



## Tietoturvakontrollit – Labra 6

### Ryhmä 3

Juha-Matti Hietala

Markus Pollari

Topi Liljeqvist

Maija Virta

Oppimistehtävä

Huhtikuu 2023

Tekniikan ala

Tieto- ja viestintätieteiden tutkinto-ohjelma (AMK)

## Sisältö

<b>1</b>	<b>Johdanto.....</b>	<b>4</b>
<b>2</b>	<b>Teoria .....</b>	<b>4</b>
2.1	IDS & IPS .....	4
2.1.1	IDS .....	4
2.1.2	IPS.....	5
2.4	Security Onion.....	6
2.5	Zeek.....	7
2.6	Wazuh .....	7
<b>3</b>	<b>Dokumentointi .....</b>	<b>8</b>
3.1	Security Onion.....	8
3.2	Zeek.....	10
3.3	Wazuh .....	14
3.4	Testausta .....	24
<b>4</b>	<b>Pohdinta.....</b>	<b>38</b>
<b>Lähteet.....</b>	<b>39</b>	

## Kuvat

Kuva 1 Security Onion – Alerts .....	8
Kuva 2 Security Onion – Dashboards 1.....	9
Kuva 3 Security Onion – Dashboards 2.....	9
Kuva 4 Security Onion – Hunt .....	10
Kuva 5 Security Onion – Users .....	10
Kuva 6 Security Onion - Zeek etusivu .....	11
Kuva 7 Zeek - Discover ( <a href="http://www.latimes.com">www.latimes.com</a> ) .....	12
Kuva 8 Zeek - Maps .....	12
Kuva 9 Home page .....	13
Kuva 10 All logs .....	13
Kuva 11 Indicator .....	14
Kuva 12 Wazuh: 10.2.0.12.....	14
Kuva 13 Wazuh etusivu .....	15
Kuva 14 Wazuh jo valmiit agentit jotka poistettiin ja luotiin uudestaan .....	15
Kuva 15 Ohjeistus agenttien poistoon .....	15
Kuva 16 Agenttien poistoa .....	16

Kuva 17 Wazuh agenttien luomista – Operating system.....	16
Kuva 18 Kirjatuminen koneille SSH yhteyden kautta.....	17
Kuva 19 WWW agentin luomista .....	17
Kuva 20 Onnistunut agentin luonti mutta väärä IP= 10.4.0.11.....	18
Kuva 21 start wazuh-agent komentoa .....	18
Kuva 22 WS01 , vielä väärä IP.....	19
Kuva 23 Wazuh väärä IP (WS01) .....	19
Kuva 24 WS01 korjaus, oikea IP 10.2.0.12.....	20
Kuva 25 Tarkistusta .....	20
Kuva 26 Uudestaan Wazuh agentin starttaamista, oikealla IP:llä.....	21
Kuva 27 Agentin luontin, NS01.....	22
Kuva 28 NET start WazuhSvc - Powershell .....	22
Kuva 29 SRV01 Wazuh start .....	23
Kuva 30 Onnistuneesti luodut agentit Wazuh (status: active).....	23
Kuva 31 Kali - test_script.sh .....	24
Kuva 32 Kali skriptin sisältö(skannaukset).....	24
Kuva 33 Kali Nmap skan report .....	25
Kuva 34 Security Onion Kalilla ajetun skriptin jälkeen.....	26
Kuva 35 Security Onion - Alerts .....	26
Kuva 36 Security Onion - Dashboard.....	27
Kuva 37 Kali ajetun skriptin tarkastelua .....	27
Kuva 38 Wazuh - Kalilla ajetun skriptin aiheuttamat Events .....	28
Kuva 39 Wazuh Security events .....	28
Kuva 40 Wazuh Security Alerts – WS01.....	29
Kuva 41 Wazuh Security Alerts - DC01 .....	29
Kuva 42 Wazuh secyrity alerts SRV01 .....	30
Kuva 43 Wazuh security Alerts - WS01.....	30
Kuva 44 Wazuh alerttien filtteröintiä .....	31
Kuva 45 Wazuh filtteröidyn alertin tietojen tarkastelua .....	31
Kuva 46 Kalin skriptin muokkausta.....	32
Kuva 47 Kali - Oma skripti .....	32
Kuva 48 Ajettiin uudestaan Kalilla muokattu skripti, Wazuh alerts.....	33
Kuva 49 Wazuh - Kaikki agentit alerts .....	33
Kuva 50 Security Onion uudestaan ajetun skriptin jälkeen (Alerts).....	34

