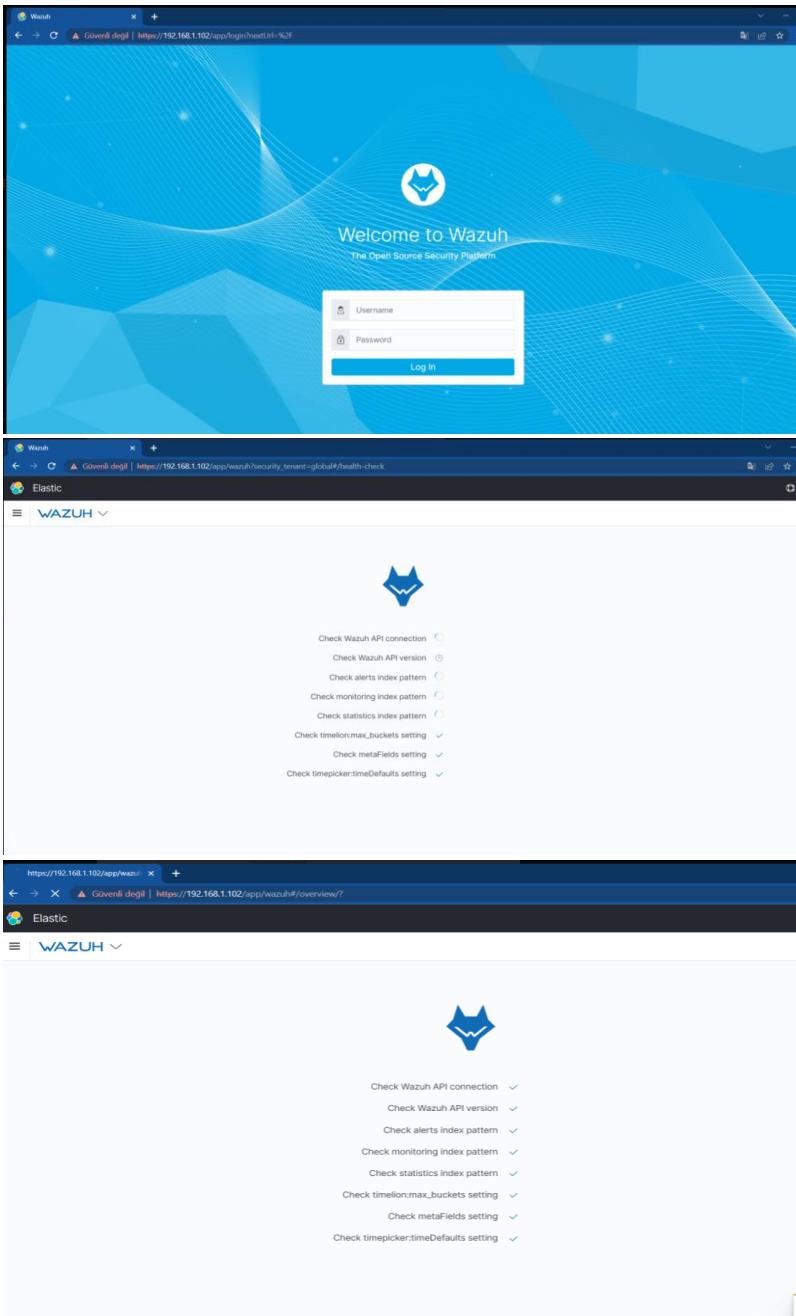
root@wazuh-manager:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:00:27:15:a5:65 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.102/24 brd 192.168.1.255 scope global dynamic eth0
        valid_lft 3351sec preferred_lft 3351sec
        inet6 fe80::a00:27ff:fe15:a565/64 scope link
            valid_lft forever preferred_lft forever
root@wazuh-manager:~#
```



6. Açılan sayfada eğer “bağlantınız gizli değildir” gibi bir uyarıla karşılaşıldığında bu uyarı dikkate alınmamalıdır.“Gelişmiş bilgileri gizle” butonuna basılarak “alınan ip adresine ilerle” butonuna tıklanır.

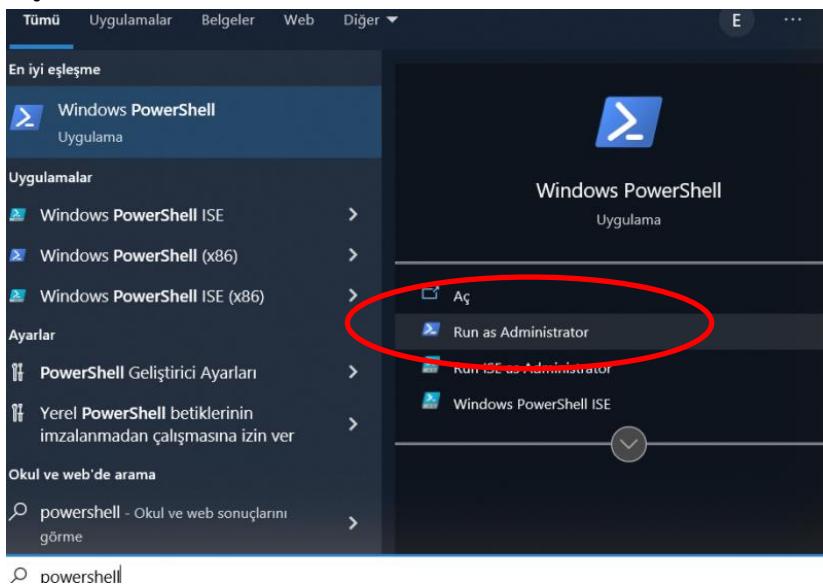


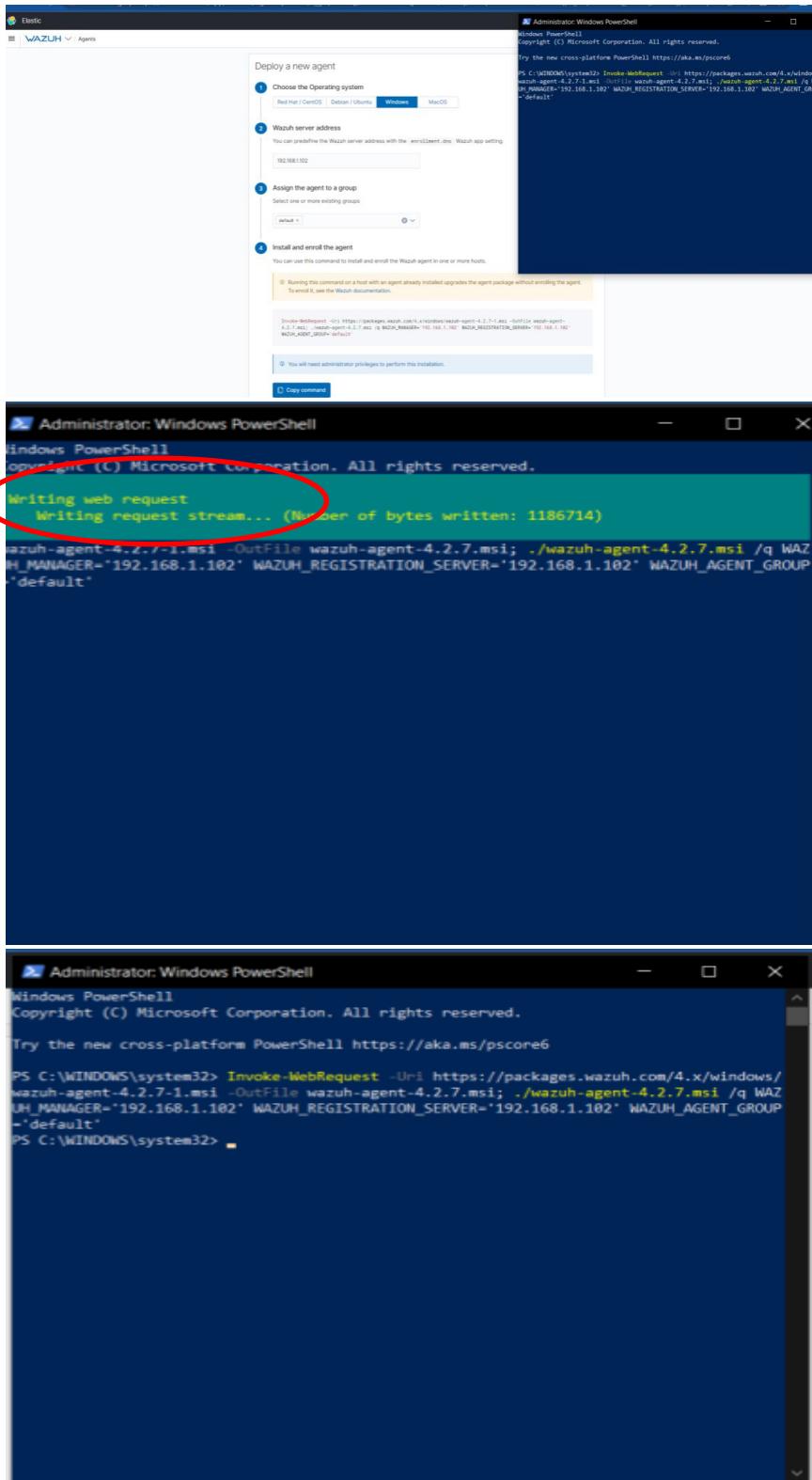
7. Açılan arayüzde “kibana server is not ready yet” gibi bir hata verildiğinde 4. Aşamaya geri dönülmeli ve statusler control edilmelidir.Bir hata ile karşılaşıldığını durumda açılan Wazuh arayüzüne “username” ve “password” kısımlarının ikisine de “wazuh” yazılır ve sisteme giriş yapılır. Açılan sayfada tüm bağlantıların tam olması gerekmektedir.



