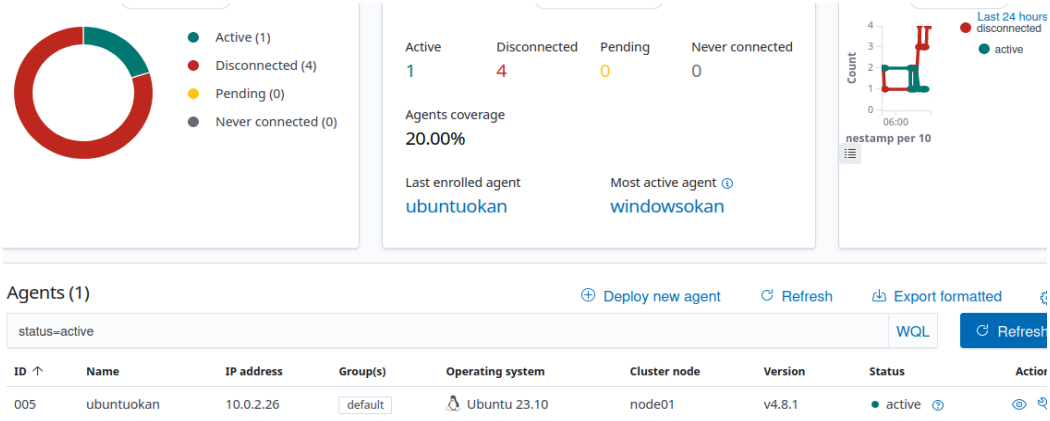
Wazuh-Manager ile Linux ve Windows Log Yönetimi ve Entegrasyon

Wazuh-Manager ile Linux ve Windows Log Yönetimi ve Entegrasyon 1
Wazuh agent kurulumu 2
Windows loglarının toplanması 3
Windows Sysmon loglarının toplanması 4
Linux loglarının alınması 7
Apache Kurulumu ve Loglarının alınması 9
Suricata kurulumu ve logların Wazuha alınması 11
Özet 13
Troubleshooting 13
Kaynakça 14

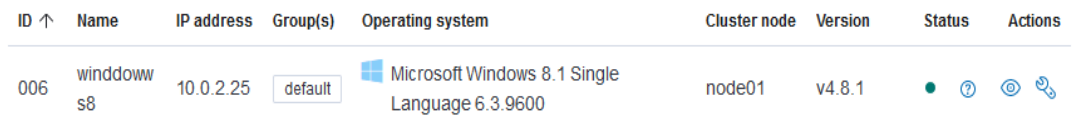
Wazuh agent kurulumu

Wazuh ara yüzüne erişimin ardından “add agent” seçeneğine gidilerek Wazuh sunucusunun ip adresi ve ilgili işletim sistemi seçildi. Devamında alt tarafta ilgili kurulum için komutlar alındı. Windowsda Powershell ayrıcalıklı modda Linux da ise root olarak kodlar çalıştırıldı ve kurulumlar tamamlandı.

```
root@okan:~# wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/waz
uh-agent_4.8.1-1_amd64.deb && sudo WAZUH_MANAGER='10.0.2.24' WAZUH_AGENT_NAME='u
buntuokan' dpkg -i ./wazuh-agent_4.8.1-1_amd64.deb
--2024-08-17 23:06:58--  https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-ag
ent/wazuh-agent_4.8.1-1_amd64.deb
Resolving packages.wazuh.com (packages.wazuh.com)    108.157.60.83, 108.157.60.1
```




```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.8.1-1.msi -OutFile
{env.tmp}\wazuh-agent; msiexec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='10.0.2.24' WAZUH_AGENT_NAME='winddowws8
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.8.1-1.msi -OutFile ${env.tmp}\wazuh-agent;
siexec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='10.0.2.24' WAZUH_AGENT_NAME='winddowws8'
PS C:\Windows\system32> NET START WazuhSvc
Wazuh hizmeti başlatılıyor.
Wazuh hizmeti başarıyla başlatıldı.

PS C:\Windows\system32>
```