Kuva 51 Security Onion - Events (round 2).....	34
Kuva 52 Wazuh dashboard – 1061 total ILMAN 007 (ws01) .....	35
Kuva 53 Wazuh kaikki agentit Alerts .....	35
Kuva 54 Wazuh security alerts – Win application error event .....	36
Kuva 55 Wazuh filter ilman 007 agent (WS01).....	36
Kuva 56 Wazuh Dashboard - 1770 total vielä uudestaan (Kaikki agentit) .....	37
Kuva 57 Wazuh alert table information – SRV01 .....	37
Kuva 58 Total alerts.....	38

## 1 Johdanto

Kuudennen laboratorioharjoituksen tarkoituksena on tutustua Security Onioniin sekä Security Onionin työkaluihin, Zeek:iin ja Wazuhiin.

Harjoituksessa aluksi tutustutaan Security Onionin ominaisuuksiin. Sitten asennetaan Wazuhiin agentit DC01, WS01, NS1, WWW, WSUS & SR01 työasemille ja palvelimille. Sen jälkeen tutkitaan Wazuhin ominaisuuksia tarkemmin. Kalin kautta ajetaan test\_script.sh sisältö, jonka ajaminen aiheuttaa paljon verkkoliikennettä, jonka avulla voidaan tutkia millaisia hälytyksiä Wazuhiin tulee.

Harjoitustyössä dokumentoidaan kaikki tehdyt toimenpiteet ja testaukset. Sekä lisäksi käydään läpi teoria IDS (Intrusion Detection Systems) ja siihen liittyvistä termeistä, teoria Security Onionista, Zeekistä ja Wazuhista. Harjoitustyön lopussa on pohdita harjoitustyön työstämisestä ja kokonaisuudesta.

## 2 Teoria

### 2.1 IDS & IPS

IDS tarkoittaa tunkeutumisen havaitsemisjärjestelmää (Intrusion Detection System) ja IPS tunkeutumisenestojärjestelmää (Intrusion Prevention System). Järjestelmien pääasiallinen ero on siinä, että IDS sisältää seurantajärjestelmiä ja IPS kontrollointijärjestelmiä. IDS ei muuta verkkoliikennettä, kun taas IPS estää pakettien liikkumisen riippuen niiden sisällöstä, palomuurin tapaan.  
(Tunggal, 2023)

#### 2.1.1 IDS

IDS on laite tai ohjelmisto, joka seuraa verkkoa tai järjestelmää haitallisen toiminnan osalta. Havaitut haitalliset toiminnot tyypillisesti joko raportoidaan järjestelmänvalvojalle, tai kerätään keskitysti SIEM järjestelmään. On olemassa kolme yleistä havaitsemisvaihtoehtoa tunkeutumisen valvontaan: (Tunggal, 2023)

**Signature-based detection:** Tunnistaa hyökkäyksen tarkastelemalla tiettyjä malleja, kuten bittijärjestyksiä (byte sequences) verkkoliikenteessä tai tiedettyä tunnistetta, jota haittaohjelma käyttää. (Tunggal, 2023)

**Anomaly-based detection:** Havaitsee tunkeutumiset ja väärinkäytöt sekä verkossa että tietokoneissa seuraamalla järjestelmän toimintaa ja luokittelemalla havaitut toiminnot joko normaaliksi tai poikkeaviksi. (Tunggal, 2023)

**Reputation-based detection:** Tunnistaa potentiaaliset kyberuhat mainepisteiden perusteella. (Tunggal, 2023)

IDS järjestelmät luokitellaan yleisesti kahden tyypiksiksi; Network Intrusion Detection System (NIDS), joka analysoi saapuvaa verkkoliikennettä sekä Host-based Intrusion Detection System (HIDS), joka valvoo saapuvia ja läheviä paketteja laitteesta ja varoittaa, jos epäilyttävää toimintaa havaitaan. HIDS ottaa tilannekuvia järjestelmätiedostoista ja vertaa niitä aiemmin otettuihin tilannekuviin. Mikäli tärkeitä tiedostoja on muokattu tai poistettu, annetaan hälytys. (Tunggal, 2023)