- 8. Bütün bağlantılar tamamlandıktan sonra wazuh dashboard'a giriş otomatik olarak yapılır. Bu aşamalardan sonra agent ekleme işlemlerine geçilebilir. İlk olarak "add agent" kısmına tıklanır ve çıkan sayfadan hangi işletim sistemine agent eklemek istiyorsak o işletim sistemi seçilir. Daha sonra "wazuh address server" kısmına daha önceden aldığımız ip adresi yazılır. Son olarak "install and enroll agent" kısmında bulunan komut kopyalanıp hangi işletim sistemine agent kurulmak isteniyorsa o işletim sisteminin komut satırına yapıştırılır ve enter tuşuna basılır.**

- 9. Window işletim sistemi için “PowerShell” “run as administrator” butonuna tıklanır ardından cihazda değişiklik yapılmaya onayı verilir ve alınan komut buraya yapıştırılarak enter tuşuna basılır.**





- 10. İndirme işlemi tamamlandıktan sonra Window agenta ulaşabilmek için şu yol izlenmelidir:**  
**C:\Program Files (x86). Bu klasör kısmından Windows agentin bulunduğu “ossec-agent” klasörü bulunur ve açılır. Daha sonra ekrana gelen arayüz kısmından “view” sekmesinden “view config” butonuna tıklanır ve açılan sayfadan adress kısmına bize daha önce verilen ip adresi yazılır ve kaydet butonuna tıklanır.Son olarak daha önceden karşımıza çıkan arayüz üzerinde “refresh” butonuna tıklanır ve böylelikle Windows üzerine agent kurma işlemi**

## tamamlanmış olur.

Şu an bu klasöre erişim izniniz yok.  
Bu klasöre kalıcı erişim izni almak için Devam'ı tıklatın.

Ad	Değiştirme tarihi	Tür	Boyut
Common Files	7.12.2019 12:31	Dosya klasörü	
Internet Explorer	6.10.2021 16:49	Dosya klasörü	
Microsoft	27.07.2022 17:51	Dosya klasörü	
Microsoft.NET	7.12.2019 12:31	Dosya klasörü	
<b>ossec-agent</b>	<b>8.08.2022 15:01</b>	<b>Dosya klasörü</b>	
Windows Defender	6.10.2021 16:49	Dosya klasörü	
Windows Mail	6.10.2021 16:49	Dosya klasörü	
Windows Media Player	6.10.2021 16:49	Dosya klasörü	
Windows Multimedia Platform	7.12.2019 17:45	Dosya klasörü	
Windows NT	7.12.2019 17:43	Dosya klasörü	
Windows Photo Viewer	6.10.2021 16:49	Dosya klasörü	
Windows Portable Devices	7.12.2019 17:45	Dosya klasörü	
WindowsPowerShell	7.12.2019 12:31	Dosya klasörü	

Ad	Değiştirme tarihi	Tür	Boyut
Common Files	7.12.2019 12:31	Dosya klasörü	
Internet Explorer	6.10.2021 16:49	Dosya klasörü	
Microsoft	27.07.2022 17:51	Dosya klasörü	
<b>ossec-agent</b>	<b>8.08.2022 15:01</b>	<b>Dosya klasörü</b>	
Windows Defender	6.10.2021 16:49	Dosya klasörü	
Windows Mail	6.10.2021 16:49	Dosya klasörü	
Windows Media Player	6.10.2021 16:49	Dosya klasörü	
Windows Multimedia Platform	7.12.2019 17:45	Dosya klasörü	
Windows NT	7.12.2019 17:43	Dosya klasörü	
Windows Photo Viewer	6.10.2021 16:49	Dosya klasörü	
Windows Portable Devices	7.12.2019 17:45	Dosya klasörü	
WindowsPowerShell	7.12.2019 12:31	Dosya klasörü	

Ad	Değiştirme tarihi	Tür	Boyut
queue	5.08.2022 15:37	Dosya klasörü	
rids	8.08.2022 15:01	Dosya klasörü	
ruleset	5.08.2022 15:37	Dosya klasörü	
shared	5.08.2022 15:38	Dosya klasörü	
syscheck	5.08.2022 15:37	Dosya klasörü	
tmp	8.08.2022 15:02	Dosya klasörü	
upgrade	5.08.2022 15:37	Dosya klasörü	
wodles	5.08.2022 15:37	Dosya klasörü	
<b>_agent_info</b>	<b>8.08.2022 15:00</b>	<b>AGENT_INFO Dosyası</b>	<b>1 KB</b>
<b>agent-auth</b>	<b>30.05.2022 16:00</b>	<b>Uygulama</b>	<b>984 KB</b>
<b>agent-auth.exe.manifest</b>	<b>30.05.2022 13:00</b>	<b>MANIFEST Dosyası</b>	<b>1 KB</b>
<b>client.keys</b>	<b>8.08.2022 15:01</b>	<b>KEYS Dosyası</b>	<b>1 KB</b>
<b>dbsync.dll</b>	<b>30.05.2022 13:55</b>	<b>Uygulama uzantısı</b>	<b>1.287 KB</b>
<b>help</b>	<b>30.05.2022 13:55</b>	<b>Metin Belgesi</b>	<b>2 KB</b>
<b>internal_options.conf</b>	<b>30.05.2022 13:55</b>	<b>CONF Dosyası</b>	<b>14 KB</b>
<b>libgc_c_5jf-1.dll</b>	<b>30.05.2022 13:54</b>	<b>Uygulama uzantısı</b>	<b>1.090 KB</b>
<b>libwazuhext.dll</b>	<b>30.05.2022 13:54</b>	<b>Uygulama uzantısı</b>	<b>5.506 KB</b>
<b>libwazuhshared.dll</b>	<b>30.05.2022 13:55</b>	<b>Uygulama uzantısı</b>	<b>820 KB</b>
<b>libwinguide-1.dll</b>	<b>30.05.2022 13:54</b>	<b>Uygulama uzantısı</b>	<b>522 KB</b>
<b>LICENSE</b>	<b>30.05.2022 13:55</b>	<b>Metin Belgesi</b>	<b>25 KB</b>
<b>local_internal_options.conf</b>	<b>30.05.2022 13:55</b>	<b>CONF Dosyası</b>	<b>1 KB</b>
<b>manage_agents</b>	<b>30.05.2022 16:00</b>	<b>Uygulama</b>	<b>980 KB</b>
<b>ossec.conf</b>	<b>5.08.2022 15:37</b>	<b>CONF Dosyası</b>	<b>10 KB</b>
<b>ossec</b>	<b>8.08.2022 15:02</b>	<b>Metin Belgesi</b>	<b>24 KB</b>
<b>REVISION</b>	<b>30.05.2022 13:55</b>	<b>Dosya</b>	<b>1 KB</b>
<b>rsync.dll</b>	<b>30.05.2022 13:55</b>	<b>Uygulama uzantısı</b>	<b>1.152 KB</b>
<b>syscollector.dll</b>	<b>30.05.2022 13:55</b>	<b>Uygulama uzantısı</b>	<b>1.322 KB</b>
<b>nyinfo.dll</b>	<b>30.05.2022 13:55</b>	<b>Uygulama uzantısı</b>	<b>1.237 KB</b>
<b>VERSION</b>	<b>30.05.2022 13:55</b>	<b>Dosya</b>	<b>1 KB</b>
<b>vista_sec</b>	<b>30.05.2022 13:00</b>	<b>Metin Belgesi</b>	<b>92 KB</b>
<b>wazuh-agent</b>	<b>30.05.2022 16:00</b>	<b>Uygulama</b>	<b>1.798 KB</b>
<b>wazuh-agent.state</b>	<b>8.08.2022 15:00</b>	<b>STATE Dosyası</b>	<b>1 KB</b>
<b>wazuh-logcollector.state</b>	<b>8.08.2022 15:03</b>	<b>STATE Dosyası</b>	<b>2 KB</b>
<b>win32ui</b>	<b>30.05.2022 16:00</b>	<b>Uygulama</b>	<b>909 KB</b>
<b>win32ui.exe.manifest</b>	<b>30.05.2022 13:00</b>	<b>MANIFEST Dosyası</b>	<b>1 KB</b>

The screenshot displays three windows related to Wazuh Agent Manager:

- Wazuh Agent Manager (Main Window):** Shows a file explorer view of agent files. A modal window is open showing "Status: Running". It includes fields for "Manager IP" (192.168.1.102) and "Authentication key" (MDAyERFU0UT1ATEVMUkU). Buttons for "Save" and "Refresh" are present.
