



SecurityOnion & Wazuh

Ryhmä 13

Leevi Kauranen, AC7750

Samir Benjenna, AD1437

Eelis Suhonen, AA3910

Juho Eräjärvi, AD1276

Mikke Kuula, AC7806

Tietoturvakontrollit TTC6010-3007

28.11.2024

Tieto- ja viestintätekniikka

Sisältö

1	Johdanto	3
2	Teoriaa	3
2.1	Wazuh.....	3
2.2	Security Onion	4
3	Toteutus	4
3.1	Mikä on Zeek?	11
4	Wazuh konfigurointi	12
5	Testaukset	17
	Lähteet	21
	Liitteet	22
	Liite 1. Liitteen otsikko	22
	Liite 2. Liitteen otsikko	23

Kuviot

Kuvio 1. VLE.....	3
Kuvio 2. Commands1	4
Kuvio 3. Onion UI	5
Kuvio 4. alerts.....	5
Kuvio 5.actions	6
Kuvio 6. laajennettu	6
Kuvio 7. Dashboard	7
Kuvio 8. Tools	7
Kuvio 9. cyberchef.....	8
Kuvio 10. Kibana_dashboard	8
Kuvio 11. latimes.com	9
Kuvio 12. eventcategories.....	9
Kuvio 13. file.....	10
Kuvio 14. hosts	10
Kuvio 15.zeek	11
Kuvio 16. Lokit.....	11
Kuvio 17. wazuh	12
Kuvio 18. agents.....	13
Kuvio 19. agents_view	13

Kuvio 20. agentin lisäys	14
Kuvio 21. agentin lisäys2	14
Kuvio 22. komentojen lisäys	15
Kuvio 23. agents_active	15
Kuvio 24. agents_active2	15
Kuvio 25. Linux agentit.....	16
Kuvio 26. Linux commands	16
Kuvio 27. Wazuh agents.....	17
Kuvio 28. Wazuh agents 2.....	17
Kuvio 29. test_script.....	18
Kuvio 30. alerts.....	19
Kuvio 31. alerts2.....	19

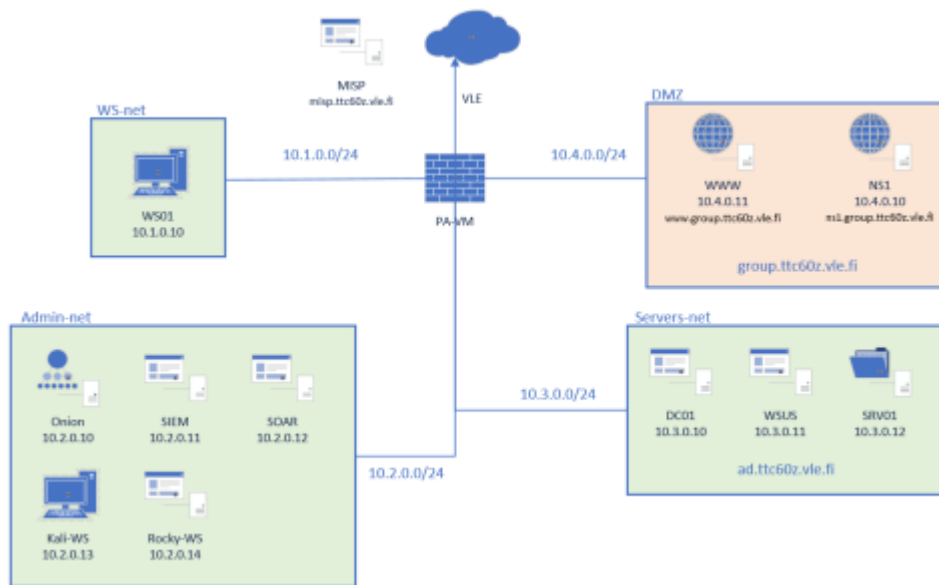
Taulukot

Taulukko 1. Taulukon otsikko, ei lähdetietoja **Virhe. Kirjanmerkkiä ei ole määritetty.**

Taulukko 2. Taulukon otsikko, ei lähdetietoja **Virhe. Kirjanmerkkiä ei ole määritetty.**

1 Johdanto

Tämä harjoitustyö keskittyy SecurityOnion ja Wazuh Järjestelmien konfiguroimiseen käyttökuuntoon ja ominaisuuksien testaamiseen. Tehtävä toteutetaan Kuvion 1 mukaiseen VLE ympäristöön.



Kuvio 1. VLE

2 Teoriaa

2.1 Wazuh

Wazuh on ilmainen, avoimen lähdekoodin tietoturva-alusta, joka tarjoaa yhdistetyt XDR (Extended Detection and Response) ja SIEM (Security Information and Event Management) -ominaisuudet. Se on suunniteltu suojaamaan erilaisia ympäristöjä, mukaan lukien julkiset ja yksityiset pilvipalvelut sekä paikallisesti hallinnoidut datakeskukset. Wazuh keskittyy erityisesti päätelaitteiden ja pilvipalveluiden työympäristöjen suojaamiseen uhkia vastaan. Wazuhin keskeisiä ominaisuuksia on esimerkiksi

- Uhkien metsäöstys ja tapahtumiin reagointi
- Tiedostojen eheyden valvonta
- Kattavat kojelaumat tietojen analysointia varten

(Brandstaetter. 2024.)

2.2 Security Onion

Security Onion on avoimenlähdekoodin SIEM järjestelmä, joka on erityisesti suunniteltu tietoturva-tapahtumien havaitsemiseen, kirjaamiseen ja analysointiin. Se yhdistää useita tehokkaita työkaluja yhteen kokonaisuuteen, jotta organisaatiot pystyvät hallitsemaan ja analysoimaan tietoturvaa tehokkaasti. (Sadhik. 2023.)

3 Toteutus

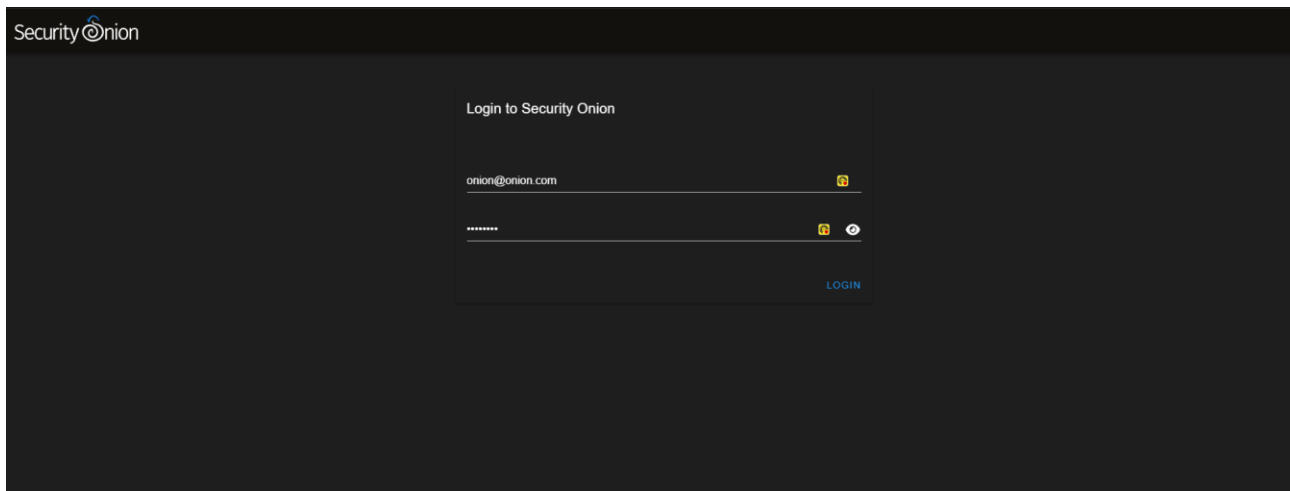
Aloitetaan konfiguroiminen käynnistämällä onion palvelin, jatkossa haluamme päästä Security-Onioniin käsiksi omalta koneeltamme Käyttämällä GlobalProtectia joka on konfiguroitu aiemmissa töissä. Onionin verkkokäyttöliittymään pääsee käsiksi <http://10.2.0.10> osoitteesta.