### 2.1.2 IPS

IPS sovellukset keskittyvät mahdollisen haitallisen toiminnan tunnistamiseen, tietojen kirjaamiseen, raportointiin ja estämiseen. Hyökkäysten estämiseksi IPS saattaa muuttaa suojausympäristöä muuttamalla hyökkäyksen sisältöä tai määrittämällä palomuurin uudelleen. IPS skannaa kaiken verkkoliikenteen yhdellä seuraavista havaitsemistyyleistä: (Tunggal, 2023)

**Signature-based detection:** Valvoo paketteja verkossa ja vertaa niitä ennalta määriteltyihin ja ennalta määritettyihin hyökkäysmalleihin. (Tunggal, 2023)

**Statistical anomaly-based detection:** Tarkkailee verkkoliikennettä verraten sitä "normaaliin" taasoon, esimerkiksi kuinka paljon kaistanleveyttä tai mitä protokollia käytetään. (Tunggal, 2023)

**Stateful protocol analysis detection:** Tunnistaa poikkeamat protokollatiloissa vertaamalla havaittuja tapahtumia ennalta määritettyihin profiileihin. (Tunggal, 2023)

IPS järjestelmät luokitellaan yleisesti neljään eri tyyppiin: (Tunggal, 2023)

**Network-based intrusion prevention system (NIPS):** Havaitsee ja estää haitallisen tai epäilyttävän toiminnan analysoimalla paketteja koko verkossa. (Tunggal, 2023)

**Wireless intrusion prevention system (WIPS):** Monitoroi radioaaltoja löytääkseen luvattomia langattomia tukiasemia ja tekee automaattisesti vastatoimia poistaakseen ne. (Tunggal, 2023)

**Network behavior analysis (NBA):** Perustuu poikkeamien havaitsemiseen. Tarvitsee "koulutusajan" määrittääkseen mikä on normaalista toimintaa järjestelmässä, johon verratessa poikkeamat havaitaan. (Tunggal, 2023)

**Host-based intrusion prevention system (HIPS):** Kriittisten tietokonejärjestelmien suojaamiseen käytetty ohjelma tai järjestelmä. Estää haitallisen toiminnan yhdellä koneella ensisijaisesti analysoimalla koodin käyttäytymistä. (Tunggal, 2023)

## 2.2 Security Onion

Security Onion on avoimen lähdekoodin tunkeutumisen havaitsemis-, tietoturvan seuranta- sekä lokihallintajärjestelmä. Se tarjoaa verkkoon ja palvelinpohjaiset tunkeutumisen havaitsemisjärjestelmät (NIDS ja HIDS), pakettien sieppauksen, sekä tehokkaat indeksointi-, haku-, visualisointi- ja analysointityökalut suuren datamäärän käsittelyn järkeistämiseen. (Meena, n.d.)

Security Onion sisältää laajan valikoiman tietoturvatyökaluja. Nimi tulee tyylistä, missä Security Onionin sisältämät työkalut on rakennettu kerroksiksi tarjoamaan puolustustekniikoita useiden erilaisten analyyttisten työkalujen muodossa. Nämä kerrokset voidaan jakaa kolmeen laajempaan alueeseen: (Meena, n.d.)

- Paketinsieppaus (Full Packet Capture)
- Verkko- ja palvelinpohjaiset tunkeutumisen havaitsemisjärjestelmät (NIDS ja HIDS)
- Analysointityökalut

## 2.3 Zeek

Zeek on passiivinen, avoimen lähdekoodin verkkoliikenteen analysaattori. Monet operaattorit käyttävät Zeekiä verkon suojausmonitorina (NSM) epäilyttävän tai haitallisen toiminnan tutkinnan tukena. Zeek tukee myös laajaa valikoimaa tietoturva-alueen ulkopuolisia liikenteen analysointi-tehtäviä, mukaan lukien suorituskyvyn mittaus ja vianmääritys. (About Zeek 2023.)

