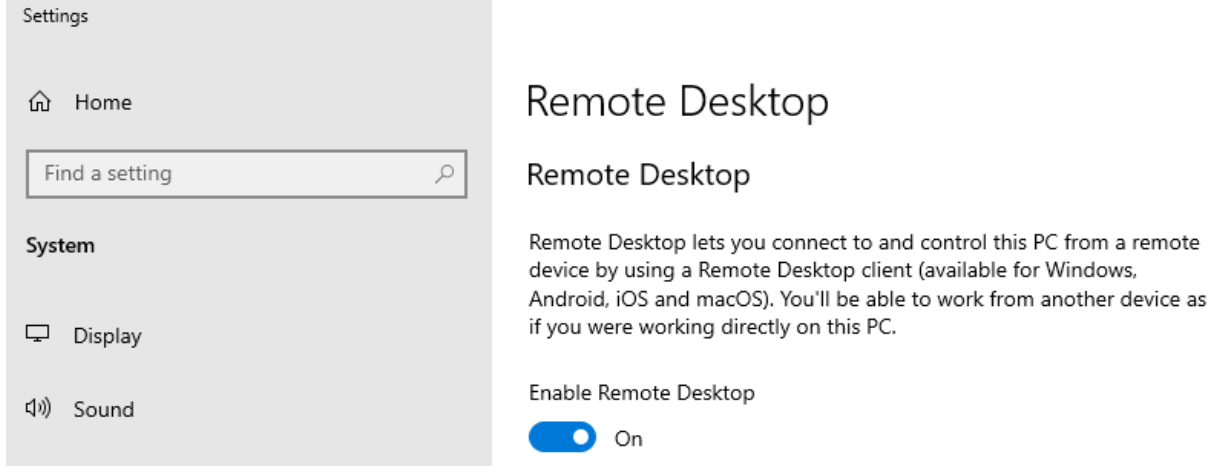


Wazuh ile SIEM Ortamı Hazırlama Raporu

1. Sanal Ortam Hazırlama

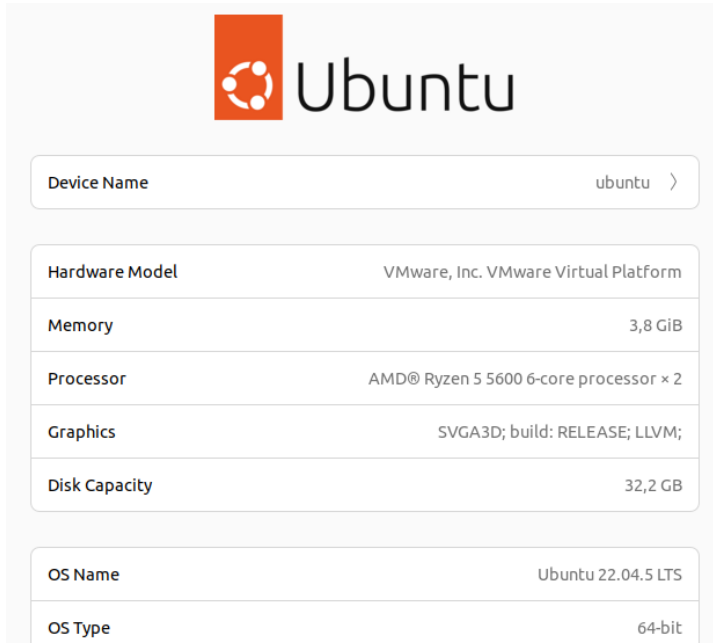
Bu örnek SIEM senaryosunda Windows Server 2019 (Versiyon 1809) ve Ubuntu 22.04.5 LTS Desktop işletim sistemlerini kullandım. Windows için 2-4 GB, 2 CPU ve Linux için 4 GB, 2 CPU önerilen değerlerini kullandım. Windows Server üzerinde Ayarlar > Remote Desktop (Uzak Masaüstü) sekmesinden RDP'yi saldırmak üzere senaryo gereği açtım.



Windows Server IP: 192.168.28.129

Ubuntu IP: 192.168.28.131

Ubuntu kurulumunu herhangi bir ek ayar yapmadan, sadece **net-tools**, **curl** gibi paketleri kurarak tamamladım. İki makineyi de VMware üzerinde NAT ağını seçerek ayağa kaldırdım. İkisinin de aynı ağda olduğundan emin oldum.

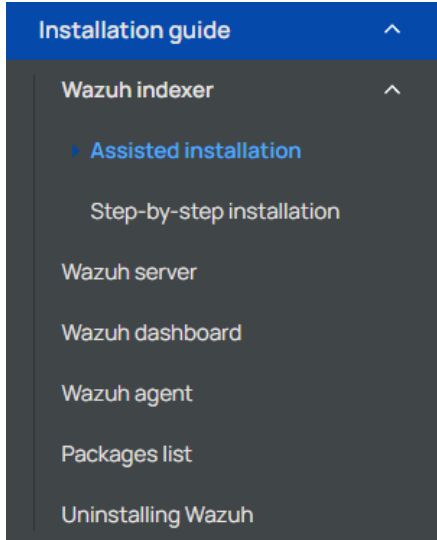


30 GB ve üzeri disk alanı tanımlamanız daha iyi olacaktır.

2. Wazuh Server Kurulumu

Bu aşamada Wazuh'un kendi dokümanını kullanarak ilerledim.