- Wazuh Agent Manager (Sub-Window):** A smaller window titled "Manage" with tabs for "View Logs" and "View Config". It also shows "Status: Running".
- ossec.conf - Not Deferrable (Code Editor):** Displays the configuration file content. Key sections include:
  - Wazuh - Agent - Default configuration for Windows
  - ossec\_config section containing client and server configurations.
  - client\_buffer options section.
  - Log analysis section with localfile and log\_format configurations.

**11. Tüm işlemler tamamlandıktan sonra wazuh arayüzüne girildiğinde agentin kurulu olduğu görülebilecektir.**

**12.** Alınan ip adresinden sonra wazuh arayüzünde “bu siteye ulaşılamıyor” hatası wazuh ova kısmında bize verilen ip adresi dinamik bi rip adresi olduğundan ve değişebildiğinden bu hata ile karşılaşılabilir. Bu durumda ip add rile yeni bi ip afresi alınıp süreç kontrol altına alınabilir.

**13.** Ubuntu işletim sistemi üzerine agent kurulumu içinde süreç aynı şekilde işlemektedir.Ubuntu üzerine agent kurmak isteyen kullanıcılar yazılan aşamaları aynı şekilde yapabilirler.

**14.** Tüm aşamalar tamamlandıktan sonra wazuh aracında “security event” genel görünümü aşağıdaki gibidir.

**WAZUH**

Overview Management Agents Dev tools Manager

### Alerts summary

Rule ID	Description	Level	Count
554	File added to the system	5	91
550	Integrity checksum changed	7	33
6105	Windows Logon Success	3	23
6137	Windows User Logout	3	4
62115	User account changed	8	3
6152	Windows System error event	5	2
65646	License Activation (idle event) failed	5	2
61104	Service startup type was changed	3	1
62055	The database engine is starting a new instance	3	1
62795	The database engine attached a database	3	1

Export: Raw ▾ Formatted ▾

### Groups summary

Group	Count
ossec	125
syscheck	124
windows	41
windows_security	30
authentication_success	23
window_application	8
account_changed	3
ica	2
window_systemsystem_error	2
window_systempolicy_changed	1

Export: Raw ▾ Formatted ▾

**WAZUH**

Overview Management Agents Dev tools Manager

### Most active users

No results found

modified (26.67%)    added (73.33%)

Events

modified    added

### Files added

No results found

● HKEY\_LOCAL\_... ● HKEY\_LOCAL\_... ● HKEY\_LOCAL\_... ● HKEY\_LOCAL\_... ● HKEY\_LOCAL\_...

### Files modified

No results found

● HKEY\_LOCAL\_... ● HKEY\_LOCAL\_... ● HKEY\_LOCAL\_... ● HKEY\_LOCAL\_... ● HKEY\_LOCAL\_...

### Files deleted

No results found

● HKEY\_LOCAL\_... ● HKEY\_LOCAL\_... ● HKEY\_LOCAL\_... ● HKEY\_LOCAL\_... ● HKEY\_LOCAL\_...

### Alerts summary

File	Description	Count
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RdpEnum\Parameters	File added to the system.	1
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RdpEnum	File added to the system.	1
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RemoteRegistry\TiggerInfo\#	File added to the system.	1
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RemoteRegistry\Parameters	File added to the system.	1
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RemoteRegistry	File added to the system.	1

**WAZUH**

Overview Management Agents Dev tools Manager

### Network interfaces

Name	MAC	State	MTU	Type
Ethernet	00:0c:27:40:42:b4	up	1500	ethernet

### Network ports

Process	Local IP	Local port	State	Protocol
wmifind.exe	0.0.0.0	49000	listening	tcp
wmifind.exe	...	49005	listening	tcp
oscheck.exe	0.0.0.0	120	listening	tcp
oscheck.exe	0.0.0.0	49000	listening	tcp
oscheck.exe	...	49007	listening	tcp
oscheck.exe	...	120	listening	tcp
oscheck.exe	...	49008	listening	tcp
oscheck.exe	...	49007	listening	tcp
spoolsv.exe	0.0.0.0	49000	listening	tcp
spoolsv.exe	...	49000	listening	tcp

Rows per page: 10 ▾ 1 2 3

### Network settings

Interface	Address	Netmask	Protocol	Broadcast
Ethernet	10.0.2.15	255.255.255.0	IPv4	10.0.2.255
Ethernet	fc00:214b:6bbb:93ff:ff:ff	ff:ff:ff:ff:ff:ff	IPv6	-

### Windows updates

Update code
ServicingStack
K300000000
K300043311
K300030791
DotNetFxSetup

### Packages

Filter packages:

Name	Architecture	Version	Vendor
Oracle VM VirtualBox Guest Additions 0.1.34	x86_64	4.1.34.0	Oracle Corporation
Windows PC System Durango Drivers	x86_64	3.6.2204.60001	Microsoft Corporation
Microsoft Update Health Tools	x86_64	3.67.0.0	Microsoft Corporation
Microsoft Edge	arm	103.0.104.71	Microsoft Corporation
Microsoft Edge Update	arm	1.3.100.21	-
Wazuh Agent	arm	3.11.4	Wazuh, Inc.

Search:

Export: Raw ▾ Formatted ▾

## CLOUD ORTAMINDA WAZUH KURULUMU

Wazuh aracı bir VirtualBox üzerinde kurulduğu gibi bir cloud ortamı üzerine de kurulabilir.Wazuh aracı genel olarak şu gereksinimlere sahip olmalıdır;

Agents	CPU	RAM	Storage (90 days)
1-25	4 vCPU	8 GiB	50 GB
25-50	8 vCPU	8 GiB	100 GB
50-100	8 vCPU	8 GiB	200 GB

Bu projede Wazuh Ova`yı kullandığımız zaman sistem yavaşlaması,kasılması gibi olaylarla karşılaştık,bu yüzden bu sorunları önlemek için ve ekip üyelerinin her birinin ayrı ayrı wazuh ovayı indirmesinin önüne geçebilmek için sanal sunucu sağlayan linode adında bir cloud ortamına wazuh aracını kurmayı tercih ettim.

### LINODE ÜZERİNDE WAZUH KURULUMU:

1. <https://cloud.linode.com/linodes> sitesine gidilerek cloud ortamını kullanabilmek için hesap açılır.Linode üzerinde hesap açılırken ödeme bilgileri kısmında sanal kart kullanıldığı takdirde Linode sistemi otomatik olarak hesabı reddetmektedir.Dolayısıyla bu kısımda fiziksel kart bilgileri kullanılmalıdır.Hesap açmak için başvuru yapıldıktan sonra gerekli koşullar sağlanıldığı takdirde hesap oluşturulur.
- 2.Hesaba giriş yapıldıktan sonra `Linodes` sekmesinden `Create Linode` butonuna tıklanır.

Enable Linode Backups to protect your data and recover quickly in an emergency.

Linodes

Label ^	Status ^	Plan ^	IP Address ^	Region ^	Last Backup ^	...
wazuh	Running	Linode 4 GB	139.162.192.250	London, UK	Never	

You have used 0.04% of your [Monthly Network Transfer Pool](#).