Zeek antaa paljon tuloksia koska siitä saa laajan lokisarjan, joka kuvailee verkon toimintaa. Nämä lokit sisältävät paitsi kattavan tietueen jokaisesta johdolla havaitusta yhteydestä, myös sovellustason transkriptioita. Näitä ovat kaikki HTTP-istunnnot pyydettyineen URI-tunnisteineen, avainotsikoinen, MIME-tyyppiineen ja palvelinvastauksineen. DNS-pyynnöt ja vastaukset, SSL-varmenteet sekä SMTP-istuntojen avainsisältö. (About Zeek 2023.)

Lokien lisäksi Zeek:issä on sisäänrakennettu toiminnallisuus erilaisiin analyysi- ja havaintotehtäviin, mukaan lukien tiedostojen poimiminen HTTP-sessioista, haittaohjelmien tunnistaminen kytkemällä ne ulkoisiin rekistereihin, verkossa nähtävien ohjelmistojen haavoittuvien versioiden raportointi, suosittujen verkkosovellusten tunnistaminen, SSH:n brute-forcing, SSL-sertifikaattiketjujen varmentaminen ja paljon muuta. (About Zeek 2023.)

## 2.4 Wazuh

Wazuh on ilmainen avoimeen lähdekoodiin pohjautuva alusta, jolla voidaan seurata tietoturva-poikkeamia, havaita uhkia ja hyökkäyksiä, analysoida lokeja sekä sitä voidaan käyttää päätelaitteiden seurantaan, mutta myös pilvipalveluiden ja konttien seurantaan sekä yhdistämään ja analysoimaan ulkoisista lähteistä saatua uhkatietoa (Särkisaari 2020, 9).

Wazuhia käytetään laitteiden tietoturvan kannalta kriittisten tietojen eli lokien keräämiseen, aggregointiin, indeksointiin ja analysointiin. Wazuhin avulla organisaatio voi havaita tunkeutumisia, uhkia ja käyttäytymisen poikkeavuuksia. Näillä ominaisuuksilla Wazuh auttaa ehkäisemään tietoturvapoikkeamien huomaamatta jäämistä. (Särkisaari 2020, 12.)

## 3 Dokumentointi

### 3.1 Security Onion

Labra 6 aloitettiin kirjautumalla DC01 koneelta selaimen kautta security Onioniin:

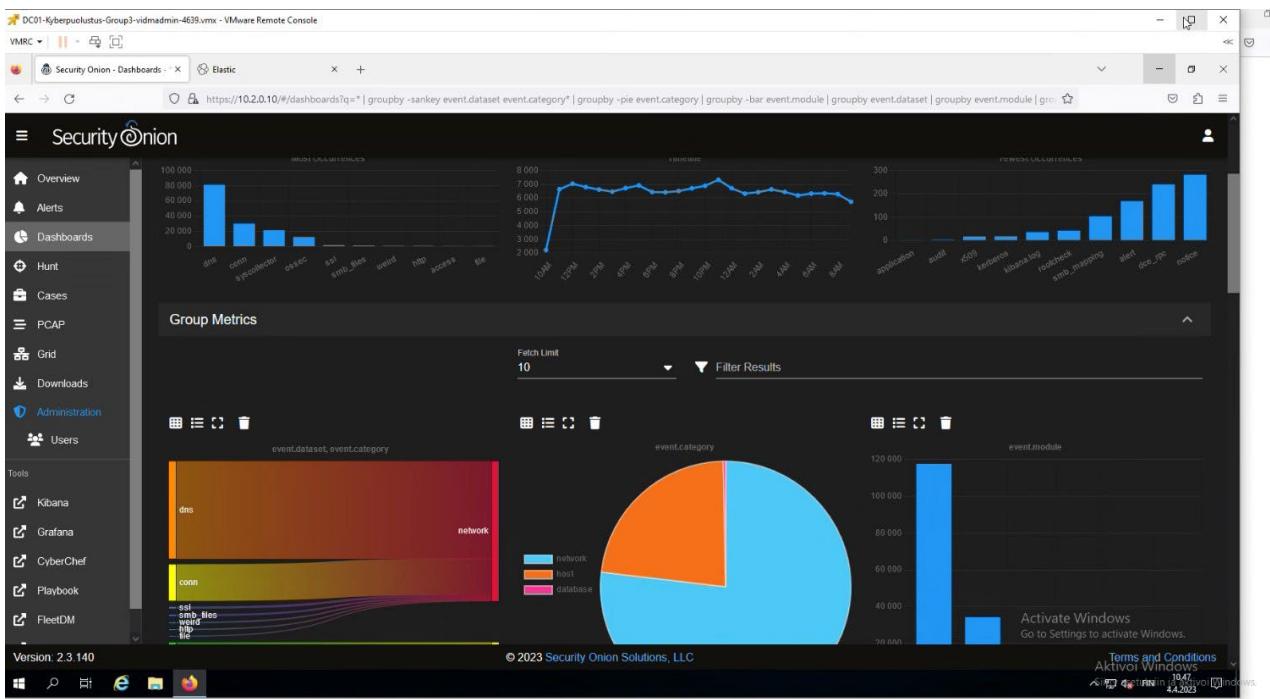
[https://10.2.0.10.](https://10.2.0.10/) Mentiin aluksi ohjeen mukaan Alerts kohtaan. Sitten aloimme tutkimaan Security Onionin muita ominaisuuksia. Esitetty kuvissa alla.