[“Installation guide · Wazuh documentation”](#) sayfasından sırasıyla Wazuh Indexer, Wazuh Server ve Dashboard'ın kurulumunu anlatacağım. Kendileri iki çeşit kurulum sunuyor. Adım adım olan daha detaylı ve Destekli Kurulum olan daha pratik bir şekilde ilerliyor. Daha hızlı ilerlemek için Destekli kurulum sayfalarından ilerledim.



Öncelikle “wazuh” isimli bir dosya açarak işlemlere buradan açtığım terminalle devam ettim.

Dokümanı takip ederek;

```
curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh
```

```
curl -sO https://packages.wazuh.com/4.11/config.yml
```

komutlarıyla gerekli ilk dosyaları indirdim. “config.yml” dosyasında Wazuh Server olarak kullanacağım Ubuntu makinenin IP'sini uygun alanlara yazdım.

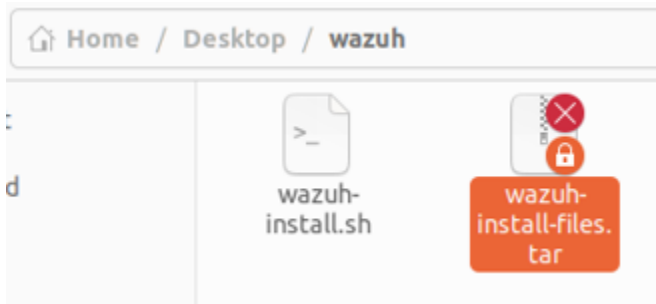
```
Open  [icon] *config.yml
~/Desktop/wazuh

1 nodes:
2 # Wazuh indexer nodes
3 indexer:
4   - name: node-1
5     ip: "192.168.28.131"
6   #- name: node-2
7   # ip: "<indexer-node-ip>"
8   #- name: node-3
9   # ip: "<indexer-node-ip>"
10
11 # Wazuh server nodes
12 # If there is more than one Wazuh server
13 # node, each one must have a node_type
14 server:
15   - name: wazuh-1
16     ip: "192.168.28.131"
17   # node_type: master
18   #- name: wazuh-2
19   # ip: "<wazuh-manager-ip>"
20   # node_type: worker
21   #- name: wazuh-3
22   # ip: "<wazuh-manager-ip>"
23   # node_type: worker
24
25 # Wazuh dashboard nodes
26 dashboard:
27   - name: dashboard
28     ip: "192.168.28.131"
```

```
user@ubuntu:~/Desktop/wazuh$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING
    inet 192.168.28.131 netmask 2
    inet6 fe80::9628:520a:ce59:224
    ether 00:0c:29:4f:02:65 txque
    RX packets 3794897 bytes 5488
    RX errors 0 dropped 0 overru
    TX packets 533962 bytes 34003
    TX errors 0 dropped 0 overrun

lo: flags=73<UP,LOOPBACK,RUNNING> mtu
    inet 127.0.0.1 netmask 255.0.
    inet6 ::1 prefixlen 128 scop
    loop txqueuelen 1000 (Local
    RX packets 705317 bytes 14938
    RX errors 0 dropped 0 overru
    TX packets 705317 bytes 14938
    TX errors 0 dropped 0 overrun
```

Daha sonra `bash wazuh-install.sh --generate-config-files` komutuyla kurulum için gerekli “wazuh-install-files.tar” dosyasını oluşturdum.



```
ubuntu$ sudo bash wazuh-install.sh --generate-config-files
Starting Wazuh installation assistant. Wazuh version:
Verbose logging redirected to /var/log/wazuh-install.l

--- Dependencies ---
Installing gawk.
Verifying that your system meets the recommended minimum

--- Configuration files ---
Generating configuration files.
Generating the root certificate.
Generating Admin certificates.
Generating Wazuh indexer certificates.
Generating Filebeat certificates.
Generating Wazuh dashboard certificates.
```

`bash wazuh-install.sh --wazuh-indexer node-1` ile Indexer kurulumu, ardından

`bash wazuh-install.sh --start-cluster` komutu ile Indexer’i başlattım.

```
28/04/2025 17:50:21 INFO: Updating the internal users.
28/04/2025 17:50:27 INFO: A backup of the internal users has been saved in the /
etc/wazuh-indexer/internalusers-backup folder.
28/04/2025 17:50:40 INFO: The filebeat.yml file has been updated to use the File
beat Keystore username and password.
28/04/2025 17:51:10 INFO: Wazuh indexer cluster started.
```

Bu kurulumdan sonra aşağıdaki komutla kurulumda tanımlanan node-1 için oluşturulan Keystore indexer_username ve indexer_password değerlerini bir kenara kaydediyoruz.

