Wazuh is a free and open source security platform that combines XDR and SIEM features. Protects workloads in on-premises, virtualized, containerized, and cloud-based environments. The solution consists of a single universal agent and three central components: Wazuh server, Wazuh indexer and Wazuh dashboard.

Wazuh Server: The Wazuh server is responsible for analyzing data received from Wazuh agents, triggering alerts when threats or anomalies are detected. It is also used to remotely manage the configuration of agents and monitor their status.

Elastic Stack: Elastic stack is a unified suite of popular open source projects including Elasticsearch, Kibana, Filebeat and others for log management. Indexes and stores alerts generated by the Wazuh server. In addition, the integration between Wazuh and Kibana* provides a user interface for data visualization and analysis. This interface is also used to manage the Wazuh configuration and monitor its status.

There are three main components related to Wazuh:
Filebeat: Used in Wazuh server to send events and alerts to Elasticsearch. It reads the output of the Wazuh analysis engine and sends the events in real time via an encrypted channel.

Elasticsearch: It is a highly scalable, full-text search and analytics engine. Elasticsearch is distributed, meaning data indices are split into chunks and each chunk can have zero or more copies. Wazuh uses different indices for alert data, raw events and condition monitoring information

Kibana: It is a flexible and intuitive web interface for data mining, analysis and visualization. It runs on top of indexed content in an Elasticsearch cluster. The Wazuh web UI is fully embedded in Kibana as a plugin. Security events include out-of-the-box dashboards for regulatory compliance (e.g. PCI DSS, GDPR, CIS, HIPAA, NIST 800-53), detected vulnerable applications, file integrity monitoring data, configuration evaluation results, cloud infrastructure monitoring events.

Wazuh Dashboard: This central component is a flexible and intuitive web interface for mining, analysis and visualization of data. Provides ready-to-use dashboards that allow you to navigate the user interface seamlessly. Users can quickly visualize security events, detect vulnerable applications, file integrity monitoring data, configuration evaluation results, cloud infrastructure monitoring events, and PCI DSS, GDPR, CIS, HIPAA, and NIST It can detect legal compliances such as 800-53 standards.

Wazuh Indexer: Wazuh indexer is a highly scalable, full-text search and analytics engine. This Wazuh central component indexes and stores alerts generated by the Wazuh server and provides near real-time data search and analytics capabilities.

Wazuh Agent: Wazuh agent is multiplatform and runs on the hosts the user wants to monitor. It communicates with the Wazuh administrator, sending data in near real-time via an encrypted and authenticated channel. The agent was developed with the need to monitor a wide variety of different endpoints without affecting their performance. It requires an average of 35 MB of RAM. Therefore, it is supported on most popular operating systems.

Wazuh agent provides key features to increase the security of your system.

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

WAZUH INSTALLATION

There are many alternative ways to download the Wazuh tool. The first of these ways and the installation featured on its page; To complete the download process step by step from https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html.

As an alternative to this method, the following can be shown:

Deployment in Docker:

Docker is an open platform for building, delivering, and running applications in software containers. Docker containers bundle software, including everything needed to run it: code, runtime, system tools, system libraries, and settings. Docker enables to separate applications from infrastructure. This ensures that the application will always run the same regardless of the environment the container is running in. Containers can run in the cloud or on-premises. You can install Wazuh using Docker images such as wazuh/wazuh-manager, wazuh/wazuh-indexer, and wazuh/wazuh-dashboard. All these Wazuh Docker images are available in the Docker hub.

Installing from Packages:

Wazuh manager and agent can be installed via sources as an alternative to installing from packages.

Amazon Machine Images (AMI):

Wazuh provides a prebuilt Amazon Machine Image (AMI). AMI is a ready-to-use, preconfigured template for creating a virtual computing environment in Amazon Elastic Compute Cloud (Amazon EC2).

In addition to these alternative ways, we preferred the installation of OVA 4.2 version, which is another alternative way in this project.

Virtual Machine (OVA):

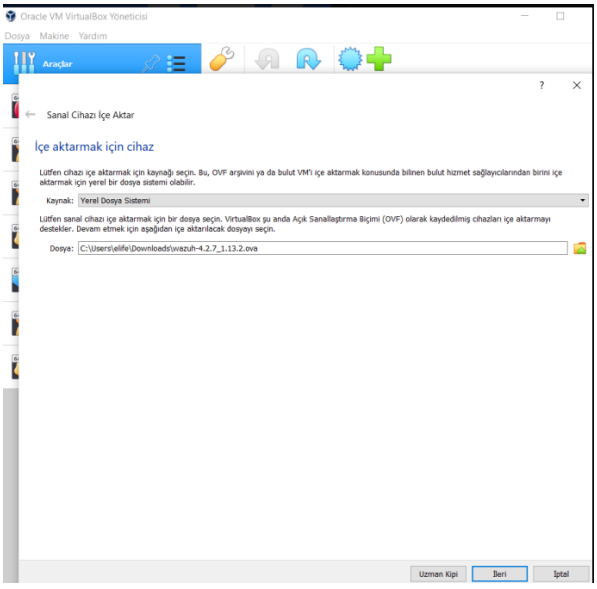
Wazuh provides a prebuilt virtual machine image (OVA) that you can import directly using VirtualBox or other OVA compatible virtualization systems. Note that this VM only works on 64-bit systems and does not provide high availability and scalability of the product.

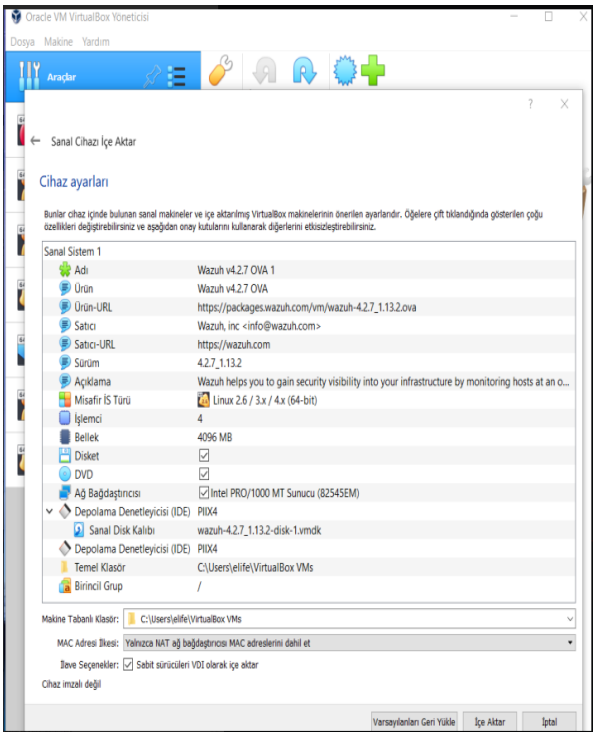
The OVA includes the following components:

- **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**

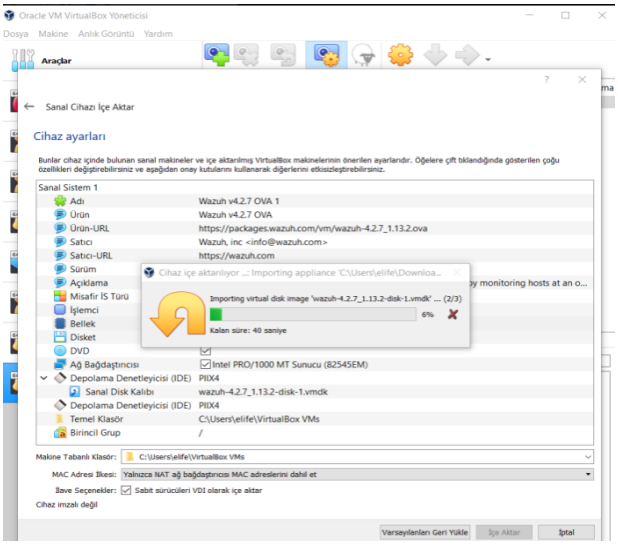
After downloading the above mentioned OVA in our project, we followed these steps for installation:

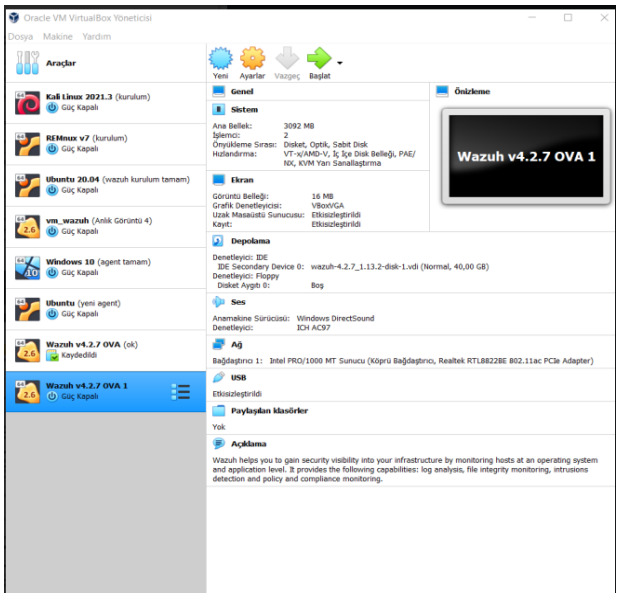
The downloaded OVA file is imported into VirtualBox.





Default values can be changed during the installation process. After the import process is done, changes cannot be performed.

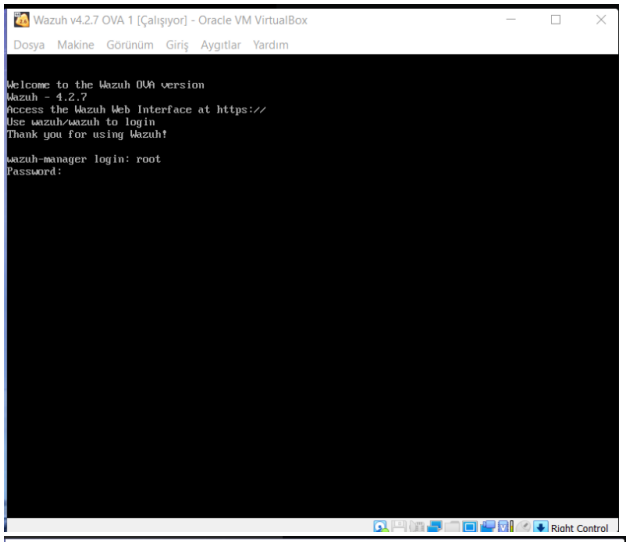


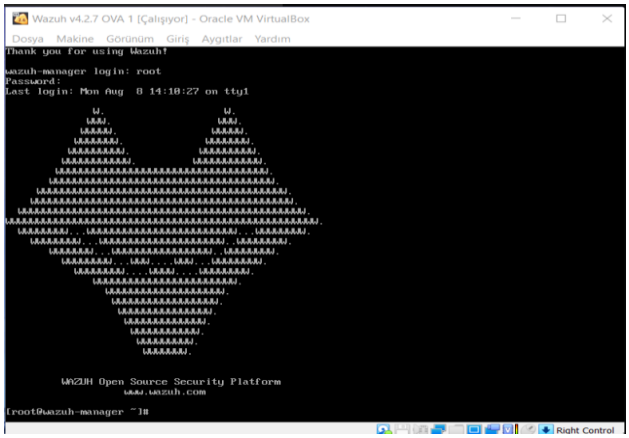


Wazuh OVA is run.

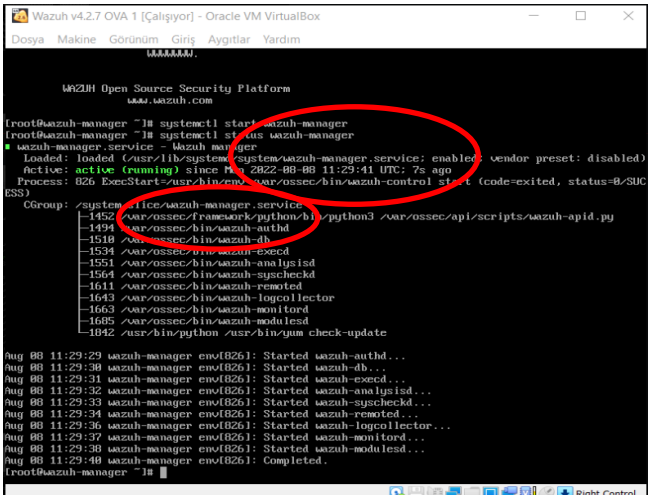
In the window that opens, type “root” in the wazuh-manager login section and “wazuh” in the Password section and press the enter key to login.