The screenshot shows the 'Alerts' page of the Security Onion web interface. The left sidebar includes links for Overview, Alerts (which is selected), Dashboards, Hunt, Cases, PCAP, Grid, Downloads, Administration, and Users. The main area has a search bar and filter options for 'Last 24 hours'. A table lists alerts with the following data:

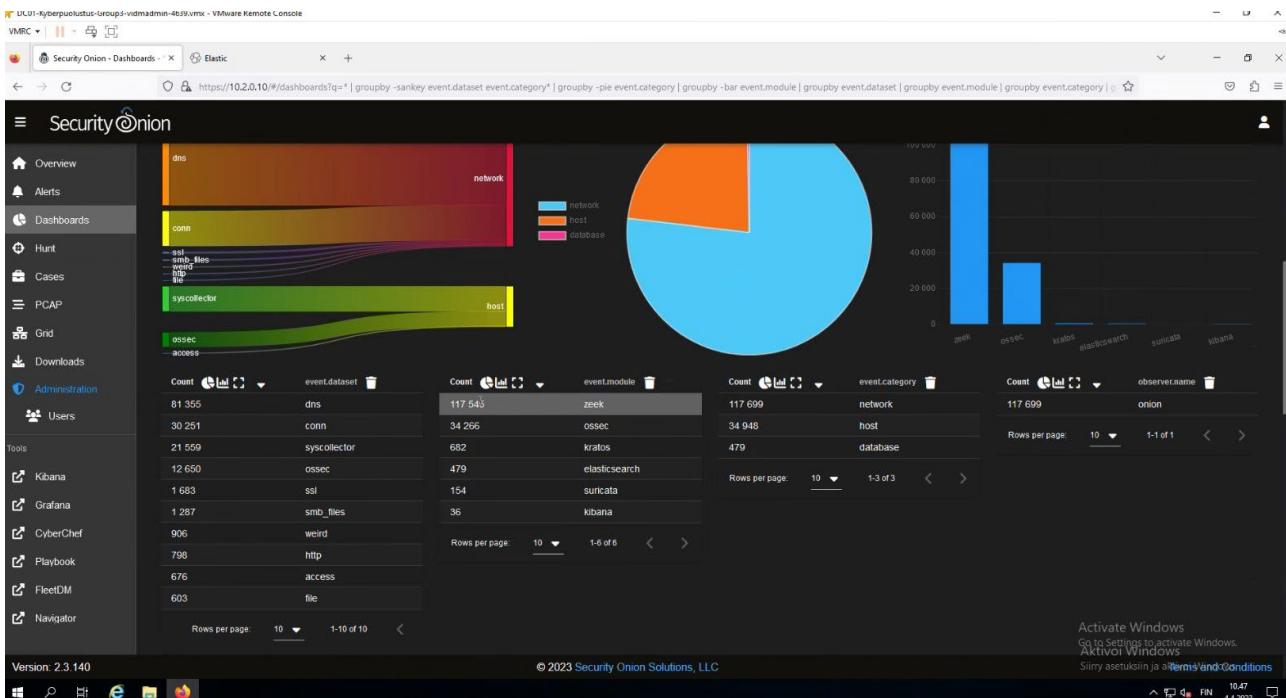
Count	Rule name	event.module	event.severity_label
81	ET HUNTING Suspicious NULL DNS Request	suricata	low
72	ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent	suricata	low
14	System Audit event.	ossec	low
1	Host-based anomaly detection event (rootcheck)	ossec	low
1	ET INFO Windows OS Submitting USB Metadata to Microsoft	suricata	low