`sudo` ile

```
tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O |
grep -P "'admin'" -A 1
```

```
user@ubuntu:~/Desktop/wazuh$ sudo tar -axf wazuh-install-files.tar wazuh-install
-files/wazuh-passwords.txt -O | grep -P "'admin'" -A 1
  indexer_username: 'admin'
  indexer_password: 'N1U+XmAaw?8p1n1S3ySd*qWRerxFhkkzL'
```

(Bu şifre değeri önemsiz olduğu için bu rehberde gizleme gereği duymadım.)

Daha sonra `curl -k -u admin:<Admin_şifreniz> https://<Wazuh_Indexer_IPniz>:9200`

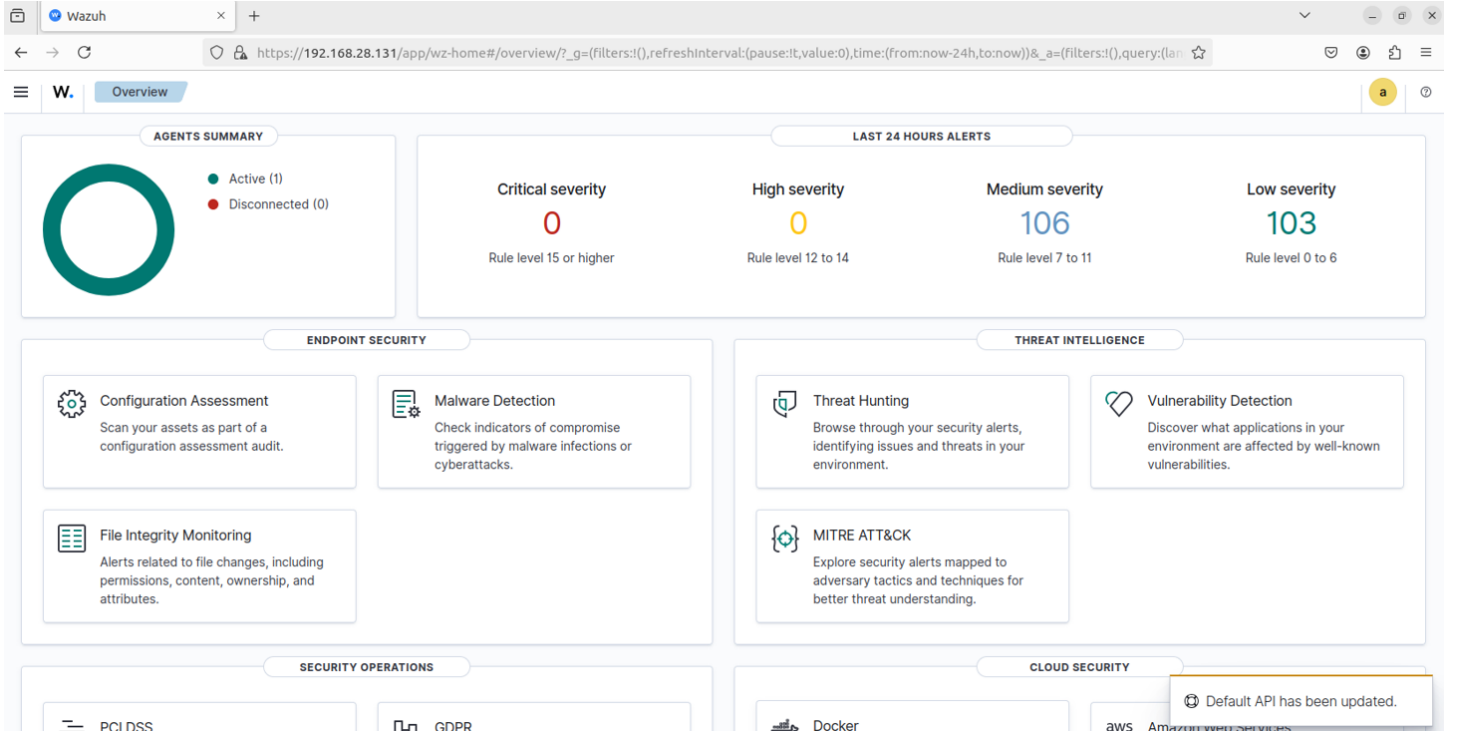
```
user@ubuntu:~/Desktop/wazuh$ curl -k -u admin:N1U+XmAaw?8p1n1S3ySd*qWRerxFhkkzL h
https://192.168.28.131:9200
{
  "name" : "node-1",
  "cluster_name" : "wazuh-indexer-cluster",
  "cluster_uuid" : "USWtRr4dRUu40Hmp6f0tFg",
  "version" : {
    "number" : "7.10.2",
    "build_type" : "deb",
    "build_hash" : "e5a68d19815af94a9883fead7927edb40181f32d",
    "build_date" : "2025-03-26T19:08:40.098412Z",
    "build_snapshot" : false,
    "lucene_version" : "9.11.1",
    "minimum_wire_compatibility_version" : "7.10.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "The OpenSearch Project: https://opensearch.org/"
}
```

komutuyla beraber cluster kontrolü yaptım. Her şey yolunda gözüküyor.