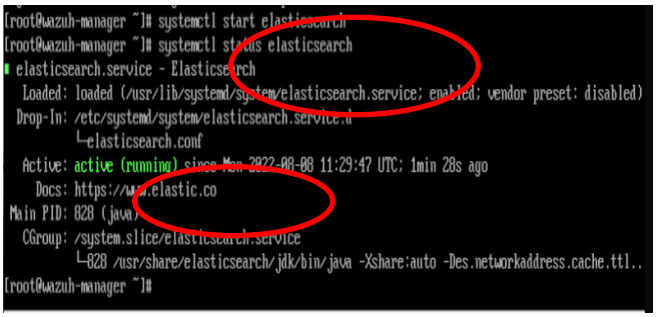
(password does not appear on the screen while typing)

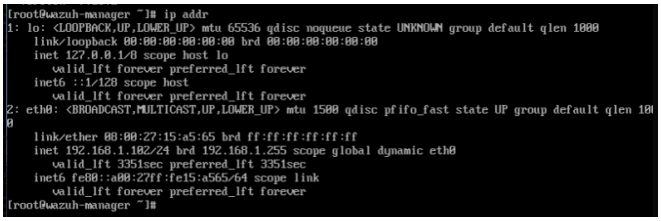


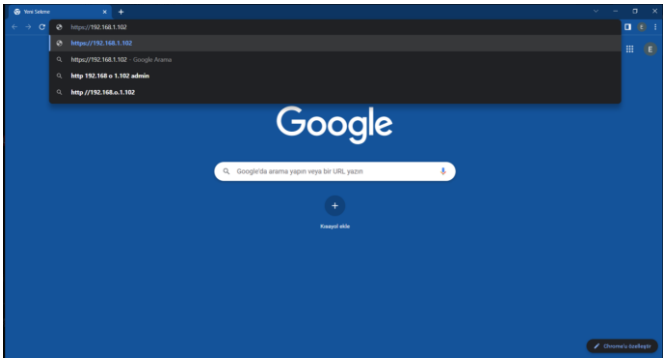


After the system is turned on, "systemctl status kibana", "systemctl status wazuh-manager", "systemctl status elasticsearch" should be typed and kibana, wazuh-manager and elasticsearch should be running actively. If the status is not active, for example, “systemctl start elasticsearch” should be typed and the status of elasticsearch should be checked again.

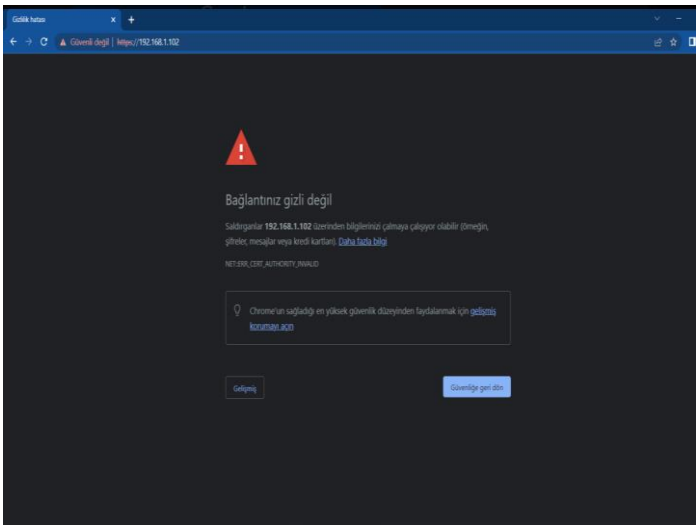


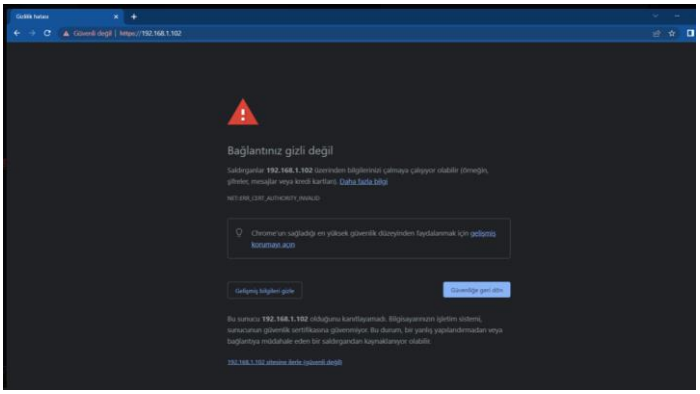




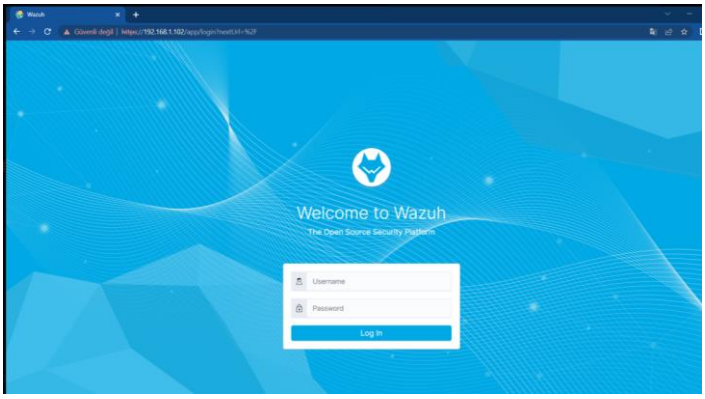


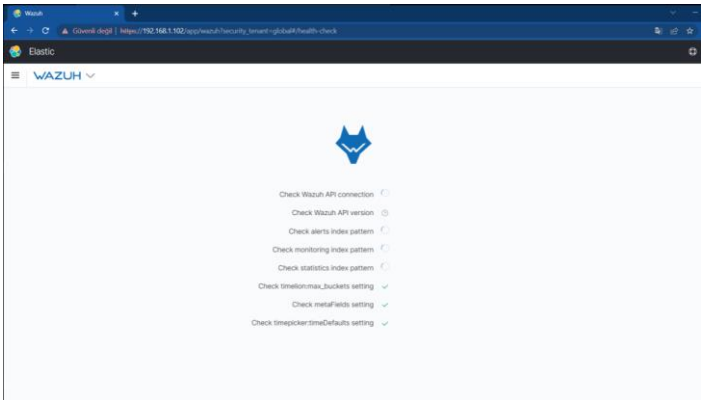
On the page that opens, if a warning such as "your connection is not confidential" is encountered, this warning should not be taken into account, by clicking on the "hide advanced information" button and clicking the "advance to the received IP address" button.

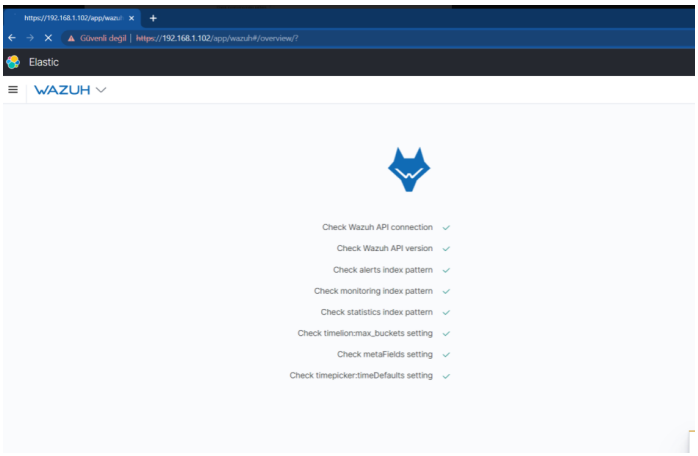




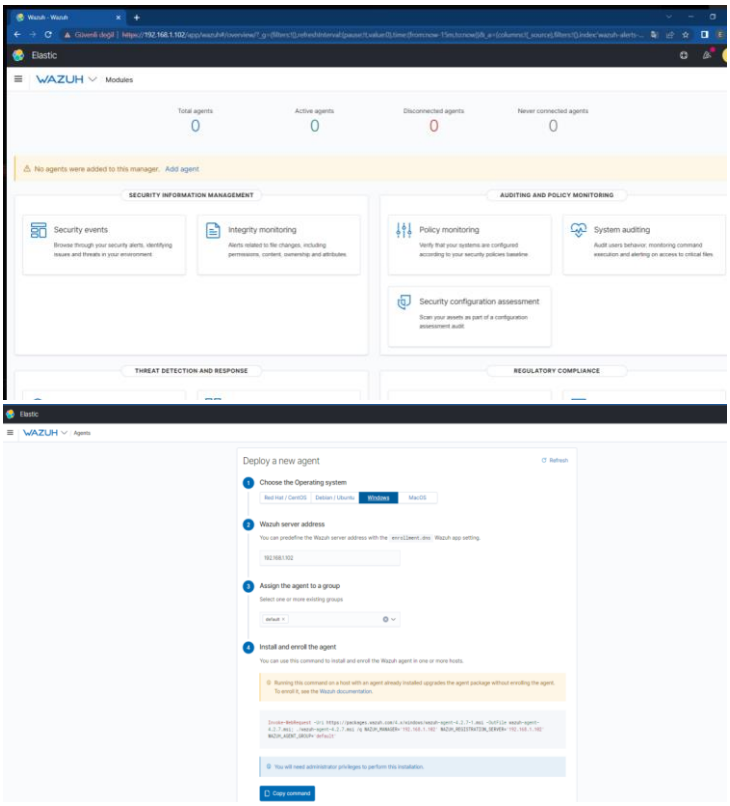
When an error such as “kibana server is not ready yet” is given in the interface that opens, step 4 should be returned and the statuses should be checked. All links must be complete on the page that opens.



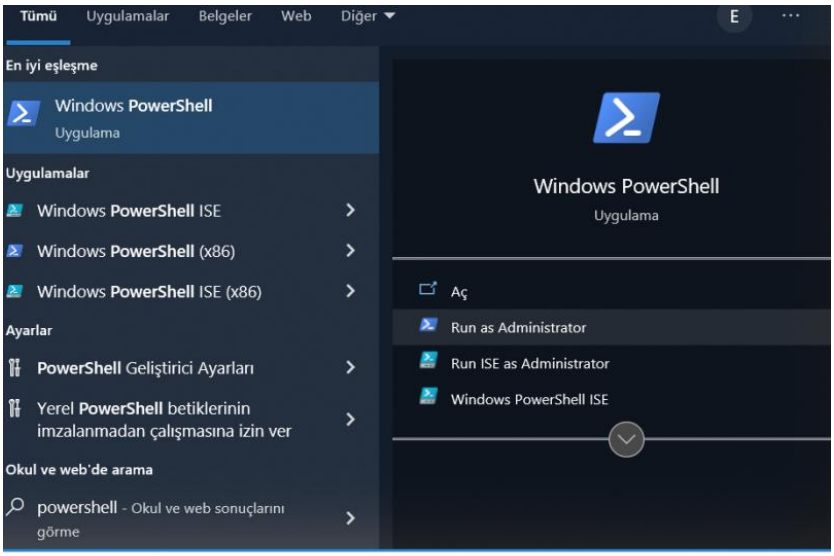


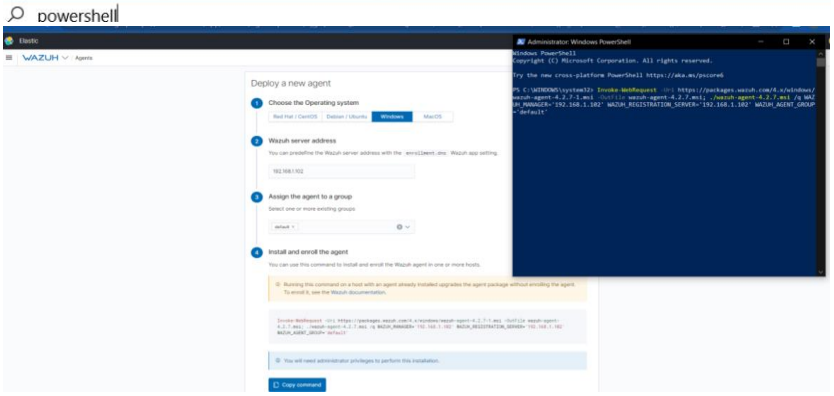


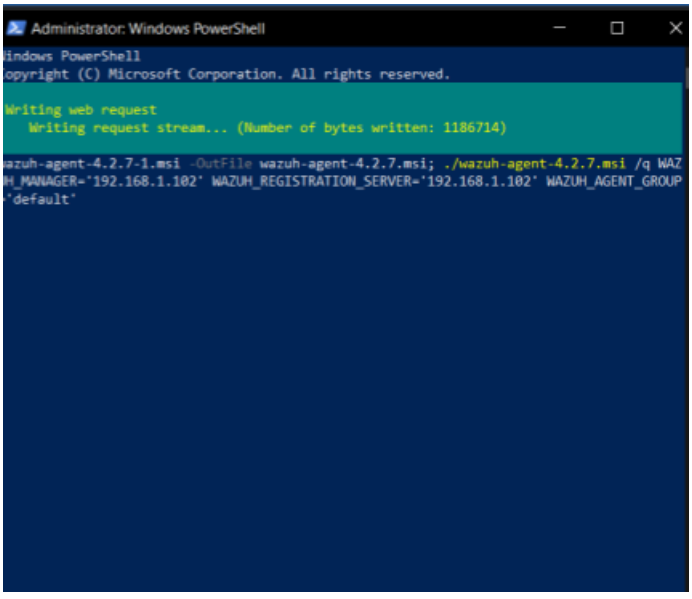
After all connections are completed, login to wazuh dashboard is made automatically. After these stages, agent adding processes can be started. First, click on the “add agent” section and select the operating system that we want to add an agent to from the page that appears. Then “wazuh address server” Finally, the command in the "install and enroll agent" section is copied and pasted into the command line of the operating system in which the agent is desired to be installed, and press enter.

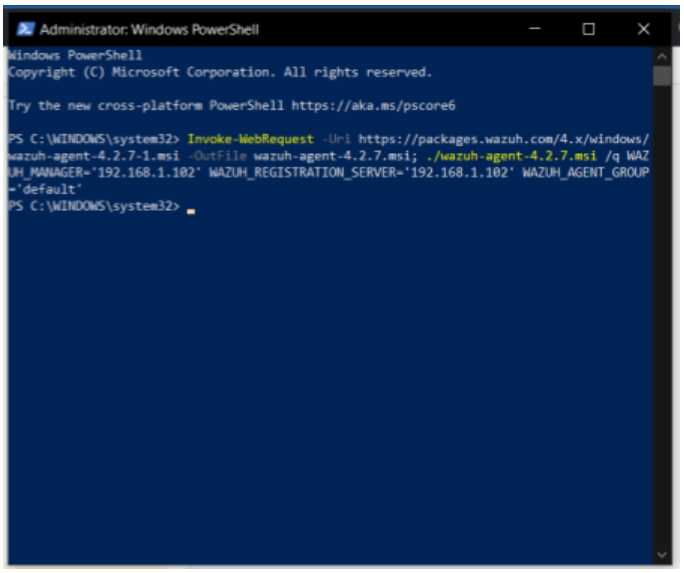


For the Window operating system, click the “PowerShell” “run as administrator” button, then the device is approved to make changes and the command received is pasted here and the enter key is pressed.