aloitetaan ajamalla komennot. (Kuvio 2)

```
onion@onion ~]$ sudo so-allow
[sudo] password for onion:
Choose the role for the IP or Range you would like to allow
[a] - Analyst - 80/tcp, 443/tcp
[b] - Logstash Beat - 5044/tcp
[c] - Elasticsearch REST API - 9200/tcp
[d] - Strelka frontend - 57314/tcp
[e] - Osquery endpoint - 8090/tcp
[f] - Syslog device - 514/tcp/udp
[g] - Wazuh agent - 1514/tcp/udp
[h] - Wazuh API - 55000/tcp
[i] - Wazuh registration service - 1515/tcp
Please enter your selection: a
Enter a single ip address or range to allow (ex: 10.10.10.10 or 10.10.0.0/16): 10.255.254.0/24
```

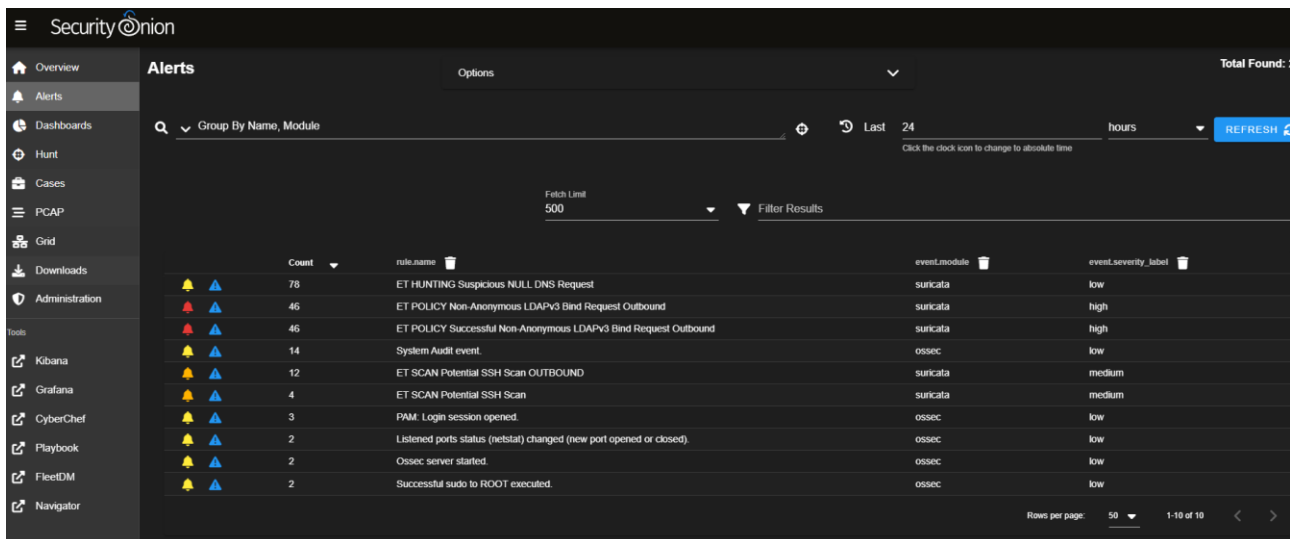
Kuvio 2. Commands1

Nyt pääsemme omalla laitteellamme onioniin. (Kuvio 3)



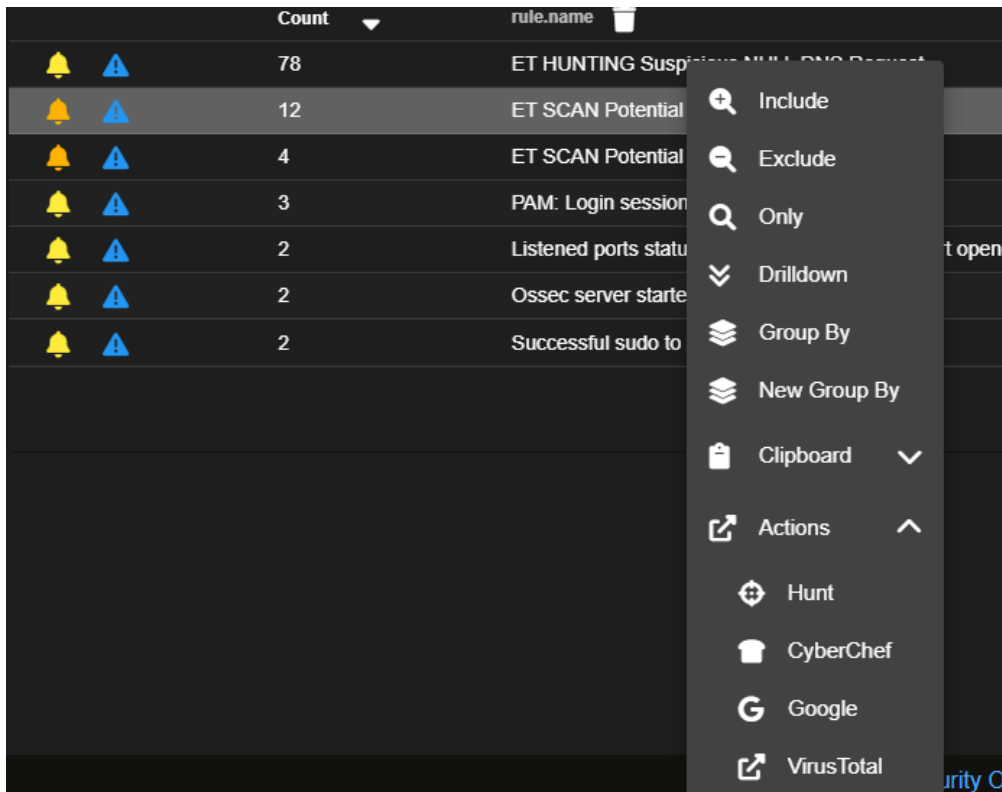
Kuvio 3. Onion UI

Seuraavaksi alamme tutkimaan SecurityOnionista löytyviä ominaisuuksia. siirrytään ensin tutki-
maan alert näkymää. (Kuvio 4)



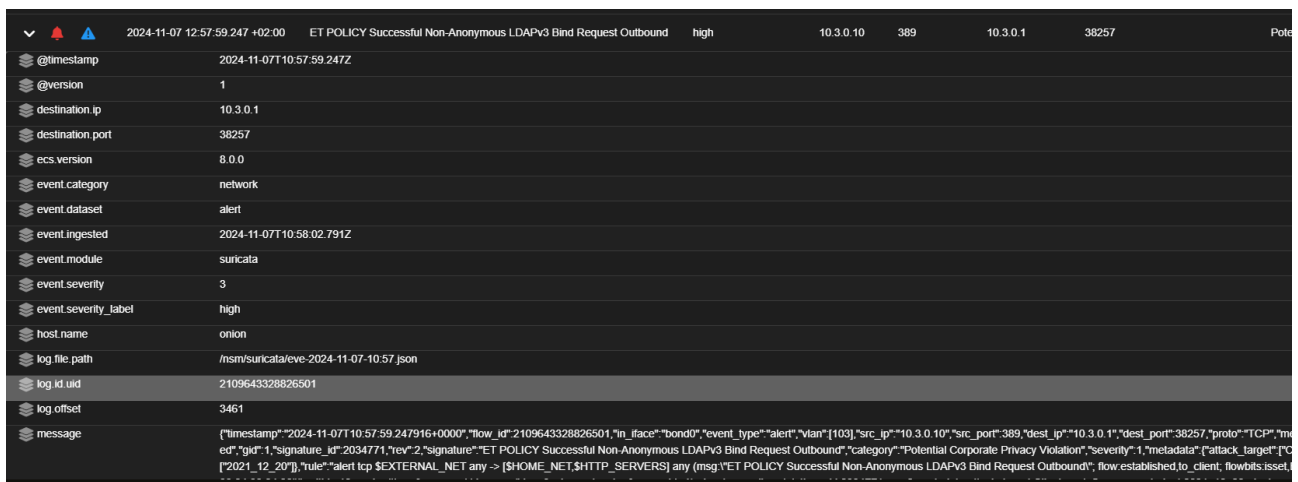
Kuvio 4. alerts

Kun jotain hälytystä painaa, aukeaa valikko, josta voimme viedä hälytyksen esimerkiksi tarkastelta-
vaksi. Esimerkiksi actions välilehden alta virustotaliin. (Kuvio 5)