Bir sonraki adımda `bash wazuh-install.sh --wazuh-server wazuh-1` komutuyla Wazuh Server kurulumu yaptım. Kurulumlar bazen uzun sürebilir, işlem tamamen bitene kadar iptal etmeyin. Sorunsuz kurulduktan sonra `bash wazuh-install.sh --wazuh-dashboard dashboard` komutuyla Ubuntu tarafındaki son kurulumu yaptım. Dashboard tarafında varsayılan port 443 olarak belirleniyor. Kurulumdan sonra giriş yapmamız için aynı username:password ekrana çıkıyor.

```
INFO: --- Summary ---
INFO: When Wazuh dashboard is able to connect to your Wazuh
indexer cluster, you can access the web interface https://192.168.28.131
User: admin
Password: N1U+XmA7?8p1n1S3ySd*qWReRxFhkkzL
```

Kontrol etmek için giriş yapıyoruz. Ve API doğru şekilde ayarlanmış, çalışır durumda gözüküyor.



Aynı zamanda `sudo systemctl status wazuh-manager`, `sudo systemctl status filebeat`, `sudo systemctl status wazuh-indexer` gibi komutlarla servislerin sistem üzerinden durumlarını kontrol ettim.

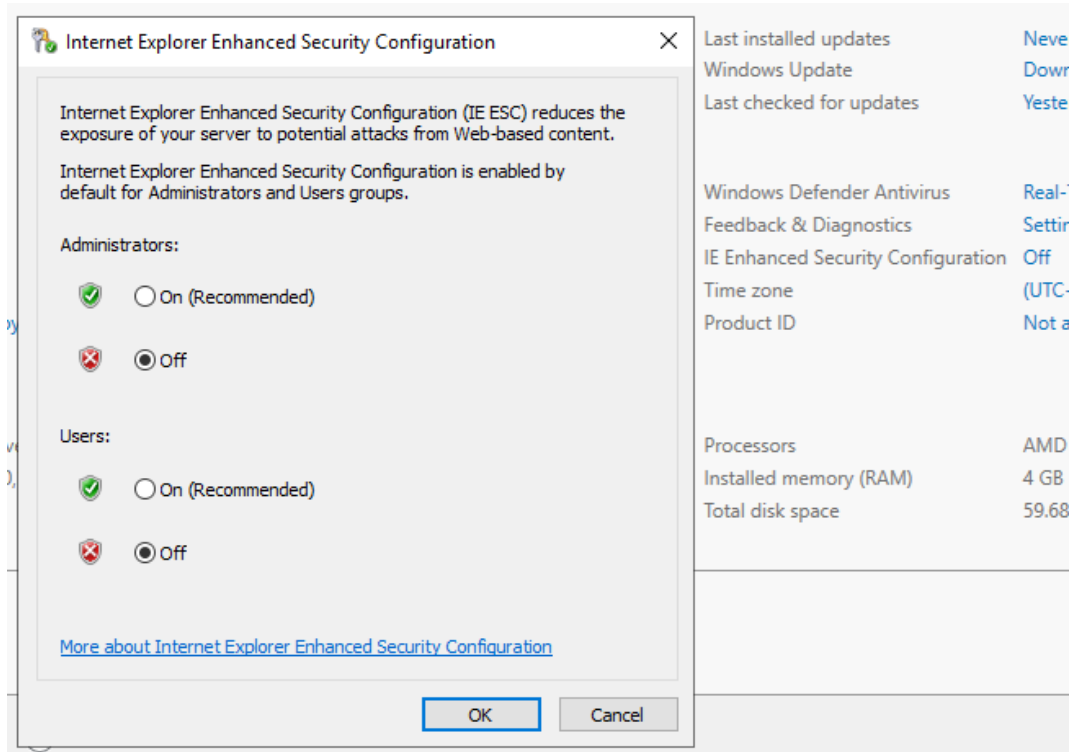
```
● wazuh-manager.service - Wazuh manager
   Loaded: loaded (/lib/systemd/systemd; vendor preset: enabled)
   Active: active (running) since Mon 2023-10-23 14:14:14 CEST; 1min ago
     Tasks: 154 (limit: 4551)
   Memory: 1.1G
   CGroup: /systemd/systemd/wazuh-manager.service

● wazuh-indexer.service - wazuh-indexer
   Loaded: loaded (/lib/systemd/systemd; vendor preset: enabled)
   Active: active (running) since Mon 2023-10-23 14:14:14 CEST; 1min ago
     Docs: https://documentation.wazuh.com/4.4.0/indexer.html
   Memory: 1.1G
   CGroup: /systemd/systemd/wazuh-indexer.service

● filebeat.service - Filebeat sends log
   Loaded: loaded (/lib/systemd/systemd; vendor preset: enabled)
   Active: active (running) since Mon 2023-10-23 14:14:14 CEST; 1min ago
     Docs: https://www.elastic.co/products/logstash
```

3. Wazuh Agent Kurulumu (Windows)

Windows Server tarafında internete rahat erişebilmek için öncelikle Server Manager > Local Server kısmından “IE Enhanced Security Configuration” kısmını Off durumuna getiriyoruz.