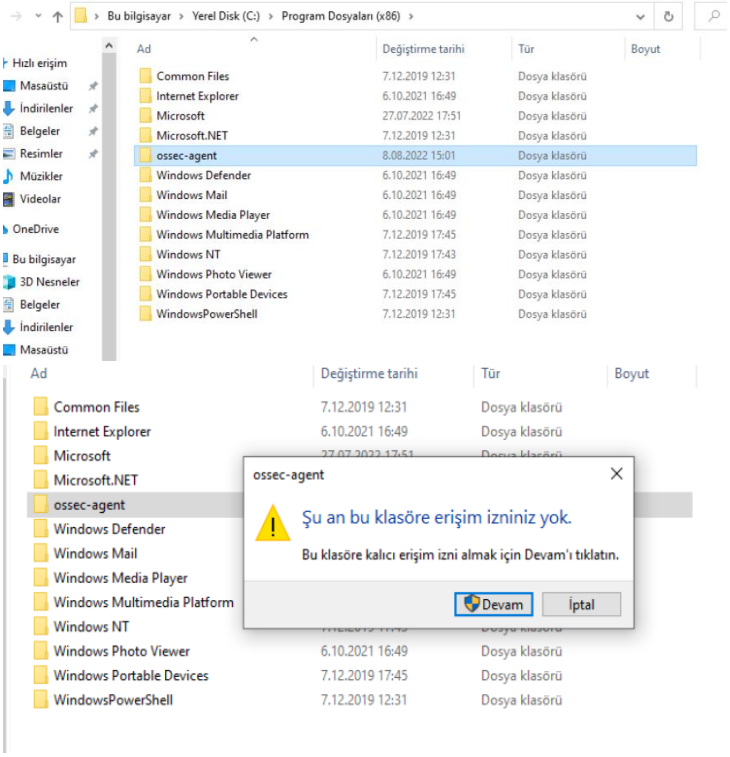

Tümü
Uygulamalar
Belgeler
Web
Diğer
En iyi eşleşme
Windows PowerShell
Uygulama
Uygulamalar
Windows PowerShell ISE
Windows PowerShell (x86)
Windows PowerShell ISE (x86)
Ayarlar
PowerShell Geliştirici Ayarları
Yerel PowerShell betiklerinin imzalanmadan çalışmasına izin ver
Okul ve web'de arama
powershell - Okul ve web sonuçlarını görme
Windows PowerShell
Uygulama
Aç
Run as Administrator
Run ISE as Administrator
Windows PowerShell ISE
powershell

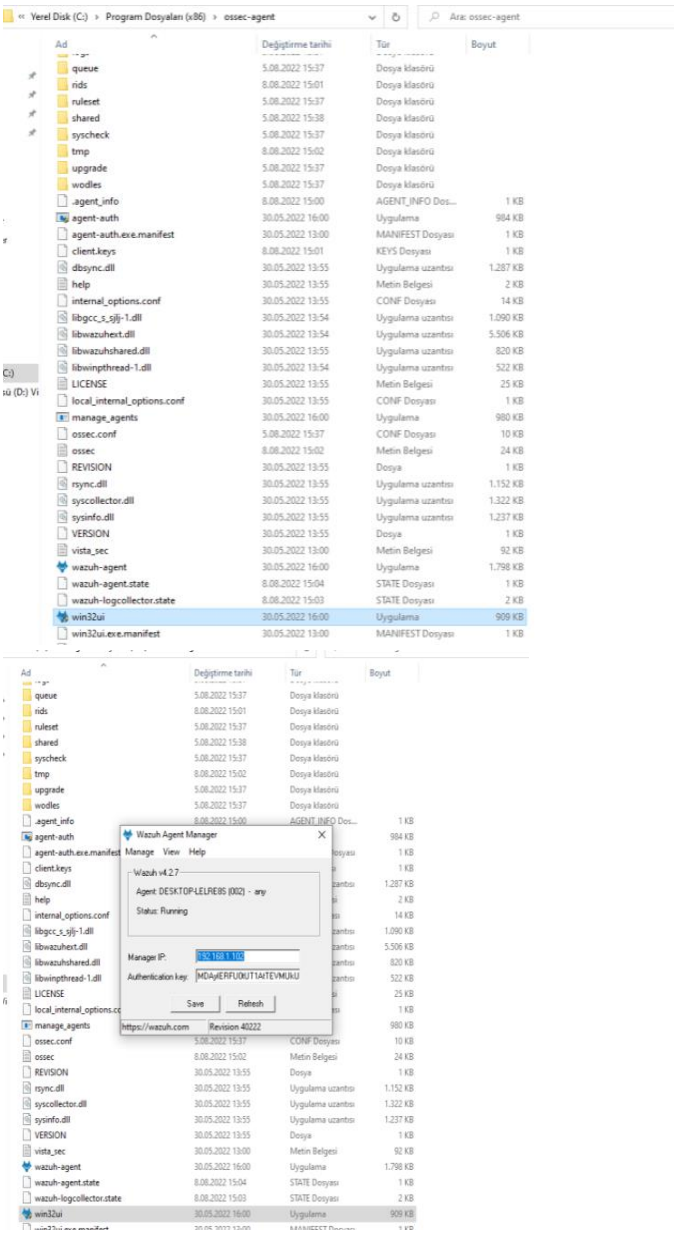

Deploy a new agent
Choose the Operating system
Wazuh server address
Assign the agent to a group
Install and enroll the agent
Copy command

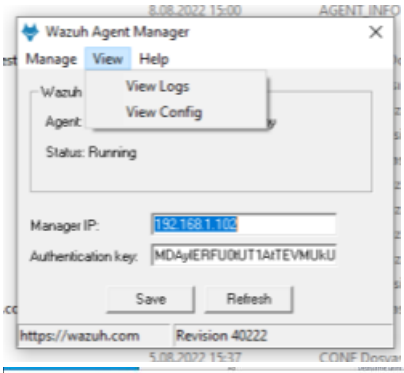

Administrator: Windows PowerShell
Writing web request
Writing request stream... (Number of bytes written: 1186714)
wazuh-agent-4.2.7-1.msi -OutFile wazuh-agent-4.2.7.msi; ./wazuh-agent-4.2.7.msi /q WAZ
H_MANAGER='192.168.1.102' WAZUH_REGISTRATION_SERVER='192.168.1.102' WAZUH_AGENT_GROUP
'default'

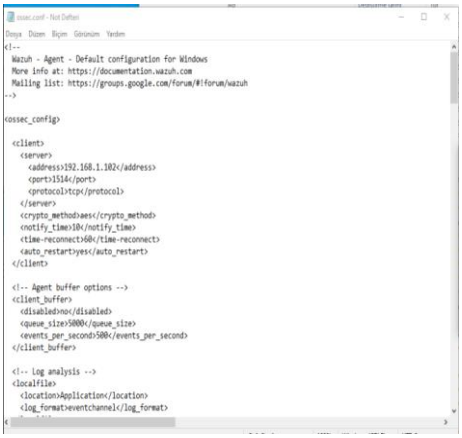


After the download is complete, the following path must be followed to access the Window agent: C:\Program Files (x86). From this folder section, the “ossec-agent” folder where the Windows agent is located is found and opened. Then, from the "view" tab on the screen, click the "view config" button and from the opened page, the ip address given to us before is written to the address section and the save button is clicked. The agent installation process is completed.

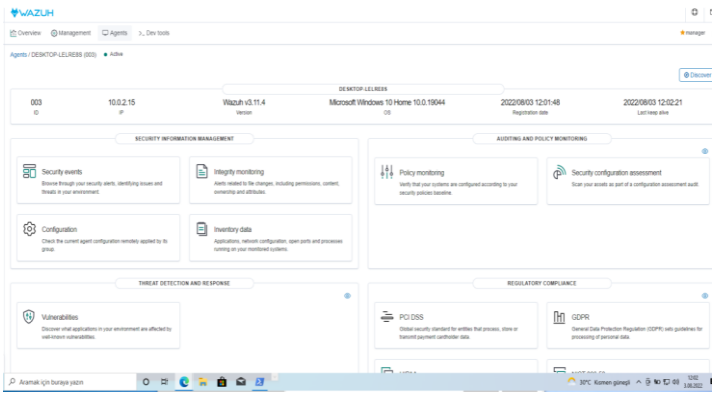



« Yerel Disk (C:) › Program Dosyaları (x86) › ossec-agent
Ara: ossec-agent
Ad
Değiştirme tarihi
Tür
Boyut
queue 5.08.2022 15:37 Dosya klasörü
rids 8.08.2022 15:01 Dosya klasörü
ruleset 5.08.2022 15:37 Dosya klasörü
shared 5.08.2022 15:38 Dosya klasörü
syscheck 5.08.2022 15:37 Dosya klasörü
tmp 8.08.2022 15:02 Dosya klasörü
upgrade 5.08.2022 15:37 Dosya klasörü
wodles 5.08.2022 15:37 Dosya klasörü
.agent_info 8.08.2022 15:00 AGENT_INFO Dos... 1 KB
agent-auth 30.05.2022 16:00 Uygulama 984 KB
agent-auth.exe.manifest 30.05.2022 13:00 MANIFEST Dosyası 1 KB
client.keys 8.08.2022 15:01 KEYS Dosyası 1 KB
dbsync.dll 30.05.2022 13:55 Uygulama uzantısı 1.287 KB
help 30.05.2022 13:55 Metin Belgesi 2 KB
internal_options.conf 30.05.2022 13:55 CONF Dosyası 14 KB
libgcc_s_sjlj-1.dll 30.05.2022 13:54 Uygulama uzantısı 1.090 KB
libwazuhext.dll 30.05.2022 13:54 Uygulama uzantısı 5.506 KB
libwazuhshared.dll 30.05.2022 13:55 Uygulama uzantısı 820 KB
libwinpthread-1.dll 30.05.2022 13:54 Uygulama uzantısı 522 KB
LICENSE 30.05.2022 13:55 Metin Belgesi 25 KB
local_internal_options.conf 30.05.2022 13:55 CONF Dosyası 1 KB
manage_agents 30.05.2022 16:00 Uygulama 980 KB
ossec.conf 5.08.2022 15:37 CONF Dosyası 10 KB
ossec 8.08.2022 15:02 Metin Belgesi 24 KB
REVISION 30.05.2022 13:55 Dosya 1 KB
rsync.dll 30.05.2022 13:55 Uygulama uzantısı 1.152 KB
syscollector.dll 30.05.2022 13:55 Uygulama uzantısı 1.322 KB
sysinfo.dll 30.05.2022 13:55 Uygulama uzantısı 1.237 KB
VERSION 30.05.2022 13:55 Dosya 1 KB
vista_sec 30.05.2022 13:00 Metin Belgesi 92 KB
wazuh-agent 30.05.2022 16:00 Uygulama 1.798 KB
wazuh-agent.state 8.08.2022 15:04 STATE Dosyası 1 KB
wazuh-logcollector.state 8.08.2022 15:03 STATE Dosyası 2 KB
win32ui 30.05.2022 16:00 Uygulama 909 KB
win32ui.exe.manifest 30.05.2022 13:00 MANIFEST Dosyası 1 KB
Wazuh Agent Manager
Manage View Help
Wazuh v4.2.7
Agent: DESKTOP-LELRE8S (002) - any
Status: Running
Manager IP:
Authentication key: MD4yERFUDUT1AiTEVMUkU
Save
Refresh
https://wazuh.com
Revision 40222



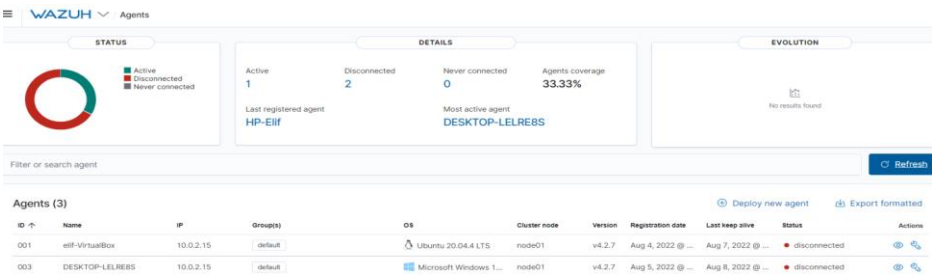


After all the processes are completed, when the wazuh interface is entered, it will be seen that the agent is installed.