At the bottom, there are links for Kibana, Grafana, CyberChef, Playbook, FleetDM, and a note about activating Windows.

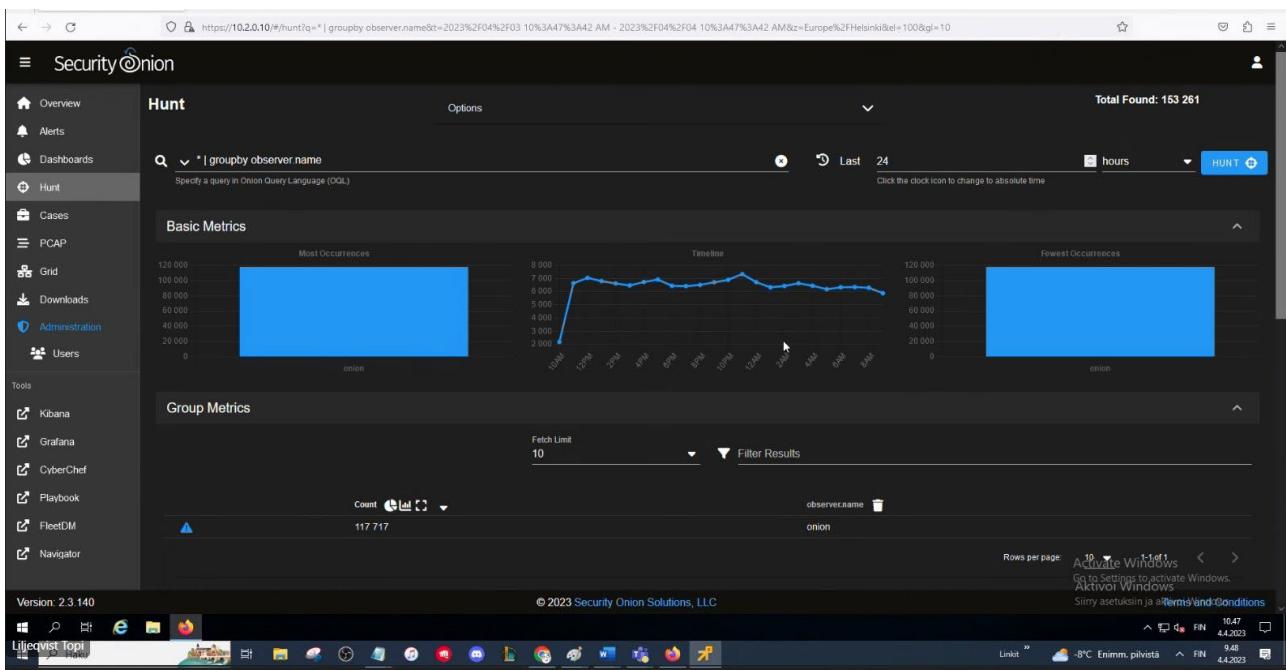
Kuva 1 Security Onion – Alerts



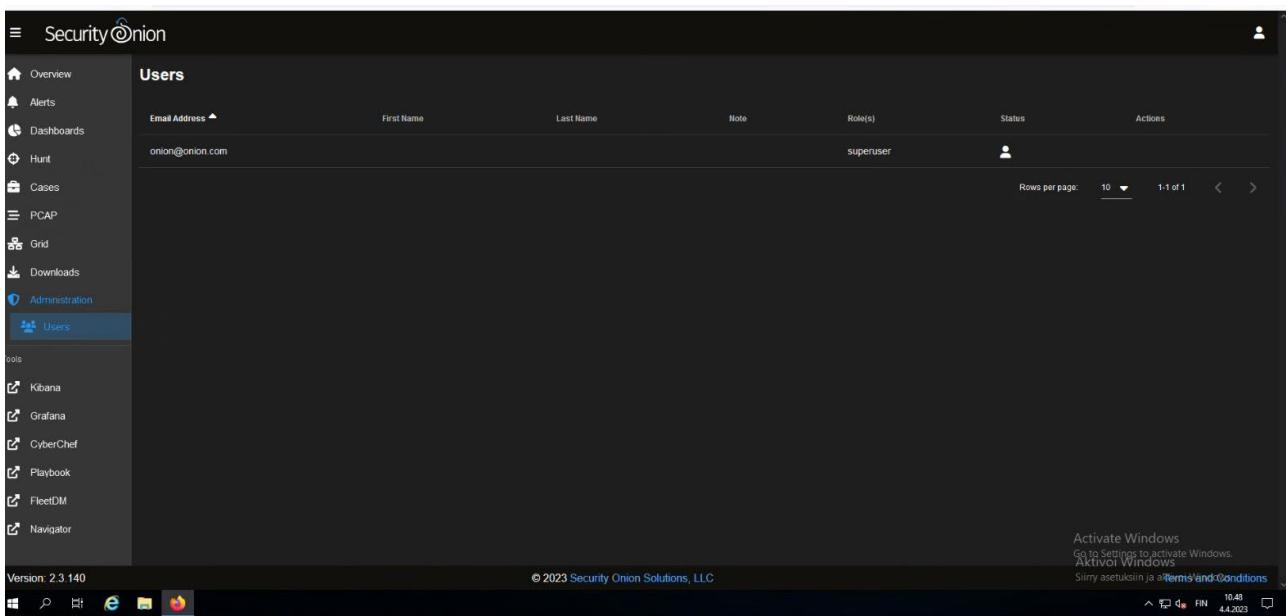
Kuva 2 Security Onion – Dashboards 1