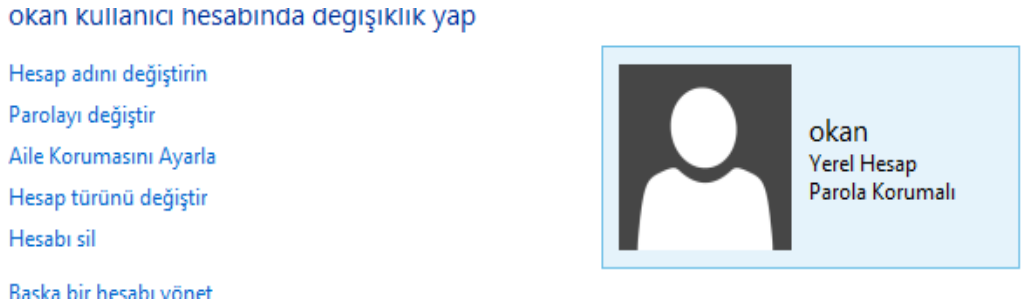


Windows loglarının toplanması

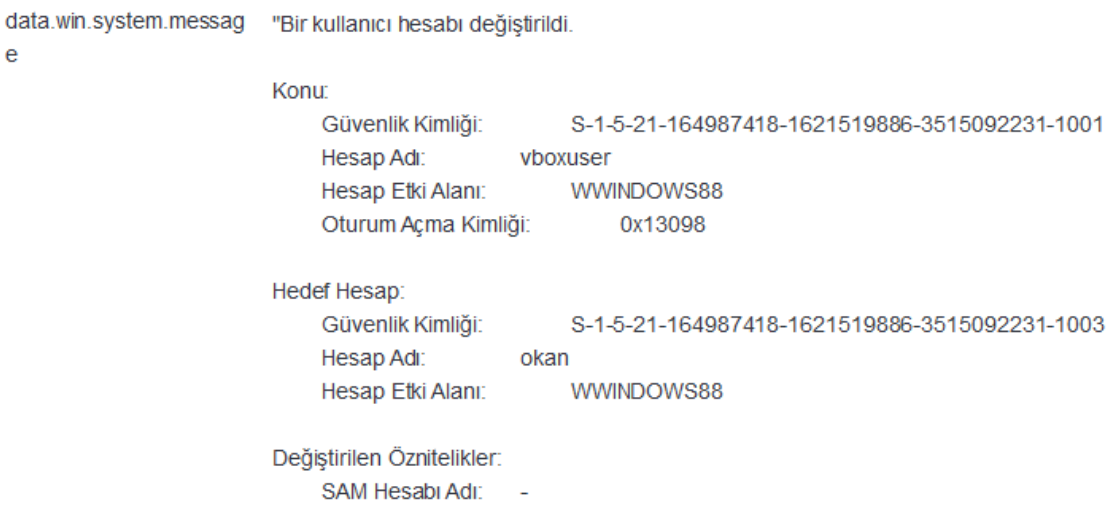
1- Windowsda “C:\Program Files (x86)\ossec-agent\ossec.conf” dosyasına ayrıcalıklı çalıştırma yetkisi alınarak aşağıdaki eklemeler yapıldı.

```
<localfile>
  <location>Application</location>
  <log_format>eventlog</log_format>
</localfile>
   <localfile>
    <location>System</location>
    <log_format>syslog</log_format>
  </localfile>



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

2- Windowsa okan adında kullanıcı eklendi. Ardından silindi.



3- Yapılan işlemler dashboard üzerinden kontrol edildi.

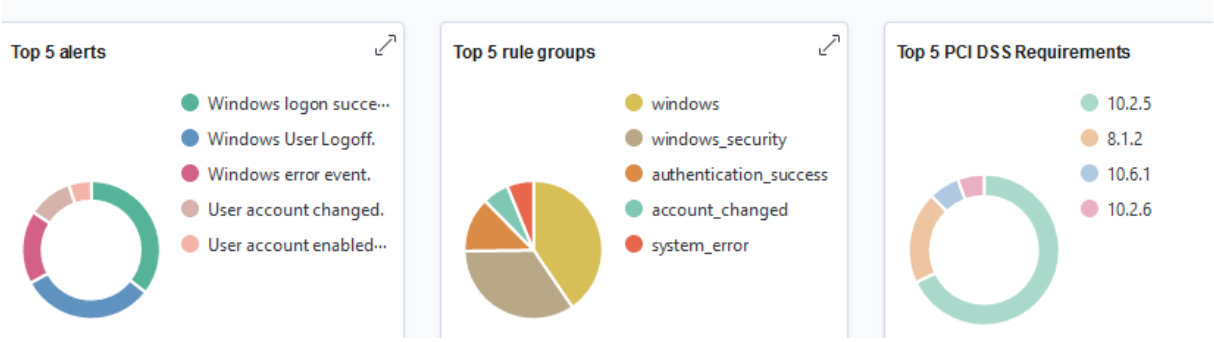


data.win.system.messag e "Bir kullanıcı hesabı silindi.

Konu:
Güvenlik Kimliği: S-1-5-21-164987418-1621519886-3515092231-1001
Hesap Adı: vboxuser
Hesap Etki Alanı: WWINDOWS88
Oturum Açma Kimliği: 0x13098

Hedef Hesap:
Güvenlik Kimliği: S-1-5-21-164987418-1621519886-3515092231-1003