v1.73.0 API Reference Provide Feedback

**3.Açılan sayfadan “marketplace” sekmesine gidilir.Bu kısımda Linode üzerinde kullanılabilen araçlar bulunmaktadır.Bu araçlar içerisinde Wazuh aracı seçilir.**

Saltcorn		ServerWand		Shadowsocks	
Splunk		Terraria		TF2	
Uptime Kuma		UTunnel VPN		Valheim	
VictoriaMetrics Single		Virtualmin		VS Code Server	
WarpSpeed		<b>Wazuh</b>		Webmin	
Webuzo		WireGuard®		WooCommerce	
Yacht		Zabbix			

Select Image

**4.Açılan sayfada bulunan “Wazuh options” kısmında bulunan bilgiler doldurulur.**

The screenshot shows two stacked configuration screens from the Linode setup wizard.

**Wazuh Options:**

- Email address (for the Let's Encrypt SSL certificate) (required): user@domain.tld
- Advanced Options:** These fields are additional configuration options and are not required for creation.
- The limited sudo user to be created for the Linode: (empty input field)
- The password for the limited sudo user: an0th3r\_s3cure\_p4ssw0rd (Weak)
- The SSH Public Key that will be used to access the Linode: (empty input field)
- Disable root access over SSH? (radio buttons: Yes, No - No is selected)

**Your Linode API token:** This is needed to create your WordPress server's DNS records.

- Enter a password: (empty input field)
- Subdomain: (empty input field)
- The subdomain for the DNS record: www (Requires Domain)
- Domain: (empty input field)
- The domain for the DNS record: example.com (Requires API token)

**Select an Image:**

- Images: Ubuntu 20.04 LTS

**Region:**

- You can use [our speedtest page](#) to find the best region for your current location.
- Region: Select a Region

**5.Bilgiler doldurulan sonra “Linodeplan” kısmında “Shared Cpu” bölümüne gidilerek CPU ve RAM seçimi yapılır.**

The screenshot shows the Linode Plan selection screen with the "Shared CPU" tab selected.

Shared CPU instances are good for medium-duty workloads and are a good mix of performance, resources, and price.

	Monthly	Hourly	RAM	CPUs	Storage	Transfer	Network In / Out
Nanode 1 GB	\$5	\$0.0075	1 GB	1	25 GB	1 TB	40 Gbps / 1 Gbps
Linode 2 GB	\$10	\$0.015	2 GB	1	50 GB	2 TB	40 Gbps / 2 Gbps
Linode 4 GB	\$20	\$0.03	4 GB	2	80 GB	4 TB	40 Gbps / 4 Gbps
Linode 8 GB	\$40	\$0.06	8 GB	4	160 GB	5 TB	40 Gbps / 5 Gbps
Linode 16 GB	\$80	\$0.12	16 GB	6	320 GB	8 TB	40 Gbps / 6 Gbps
Linode 32 GB	\$160	\$0.24	32 GB	8	640 GB	16 TB	40 Gbps / 7 Gbps
Linode 64 GB	\$320	\$0.48	64 GB	16	1280 GB	20 TB	40 Gbps / 9 Gbps
Linode 96 GB	\$480	\$0.72	96 GB	20	1920 GB	20 TB	40 Gbps / 10 Gbps
Linode 128 GB	\$640	\$0.96	128 GB	24	2560 GB	20 TB	40 Gbps / 11 Gbps

**6.Bütün işlemler tamamlandıktan sonra wazuh aracı Linode üzerine kurulmuş olur. Wazuh arayüzüne kullanıcıların ulaşabilmesi için bir “ip” adresi verilir.Bu ip adresi tarayıcı üzerine başına https:// yazılarak aratılır.**

Enable Linode Backups to protect your data and recover quickly in an emergency.

Linodes

Label	Status	Plan	IP Address	Region	Last Backup	⋮
wazuh	Running	Linode 4 GB	139.162.192.250	London, UK	Never	...

You have used 0.04% of your Monthly Network Transfer Pool.

Docs Create Linode Download CSV

7. Açılan sayfada eğer “bağlantınız gizli değildir” gibi bir uyarıla karşılaşıldığında bu uyarı dikkate alınmamalıdır.”Gelişmiş bilgileri gizle” butonuna basılarak “alınan ip adresine ilerle” butonuna tıklanır.

Güvenlik hatası

⚠️ Gözleme değil | https://192.168.1.102

Bağlantınız gizli değil

Saldırıya 192.168.1.102 üzerinden bilgilerinizi almak isteyen bir saldırgan var. (örneğin, şifreler, mesajlar veya kredi kartları) [Daha fazla bilgi](#)

NET-ERR-CERT-AUTHORITY-INVALID

Chrome'un sağladığı en yüksek güvenlik düzeyinden faydalamarak için [gelişmiş konumaya geç](#)

Gizle Gizleme geçti

Güvenlik hatası

⚠️ Gözleme değil | https://192.168.1.102

Bağlantınız gizli değil

Saldırıya 192.168.1.102 üzerinden bilgilerinizi almak isteyen bir saldırgan var. (örneğin, şifreler, mesajlar veya kredi kartları) [Daha fazla bilgi](#)

NET-ERR-CERT-AUTHORITY-INVALID

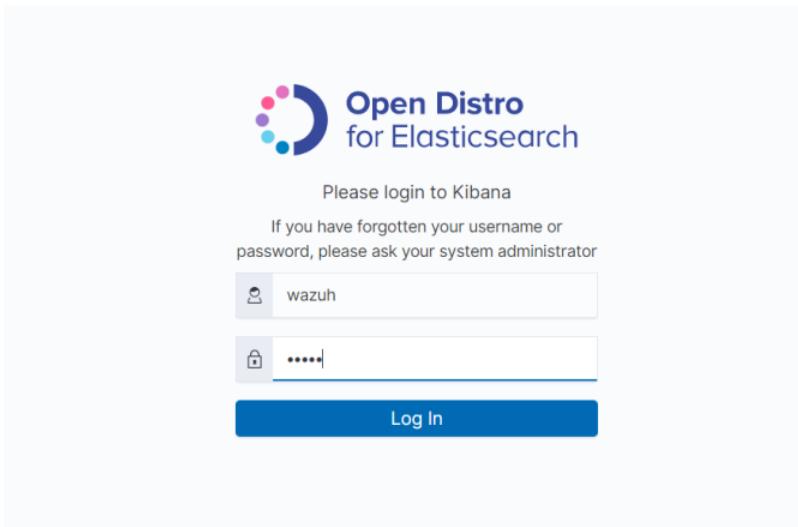
Chrome'un sağladığı en yüksek güvenlik düzeyinden faydalamarak için [gelişmiş konumaya geç](#)

Gizle Gizleme geçti

Bu sunucu 192.168.1.102 olduğunu kanıtlamadı. Bilgisayarınızın işletim sistemi, sunucunun güvenilirliğini sertifikasını göremiyor. Bu durum, bir yanlış yapılandırmadan veya bağlantıya mütakalle eden bir saldırganın kaynaklandığı olabilir.

192.168.1.102 sitenize direkt (gizli değil)

8. Açılan sayfada wazuh aracına giriş yapmak için username ve password kısımlarına “wazuh” yazılır ve sisteme giriş yapılır.