Kuva 3 Security Onion – Dashboards 2



Kuva 4 Security Onion – Hunt



Kuva 5 Security Onion – Users

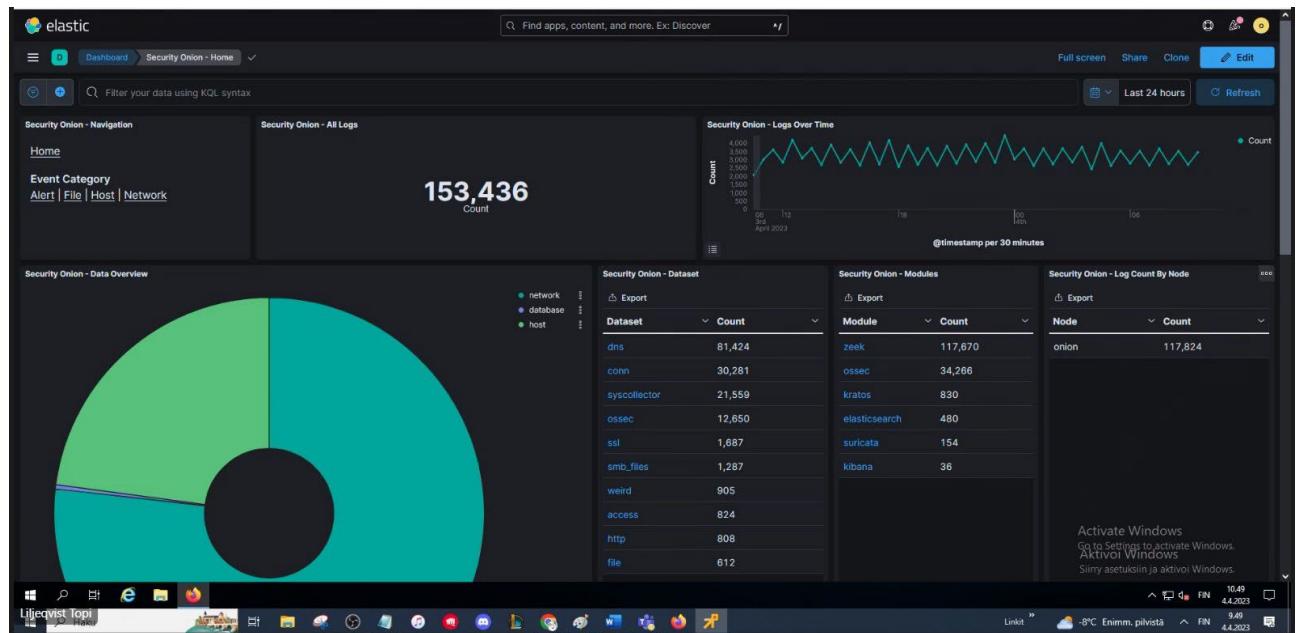
### 3.2 Zeek

Seuraavaksi tutkittiin Security Onionin alla olevia työkaluja kuten Kibanaa/Zeekia. Mentiin ohjeistukseen mukaan esimerkiksi