Hesap Adı: okan
Hesap Etki Alanı: WWINDOWS88

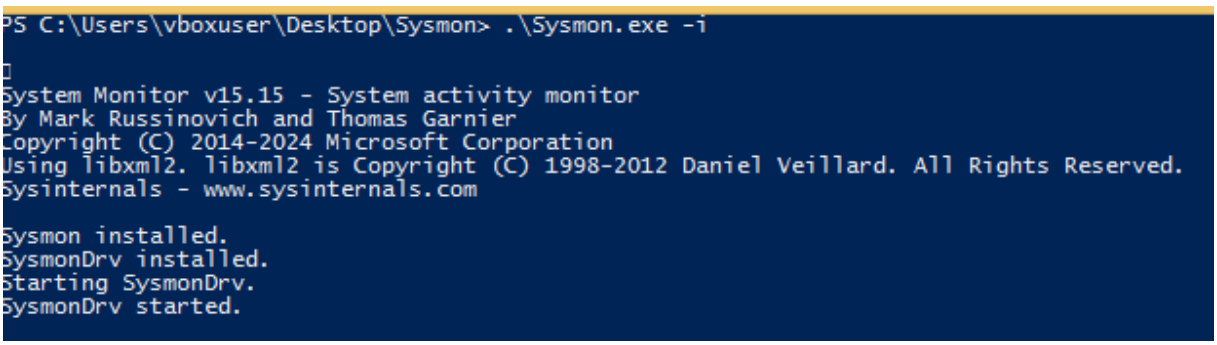
Ek Bilgi:
Ayrıcalıklar: -"



Windows Sysmon loglarının toplanması

Sysmon (System Monitor), Microsoft'un Windows işletim sistemleri için geliştirdiği bir araçtır ve sistemdeki önemli olayları detaylı şekilde kaydeder. Sysmon, süreçler, ağ bağlantıları, dosya sistemindeki değişiklikler ve kayıt defteri değişiklikleri gibi olayları izleyerek, güvenlik analizi ve tehdit tespiti için kapsamlı loglar sağlar.

1- Microsoftun https://download.sysinternals.com/files/Sysmon.zip URL'i üzerinden sysmon indirilir, Powershell yönetici olarak çalıştırılarak aşağıdaki işlemler yapılarak kurulur. XML konfigürasyon dosyası sysmonun çalışabilmesi için gerekli dosyadır. Burada bu dosya powershell ve cmd işlemleri adına konfigüre edildi.

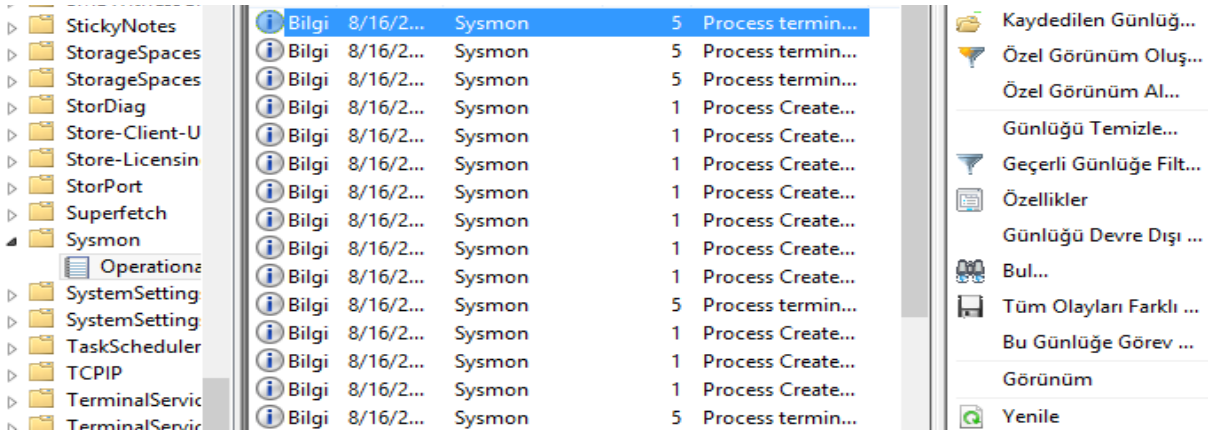


2- Ardından aşağıdaki komut kullanılarak sistemin mevcut konfigürasyonu görüntülendi.