Daha sonra farklı bir tarayıcı indirip oradan devam edebilirsiniz veya doğrudan

“[Installing Wazuh agents on Windows endpoints - Wazuh agent](#)” sayfasında bulunan Windows Installer “.msi” dosyasını indirebilirsiniz. Bu kurulumu yaparak GUI ile veya PowerShell üzerinden dokümanda belirtilen `.\wazuh-agent-4.11.2-1.msi /q WAZUH_MANAGER="192.168.28.131"` komutu ve ardından **NET START Wazuh**

komutuyla Windows Server tarafında Wazuh Agent servisini aktif hale getirdim.

```
PS C:\Users\serveruser\Downloads> .\wazuh-agent-4.11.2-1.msi /q WAZUH_MANAGER="192.168.28.131"
PS C:\Users\serveruser\Downloads> NET START Wazuh

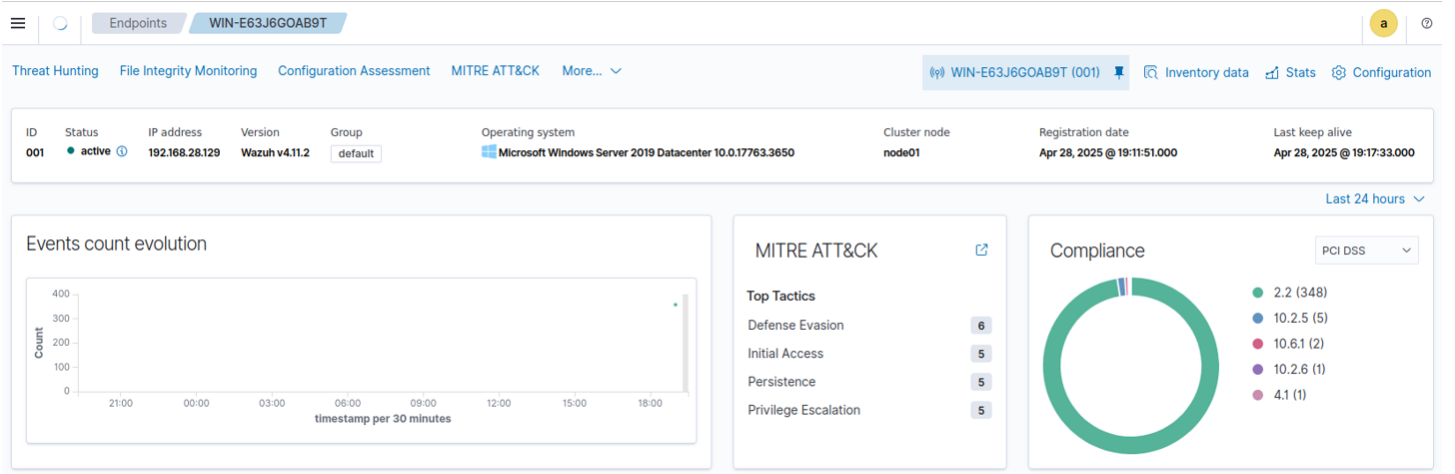
The Wazuh service was started successfully.
```



Servisler kısmından kontrol ettiğimde çalışır durumda gözüküyor. İki makinenin haberleştiğinden emin olmak için ping atıyorum.

```
C:\Users\serveruser>ping 192.168.28.131

Pinging 192.168.28.131 with 32 bytes of data:
Reply from 192.168.28.131: bytes=32 time=1ms TTL=64
Reply from 192.168.28.131: bytes=32 time<1ms TTL=64
Reply from 192.168.28.131: bytes=32 time<1ms TTL=64
Reply from 192.168.28.131: bytes=32 time<1ms TTL=64
```

Wazuh arayüzüne tekrar döndüğümüzde makine bağlı şekilde gözüküyor.

4. Brute-Force Saldırısı İçin Alert (Uyarı) Oluşturma ve İnceleme

Wazuh, Windows Server üzerindeki brute-force saldırılarını algılamak için varsayılan olarak kural ID 60122'yi kullanır. Bu kural, Windows Security logundaki olay kimlikleri 4625 ve 529'u (başarısız oturum açma girişimleri) izler. Dolayısıyla hem manuel olarak hem de Wazuh Dashboard üzerinden ilgili kuralı kontrol ettim.

The screenshot shows the Wazuh Rules configuration page. The top navigation bar includes Rules. The main content area displays a table of rules, with rule 60122 selected. The table columns are ID, Description, Groups, Regulatory compliance, Level, and File.