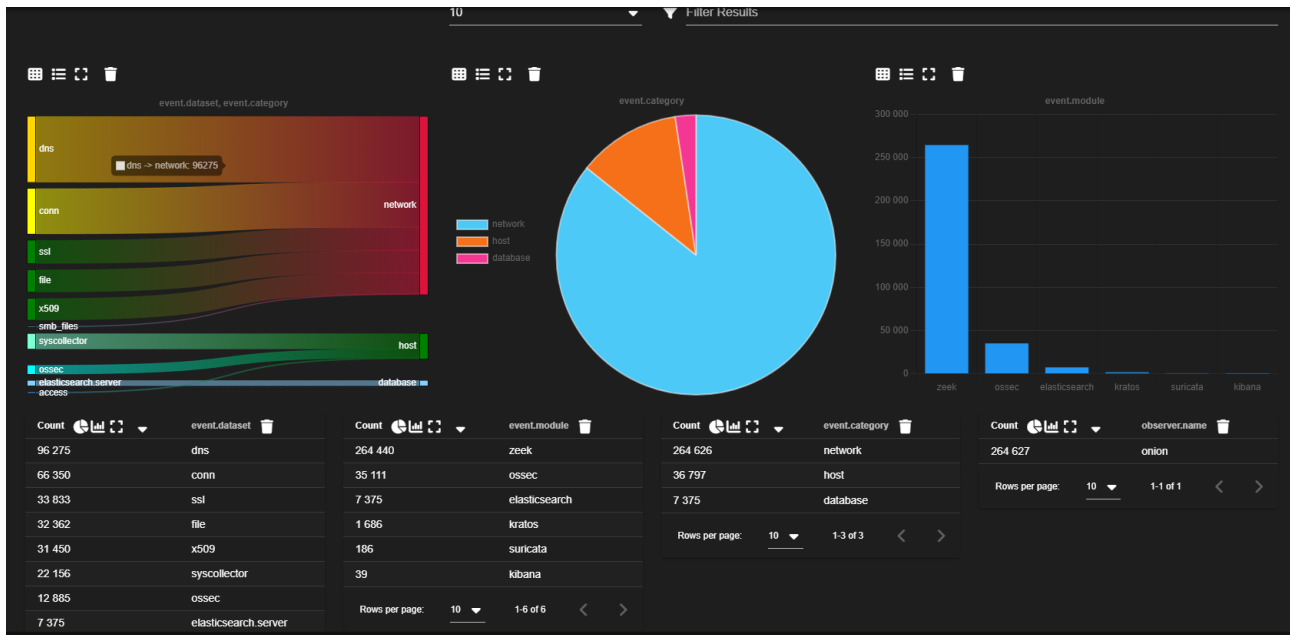
Kuvio 5.actions

Alertin saa laajennettua, kun painaa alaspäin nuolta hälytyksen vasemmasta laidasta. (Kuvio 6)



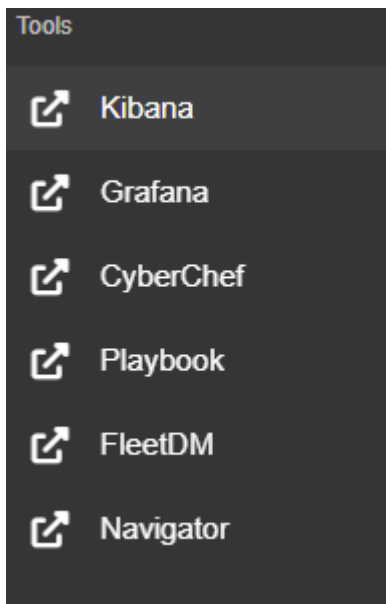
Kuvio 6. laajennettu

Dashboards välilehdellä saamme näkymään visuaalisia kuvauksia havaitusta liikenteestä ja pystymme analysoimaan esimerkiksi lähteitä, joista dataa on tullut. (Kuvio 7)



Kuvio 7. Dashboard

Tools osiosta löytyy security onioniin liitettyjä ja yleisesti käytettyjä työkaluja (Kuvio 8)



Kuvio 8. Tools

Otetaan esimerkiksi CyberChef jonka avulla voidaan käsitellä vaikka salauksia. Kuviossa 9 on käännetty base64 salauksesta merkkijono.

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars

Input

length: 94
lines: 2

U29tZS8kYXRhoIAxOTIuMTY4LjAuMQ==,IE90aGVyIGRhdGE6IDIxNl4yMy4zMy40dHlwRGF0YTogMTkyLjE2OC4wLjI=