```
PS C:\Windows\system32> Sysmon64.exe -c
```

```
urrent configuration:
- Service name:                 Sysmon64
- Driver name:                  SysmonDrv
- Config file:                  C:\Users\vboxuser\Desktop\Sysmon\sysconfig.xml
- Config hash:                  SHA256=6816FFAB4A639F77754D600CA82062E65769AA2DC9E92321D69

- HashingAlgorithms:            MD5
- Network connection:           disabled
- Archive Directory:            -
- Image loading:                disabled
- CRL checking:                 enabled
- DNS lookup:                   enabled

ule configuration (version 4.90):
- ProcessCreate                     onmatch: include    combine rules using 'And'
      Image                          filter: contains      value: 'powershell.exe'
- FileCreateTime                    onmatch: include    combine rules using 'And'
- NetworkConnect                    onmatch: include    combine rules using 'And'
- ProcessTerminate                  onmatch: include    combine rules using 'And'
- DriverLoad                        onmatch: include    combine rules using 'And'
- ImageLoad                         onmatch: include    combine rules using 'And'
- CreateRemoteThread                onmatch: include    combine rules using 'And'
- RawAccessRead                     onmatch: include    combine rules using 'And'
- ProcessAccess                     onmatch: include    combine rules using 'And'
- FileCreate                        onmatch: include    combine rules using 'And'
- RegistryEvent                     onmatch: include    combine rules using 'And'
- FileCreateStreamHash              onmatch: include    combine rules using 'And'
- PipeEvent                         onmatch: include    combine rules using 'And'
S C:\Windows\system32>
```

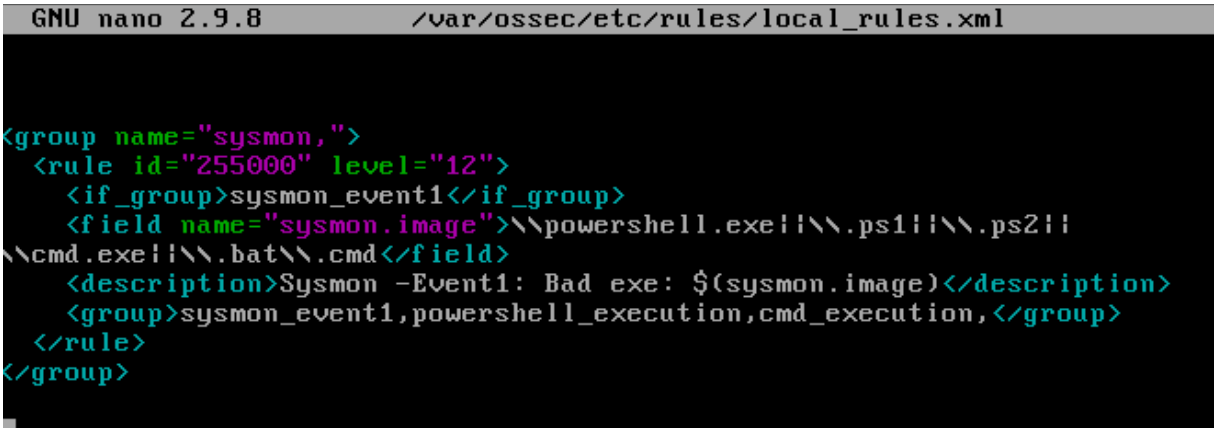
3- Windows olay günlüklerinden, ” Applications and Services Logs/Microsoft/Windows/Sysmon/Operational” sysmon entegrasyonunun durumu kontrol edildi.