## 9. Wazuh agent kurma kısmı wazuh ova kurma kısmında anlatıldığı gibidir.

ID	Name	IP	Group(s)	OS	Cluster node	Version	Registration date	Last keep alive	Status	Actions	
001	DESKTOP-LELREBS	10.0.2.15	default	Microsoft Windows 10...	node01	v4.3.6	Jan 1, 1970 @...	Aug 12, 2022 @...	● disconnected		
002	elf-VirtualBox	10.0.2.15	default	Ubuntu 20.04.4 LTS	node01	v4.3.6	Aug 11, 2022 @...	Aug 11, 2022 @...	● disconnected		
003	compeng	10.0.2.15	default	Ubuntu 20.04.4 LTS	node01	v4.3.6	Aug 11, 2022 @...	Aug 13, 2022 @...	● disconnected		
004	DESKTOP-UQEOKRL	10.0.2.15	default	Microsoft Windows 10...	node01	v4.3.6	Aug 12, 2022 @...	Aug 12, 2022 @...	● disconnected		

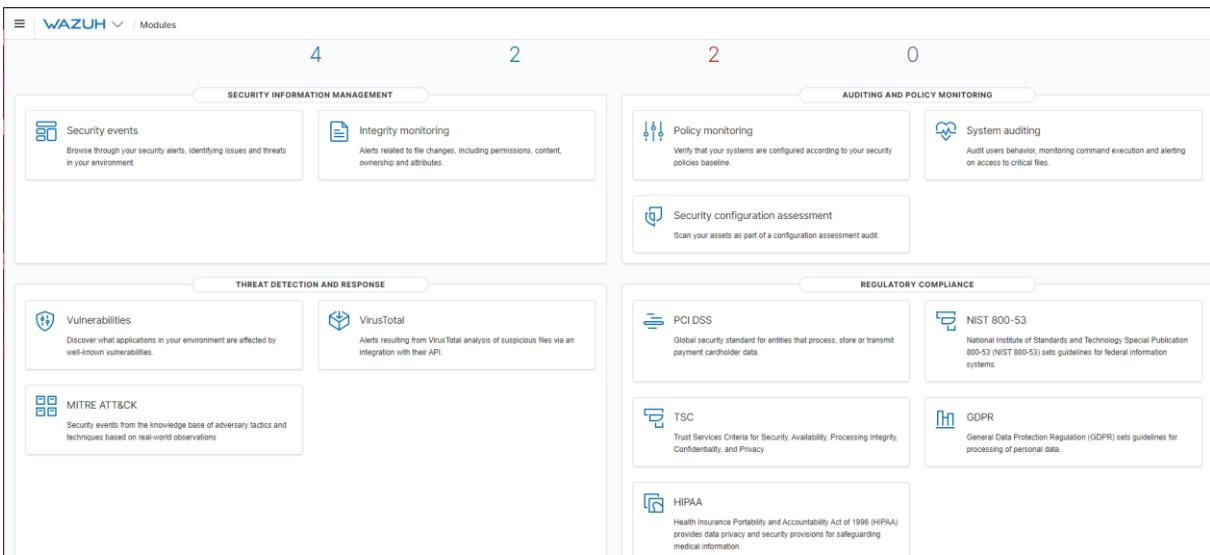
# WAZUH MODÜLLERİ

## 1. Security Event

## 2. Integrity Monitoring

## 3. Vulnerabilities

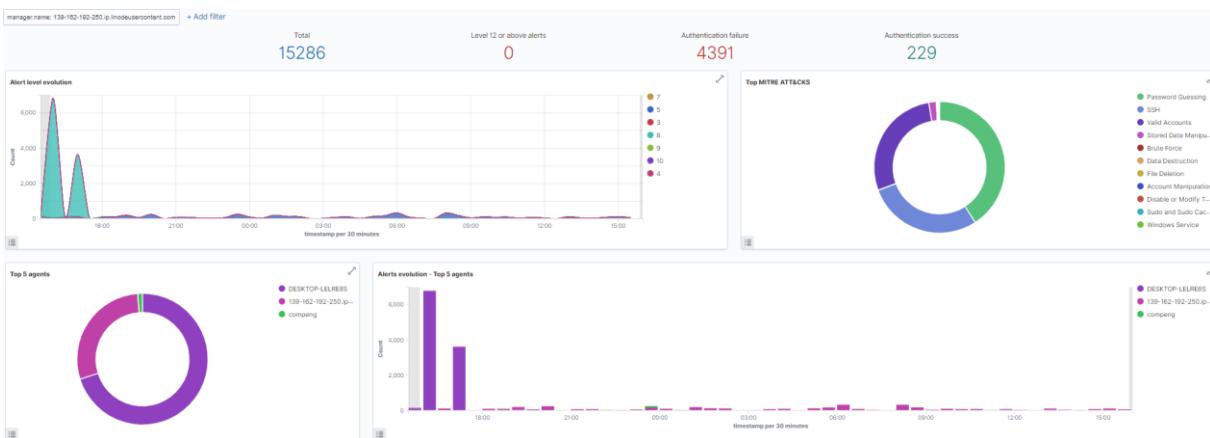
## 4. MITRE ATT&CK



## 1. SECURITY EVENT:

Ortamdaki sorunları ve tehitleri belirleyerek güvenlik uyarılarında bulunur. 2 bileşenden oluşur. Dasboard ve Events.

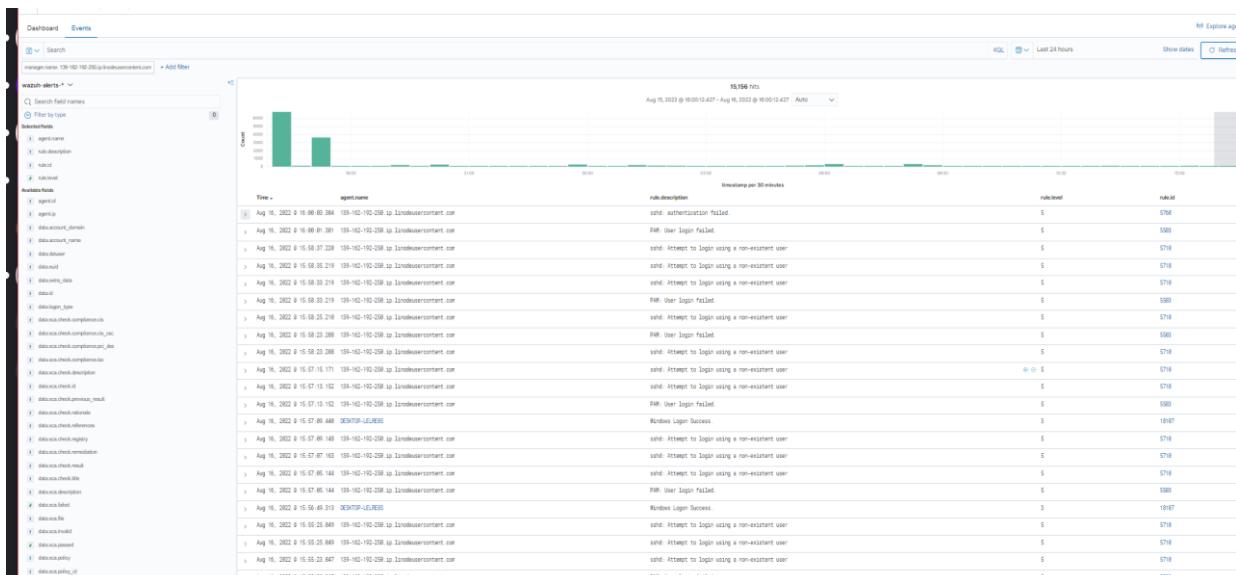
Dashboard kısmında verilen uyarıların ve bulunan tehitler daha çok grafiksel olara gösterillir ve Güvenlik uyarıları bulunur, bu uyarıları tablo, JSON ve rule şeklinde bu kısımda inceleyebiliriz.



Security Alerts							
Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Aug 16, 2022 @ 15:52:26.886	000	139-162-192-250.ip.linodeusercontent.com	T1110.001 T1078	T1021.004	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access sshd: Attempt to login using a non-existent user	5	5710
> Aug 16, 2022 @ 15:52:24.894	000	139-162-192-250.ip.linodeusercontent.com	T1110.001 T1078	T1021.004	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access sshd: Attempt to login using a non-existent user	5	5710
> Aug 16, 2022 @ 15:52:20.879	000	139-162-192-250.ip.linodeusercontent.com	T1110.001 T1078	T1021.004	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access sshd: Attempt to login using a non-existent user	5	5710
> Aug 16, 2022 @ 15:52:20.879	000	139-162-192-250.ip.linodeusercontent.com	T1110.001		Credential Access PAM: User login failed.	5	5503
> Aug 16, 2022 @ 15:51:58.859	000	139-162-192-250.ip.linodeusercontent.com	T1110.001	T1021.004	Credential Access, Lateral Movement sshd: authentication failed.	5	5760
> Aug 16, 2022 @ 15:51:56.856	000	139-162-192-250.ip.linodeusercontent.com	T1110.001		Credential Access PAM: User login failed.	5	5503
> Aug 16, 2022 @ 15:51:30.831	000	139-162-192-250.ip.linodeusercontent.com	T1110.001	T1021.004	Credential Access, Lateral Movement sshd: authentication failed.	5	5760
> Aug 16, 2022 @ 15:51:26.827	000	139-162-192-250.ip.linodeusercontent.com	T1110.001		Credential Access PAM: User login failed.	5	5503
> Aug 16, 2022 @ 15:51:02.804	000	139-162-192-250.ip.linodeusercontent.com	T1110.001 T1078	T1021.004	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access sshd: Attempt to login using a non-existent user	5	5710
> Aug 16, 2022 @ 15:51:02.804	000	139-162-192-250.ip.linodeusercontent.com	T1110.001 T1078	T1021.004	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access sshd: Attempt to login using a non-existent user	5	5710

Table	JSON	Rule
agent.name	139-162-192-250.ip.linodeusercontent.com	T1110.001 T1021.004
agent.id	000	T1078
manager.name	139-162-192-250.ip.linodeusercontent.com	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access
rule.mail	false	sshd: Attempt to login using a non-existent user
rule.level	5	
rule.hipaa	164.312.b	
rule.pci_dss	10.2.4, 10.2.5, 10.6.1	
rule.tsc	C06.1, C06.8, CC7.2, CC7.3	
rule.description	sshd: Attempt to login using a non-existent user	
rule.groups	syslog, sshd, authentication_tailed, invalid_login	
rule.mitre_800_53	AU.14, AC.7, AU.6	
rule.garpr	N.35.7.0, N.32.2	
rule.firetimes	100	
rule.mitre_technique	Password Guessing, SSH, Valid Accounts	
rule.mitre_id	T1110.001, T1021.004, T1078	
rule.mitre_tactic	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	
rule.id	5710	
rule.gpg13	7.1	
decoder.parent	sshd	
decoder.name	sshd	
full_log	Aug 16 12:52:25 139-162-192-250 sshd[81512]: Disconnected from invalid user admin@01.43.135.157.113 port 49402 [preauth]	
location	/var/log/auth.log	

Events kısmında ise gelen uyarı ve tehditlerin ayrıntılı incelemesi yapılabilir. Aranan nitelikteki uyarılar filtreleme işlemlerle bulunabilir. Bu kısımda ayrıca gelen uyarının lokasyon, hash, full log gibi değerlere bakılarak tehdit incelemesi yapılabilir.