Output

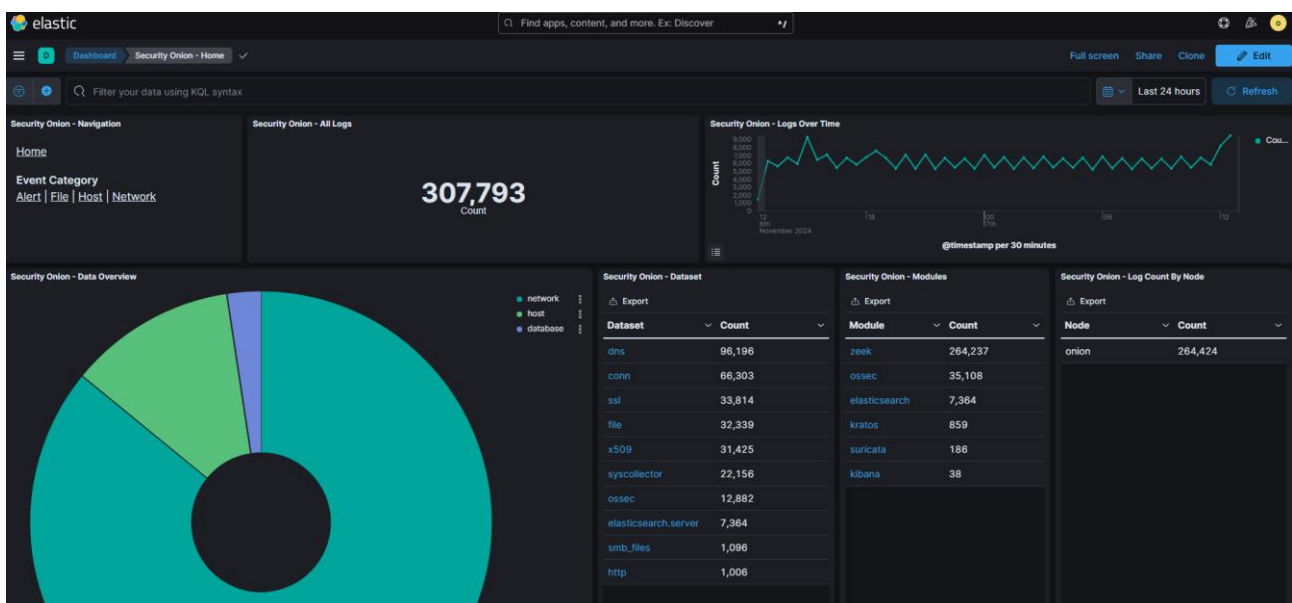
time: 0m
length: 64
lines: 1

Some data: 192.168.0.1 Other data: 216.23.33.12, Data: 192.168.0.2

Kuvio 9. cyberchef

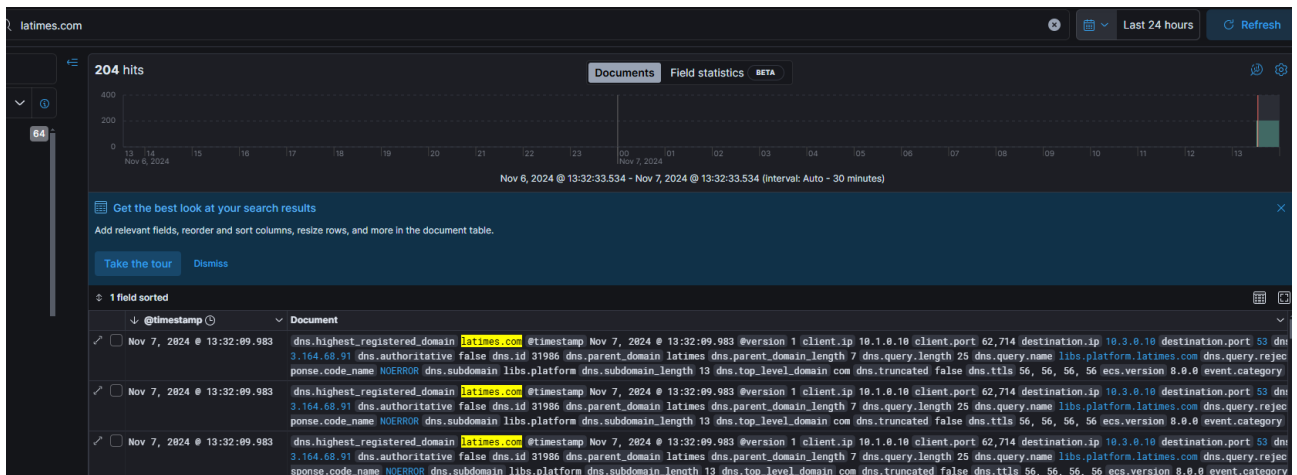
avataan seuraavaksi kibana vasemmasta palkista tools osion alta

Kibana aukeaa dashboard näkymään. (Kuvio 10)



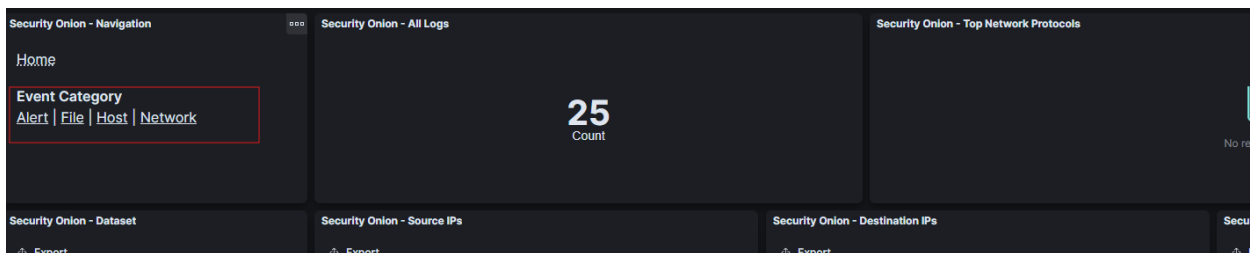
Kuvio 10. Kibana_dashboard

Kokeillaan mitä saamme näkyviin, kun menemme WS01:llä osoitteeseen www.latimes.com ja avataan kibanasta discover välilehti. Täällä näemme ws01 menneen sivustolle latimes.com. (Kuvio 11)



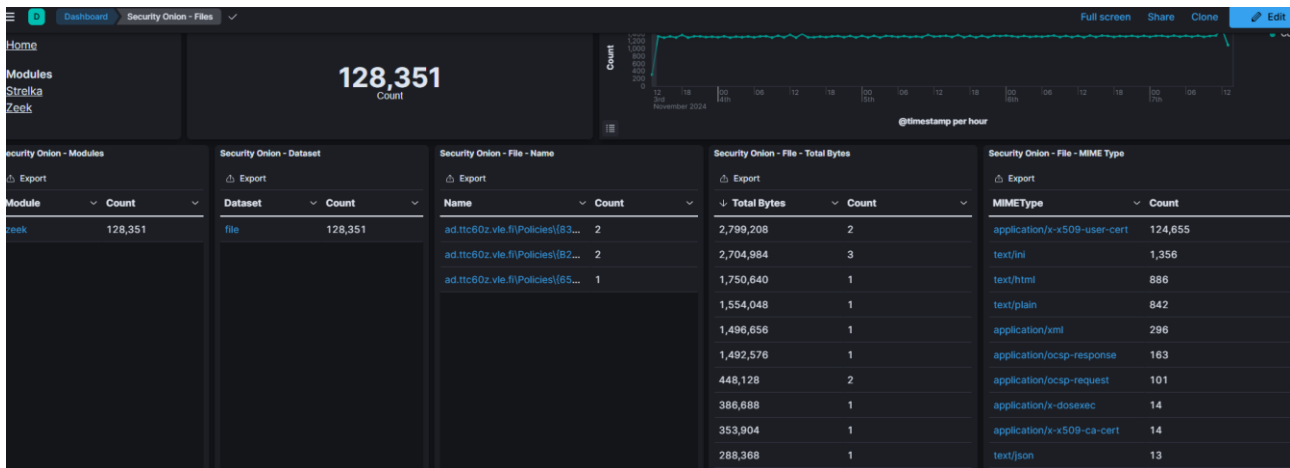
Kuvio 11. latimes.com

Kun palaamme dashboard välilehdelle, saa sieltä auki erilaisia näkymiä tapahtumiin liittyen. (Kuvio 12)



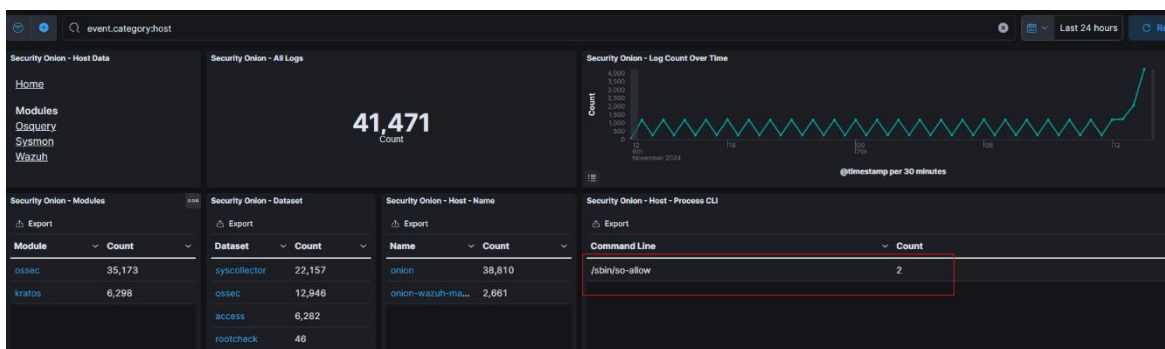
Kuvio 12. eventcategories

mennään file näkymään, jossa pystymme tarkastelemaan liikutettuja tiedostoja. (Kuvio 13)



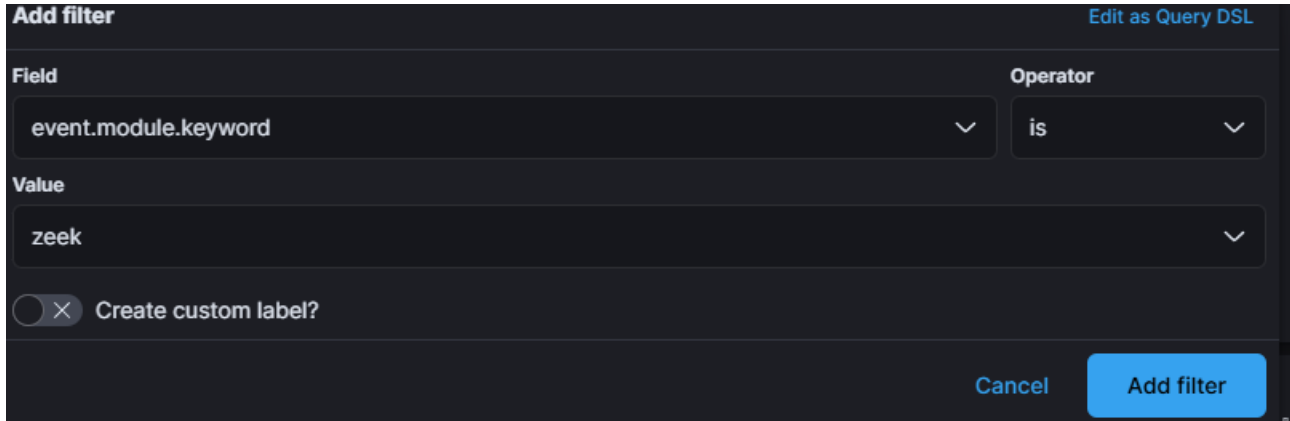
Kuvio 13. file

hosts osiossa näkyy aiemmin tekemämme muutokset onion palvelimella, kun sallimme Global-Protectin avulla yhteyden luomisen. (Kuvio 14)