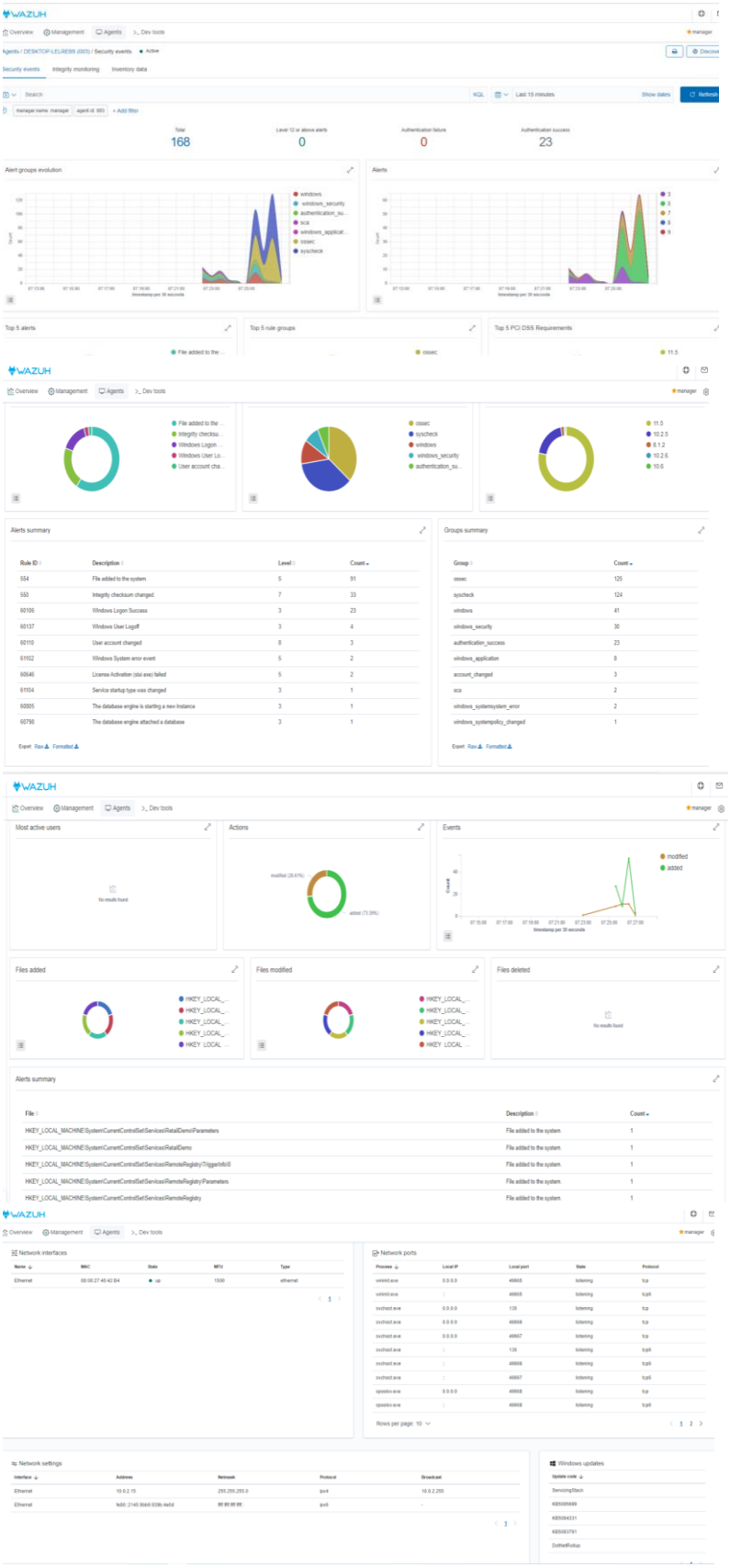


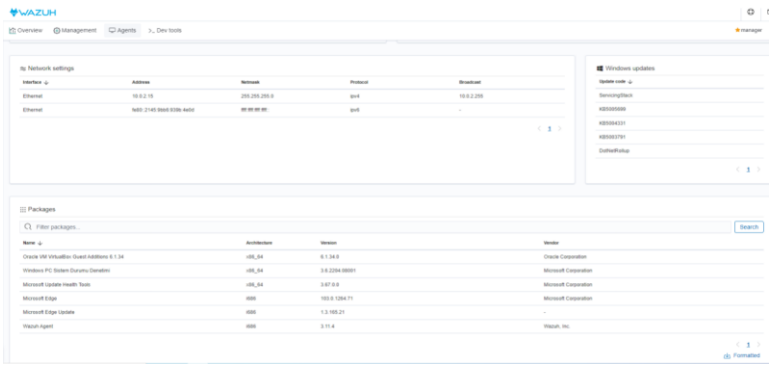
After the received ip address, "this site cannot be reached" error in the wazuh interface can be encountered because the ip address given to us in the wazuh ova section is a dynamic rip address and can change. In this case, a new ip address can be taken with ip add and the process can be taken under control.

The process of installing agents on Ubuntu operating system is the same. Users who want to install agents on Ubuntu can do the same steps.



After all the stages are completed, the "security event" overview in the wazuh tool is as follows.





INSTALLING WAZUH IN CLOUD ENVIRONMENT

Wazuh tool can be installed on a cloud environment as well as on a VirtualBox. Wazuh tool should have the following requirements in general;

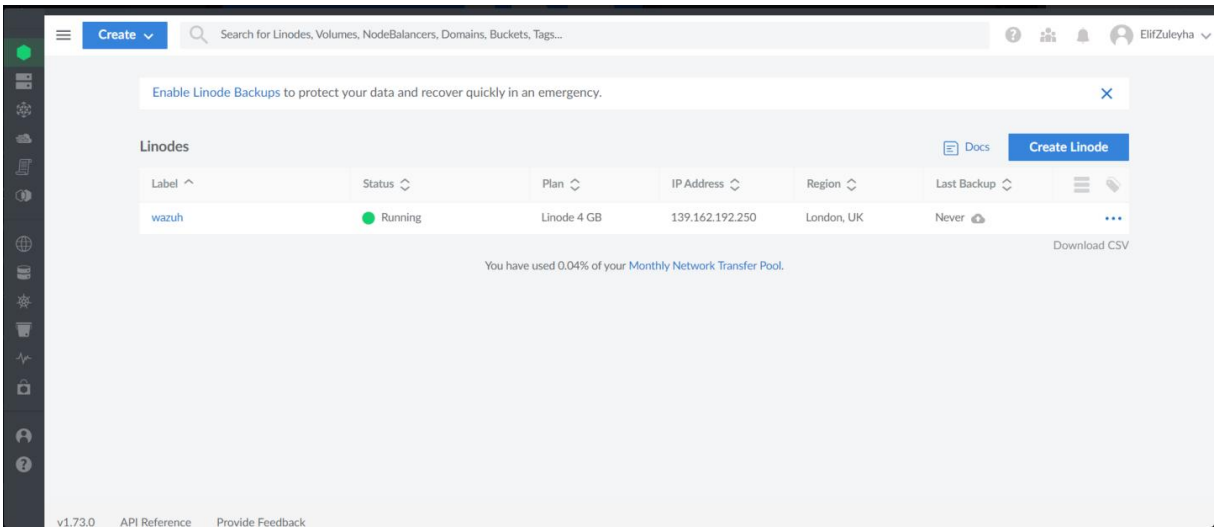
Agents	CPU	RAM	Storage (90 days)
1-25	4 vCPU	8 GiB	50 GB
25-50	8 vCPU	8 GiB	100 GB
50-100	8 vCPU	8 GiB	200 GB

When we used Wazuh Ova in this project, we encountered events such as system slowdowns, contractions, so we preferred to install the wazuh tool in a cloud environment called linode, which provides a virtual server, in order to prevent these problems and to prevent each team member from downloading wazuh ova separately.

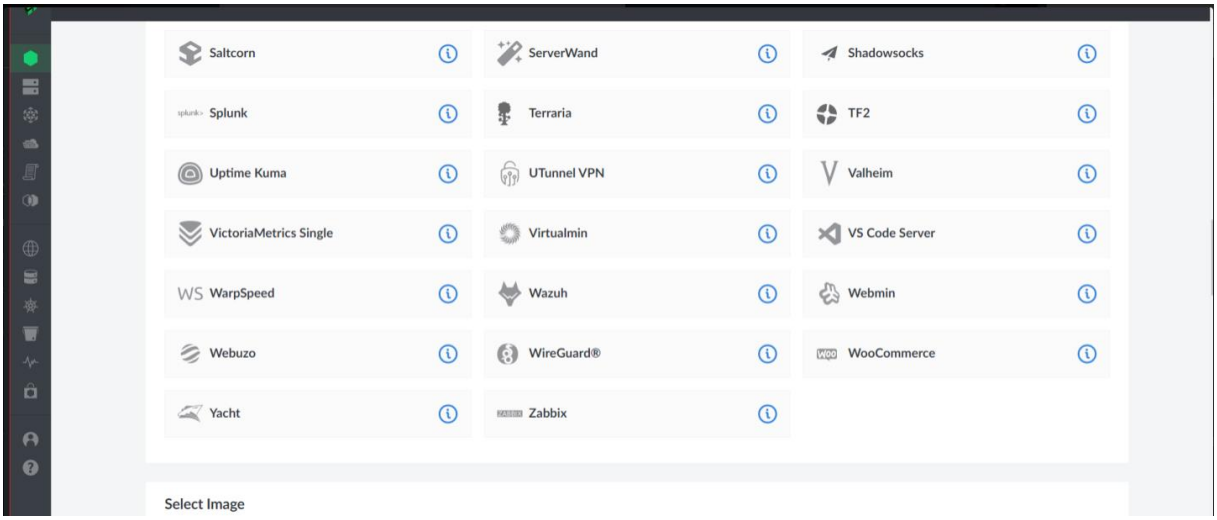
INSTALL WAZUH ON LINODE:

Go to https://cloud.linode.com/linodes and open an account to use the cloud environment. If a virtual card is used in the payment information section when opening an account on Linode, the Linode system automatically rejects the account. Therefore, physical card information should be used in this section. Opening an account After the application is made, an account is created if the necessary conditions are met.

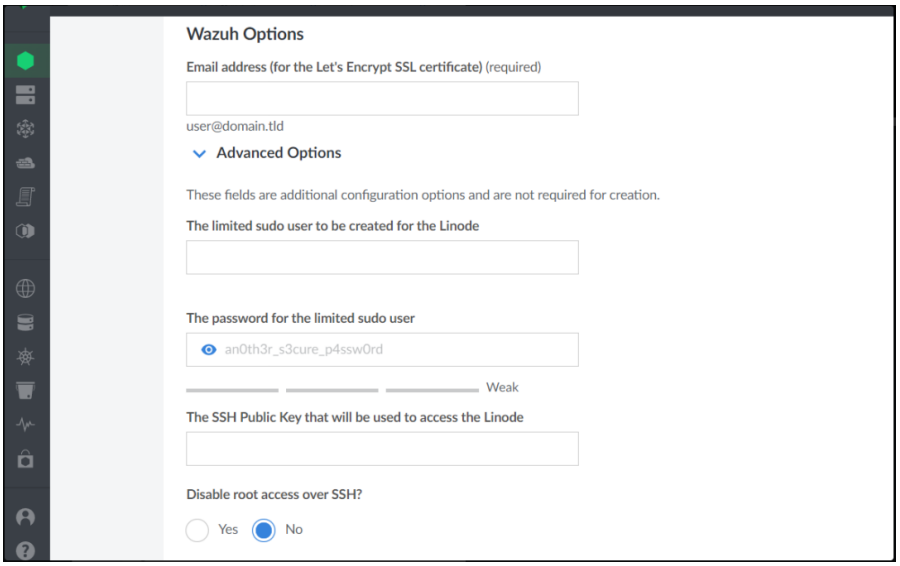
After logging into the account, click on the 'Create Linode' button from the 'Linodes' tab.

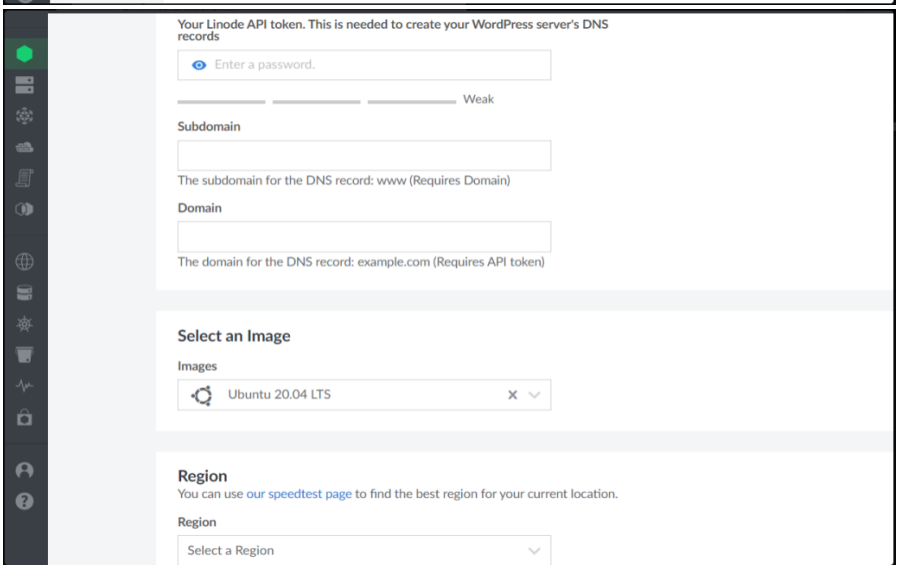


From the page that opens, go to the “marketplace” tab. In this section, there are tools that can be used on Linode. Among these tools, the Wazuh tool is selected.