ID	Description	Groups	Regulatory compliance	Level	File
60122	Logon Failure - Unknown user or bad password	authentication_failed, windows, windows_security	PCI_DSS, GPG13, HIPAA, GDPR, NIST_800_53, TSC, MITRE	5	0580-win-security_rules.xml

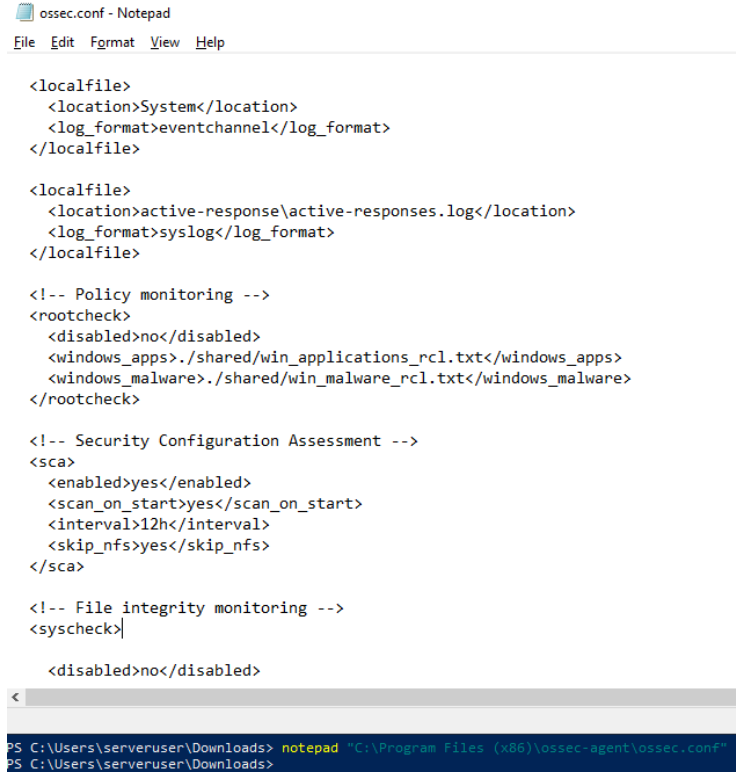
Wazuh üzerinde varsayılan kurulum halinde ilgili kural aktif gelmiş gözüküyor.

Aynı zamanda `sudo nano /var/ossec/ruleset/rules/0580-win-security_rules.xml` komutuyla da kontrol ettim.

```
GNU nano 6.2 /var/ossec/ruleset/rules/0580-win-security_rules.xml
</rule>
```

```
<!-- Granular windows login rules -->
<rule id="60122" level="5">
  <if_sid>60105</if_sid>
  <field name="win.system.eventID">^529$|^4625$</field>
  <description>Logon Failure - Unknown user or bad password</description>
  <options>no_full_log</options>
  <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,gpg13_7.1,gdpr_I<
  <mitre>
    <id>T1531</id>
  </mitre>
</rule>
```

Windows Server üzerinde **notepad** "C:\Program Files (x86)\ossec-agent\ossec.conf" konumundaki "ossec.conf" dosyasındaki **<localfile>** kısımlarını kontrol ediyoruz. Yetki gerektirdiği için PowerShell'i **yönetici** olarak başlatın.



```
ossec.conf - Notepad
File Edit Format View Help

<localfile>
  <location>System</location>
  <log_format>eventchannel</log_format>
</localfile>

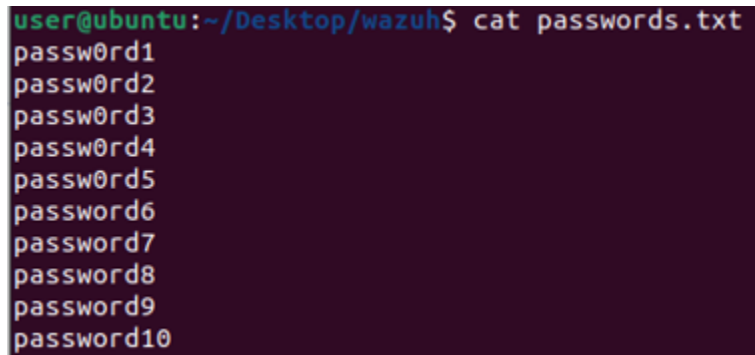
<localfile>
  <location>active-response\active-responses.log</location>
  <log_format>syslog</log_format>
</localfile>

<!-- Policy monitoring -->
<rootcheck>
  <disabled>no</disabled>
  <windows_apps>.\shared\win_applications_rcl.txt</windows_apps>
  <windows_malware>.\shared\win_malware_rcl.txt</windows_malware>
</rootcheck>

<!-- Security Configuration Assessment -->
<sca>
  <enabled>yes</enabled>
  <scan_on_start>yes</scan_on_start>
  <interval>12h</interval>
  <skip_nfs>yes</skip_nfs>
</sca>

<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>
```

Artık emin olduğumuza göre saldırı için **sudo apt install -y hydra** komutuyla Hydra aracını indirerek devam edelim.



```
user@ubuntu:~/Desktop/wazuh$ cat passwords.txt
passw0rd1
passw0rd2
passw0rd3
passw0rd4
passw0rd5
password6
password7
password8
password9
password10
```

Bu aşamada passwords.txt adında bir dosya oluşturup rastgele şifreler yazabilirsiniz veya hazır listenizi kullanabilirsiniz. Hedef makinenin IP'si 192.168.28.129 olduğu için

sudo hydra -l randomuser -P passwords.txt rdp://192.168.28.129 komutu ile Remote Desktop Protokolü'ne bir saldırı deniyoruz. Arından Wazuh arayüzünü kontrol edelim.