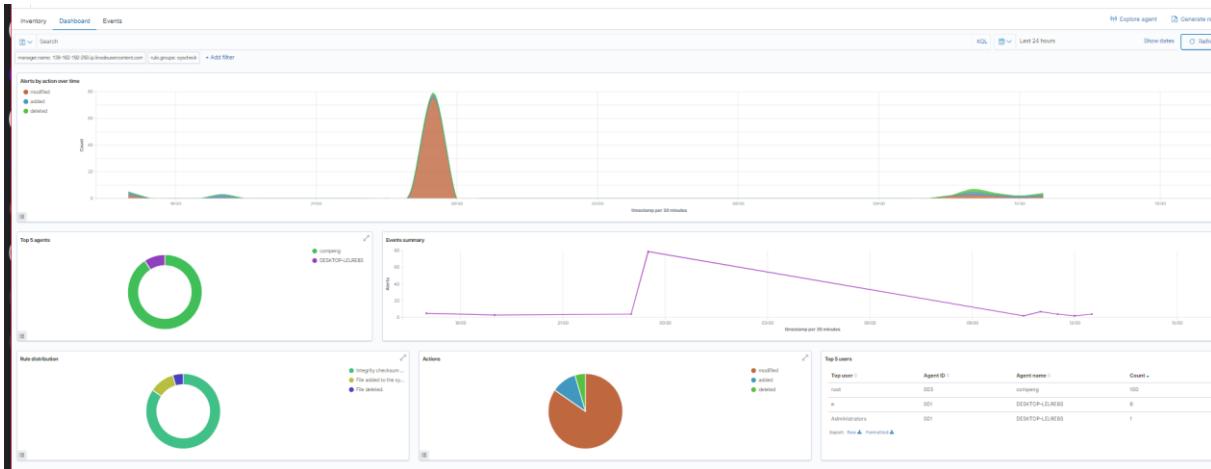


## Örneğin; Wazuh serverimize izinsiz giriş yapılmaya çalışıldığından önce aşağıdaki gibi bir uyarı aldık

Time	agent.name	rule.description	rule.level	rule.id
Aug 16, 2022 @ 16:00:03.304	139-162-192-250.ip.linodeusercontent.com	sshd: authentication failed.	5	5760
Expanded document				<a href="#">View surrounding documents</a> <a href="#">View single document</a>
<a href="#">Table</a> <a href="#">JSON</a>				
t GeoLocation.city_name	Duluth			
t GeoLocation.country_name	United States			
@ GeoLocation.location	{ "lon": -92.1998, "lat": 46.8147 }			
t GeoLocation.region_name	Minnesota			
t _index	wazuh-alerts-4.x-2022.08.16			
t agent.id	000			
t agent.name	139-162-192-250.ip.linodeusercontent.com			
t data.dstuser	root			
t data.srcip	143.110.179.172			
t data.srcport	60690			
t decoder.name	sshd			
t decoder.parent	sshd			
t full_log	Aug 16 13:00:03 139-162-192-250 sshd[635092]: Failed password for root from 143.110.179.172 port 60690 ssh2			
t id	1660654803.1632522			
t input.type	log			
t input.type	log			
t location	/var/log/auth.log			
t manager.name	139-162-192-250.ip.linodeusercontent.com			
t predecoder.hostname	139-162-192-250			
t predecoder.program_name	sshd			
t predecoder.timestamp	Aug 16 13:00:03			
t rule.description	sshd: authentication failed.			
# rule.firetimes	1			
t rule.gdpr	IV_35.7.0, IV_32.2			
t rule.gppg13	7.1			
t rule.groups	syslog, sshd, authentication_failed			
t rule.hipaa	164.312.b			
t rule.id	5760			
# rule.level	5			
Q rule.mail	false			
t rule.mitre.id	T1110, 001, T1021, 004			
t rule.mitre.tactic	Credential Access, Lateral Movement			
t rule.mitre.technique	Password Guessing, SSH			
t rule.nist_800_53	AU.14, AC.7			
t rule.pci_dss	10.2.4, 10.2.5			
t rule.tsc	CC6.1, CC6.8, CC7.2, CC7.3			
t rule.id	5760			
# rule.level	5			
Q rule.mail	false			
t rule.mitre.id	T1110, 001, T1021, 004			
t rule.mitre.tactic	Credential Access, Lateral Movement			
t rule.mitre.technique	Password Guessing, SSH			
t rule.nist_800_53	AU.14, AC.7			
t rule.pci_dss	10.2.4, 10.2.5			
t rule.tsc	CC6.1, CC6.8, CC7.2, CC7.3			
□ timestamp	Aug 16, 2022 @ 16:00:03.304			

## 2.Integrity Monitoring:

İzin, içerik, sahiplik ve öznitelikler dahil olmak üzere ilgili dosya değişiklikleriyle ilgili uyarılar bu kısımda görülmektedir. Örneğin sisteme bir dosya eklendiğinde, dosyanın içeriği değiştirildiğinde, silindiğinde veya sisteme bir dosya indirildiğinde ayrıntılı inceleme işlemlerini Integrity Monitoring kısmından yapabiliriz. Dashboard, Inventory ve Events olmak üzere 3 kısımdan oluşmaktadır. Dashboard kısmından grafiksel olarak monitörleme işlemi yapabiliriz.

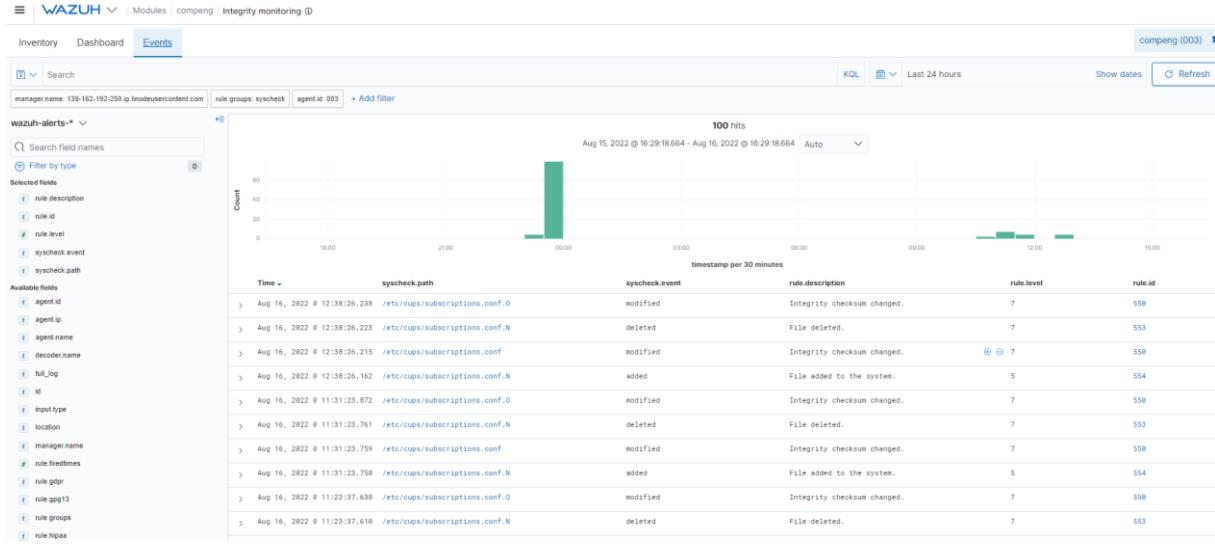


Inventory kısmında hangi dosyanın en son değişikliğinin ne zaman ve kim tarafından yapıldığı gösterilmektedir.