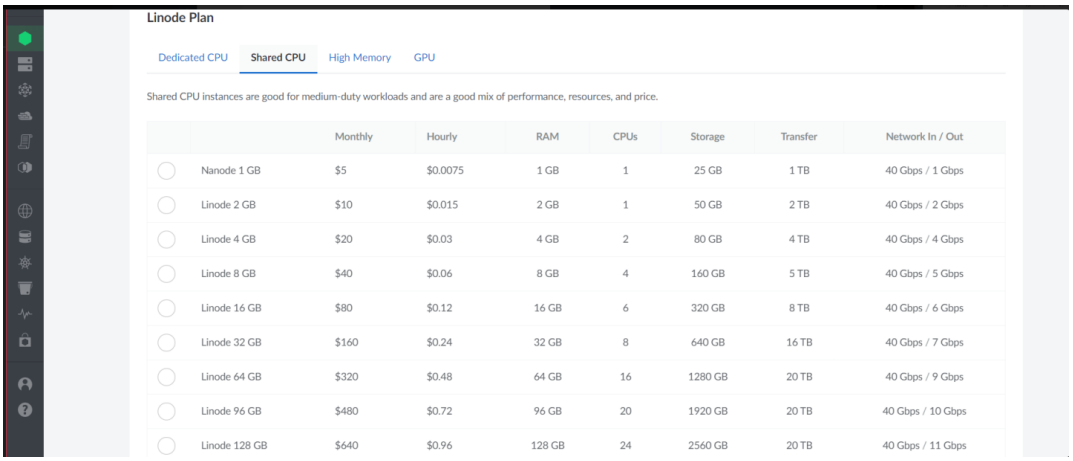


Fill in the information in the "Wazuh options" section on the page that opens.

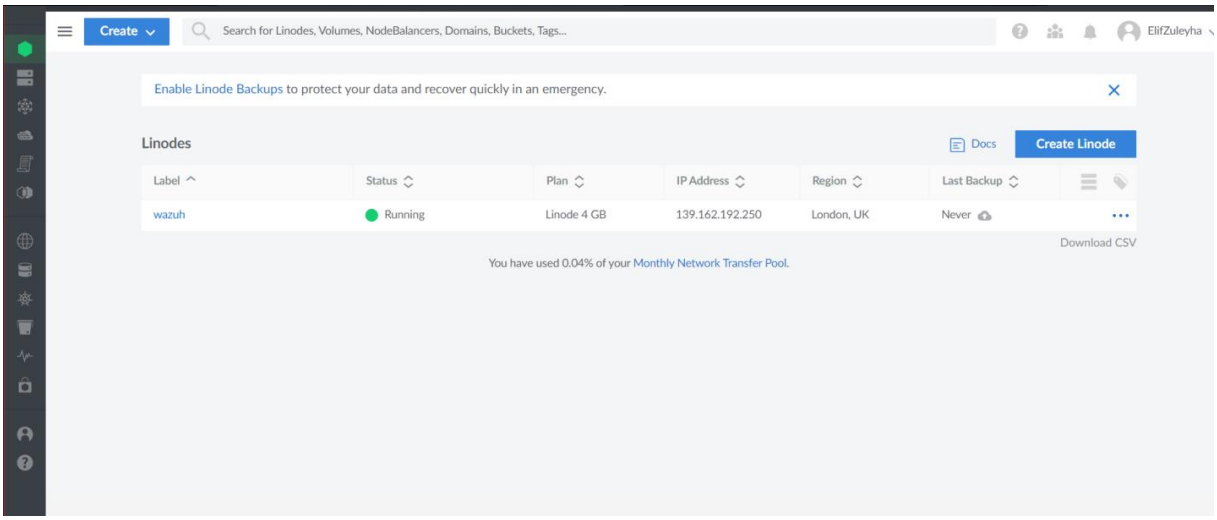




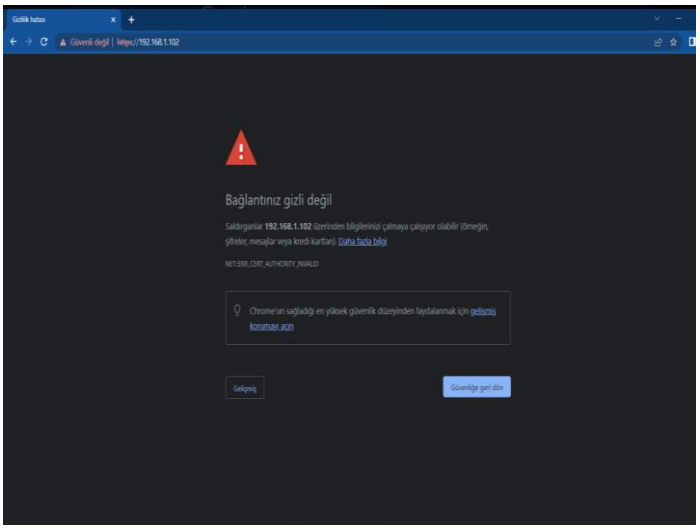
After the information is frozen, go to the “Shared Cpu” section in the “Linode Plan” section and select the CPU and RAM.

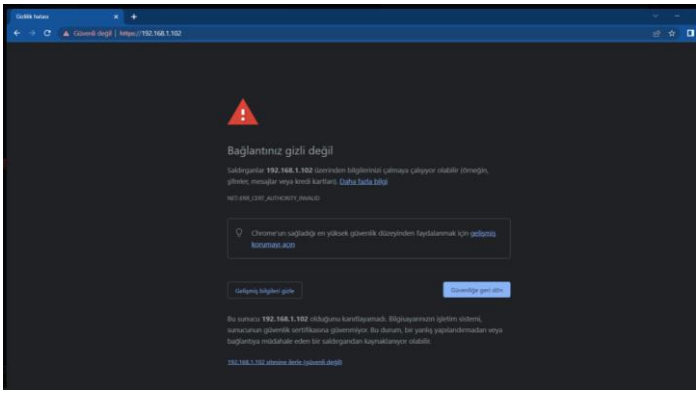


After all the processes are completed, the wazuh tool is installed on Linode. An "ip" address is given for users to access the Wazuh interface. This IP address is searched by typing https:// on the browser.

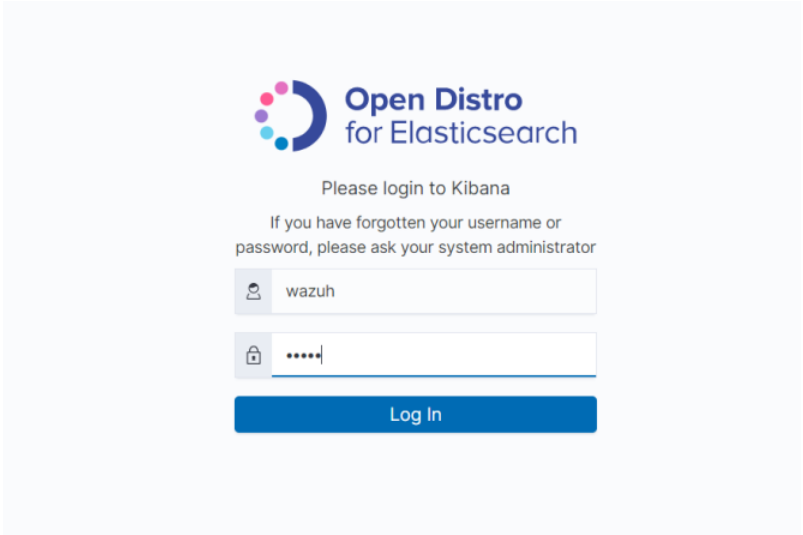


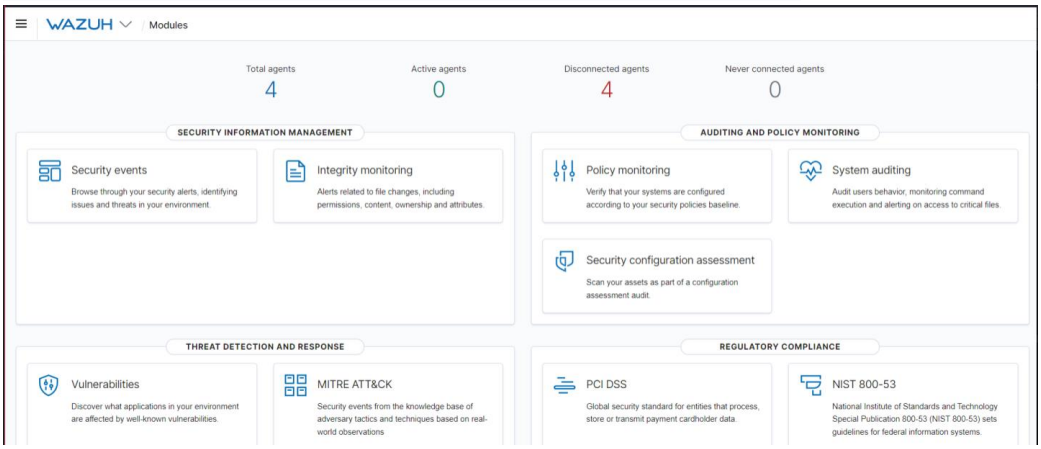
On the page that opens, if a warning such as "your connection is not confidential" is encountered, this warning should not be taken into account.



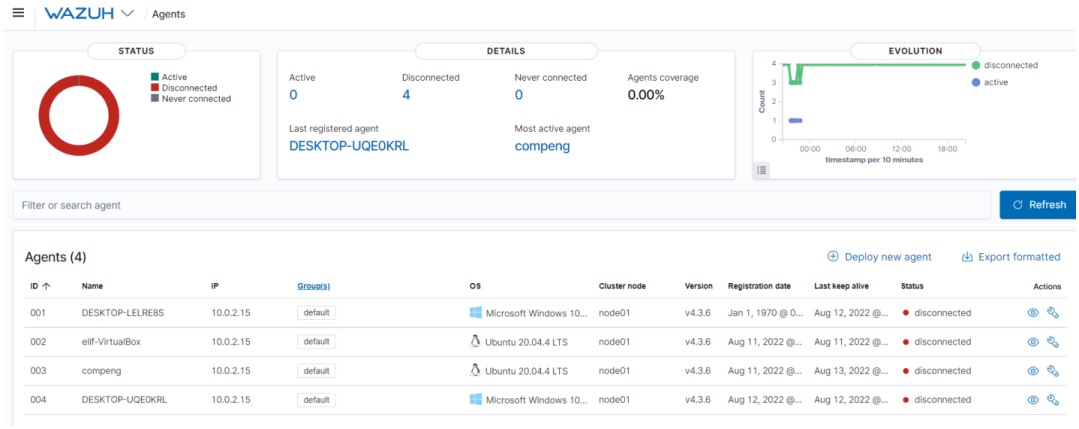


Açılan sayfada wazuh aracına giriş yapmak için username ve pasword kısımlarına "wazuh" yazılır ve sisteme giriş yapılır.





Wazuh agent kurma kısmı wazuh ova kurma kısmında anlatıldığı gibidir.