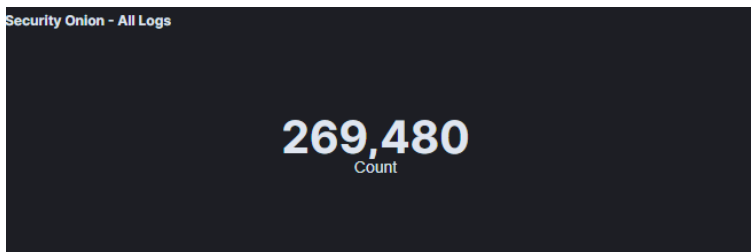
Kuvio 14. hosts

lisätään seuraavaksi suodatin dashboard näkymässä, jotta voimme suodattaa haluamamme datan suuresta data määrästä. Otetaan vaikka vain Zeek avainsanan sisältävät tapahtumat näkyviin. (Kuvio 15)



Kuvio 15.zeek

Zeek antaa valtavan määrän dataa. (Kuvio 16)



Kuvio 16. Lokit

Tämä johtuu siitä, että Zeek kerää loki tietoa niin laajasti, tutkien verkkoliikennettä pakettien sovelluskerroksen tasolla asti.

3.1 Mikä on Zeek?

Zeek on passiivinen, avoimen lähdekoodin verkkoliikenteen analysointityökalu. Sen ensisijainen tarkoitus on toimia verkon turvallisuusmonitorina, mutta se tukee myös hyvin muita liikenteen analyysitehtäviä. Zeek koostuu kahdesta pääkomponentista.

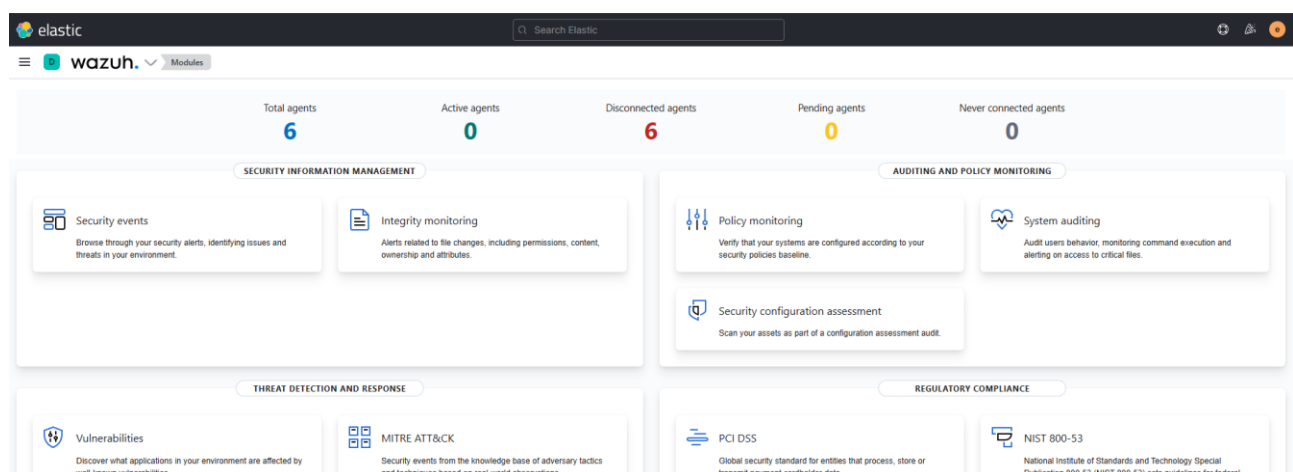
- **Tapahtumamoottori:** Tämä muuttaa saapuvan pakettiliikenteen korkeamman tason tapahtumiksi. Se kuvaa neutraalisti, mitä verkossa on havaittu, mutta ei tulkitse havaintojen merkitystä
- **Skriptitulkki:** Suorittaa Zeekin omalla skriptikielellä kirjoitettuja tapahtumankäsittelijöitä. Skriptit voivat ilmaista organisaation tietoturvakäytäntöjä ja määritellä tapahtumiin reagointia

Zeek reagoi verkkotapahtumien perusteella, kuten verkkoyhteydenotot ja DNS-kyselyt. Työkalu ymmärtää tunnetuimmat verkkoliikenneprotokollat ja tekee verkkotapahtumista selkeämpiä lokitietoja. Zeek lokeissa on tärkeitä tiedot tapahtumista, kuten lähde- ja kohde IP-osoitteet, hostit ja SSL-sertifikaatit. Sillä voidaan myös tutkia tallennettuja pcap tiedostoja, joiden datan, kuten HTTP kyselyt se esittää lokimuodossa. (Zeek Hello World. 2024)

4 Wazuh konfigurointi

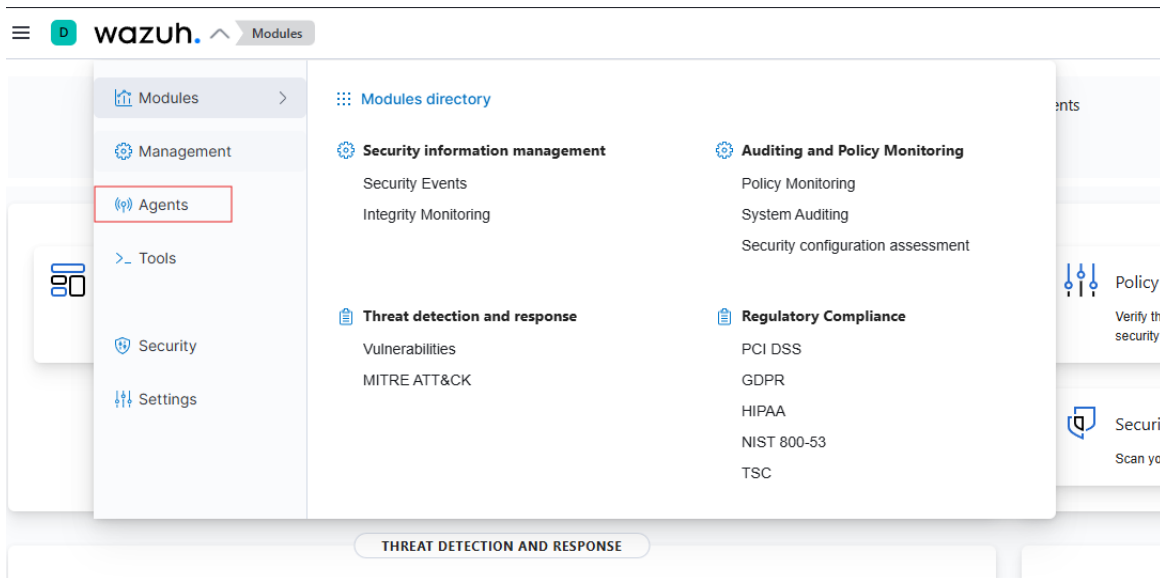
Wazuh käyttöliittymään pääsee kirjautumaan osoitteella [HTTPS://10.2.0.12](https://10.2.0.12)

myös Wazuh käyttää Elastic:iä. (Kuvio 17)