The screenshot shows the Inventory section with a table of files:

File	Last Modified	User	User ID	Group	Group ID	Permissions	Size
/bin	Aug 11, 2022 @ 17:56:01.000	root	0	root	0	rwxrwxrwx	7
/boot/System.map-5.13.0-30-generic	Feb 7, 2022 @ 17:01:37.000	root	0	root	0	r-----	5960334
/boot/System.map-5.15.0-46-generic	Aug 4, 2022 @ 21:44:38.000	root	0	root	0	r-----	6220961
/boot/config-5.13.0-30-generic	Feb 7, 2022 @ 17:01:37.000	root	0	root	0	r-----r--	257734
/boot/config-5.15.0-46-generic	Aug 4, 2022 @ 21:44:38.000	root	0	root	0	r-----r--	262223
/boot/grub/fonts/unicode.pf2	Aug 11, 2022 @ 18:39:17.000	root	0	root	0	r-----r--	2395475
/boot/grub/grubblacklist.txt	Feb 23, 2022 @ 11:50:58.000	root	0	root	0	r-----r--	712
/boot/grub/grub.cfg	Aug 11, 2022 @ 19:24:15.000	root	0	root	0	r-----r--	10019
/boot/grub/grubenv	Aug 16, 2022 @ 10:20:58.000	root	0	root	0	r-----r--	1024
/boot/grub/386-pc/915resolution.mod	Aug 11, 2022 @ 18:39:14.000	root	0	root	0	r-----r--	8016
/boot/grub/386-pc/acpi.mod	Aug 11, 2022 @ 18:39:08.000	root	0	root	0	r-----r--	10764
/boot/grub/386-pc/adler32.mod	Aug 11, 2022 @ 18:38:59.000	root	0	root	0	r-----r--	1396
/boot/grub/386-pc/afs.mod	Aug 11, 2022 @ 18:39:14.000	root	0	root	0	r-----r--	5856
/boot/grub/386-pc/afs.mod	Aug 11, 2022 @ 18:38:59.000	root	0	root	0	r-----r--	6308
/boot/grub/386-pc/ahci.mod	Aug 11, 2022 @ 18:39:11.000	root	0	root	0	r-----r--	15640

Events kısmından ise daha ayrıntılı olarak monitörleme işlemini yapabiliriz. Projemize hazırlık olarak ossec.conf dosyasını düzenleyerek agentlarımıza özelleştirdik ve agentlar bizim bakmak istediğimiz dosyalara bakarak sistemde dosya ekleme,silme,içerik değiştirme ve indirme işlemleri olduğunda wazuh server'a uyarı gönderdi bunlar sonucunda gözlemeleme sonuçlarımız şu şekildedir;



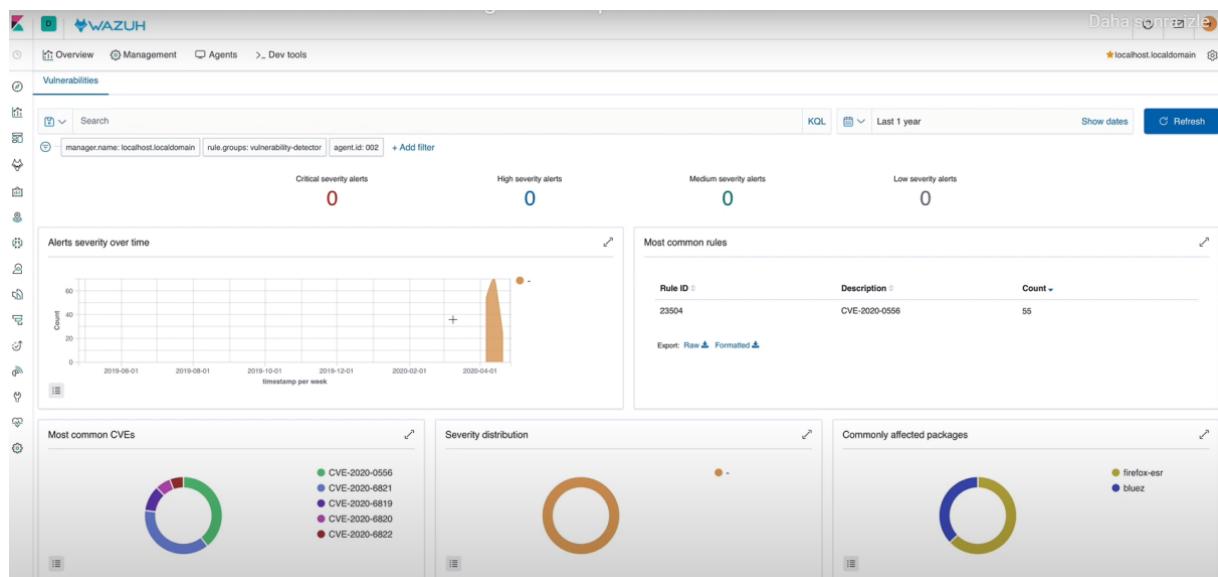
Bu kısımda yine yapılan işlemlerin tüm ayrıntıları incelenebilir.

Time	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
> Aug 16, 2022 @ 12:38:26.238	/etc/cups/subscriptions.conf.O	modified	Integrity checksum changed.	7	550
Expanded document					
<a href="#">View surrounding documents</a> <a href="#">View single document</a>					
<b>Table</b> JSON					
<pre> @ _index : wazuh-alerts-4.x-2022.08.16 @ _id   : 1660642706.1214617 @ _score: 1.0 @ _type: log  t agent.id    : 003 t agent.ip    : 10.0.2.15 t agent.name  : compeng t decoder.name: syscheck_integrity_changed t full_log    :   &gt; File '/etc/cups/subscriptions.conf.O' modified     Mode: realtime     Changed attributes: mtime,inode,md5,sha1,sha256     Old modification time was: '1660638217', now it is '1660638683'     Old inode was: '524435', now it is '527310'     Old md5sum was: '23d8c0217dec7251492622313dd0e'     New md5sum is: '4081a0aa0a61ff722ff0a0-d8f4ca41a727' t id          : 1660642706.1214617 t input.type  : log t location    : syscheck t manager.name: 139-162-192-250.ip.linodeusercontent.com t rule.description: Integrity checksum changed. # rule.firedtimes: 3 t rule.gdpr   : II_5.1.f t rule.gpg13  : 4.11 t rule.groups: ossec, syscheck, syscheck_entry_modified, syscheck_file </pre>					

### 3.Vulnerabilities:

Wazuh, Vulnerability Detector modülünü kullanarak ajanlara yüklenen uygulamalardaki güvenlik açıklarını tespit edebilmektedir. Güvenlik açıklarını tespit edebilmek için, ajanlar kurulu uygulamaların bir listesini yerel olarak toplayabilir ve bunu periyodik olarak yöneticiye gönderebilir (burada her ajan için bir tane olmak üzere yerel SQLite veritabanlarında depolanır). Ayrıca yönetici, daha sonra bu bilgileri ajanının uygulama envanter verileriyle çapraz ilişkilendirmek için kullanarak, herkese açık CVE havuzlarından küresel bir güvenlik açığı veritabanı oluşturur.