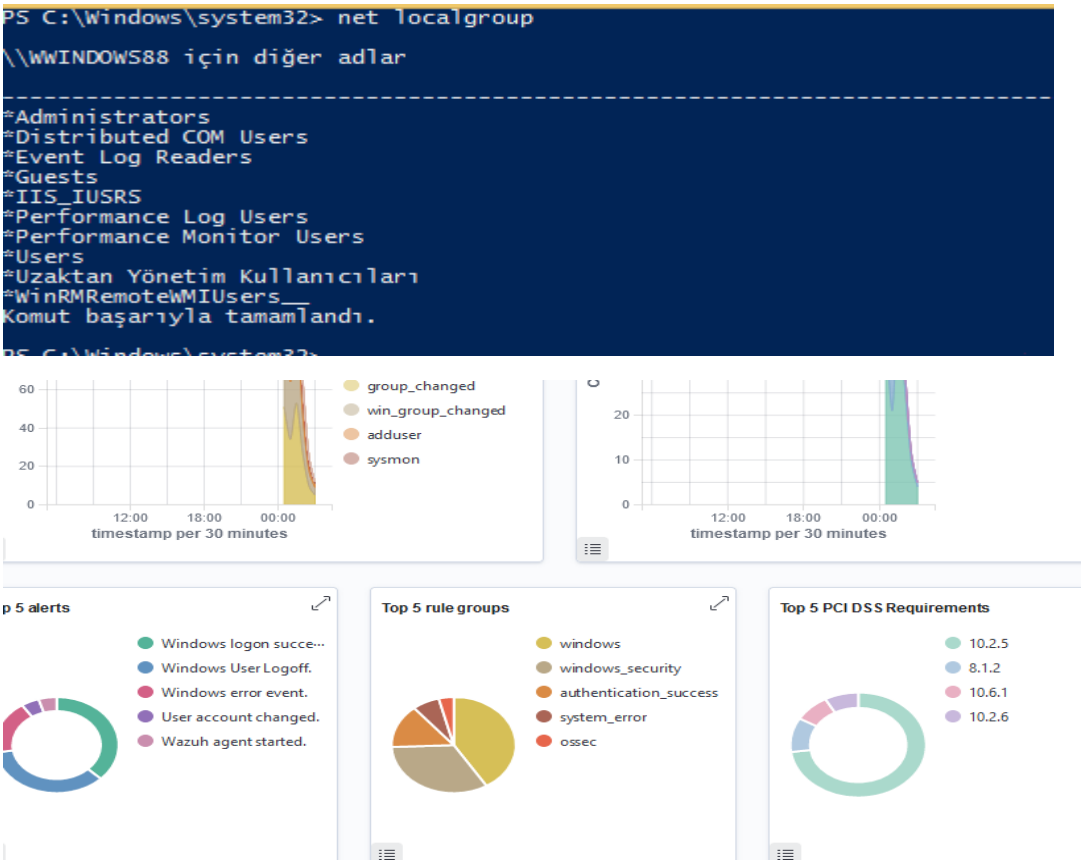
4- Windows agentında “ossec.conf” dosyasında gibi ekleme yapıldı. Ardından wazuh agentı yeniden başlatıldı.

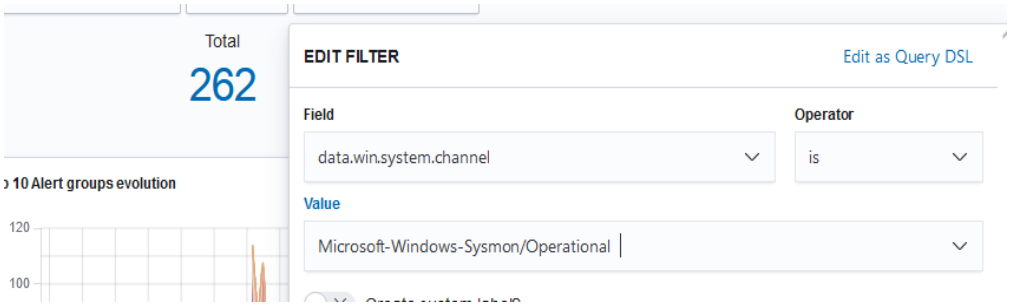
```
  <localfile>
<location>Microsoft-Windows-Sysmon/Operational</location>
<log_format>eventchannel</log_format>
</localfile>
```

5- Wazuh sunucusunda “ /var/ossec/etc/rules/local_rules.xml” dosyasında aşağıdaki gibi kural konfigürasyonu yapıldı. Ardından wazuh manager yeniden başlatıldı. Bu yapılandırma, Sysmon loglarını izlemek için kullanılan bir Wazuh kuralıdır ve özellikle şüpheli uygulama yürütmelerini hedef alır. Kural, sysmon.image alanında belirtilen dosyalar (powershell.exe, .ps1, .ps2, cmd.exe, .bat, .cmd) ile ilgili olayları tanımlar ve bu olayları sysmon_event1, powershell_execution, ve cmd_execution gruplarına atar. Bu şekilde, Sysmon'un Event ID 1'e göre belirli kötü niyetli veya şüpheli yürütme işlemleri izlenir ve raporlanır.



6- Windows üzerinde belirli komutlar çalıştırıldı ve Wazuh ara yüzünde ilgili filtre uygulanarak işlem görüntülendi.





data.win.eventdata.parentCommandLine	\"C:\\Windows\\system32\\net.exe\" localgroup
data.win.eventdata.parentImage	C:\\Windows\\System32\\net.exe
data.win.system.channel	Microsoft-Windows-Sysmon/Operational
rule.groups	sysmon, sysmon_eid1_detections, windows

Linux loglarının alınması

1- Wazuh sunucusunda aşağıdaki işlemler yapıldı. Burada “connection” parametresinin “syslog” olarak ayarlanması, log mesajlarının ip iletilmesi adına; “port” parametresi gönderilecek portu belirtti syslog 514 portunu kullanır. “allowed-ips” parametresi ilgili ağdaki cihazların bu işleme tabi tutulması adına tanımlandı.Bu işlemlerin ardından Wazuh manager yeniden başlatıldı.

2- Ardından rsyslog Ubuntu uç cihazına kuruldu. Rsyslog, bir IP ağında günlük mesajlarını iletmek için UNIX ve Unix benzeri bilgisayar sistemlerinde kullanılan açık kaynaklı bir yazılım yardımcı programıdır.