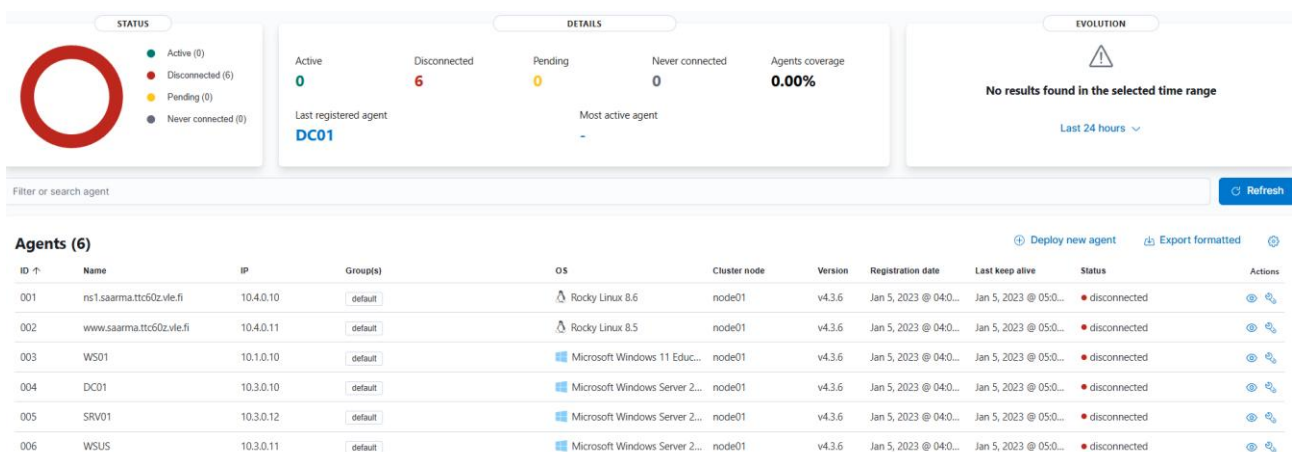
Kuvio 17. wazuh

seuraavaksi lisätään agentit päätelaitteille DC01, WS01, WSUS, NS12 ja WWW. Siirrytään agents välilehdelle. (Kuvio 18)



Kuvio 18. agents

Agents välilehdellä näkyy meidän haluamat laitteet mutta agentin tila on disconnected. (Kuvio 19)



Kuvio 19. agents_view

poistetaan disconnected agentit myöhemmin, lisätään aluksi uusi WS01. (Kuvio 20)

1 Choose the Operating system

Red Hat / CentOS Debian / Ubuntu **Windows** MacOS

2 Wazuh server address

This is the address the agent uses to communicate with the Wazuh server. It can be an IP address or a fully qualified domain name (FQDN).

10.2.0.12

3 Assign the agent to a group

Select one or more existing groups

default x

4 Install and enroll the agent

You can use this command to install and enroll the Wazuh agent in one or more hosts.

ⓘ If the installer finds another Wazuh agent in the system, it will upgrade it preserving the configuration.

ⓘ Requirements

- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

Kuvio 20. agentin lisäys

ajetaan seuraavat komennot. (Kuvio 21)

4 Install and enroll the agent

You can use this command to install and enroll the Wazuh agent in one or more hosts.

ⓘ If the installer finds another Wazuh agent in the system, it will upgrade it preserving the configuration.

ⓘ Requirements

- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

Keep in mind you need to run this command in a Windows PowerShell terminal.

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.3.6-1.msi -OutFile $(env:tmp)\wazuh-agent-4.3.6.msi; msexec.exe /i $(env:tmp)\wazuh-agent-4.3.6.msi /q WAZUH_MANAGER="10.2.0.12" WAZUH_REGISTRATION_SERVER="10.2.0.12" WAZUH_AGENT_GROUP="default"
```

5 Start the agent

```
NET START WazuhSvc
```

Kuvio 21. agentin lisäys2

suoritetaan komennot WS01:llä. (Kuvio 22)

```
PS C:\WINDOWS\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.3.6-1.msi -Out
File ${env:tmp}\wazuh-agent-4.3.6.msi; msixexec.exe /i ${env:tmp}\wazuh-agent-4.3.6.msi /q WAZUH_MANAGER='10.2.0.12'
' WAZUH_REGISTRATION_SERVER='10.2.0.12' WAZUH_AGENT_GROUP='default'
PS C:\WINDOWS\system32> NET START WazuhSvc
The Wazuh service is starting.
The Wazuh service was started successfully.
PS C:\WINDOWS\system32>
```

Kuvio 22. kommentojen lisäys

aiemmin disconnected WS01 on nyt paikattu uudella, joka on aktiivinen. (Kuvio 23)

Agents (6) [Deploy new agent](#) [Export formatted](#)

ID ↑	Name	IP	Group(s)	OS	Cluster node	Version	Registration date	Last keep alive	Status	Actions
001	ns1.saarna.ttc60z.vle.fi	10.4.0.10	default	Rocky Linux 8.6	node01	v4.3.6	Jan 5, 2023 @ 04:0...	Jan 5, 2023 @ 05:0...	disconnected	Refresh Details
002	www.saarna.ttc60z.vle.fi	10.4.0.11	default	Rocky Linux 8.5	node01	v4.3.6	Jan 5, 2023 @ 04:0...	Jan 5, 2023 @ 05:0...	disconnected	Refresh Details
004	DC01	10.3.0.10	default	Microsoft Windows Server 2...	node01	v4.3.6	Jan 5, 2023 @ 04:0...	Jan 5, 2023 @ 05:0...	disconnected	Refresh Details
005	SRV01	10.3.0.12	default	Microsoft Windows Server 2...	node01	v4.3.6	Jan 5, 2023 @ 04:0...	Jan 5, 2023 @ 05:0...	disconnected	Refresh Details
006	WSUS	10.3.0.11	default	Microsoft Windows Server 2...	node01	v4.3.6	Jan 5, 2023 @ 04:0...	Jan 5, 2023 @ 05:0...	disconnected	Refresh Details
007	WS01	10.1.0.10	default	Microsoft Windows 11 Educ...	node01	v4.3.6	Nov 7, 2024 @ 15:2...	Nov 7, 2024 @ 15:2...	active	Refresh Details

Kuvio 23. agents_active

toistetaan sama SRV01, DC01 ja WSUS palvelimille, tämän jälkeen agents näyttää tältä. (Kuvio 24)

Agents (6) [Deploy new agent](#) [Export formatted](#)

ID ↑	Name	IP	Group(s)	OS	Cluster node	Version	Registration date	Last keep alive	Status	Actions
001	ns1.saarna.ttc60z.vle.fi	10.4.0.10	default	Rocky Linux 8.6	node01	v4.3.6	Jan 5, 2023 @ 04:0...	Jan 5, 2023 @ 05:0...	disconnected	Refresh Details
002	www.saarna.ttc60z.vle.fi	10.4.0.11	default	Rocky Linux 8.5	node01	v4.3.6	Jan 5, 2023 @ 04:0...	Jan 5, 2023 @ 05:0...	disconnected	Refresh Details
007	WS01	10.1.0.10	default	Microsoft Windows 11 Educ...	node01	v4.3.6	Nov 7, 2024 @ 15:2...	Nov 7, 2024 @ 15:3...	active	Refresh Details
008	SRV01	10.3.0.12	default	Microsoft Windows Server 2...	node01	v4.3.6	Nov 7, 2024 @ 15:2...	Nov 7, 2024 @ 15:3...	active	Refresh Details
009	DC01	10.3.0.10	default	Microsoft Windows Server 2...	node01	v4.3.6	Nov 7, 2024 @ 15:3...	Nov 7, 2024 @ 15:3...	active	Refresh Details
010	WSUS	10.3.0.11	default	Microsoft Windows Server 2...	node01	v4.3.6	Nov 7, 2024 @ 15:3...	Nov 7, 2024 @ 15:3...	active	Refresh Details

Kuvio 24. agents_active2

Seuraavaksi linux agentit WWW ja NS1 toimimaan. Agentit luotiin kuvan (Kuvio 25) mukaisilla asetuksilla.

Deploy a new agent

[X Close](#)

1 Choose the Operating system

Red Hat / CentOS Debian / Ubuntu Windows MacOS

2 Choose the version

CentOS5 CentOS6 or higher Red Hat 5 Red Hat 6 or higher

3 Choose the architecture

i386 x86_64 armhf aarch64

4 Wazuh server address

This is the address the agent uses to communicate with the Wazuh server. It can be an IP address or a fully qualified domain name (FQDN).

10.2.0.12

Kuvio 25. Linux agentit

Agentti asennettu Linux-käyttöjärjestelmälle (NS1) ja tehty samalla tavalla WWW:lle. Alla kuva, jossa ilmenee tila Running. (Kuvio 26)