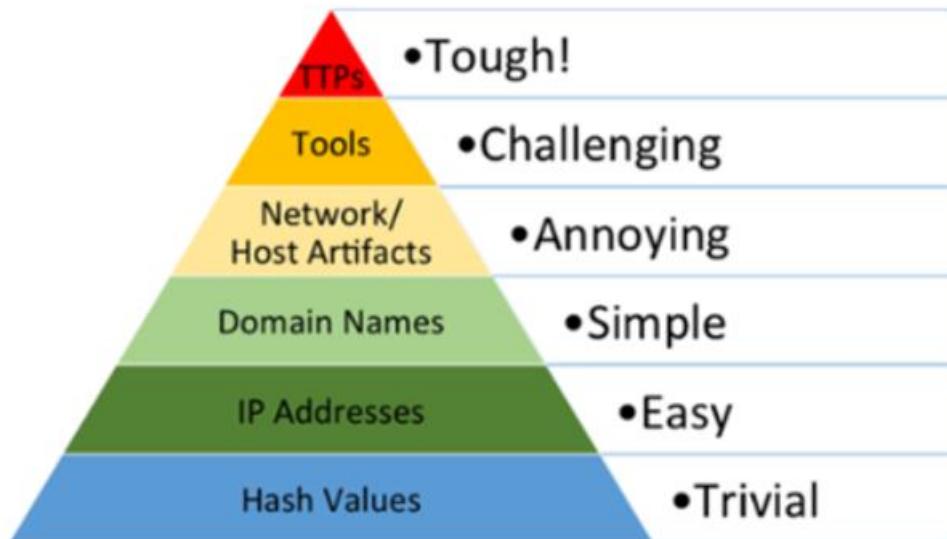
Küresel güvenlik açığı veritabanı (CVE'lerle birlikte) oluşturulduktan sonra, algılama süreci envanter veritabanlarında (ajan başına benzersiz) güvenlik açığı bulunan paketleri arar. Uyarılar, bir CVE (Ortak Güvenlik Açıkları ve Etkilenmeler), izlenen ana bilgisayarlardan birine yüklentiği bilinen bir paketi etkilediğinde oluşturulur. Bir paket, sürümü bir CVE'nin etkilenen aralığında yer aldığından güvenlik açığı olarak etiketlenir. Sonuçlar uyarılar olarak sunulur ve ayrıca ajan başına güvenlik açıkları envanterinde depolanır. Bu şekilde, son tarama uyarılarını kontrol edebilir veya her bir ajanın güvenlik açıkları envanterini sorgulayabilirsiniz.



### 4.MITRE ATT&CK:

MITRE ATT&CK, MITRE Düşmanca Taktikler, Teknikler ve Ortak Bilgi (ATT&CK) anlamına gelir. MITRE ATT&CK frameworkü, bir rakibin saldırı yaşam döngüsünün çeşitli aşamalarını ve hedefledikleri bilinen platformları yansitan, siber saldırıcı davranış için seçilmiş bir bilgi tabanı ve modelidir. Modeldeki taktik ve teknik soyutlaması, siber güvenliğin hem saldırıcı hem de savunmacı tarafları tarafından anlaşılan bireysel düşman eylemlerinin ortak bir sınıflandırmasını sağlar. Ayrıca, düşman eylemi için uygun bir kategorizasyon düzeyi ve ona karşı savunmanın belirli yollarını sağlar.

- Bir atağın davranışını gösteren en güncel bilgi merkezidir.
- Gerçek dünyada meydana gelen Ataklar Gözlemlenerek Oluşturulmuştur.
- Taktik, Teknik ve Prosedüre Dayalıdır.
- Ücretsiz, Açık ve Erişilebilir bir bilgi merkezidir.
- Community-Driven, 100+ Organizasyon ve Kişi Tarafından Desteklenmektedir.

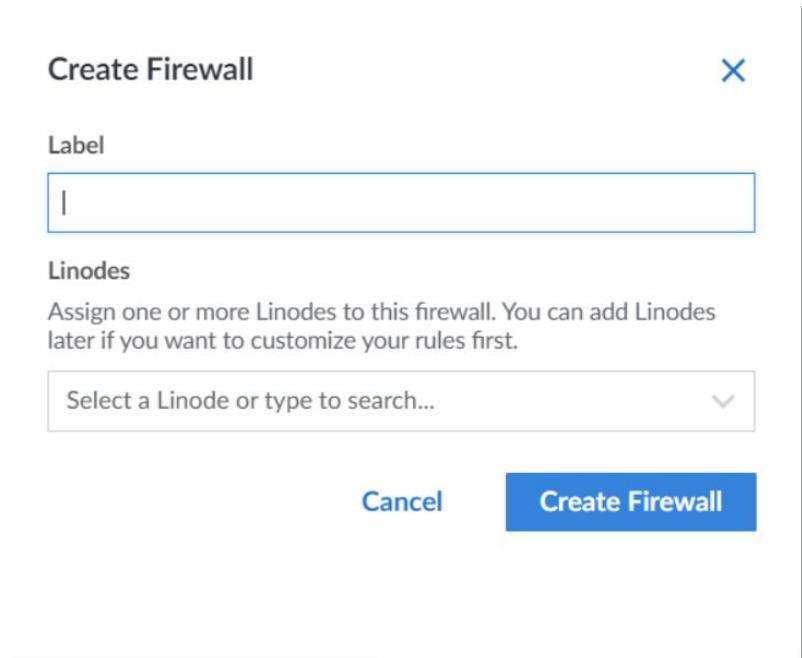


## WAZUH ÜZERİNE FIREWALL OLUSTURMA VE KURALLARINI YAZMA

1-Firewalls butonuna tıklanır.

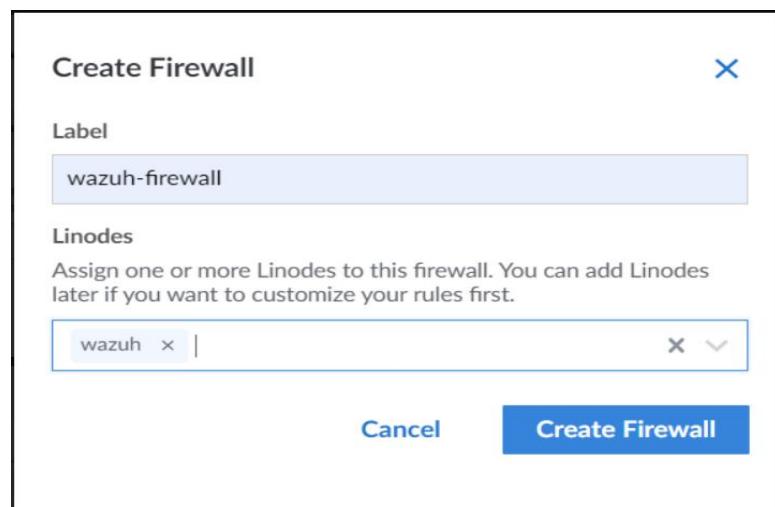
Label	Status	Plan	IP Address	Region	Last Backup
wazuh	Running	Linode 4 GB	178.79.155.124	London, UK	Never

2- Çıkan sayfadan create firewall butonuna basılır ve şu ekranla karşılaşılır;



The screenshot shows a 'Create Firewall' dialog box. At the top left is the title 'Create Firewall' and at the top right is a blue 'X' button. Below the title is a 'Label' field containing a single vertical bar character '|'. Underneath is a section titled 'Linodes' with the instruction: 'Assign one or more Linodes to this firewall. You can add Linodes later if you want to customize your rules first.' A dropdown menu below this placeholder contains the text 'Select a Linode or type to search...'. At the bottom of the dialog are two buttons: 'Cancel' on the left and a larger blue 'Create Firewall' button on the right.

3-Biz wazuh için firewall kullanacağımızdan bu ekranı şu şekilde doldurduk;  
“label” yerine firewall için isim yazılır “linode” kısmında ise firewall kullanacağımız araç seçilir ve  
create firewall butonuna tıklanır.



The screenshot shows the same 'Create Firewall' dialog box as above, but with different input. In the 'Label' field, the text 'wazuh-firewall' is entered. In the 'Linodes' section, the dropdown menu shows the entry 'wazuh' with a delete 'x' icon and a dropdown arrow. At the bottom, the 'Create Firewall' button is highlighted with a blue border.

Firewall oluşturulduğunda bu şekilde görülmektedir.

Firewalls				Docs	Create Firewall
Firewall	Status	Rules	Linodes		
wazuh-firewall	Enabled	No rules	wazuh	Disable	Delete

**4- Firewall ismine tıklanarak kuralların yazılacağı sayfa açılır bu kısımda oluşturulan Firewall için kurallar yazılabılır.**

The screenshot shows the Wazuh Firewall configuration page. At the top, there are tabs for 'Rules' (which is selected) and 'Linodes'. Below the tabs, there are two main sections: 'Inbound Rules' and 'Outbound Rules'. Each section has a table header with columns: Label, Protocol, Port Range, Sources, and Action. Under the 'Inbound Rules' section, it says 'No inbound rules have been added.' and 'Default inbound policy: This policy applies to any traffic not covered by the inbound rules listed above.' with an 'Accept' button. Under the 'Outbound Rules' section, it says 'No outbound rules have been added.' and 'Default outbound policy: This policy applies to any traffic not covered by the outbound rules listed above.' with an 'Accept' button. At the bottom right, there are 'Discard Changes' and 'Save Changes' buttons.

**Herhangi bir kural eklendikten sonra save changes butonuna tıklanarak değişiklikler kaydedilir.**