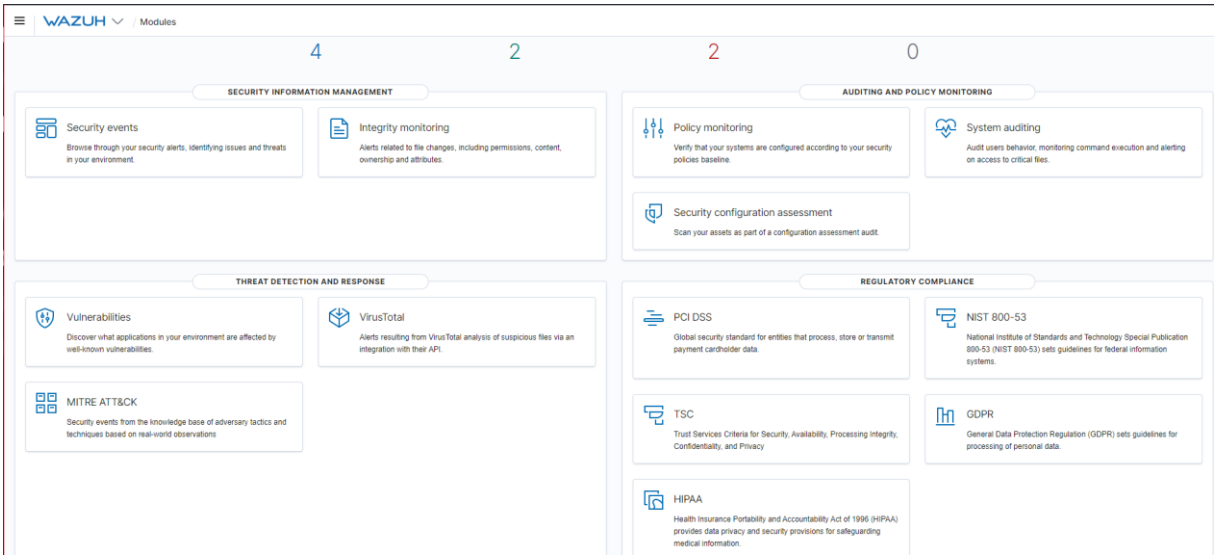
WAZUH MODULES

1.Security Event

2.Integrity Monitoring

3.Vulnerabilities

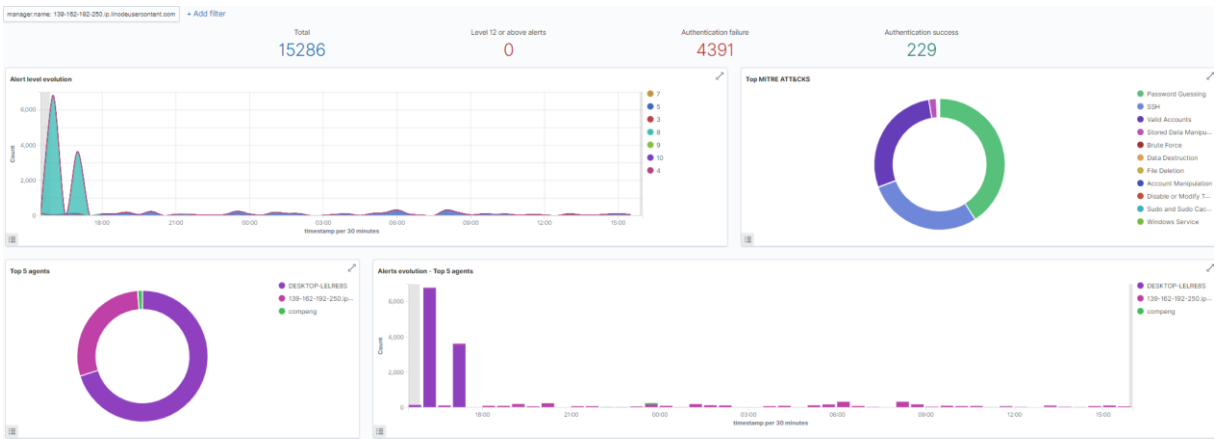
4.MITRE ATT&CK

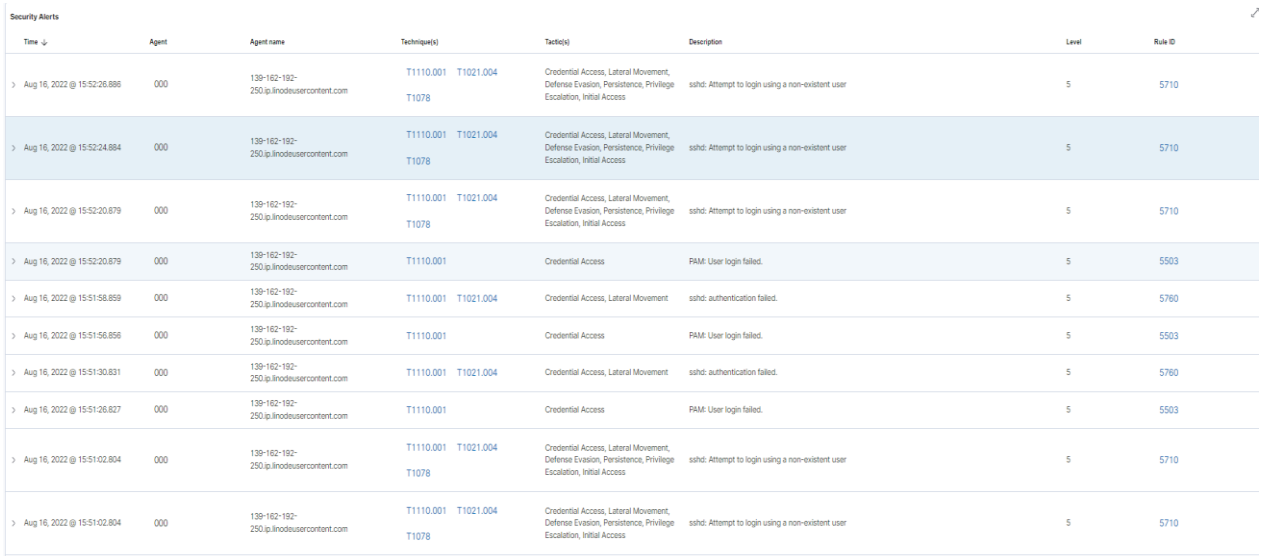


1.SECURITY EVENT:

It provides security warnings by identifying problems and threats in the environment. It consists of 2 components. Dashboard and Events.

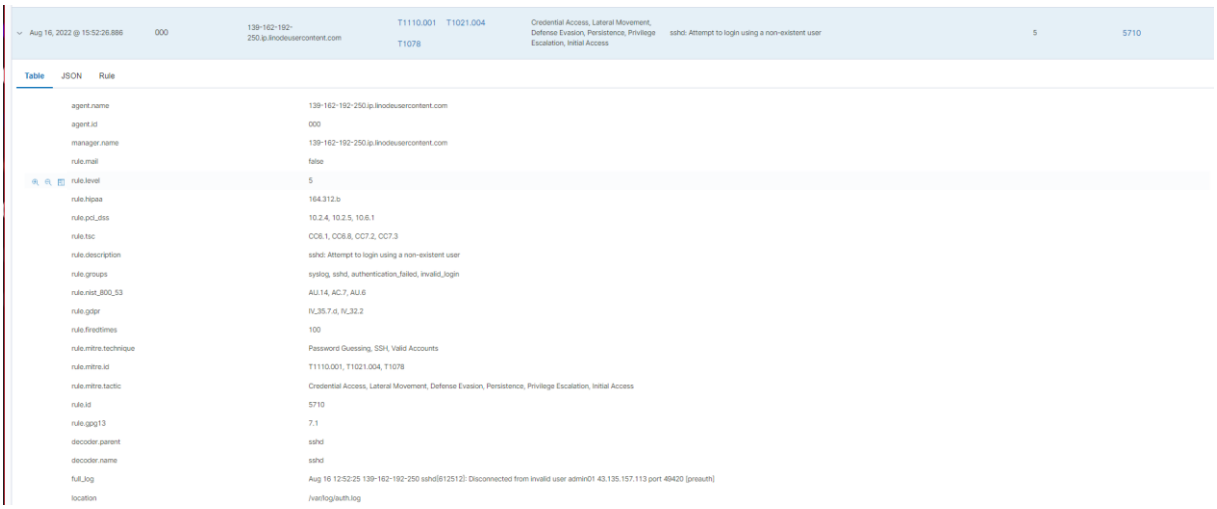
The warnings given in the Dashboard and the threats found are displayed more graphically and there are Security warnings, we can examine these warnings in the form of tables, JSON and rules in this section.





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 T1021.004 T1078	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 @ 15:52:24.884	000	139-162-192-250.ip.linodeusercontent.com	T1110.001 T1021.004 T1078	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 T1021.004 T1078	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 T1021.004 T1078	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 T1021.004 T1078	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Attempt to login using a non-existent user	5	5710

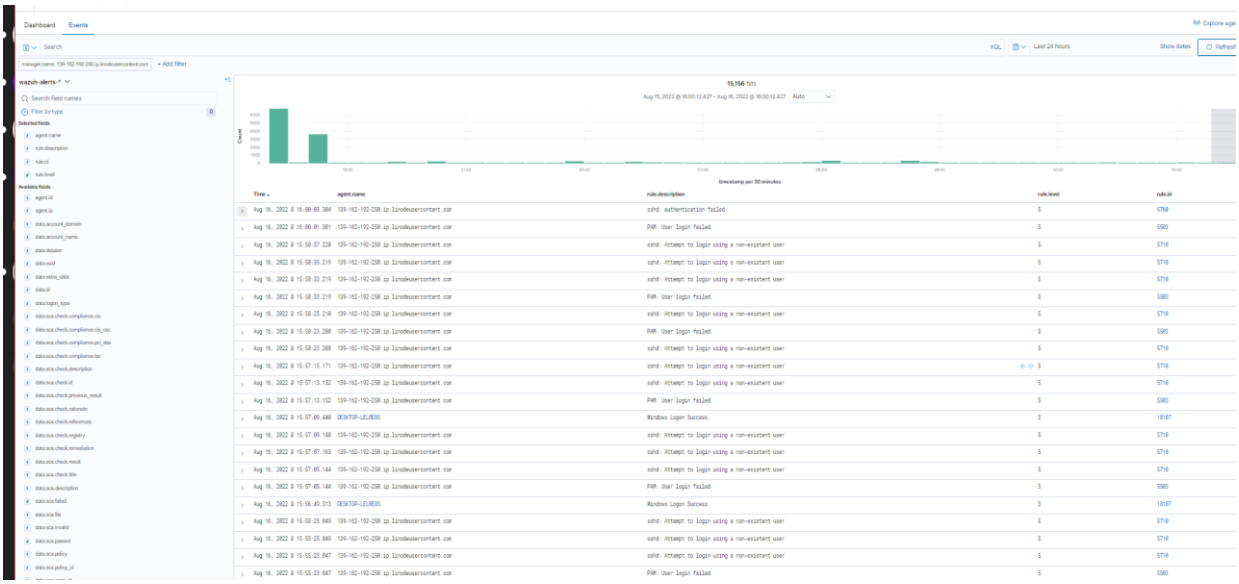


Aug 16, 2022 @ 15:52:26.886 | 000 | 139-162-192-250.ip.linodeusercontent.com | T1110.001 T1021.004 T1078 | Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access | sshd: Attempt to login using a non-existent user | 5 | 5710

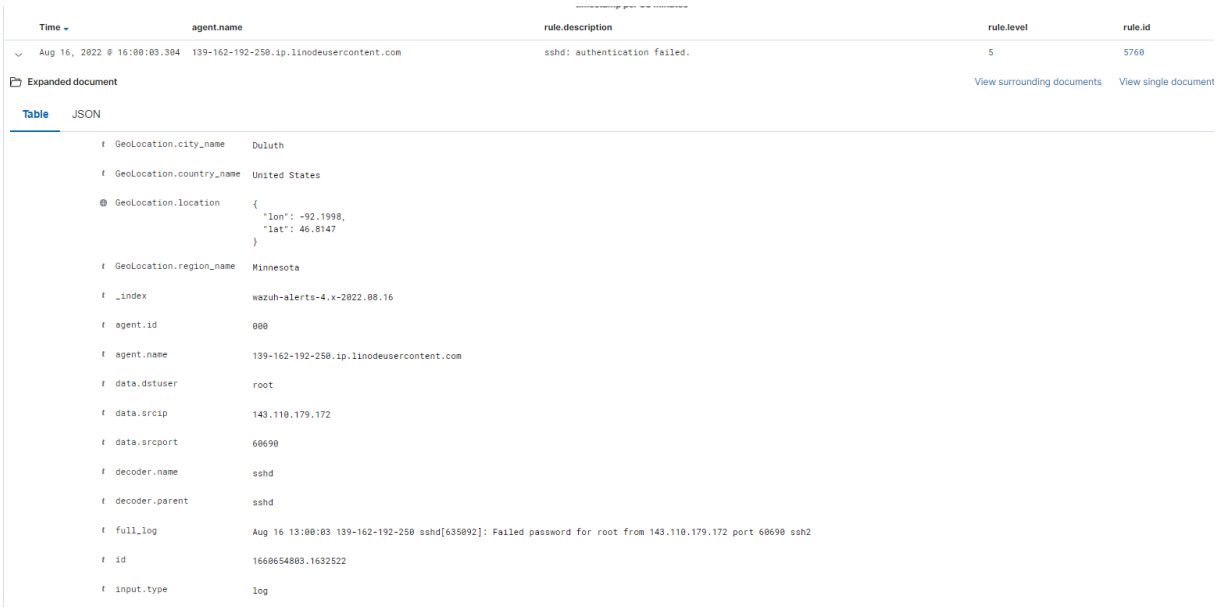
Table JSON Rule

agent.name	139-162-192-250.ip.linodeusercontent.com
agent.id	000
manager.name	139-162-192-250.ip.linodeusercontent.com
rule.mail	false
rule.level	5
rule.hipaa	164.312.b
rule.pci_dss	10.2.4, 10.2.5, 10.6.1
rule.tsc	CC6.1, CC6.8, CC7.2, CC7.3
rule.description	sshd: Attempt to login using a non-existent user
rule.groups	syslog, sshd, authentication_failed, invalid_login
rule.nist_800_53	AU.14, AC.7, AU.6
rule.gdpr	IV_35.7.d, IV_32.2
rule.firedtimes	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[612512]: Disconnected from invalid user admin01 43.135.157.113 port 49420 [preauth]
location	/var/log/auth.log

In the Events section, detailed examination of incoming warnings and threats can be made. Warnings of the desired nature can be found by filtering processes. In this section, threat analysis can also be performed by looking at the values such as location, hash, and full log of the incoming alert.



For example; We received a warning as follows when an attempt was made to gain unauthorized access to our Wazuh server.