```
root@okan:~# apt-get update
apt-get install -y rsyslog
Hit:1 http://archive.ubuntu.com/ubuntu mantic InRelease
Hit:2 http://archive.ubuntu.com/ubuntu mantic-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu mantic-security InRelease
Hit:4 http://archive.ubuntu.com/ubuntu mantic-backports InRelease
```

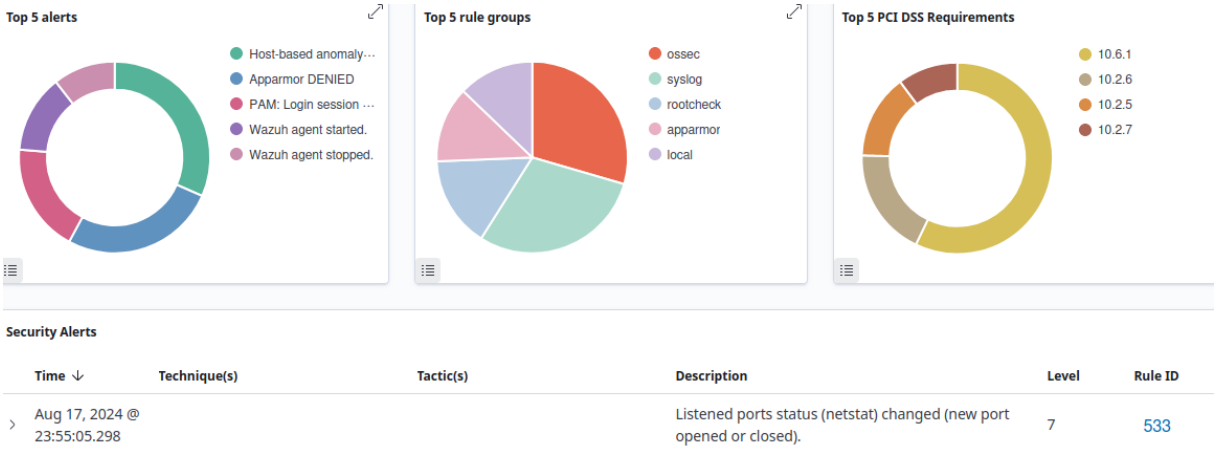
3- Ubuntu üzerinde "/etc/rsyslog.conf" dosyası üzerinde ilgili ayarlamalar yapıldı. Ilk satırdaki TCP protokolünü belirtirken 2. Satır UDP protokolünü belirtmiştir.

```
  GNU nano 7.2                          /etc/rsyslog.conf *
# /etc/rsyslog.conf configuration file for rsyslog
#
# For more information install rsyslog-doc and see
# /usr/share/doc/rsyslog-doc/html/configuration/index.html
#
# Default logging rules can be found in /etc/rsyslog.d/50-default.conf


*.* action(type="omfwd" target="10.0.2.24" port="514" protocol="tcp")
*.* action(type="omfwd" target="10.0.2.24" port="514")
```

4- Ardından rsyslog yeniden başlatıldı. Çalışma durumu kontrol edildi.

```
root@okan:~# systemctl start rsyslog
systemctl enable rsyslog
root@okan:~# systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
     Active: active (running) since Sat 2024-08-17 23:31:10 +03; 8min ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
```

5- Dashboard ekranından ise işlem böyle görüntülendi.



Security Alerts

Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
Aug 17, 2024 @ 23:55:05.298			Listened ports status (netstat) changed (new port opened or closed).	7	533

Apache Kurulumu ve Loglarının alınması

Apache Web Server, açık kaynak kodlu bir web sunucusudur ve internet üzerindeki web sitelerini barındırmak için yaygın olarak kullanılır. Yüksek esneklik ve geniş bir modül desteği sunarak, çeşitli işletim sistemlerinde stabil bir şekilde çalışır ve web uygulamalarının yönetilmesini sağlar.

1- Ubuntu uç cihazına apache kurulumu yapıldı.