```

Installed:
wazuh-agent-4.3.6-1.x86_64

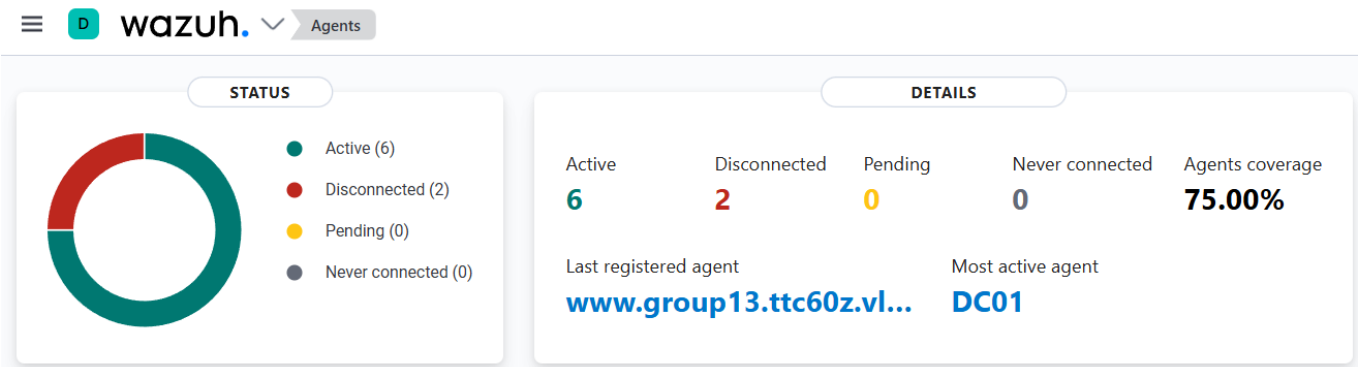
Complete!
[root@ns1 ~]#
[root@ns1 ~]# sudo systemctl daemon-reload
[root@ns1 ~]# sudo systemctl enable wazuh-agent
Synchronizing state of wazuh-agent.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /usr/lib/systemd/system/wazuh-agent.service.
[root@ns1 ~]# sudo systemctl start wazuh-agent
[root@ns1 ~]# sudo systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
   Loaded: loaded (/usr/lib/systemd/system/wazuh-agent.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2024-11-07 15:55:58 EET; 18s ago
     Process: 36063 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
    Tasks: 5 (limit: 5926)
   Memory: 147.3M
    CGroup: /system.slice/wazuh-agent.service
            └─36177 /bin/sh active-response/bin/restart.sh agent
              └─36181 /bin/sh /var/ossec/bin/wazuh-control restart
                └─36319 sleep 1
                  └─36320 /var/ossec/bin/wazuh-execd

Nov 07 15:55:51 ns1.group13.ttc60z.vle.fi systemd[1]: Starting Wazuh agent ...
Nov 07 15:55:51 ns1.group13.ttc60z.vle.fi env[36063]: Starting Wazuh v4.3.6 ...
Nov 07 15:55:52 ns1.group13.ttc60z.vle.fi env[36063]: Started wazuh-execd ...
Nov 07 15:55:53 ns1.group13.ttc60z.vle.fi env[36063]: Started wazuh-agentd ...
Nov 07 15:55:54 ns1.group13.ttc60z.vle.fi env[36063]: Started wazuh-syscheckd ...
Nov 07 15:55:55 ns1.group13.ttc60z.vle.fi env[36063]: Started wazuh-logcollector ...
Nov 07 15:55:56 ns1.group13.ttc60z.vle.fi env[36063]: Started wazuh-modulesd ...
Nov 07 15:55:58 ns1.group13.ttc60z.vle.fi env[36063]: Completed.
Nov 07 15:55:58 ns1.group13.ttc60z.vle.fi systemd[1]: Started Wazuh agent.
[root@ns1 ~]#

```

Kuvio 26. Linux commands

Saatiin myös Linux agentit (NS1, WWW) aktiivisiksi (Kuvio 27 & 28). Aiemmin varmaan opettajan toimesta luodut agentit näkyvät vieläkin listassa (ns1.saarma ja [www.saarma](#)), luotu vuonna 2023.



Kuvio 27. Wazuh agents.

Agents (8)												Deploy new agent	Export formatted	
ID ↑	Name	IP	Group(s)	OS	Cluster node	Version	Registration date	Last keep alive	Status	Actions				
001	ns1.saarma.ttc60z.vle.fi	10.4.0.10	default	Rocky Linux 8.6	node01	v4.3.6	Jan 5, 2023 @ ...	Jan 5, 2023 @ ...	disconnected					
002	www.saarma.ttc60z.vle.fi	10.4.0.11	default	Rocky Linux 8.5	node01	v4.3.6	Jan 5, 2023 @ ...	Jan 5, 2023 @ ...	disconnected					
007	WS01	10.1.0.10	default	Microsoft Windows ...	node01	v4.3.6	Nov 7, 2024 ...	Nov 7, 2024 ...	active					
008	SRV01	10.3.0.12	default	Microsoft Windows ...	node01	v4.3.6	Nov 7, 2024 ...	Nov 7, 2024 ...	active					
009	DC01	10.3.0.10	default	Microsoft Windows ...	node01	v4.3.6	Nov 7, 2024 ...	Nov 7, 2024 ...	active					
010	WSUS	10.3.0.11	default	Microsoft Windows ...	node01	v4.3.6	Nov 7, 2024 ...	Nov 7, 2024 ...	active					
011	ns1.group13.ttc60z.vle.fi	10.4.0.10	default	Rocky Linux 8.6	node01	v4.3.6	Nov 7, 2024 ...	Nov 7, 2024 ...	active					
012	www.group13.ttc60z.vle.fi	10.4.0.11	default	Rocky Linux 8.5	node01	v4.3.6	Nov 7, 2024 ...	Nov 7, 2024 ...	active					

Kuvio 28. Wazuh agents 2

5 Testaukset

Seuraavaksi aiheutamme hälytyksiä asentamiimme järjestelmiin testataksemme niiden reaktiota.

Aloitetaan ajamalla kali-ws laitteella seuraava skripti tiedosto. (Kuvio 29)





