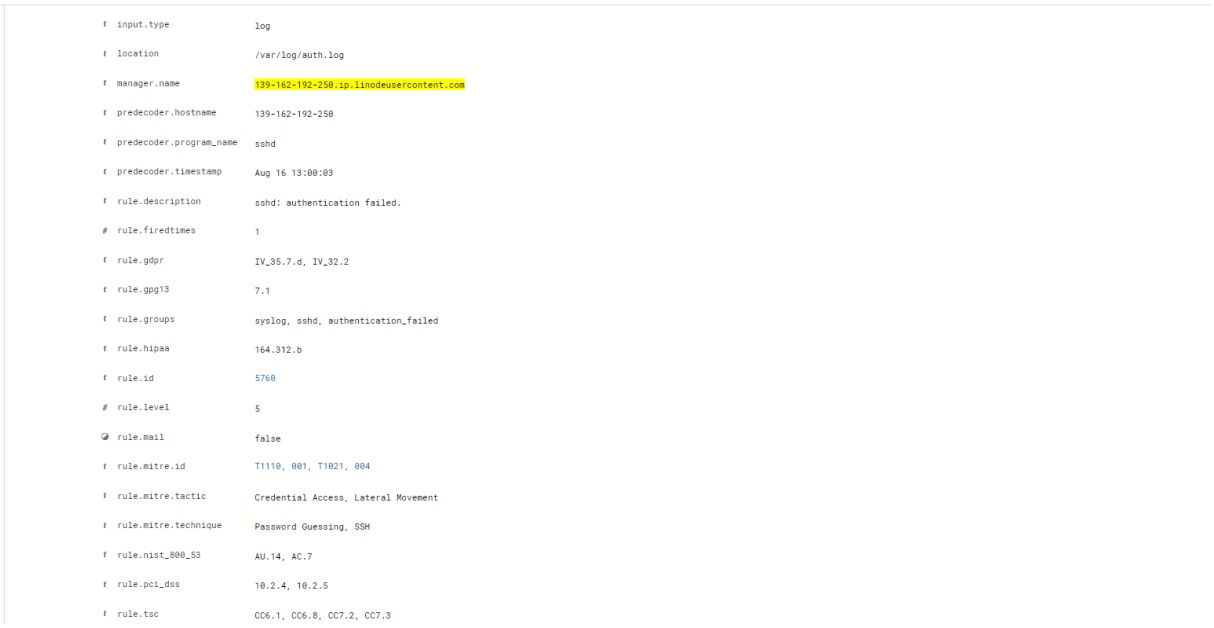


Time	agent.name	rule.description	rule.level	rule.id
Aug 16, 2022 @ 16:00:03.304	139-162-192-250.ip.linodeusercontent.com	sshd: authentication failed.	5	5760

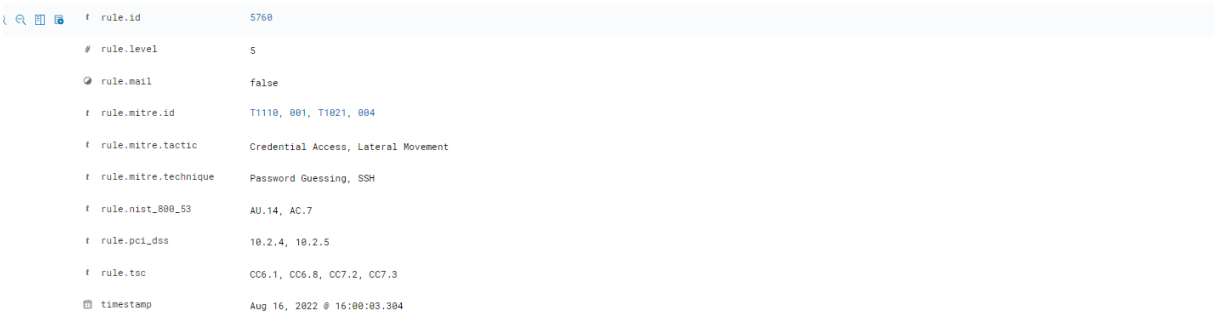
Expanded document — View surrounding documents — View single document

Table | JSON

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[635892]: Failed password for root from 143.110.179.172 port 60690 ssh2
t id	1660654803.1632522
t input.type	log



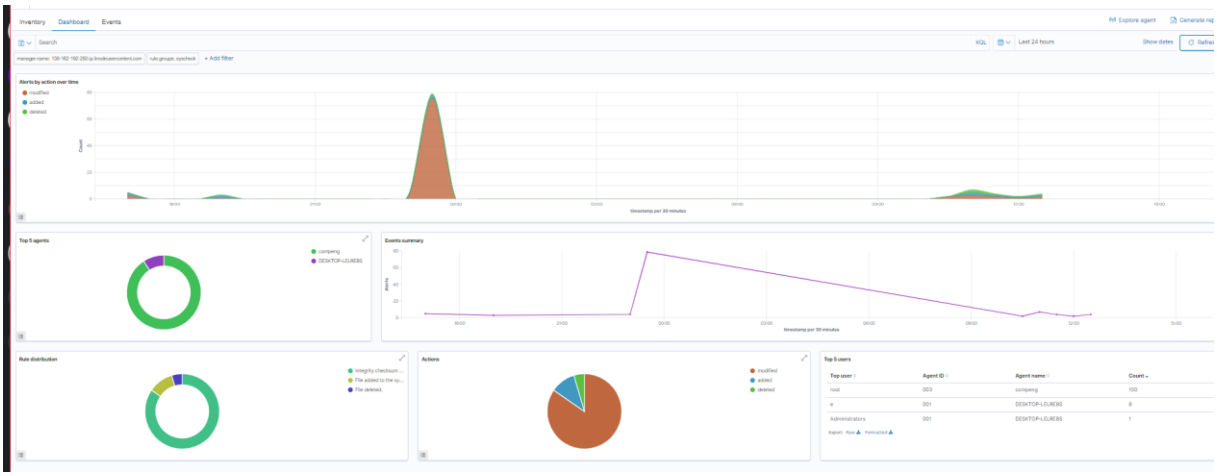
t	input.type	log
t	location	/var/log/auth.log
t	manager.name	139-162-192-250.ip.linodeusercontent.com
t	predecoder.hostname	139-162-192-250
t	predecoder.program_name	sshd
t	predecoder.timestamp	Aug 16 13:00:03
t	rule.description	sshd: authentication failed.
#	rule.firedtimes	1
t	rule.gdpr	IV_35.7.d, IV_32.2
t	rule.gpg13	7.1
t	rule.groups	syslog, sshd, authentication_failed
t	rule.hipaa	164.312.b
t	rule.id	5760
#	rule.level	5
◕	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



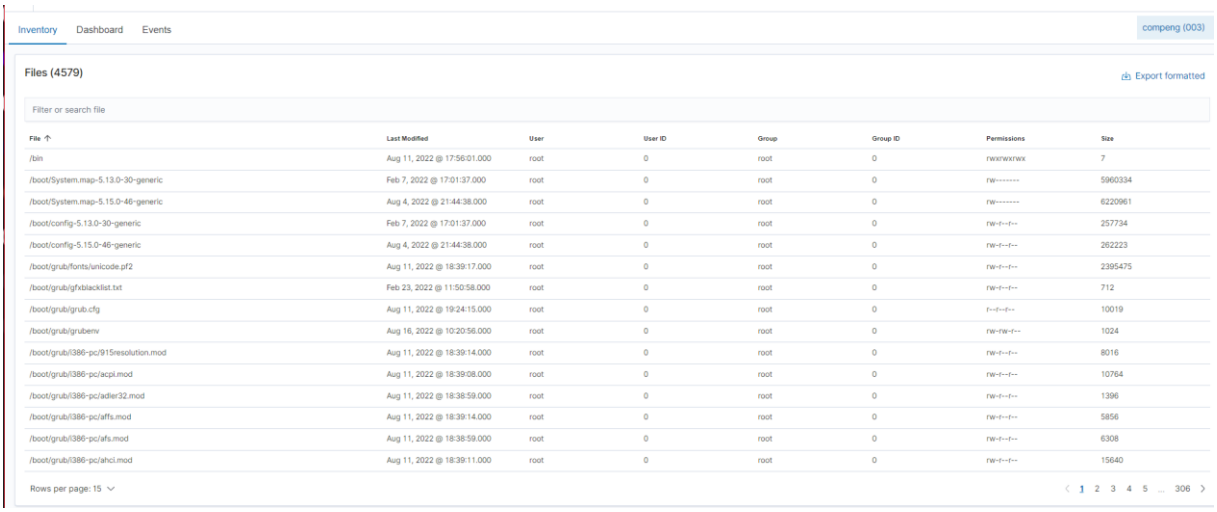
t	rule.id	5760
#	rule.level	5
◕	rule.mail	false
t	rule.mitre.id	T1110, 001, T1021, 004
t	rule.mitre.tactic	Credential Access, Lateral Movement
t	rule.mitre.technique	Password Guessing, SSH
t	rule.nist_800_53	AU.14, AC.7
t	rule.pci_dss	10.2.4, 10.2.5
t	rule.tsc	CC6.1, CC6.8, CC7.2, CC7.3
🗓	timestamp	Aug 16, 2022 @ 16:00:03.304

2.Integrity Monitoring:

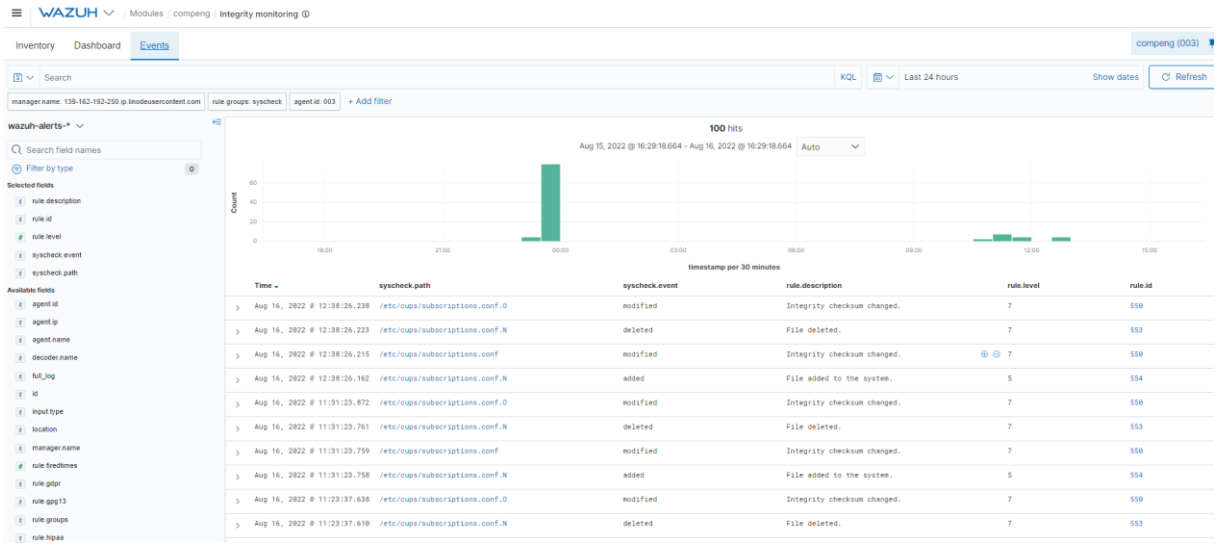
Warnings about file changes including permission, content, ownership and attributes can be seen in this section. For example, when a file is added to the system, the content of the file is changed, deleted or a file is downloaded to the system, we can perform detailed inspections from the Integrity Monitoring section. Dashboard, Inventory and Events. It consists of 3 parts. We can monitor graphically from the Dashboard part.



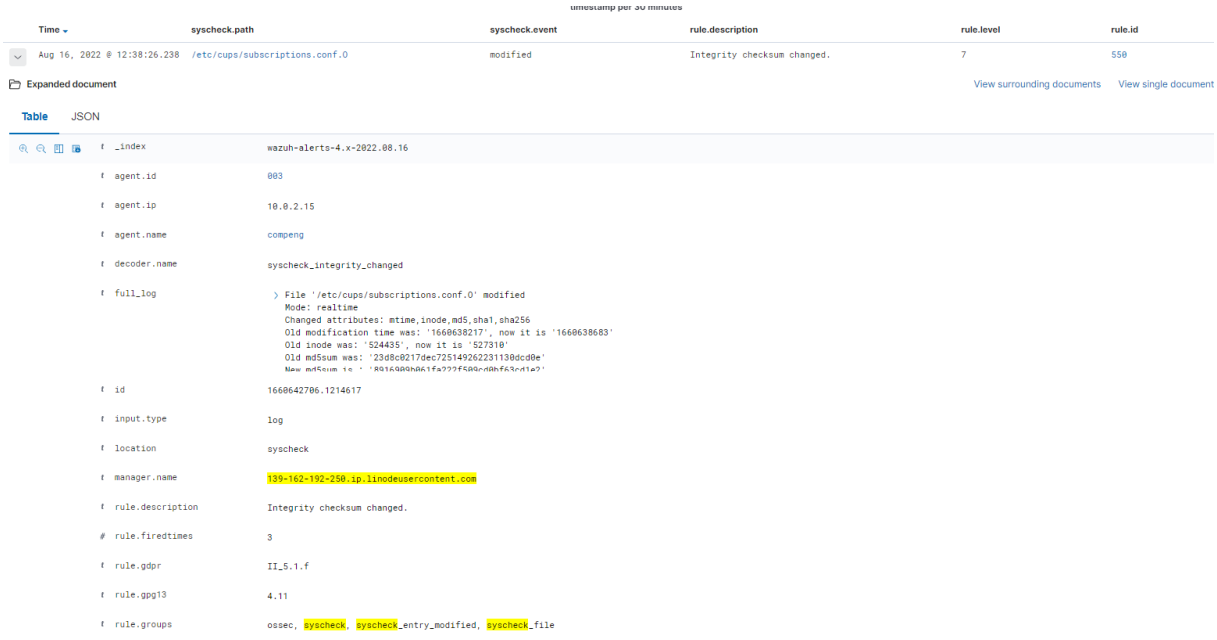
In the Inventory section, it is shown when and by whom the last change of which file was made.