```
root@okan:~# apt install -y apache2
Paket listeleri okunuyor... Bitti
Bağımlılık ağacı oluşturuluyor... Bitti
Durum bilgisi okunuyor... Bitti
Aşağıdaki ek paketler kurulacak:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap
Önerilen paketler:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
Aşağıdaki YENİ paketler kurulacak:
```

2- Bu konfigürasyon, Apache web sunucusunun hata ve erişim loglarını hem belirli dosyalara yazdırır hem de rsyslog aracılığıyla sysloga iletir.

```
  GNU nano 7.2                    /etc/apache2/sites-available/000-default.conf *
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com
ErrorLog "|/bin/sh -c '/usr/bin/tee -a /var/log/apache2/error.log | /usr/bin/logger -t apache_error: -p
local6.err'"
CustomLog "|/bin/sh -c '/usr/bin/tee -a /var/log/apache2/access.log | /usr/bin/logger -t apache_access: -p
local6.notice'" combined
```

3- Wazuh suncusunda aşağıdaki gibi kural oluşturuldu

```
<group name="web,accesslog,">


  <rule id="110001" level="5">
    <if_sid>31108</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>Apache web server</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>

</group>
```

```
GNU nano 2.9.8                    /var/ossec/etc/ossec.conf

  <remote>
    <connection>syslog</connection>
    <port>514</port>
    <protocol>tcp</protocol>
    <allowed-ips>10.0.2.0/24</allowed-ips>
    <local_ip>10.0.2.24</local_ip>
  </remote>
```

4- Ubuntu uç cihazında "/etc/rsyslog.conf" konfigürasyon dosyasına aşağıdaki eklemeler yapıldı. İlk satır, local6.notice seviyesindeki logları hedefe yönlendirirken, ikinci satır local6.err seviyesindeki logları hedefe iletir.

```
local6.notice action(type="omfwd" target="10.0.2.24" port="514" protocol="tcp")

local6.err action(type="omfwd" target="10.0.2.24" port="514" protocol="tcp")
```

5- Apache ve Rsyslog konfigürasyonu kontrolü için aşağıdaki işlemler yapıldı ve kontrol çıktısı alındı

```
root@ubuntu:~# nano /etc/apache2/sites-available/000-default.conf
root@ubuntu:~# apachectl -t
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0
'ServerName' directive globally to suppress this message
Syntax OK
root@ubuntu:~# rsyslogd -N1
rsyslogd: version 8.2306.0, config validation run (level 1), master config /etc/rsyslog.conf
rsyslogd: End of config validation run. Bye.
```

6- Rsyslog ve Apache2 servisleri yeniden başlatıldı.

```
root@ubuntu:~# systemctl restart rsyslog apache2
root@ubuntu:~#
```

7- Ardından uç cihazın,Ubuntu, ip adresi kullanılarak web sitesine erişildi ve Apache logları Wazuh ara yüzünde görüntülendi

Aug 16, 2024 @ 15:51:06.198	Apache web server	5	110001

decoder.name	web-accesslog
decoder.parent	web-accesslog
full_log	2024-08-16T15:51:05.690548+03:00 okan apache_access:: 10.0.2.15 - - [16/Aug/2024:15:51:05 +0300] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/118.0"
id	1723812666.71280
input.type	log
location	/var/log/syslog
manager.name	wazuh-server
predecoder.program_name	apache_access

Suricata kurulumu ve logların Wazuha alınması

Suricata, açık kaynak kodlu bir ağ güvenliği izleme ve saldırı tespit sistemi (IDS) olup, ağ trafiğini analiz ederek şüpheli aktiviteleri ve güvenlik tehditlerini tespit eder. Gelişmiş protokol analizi, hız ve güvenilirlik sunarak, ağ güvenliğini artırmak için kapsamlı bir koruma sağlar.

1- Suricata kurulumu adına aşağıdaki işlemler yapıldı.

```
root@ubuntu:~# sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt-get update
sudo apt-get install suricata -ysudo add-apt-repository ppa:oisf/suricata-stable
sudo apt-get update
sudo apt-get install suricata -y
Repository: 'Types: deb
URIs: https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu/
Suites: mantic
Components: main
```

2- Suricatanın ilgili konfigürasyon dosyasında ilgili kısımlar aşağıdaki gibi belirtildi. Burada "HOME_NET" için ubuntu ip adresi, kural yolu adına suricatanın kurallarının bulunduğu dosya yolu ve ara yüz için de "ifconfig" komutuylakullanılan ara yüz belirtildi. Çalışma durumu kontrol edildi
NOT: dosya içinde ilgili ayarlamaların yerleri farklılık göstermektedir burada bu şekilde belirtilmiş olma sebebi hepsini tek bir ekran görüntüsünde yakalamaktır.