```

1#!/bin/bash
2
3# Host and port scanning
4timestamp=$(date +%d-%m-%Y\ %H:%M:%S)
5echo "Starting Nmap ICMP scan at $timestamp" >> log.txt
6echo "root66" | sudo -S nmap -sn 10.3.0.10 10.3.0.12 10.4.0.11 10.3.0.11
7# sleep 120
8
9timestamp=$(date +%d-%m-%Y\ %H:%M:%S)
10echo "Starting Nmap port and service scan at $timestamp" >> log.txt
11echo "root66" | sudo -S nmap -sV -O 10.3.0.10 10.3.0.12 10.4.0.11 10.3.0.11
12# sleep 300
13
14# Web scanning
15timestamp=$(date +%d-%m-%Y\ %H:%M:%S)
16echo "Starting Nikto scan at $timestamp" >> log.txt
17nikto -h https://10.4.0.11
18# sleep 30
19
20timestamp=$(date +%d-%m-%Y\ %H:%M:%S)
21echo "Starting Wordpress scan at $timestamp" >> log.txt
22wpscan --url https://10.4.0.11
23# sleep 600
24
25# Service scanning
26timestamp=$(date +%d-%m-%Y\ %H:%M:%S)
27echo "Starting Hydra RPD brute force at $timestamp" >> log.txt
28hydra -L misc/users.txt -P misc/pass.txt rdp://10.3.0.11
29# sleep 800
30
31timestamp=$(date +%d-%m-%Y\ %H:%M:%S)
32echo "Starting RPC scanner at $timestamp" >> log.txt
33msfconsole -x "use auxiliary/scanner/dcerpc/endpoint_mapper; set RHOSTS 10.3.0.12; run; exit;"
34# sleep 100
35
36timestamp=$(date +%d-%m-%Y\ %H:%M:%S)
37echo "Starting SMB secretsdump at $timestamp" >> log.txt
38msfconsole -x "use auxiliary/scanner/smb/impacket/secretsdump; set SMBPass Root-66; set SMBUser Administrator; set RHOSTS 10.3.0.11; run; exit;"

```

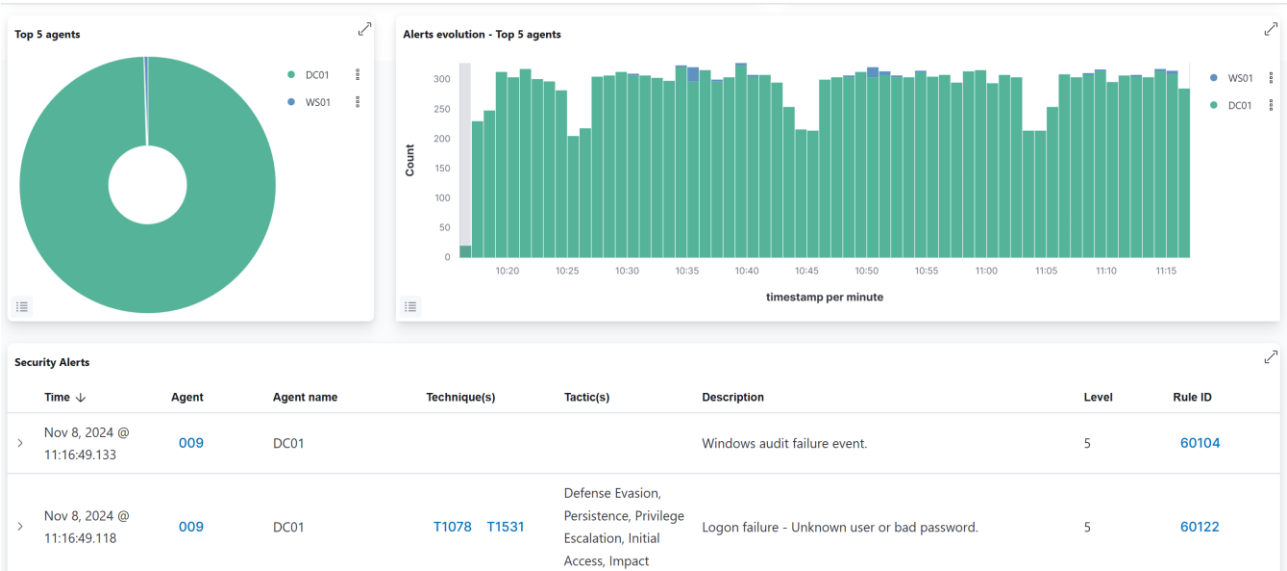
Kuvio 29. test_script

Skripti suorittaa useita eri verkkojen ja haavoittuvuuksien skannauksia, kuten porttiskannaus, verkkoskannaus sekä metasploit viitekehityksen RPC ja SMB haavoittuvuus skannaukset. Skripti suorittaa myös RDP salasanan murto yrityksen. näistä aiheutuu useita erilaisia hälytyksiä security onion järjestelmään. (Kuvio 30)

	Count	rule.name	event.module	event.severity_label
 	120	ET POLICY Non-Anonymous LDAPv3 Bind Request Outbound	suricata	high
 	96	ET SCAN NMAP OS Detection Probe	suricata	medium
 	80	ET POLICY GIOP/IIOP Request Outbound	suricata	high
 	80	ET POLICY Outbound MSSQL Connection to Non-Standard Port - Likely Malware	suricata	medium
 	48	ET SCAN MS Terminal Server Traffic on Non-standard Port	suricata	medium
 	20	ET SCAN NMAP SIP Version Detect OPTIONS Scan	suricata	medium
 	16	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	suricata	high
 	16	ET SCAN Possible Nmap User-Agent Observed	suricata	high
 	16	ET SCAN Potential SSH Scan OUTBOUND	suricata	medium
 	12	ET POLICY RMI Request Outbound	suricata	high
 	10	ET SCAN Suspicious inbound to mySQL port 3306	suricata	medium
 	8	GPL DNS named version attempt	suricata	medium
 	6	ET DOS Microsoft Remote Desktop (RDP) Syn then Reset 30 Second DoS Attempt	suricata	medium
 	6	ET POLICY External Oracle T3 Requests Inbound	suricata	high
 	5	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium
 	5	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium
 	5	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium
 	4	ET INFO TLS Handshake Failure	suricata	medium

Kuvio 30. alerts

Wazuh järjestelmässä ilmaantuu myös useita hälytyksiä. Kuviossa 31 näkyvissä esimerkiksi yksi epäonnistunut kirjautumisyritys brute-forcen jäljiltä.



Kuvio 31. alerts2

Kokeillaan ajaa LDAP-tiedustelu komento kali-ws:llä kuvion 32 mukaan.

```
(kali@kali-ws)-[~/Desktop]
$ ldapsearch -x -H ldap://10.3.0.10 -D "CN=Administrator,CN=Users,DC=AD,DC=TTC60Z,DC=VLE,DC=FI" -w "Root-66" -b "DC=AD,DC=TTC60Z,DC=VLE,DC=FI" "(objectClass=*)"
```

Kuvio 32.ldap

Komento käyttää ldap protokollaa tiedustellakseen Active Directory -ympäristöstä.

tästä aiheutuu Security Onioniin hälytyksiä.

Count	rule.name	event.module	event.severity_label
8	ET POLICY Successful Non-Anonymous LDAPv3 Bind Request Outbound	suricata	high
4	ET POLICY Non-Anonymous LDAPv3 Bind Request Outbound	suricata	high

Kuvio 33. alert_SecOnion

avataan alempi hälytys ryhmittely tarkempaan tarkasteluun Hunt ominaisuudella. Kuviossa 34 ilmenee lähde ja kohde ip osoitteet ja portit.







Timestamp	source.ip	source.port	destination.ip	destination.port	rule.name	rule.category	event.severity_label	log.id
2024-11-28 12:51:59.207 +02:00	10.2.0.13	52736	10.3.0.10	389	ET POLICY Non-Anonymous LDAPv3 Bind Request Outbound	Potential Corporate Privacy Violation	high	49779
2024-11-28 12:51:59.207 +02:00	10.2.0.13	52736	10.3.0.10	389	ET POLICY Non-Anonymous LDAPv3 Bind Request Outbound	Potential Corporate Privacy Violation	high	15198
2024-11-28 12:51:59.207 +02:00	10.2.0.13	52736	10.3.0.10	389	ET POLICY Non-Anonymous LDAPv3 Bind Request Outbound	Potential Corporate Privacy Violation	high	15051
2024-11-28 12:51:59.207 +02:00	10.2.0.13	52736	10.3.0.10	389	ET POLICY Non-Anonymous LDAPv3 Bind Request Outbound	Potential Corporate Privacy Violation	high	14499

Kuvio 34. hunt

ajetaan vielä Nmap skanni hyödyntäen NSE-skriptejä kuvion 35 komennolla.

```
(kali@kali-ws)-[~/Desktop]
$ nmap -Pn -p 389,636,88,464,53 --script "ldap*,smb-enum*" -oN ad_scan.txt 10.3.0.10
```

Security Onion hälytykset kuviossa 35. Samoja hälytyksiä syntyi aiemmasta testistä, mutta niiden määrä on lisääntynyt ja ylin rivi on uusi.

	Count	rule.name	event.module	event.severity_label
 	16	ET POLICY Anonymous LDAPv3 Bind Request Outbound	suricata	high
 	12	ET POLICY Successful Non-Anonymous LDAPv3 Bind Request Outbound	suricata	high
 	8	ET POLICY Non-Anonymous LDAPv3 Bind Request Outbound	suricata	high

Kuvio 35.Alerts_SecOnion2

Lähteet

Sigmund Brandstatetter. Understanding Wazuh: The Free, Open Source Security Platform For XDR & SIEM. Medium-verkkosivun artikkeli. 25.2.2024. Viitattu 7.11.2024. <https://osintph.medium.com/understanding-wazuh-the-free-open-source-security-platform-for-xdr-siem-48b3c3dfba9d>

Zeek Hello World. Zeek opetus sivusto. 2024. Viitattu 7.11.2024. <https://try.zeek.org/#/tryzeek/saved/8603a937b2454fa4bfdc58b579f7f704>

Jadhusan Sadhik. Basic Overview of a Powerful Security Monitoring Platform. Medium artikkeli. 2023. Viitattu 28.11.2024. <https://medium.com/@jadhusan24/basic-overview-of-a-powerful-security-monitoring-platform-fd8ce3db445b>

Liitteet

Liite 1. Liitteen otsikko

Liite 2. Liitteen otsikko