LAST 24 HOURS ALERTS

Critical severity

0

Rule level 15 or higher

High severity

0

Rule level 12 to 14

Medium severity

412

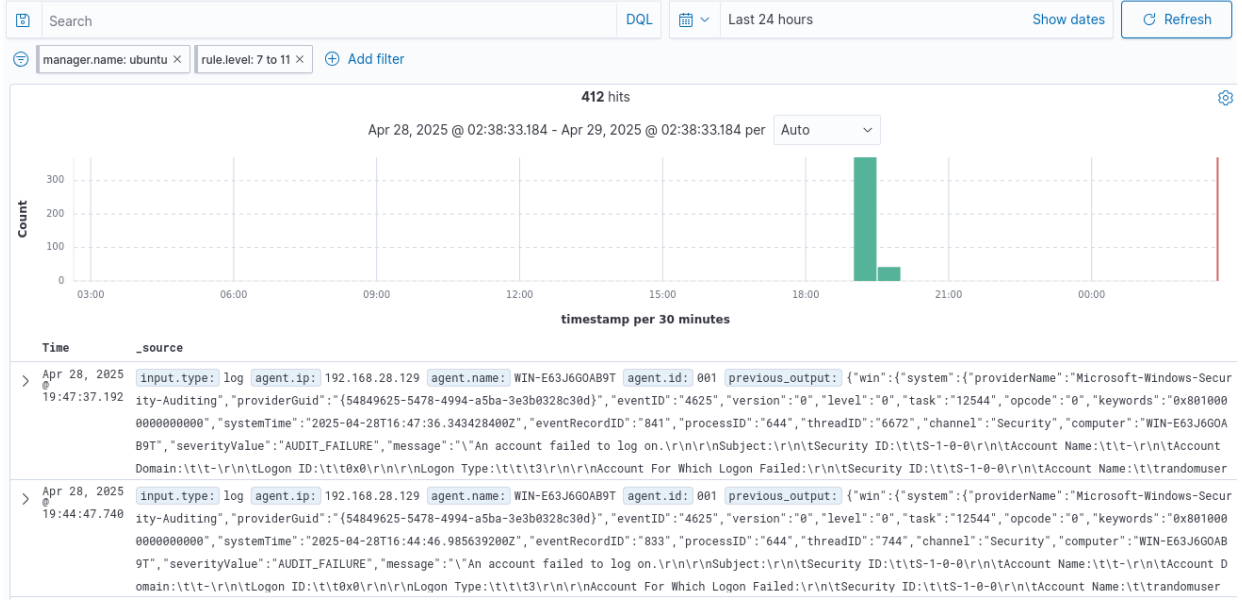
Rule level 7 to 11

Low severity

356

Rule level 0 to 6

Arayüzün anasayfasındaki Medium kısmına tıklayarak ilgili Discover sayfasına gidelim.



Ve Alert kısmında bir deneme olduğunu görüyoruz. Tıklayıp detaylarına baktığımızda saldırı denemesinin içeriği net olarak anlaşılıyor.

data.win.system.message

"An account failed to log on.

Subject:

Security ID: S-1-0-0
 Account Name: -
 Account Domain: -
 Logon ID: 0x0

Logon Type:

3

Account For Which Logon Failed:

Security ID: S-1-0-0
 Account Name: randomuser
 Account Domain: -

Failure Information:

Failure Reason: Unknown user name or bad password.
 Status: 0xC000006D
 Sub Status: 0xC0000064

Process Information:

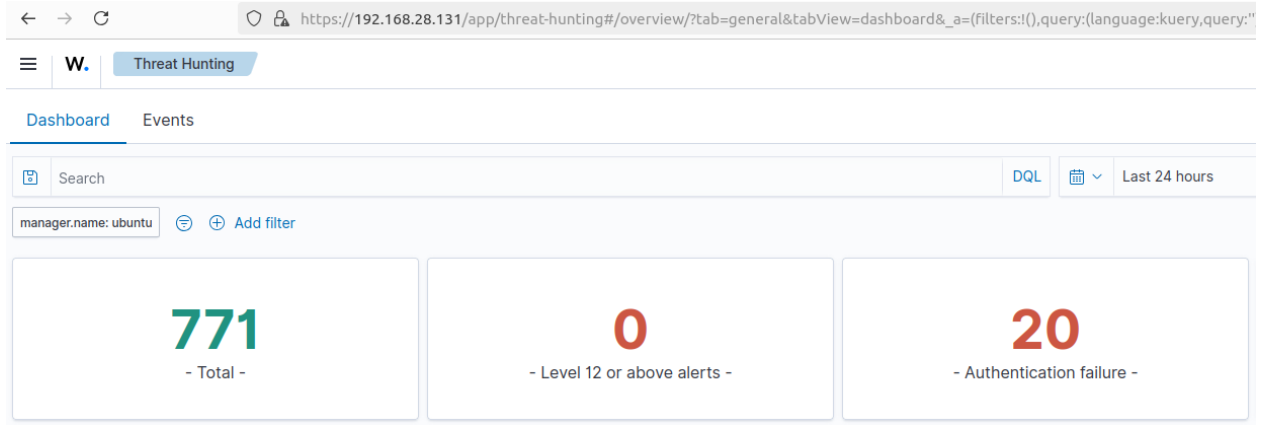
Caller Process ID: 0x0
 Caller Process Name: -