```
  GNU nano 7.2                                  /etc/suricata/suricata.yaml *
%YAML 1.1
---
HOME_NET: "<UBUNTU_IP>"
EXTERNAL_NET: "any"

default-rule-path: /etc/suricata/rules
rule-files:
- "*.rules"

# Global stats configuration
stats:
enabled: yes

# Linux high speed capture support
af-packet:
  - interface: enp0s3
```

```
root@okan:/etc/suricata# nano suricata.yaml
root@okan:/etc/suricata# systemctl restart suricata
root@okan:/etc/suricata# systemctl restart wazuh-agent
root@okan:/etc/suricata# systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/lib/systemd/system/suricata.service; enabled; preset: ena>
     Active: active (running) since Fri 2024-08-16 16:47:24 +03; 27s ago
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
    Process: 16816 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/>
   Main PID: 16818 (Suricata-Main)
      Tasks: 1 (limit: 3481)
     Memory: 183.3M
```

3- Ubuntu uç cihazı üzerindeki "/var/ossec/etc/ossec.conf" dosyasında Suricata logları toplanması adına aşağıdaki işlemler yapıldı ve agent yeniden başlatıldı. Suricata logları "eve.json" dosyasında olduğundan nu dosya belirtildi.

```
<ossec_config>
  <localfile>
    <log_format>json</log_format>
    <location>/var/log/suricata/eve.json</location>
  </localfile>
```

4- Wazuh sunucusu üzerinde uç cihaza ping atıldı ve loglar Wazuh ara yüzünde incelendi.

```
root@wazuh-server ~]# ping -c 20 10.0.2.15
ING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
4 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.983 ms
4 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.990 ms
4 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=1.06 ms
4 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.988 ms
```

Time ▾	rule.description	rule.level	rule.id
Aug 16, 2024 @ 17:01:41.193	Suricata: Alert - GPL ICMP_INFO PING *NIX	3	86601
Aug 16, 2024 @ 17:01:39.361	Suricata: Alert - GPL ICMP_INFO PING *NIX	3	86601
Aug 16, 2024 @ 17:01:39.190	Suricata: Alert - GPL ICMP_INFO PING *NIX	3	86601

Özet

Wazuh ile log yönetimi ve entegrasyonu sürecinde, Windows ve Linux sistemlerinde log toplama ve analiz işlemleri gerçekleştirilmiştir. Windows için Wazuh agent'ı kurularak, Sysmon kullanılarak sistem olayları detaylı şekilde izlenmiş ve konfigürasyon dosyaları güncellenmiştir. Linux tarafında, rsyslog ile log iletimi sağlanmış, Apache ve Suricata kurulumları yapılmış ve Wazuh'a entegrasyonları gerçekleştirilmiştir. Bu süreçler, logların toplanması, yapılandırılması ve Wazuh arayüzünde görselleştirilmesi ile güvenlik analizi için kapsamlı bir izleme ve yönetim ortamı oluşturmuştur.

Troubleshooting

1- Sysmon “sysconfig.xml” dosyası sysmon işlemini başlatma sırasında “schemaversion” 4.90 olması gerektiğinden bu ayarlama dosya üzerinde sağlandı.
2- Windows başladıktan sonra ekranda kesik kesik görüntüler oluştu. Bu durum da Virtualboxda görüntüleme ayarlarından display memory kısmının artırılmasıyla çözüldü.
3- Sysmon loglarının wazuha iletimi sırasında sorun yaşandı. Wazuh sunucusunda ve windows üzerinde “sysconfig.xml” dosyalarında işlemlerin kontrolü sağlandı. Farklı konfigürasyon dosyalaarı üzerinden işlemler denendi.

Kaynakça

1- https://wazuh.com/blog/using-wazuh-to-monitor-sysmon-events/

2- https://kilincfurkan.com/2022/10/22/wazuh-ile-sysmon-loglarini-goruntuleme/

3- https://aliahmeddarhere.medium.com/wazuh-host-integration-log-collection-a8b1175ae1f4

4- https://aliahmeddarhere.medium.com/wazuh-host-integration-log-collection-a8b1175ae1f4

5- https://reddit.com/r/Wazuh/comments/o7jwq9/forwading_syslogs_to_wazuh/

6- https://github.com/wazuh/wazuh/issues/5452

7- https://www.digitalocean.com/community/tutorials/how-to-install-suricata-on-ubuntu-20-04

8- https://betterstack.com/community/guides/logging/rsyslog-explained/

9- https://www.rsyslog.com/doc/index.html

10- https://wiki.gentoo.org/wiki/Rsyslog

11- https://medium.com/@akobeajiboluemmanuel/step-by-step-setup-of-wazuh-siem-on-ubuntu-22-04-3-lts-4663104fe69b

12- https://kb.blackbaud.com/knowledgebase/Article/75433