In the Events section, we can monitor in more detail. As preparation for our project, we customized our agents by editing the ossec.conf file and the agents sent a warning to the wazuh server when there were file adding, deleting, content modification and download processes in the system by looking at the files we want to look at. as such;



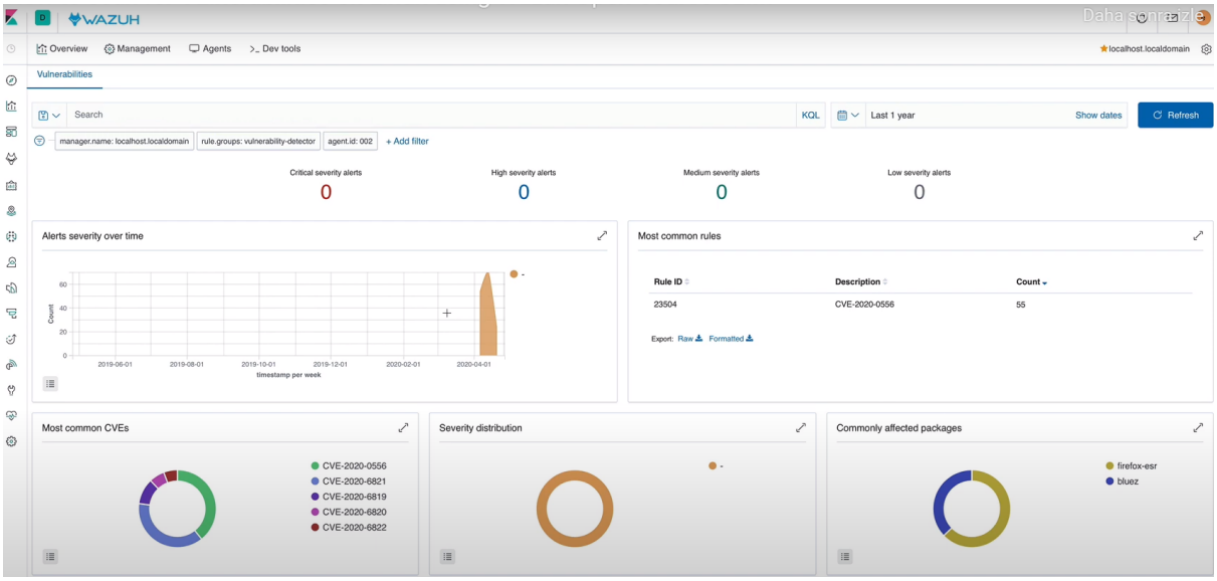
In this section, all the details of the transactions can be examined.



3.Vulnerabilities:

Using the Vulnerability Detector module, Wazuh is able to detect vulnerabilities in applications installed on agents. To detect vulnerabilities, agents can collect a list of installed applications locally and periodically send it to the administrator (where it is stored in local SQLite databases, one for each agent). In addition, the administrator creates a global database of vulnerabilities from public CVE repositories, which he then uses to cross-correlate with his agent's application inventory data.

After the global vulnerability database (with CVEs) is created, the detection process searches the inventory databases (unique per agent) for vulnerable packages. Alerts are generated when a CVE (Common Vulnerabilities and Exposures) affects a package known to have been installed on one of the monitored hosts. A package is labeled as a vulnerability when its version is within the affected range of a CVE. Results are presented as alerts and are also stored in a per-agent vulnerabilities inventory. This way, you can check for recent scan alerts or query each agent's inventory of vulnerabilities.



4.MITRE ATT&CK:

MITER stands for ATT&CK, MITER stands for Hostile Tactics, Techniques and Common Knowledge (ATT&CK). The MITER ATT&CK framework is a selected knowledge base and model for cyber attacker behavior that reflects the various stages of an adversary's attack lifecycle and the known platforms they target. Its tactical and technical abstraction in the model provides a common classification of individual enemy actions understood by both the offensive and defensive sides of cybersecurity. It also provides an appropriate level of categorization for enemy action and specific ways to defend against it.

-The most up-to-date information center showing the Behavior antomy of an attack.

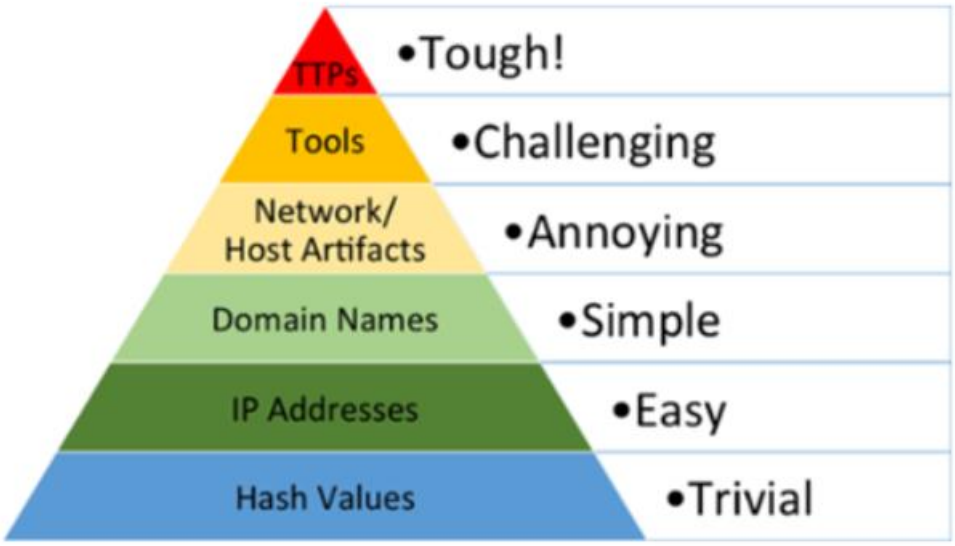
- Created by Observing Attacks that occur in the real world.

- Based on Tactics, Techniques and Procedures.

It is a free, open and accessible information center.

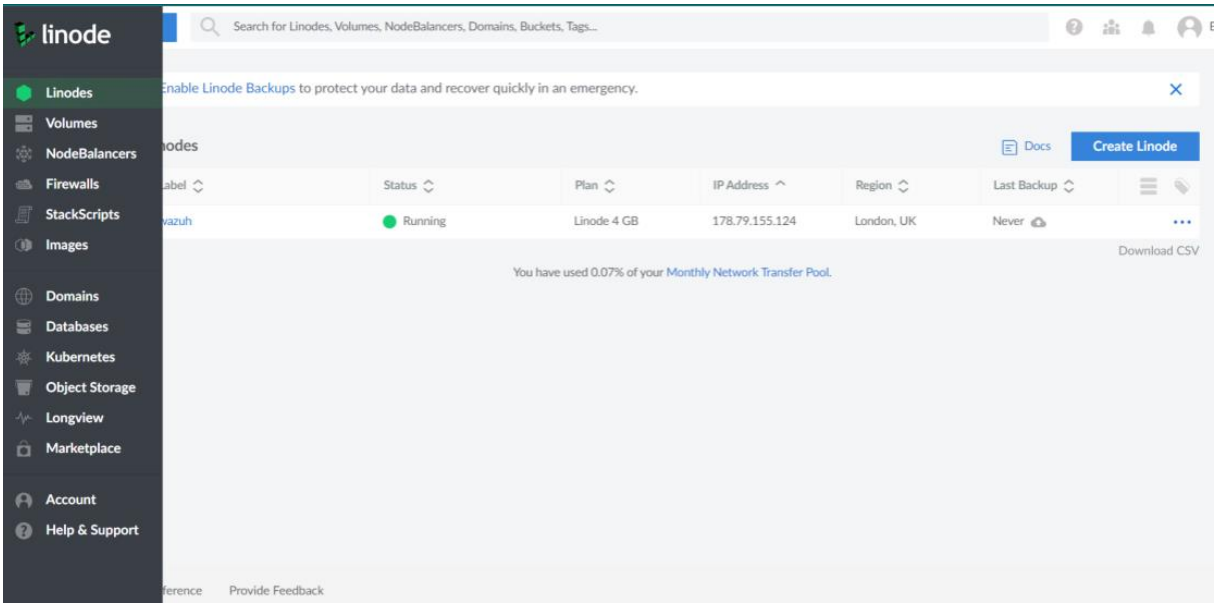
-Community-Driven, Supported by 100+ Organizations and People

.

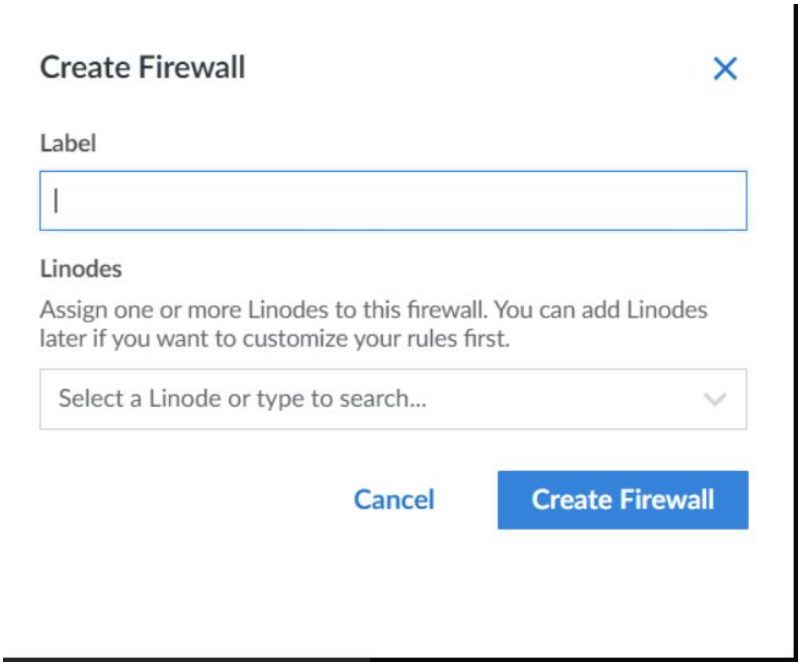


CREATING A FIREWALL ON WAZUH AND WRITE RULES

1- Click the Firewalls button.

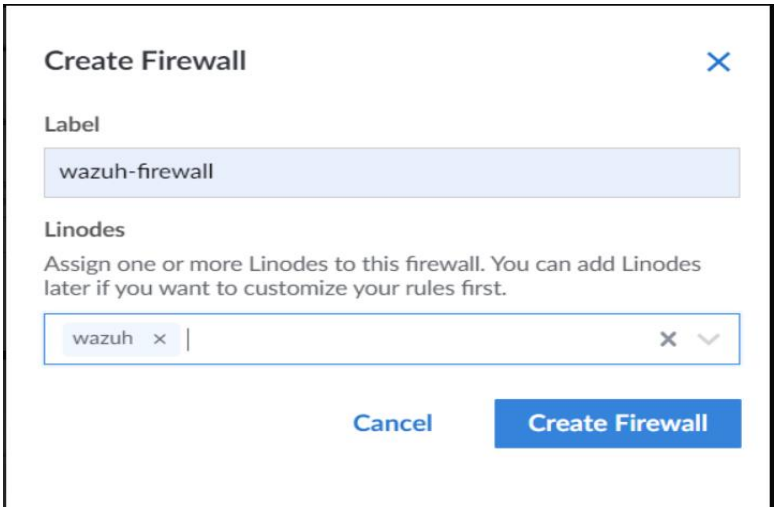


2- Click on the create firewall button from the page that appears and the following screen is encountered;

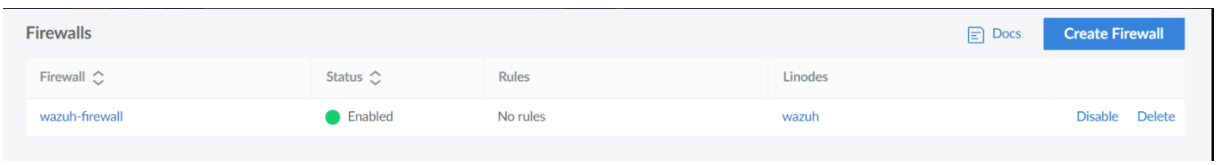


3- Since we will use firewall for wazuh, we filled this screen as follows;

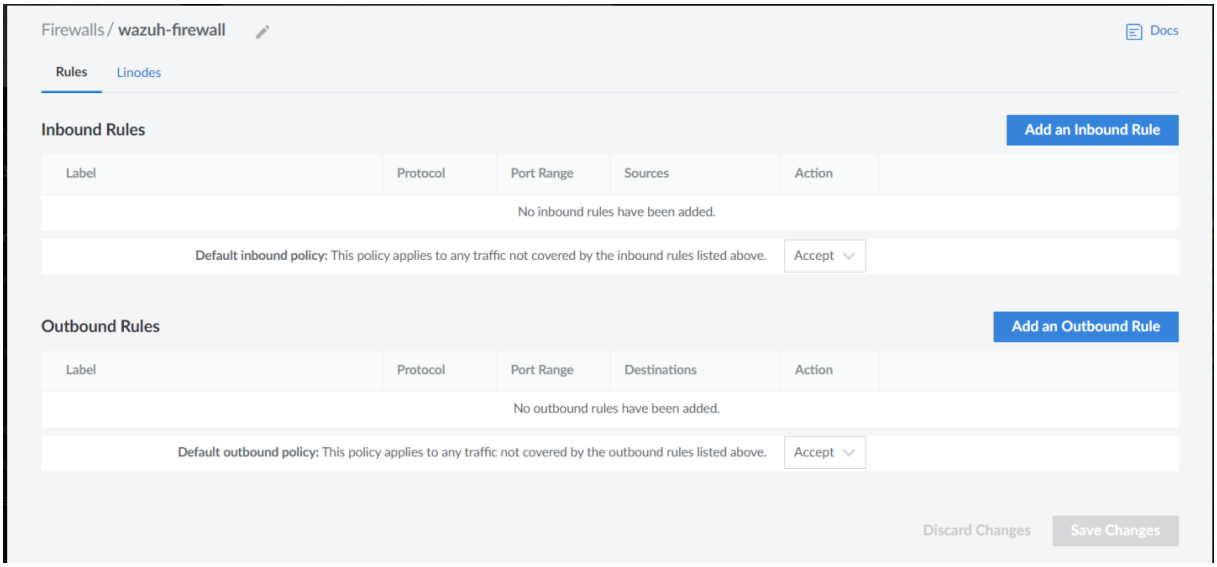
Instead of “label”, the name for the firewall is written. In the “linode” part, the tool that we will use the firewall is selected and the create firewall button is clicked.



This is how it looks when the firewall occurs.



4- Clicking on the name of the Firewall opens the page where the rules are written. Rules can be written for the Firewall created in this section.



After adding any rule, click the save changes button to save the changes.