Network Information:

Workstation Name: ubuntu
 Source Network Address: 192.168.28.131
 Source Port: 0

Detailed Authentication Information:

Logon Process: NtLmSsp
 Authentication Package: NTLM
 Transited Services: -
 Package Name (NTLM only): -
 Key Length: 0



Ayrıca Wazuh > Threat Hunting sekmesinde de Authentication failure olarak denemeler gözüküyor.

Daha detaylı incelemek için Events kısmına geçtim. Burada gördüğümüz üzere **"Logon Failure - Unknown user or bad password" 60122** ve **"Multiple Windows Logon Failures" 60204** alertleri belirmiş. Seviye olarak çoğunlukla 5. Seviye yani orta düzey kabul ediliyor.

20 hits				
Apr 27, 2025 @ 19:48:38.071 - Apr 28, 2025 @ 19:48:38.071				
timestamp	agent.name	rule.description	rule.level	rule.id
Apr 28, 2025 @ 19:47:37.254	WIN-E63J6GOAB9T	Logon Failure - Unknown user or bad password	5	60122
Apr 28, 2025 @ 19:47:37.238	WIN-E63J6GOAB9T	Logon Failure - Unknown user or bad password	5	60122
Apr 28, 2025 @ 19:47:37.222	WIN-E63J6GOAB9T	Logon Failure - Unknown user or bad password	5	60122
Apr 28, 2025 @ 19:47:37.207	WIN-E63J6GOAB9T	Logon Failure - Unknown user or bad password	5	60122
Apr 28, 2025 @ 19:47:37.192	WIN-E63J6GOAB9T	Multiple Windows Logon Failures	10	60204
Apr 28, 2025 @ 19:47:37.177	WIN-E63J6GOAB9T	Logon Failure - Unknown user or bad password	5	60122
Apr 28, 2025 @ 19:47:37.160	WIN-E63J6GOAB9T	Logon Failure - Unknown user or bad password	5	60122
Apr 28, 2025 @ 19:47:37.145	WIN-E63J6GOAB9T	Logon Failure - Unknown user or bad password	5	60122
Apr 28, 2025 @ 19:47:37.119	WIN-E63J6GOAB9T	Logon Failure - Unknown user or bad password	5	60122
Apr 28, 2025 @ 19:47:37.118	WIN-E63J6GOAB9T	Logon Failure - Unknown user or bad password	5	60122
Apr 28, 2025 @ 19:44:47.785	WIN-E63J6GOAB9T	Logon Failure - Unknown user or bad password	5	60122
Apr 28, 2025 @ 19:44:47.755	WIN-E63J6GOAB9T	Logon Failure - Unknown user or bad password	5	60122
Apr 28, 2025 @ 19:44:47.740	WIN-E63J6GOAB9T	Multiple Windows Logon Failures	10	60204
Apr 28, 2025 @ 19:44:47.723	WIN-E63J6GOAB9T	Logon Failure - Unknown user or bad password	5	60122
Apr 28, 2025 @ 19:44:47.707	WIN-E63J6GOAB9T	Logon Failure - Unknown user or bad password	5	60122

5. Özel Kuralı Sonradan Eklemek

Eğer Wazuh üzerinde ilgili kural olmasaydı, sonradan eklemek isteseydik ya da bu kurala bağlı bir kural eklemek istedeysdik şu adımları takip etmemiz gerekirdi:

`/var/ossec/ruleset/rules/local_rules.xml` dosyasına

```
<rule id="100001" level="10">  
  <if_sid>60122</if_sid>  
  <options>no_full_log</options>  
  <description>Brute-Force Saldırısı Tespit Edildi</description>  
</rule>
```

Kuralını ekleyerek ek bir Alert oluşturabiliriz.

Bu kurallara ek olarak daha önce bahsettiğim “ossec.conf” u düzenleyerek e-posta bildirimi de eklenebilir. Daha sonra kuralın aktif hale gelmesi için `systemctl restart wazuh-manager` komutuyla Wazuh yeniden başlatılır.

Değerlendirme

Bu raporda genel olarak bir kurulum ve süreçten bahsettik. Ubuntu üzerinde Wazuh SIEM kullanılarak Windows Server 2019 sistemine yapılan brute-force saldırıları başarıyla algılandı. Varsayılan 60122 ve 60204 numaralı kurallar ile başarısız oturum açma girişimleri tespit edildi. Elde edilen sonuçlar, SIEM sistemlerinin güvenlik izleme süreçlerindeki önemini ve Wazuh’un bu alandaki etkinliğini göstermiş oldu.