osoitteeseen [www.latimes.com](http://www.latimes.com) ja tarkistettiin Analyticsin alta etsimällä, löytyykö käynti sivustolla. Esitettynä kuvissa alla työkalun tutkimista ja siihen tutustumista, sekä vastattu harjoituksessa olevaan kysymykseen.

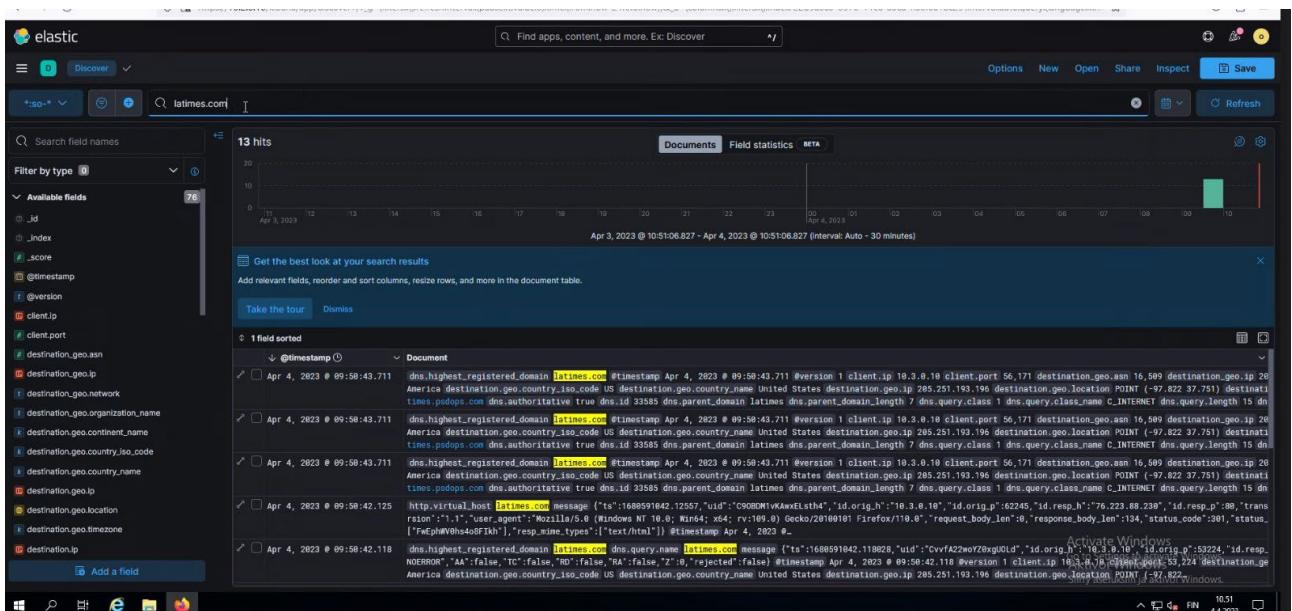
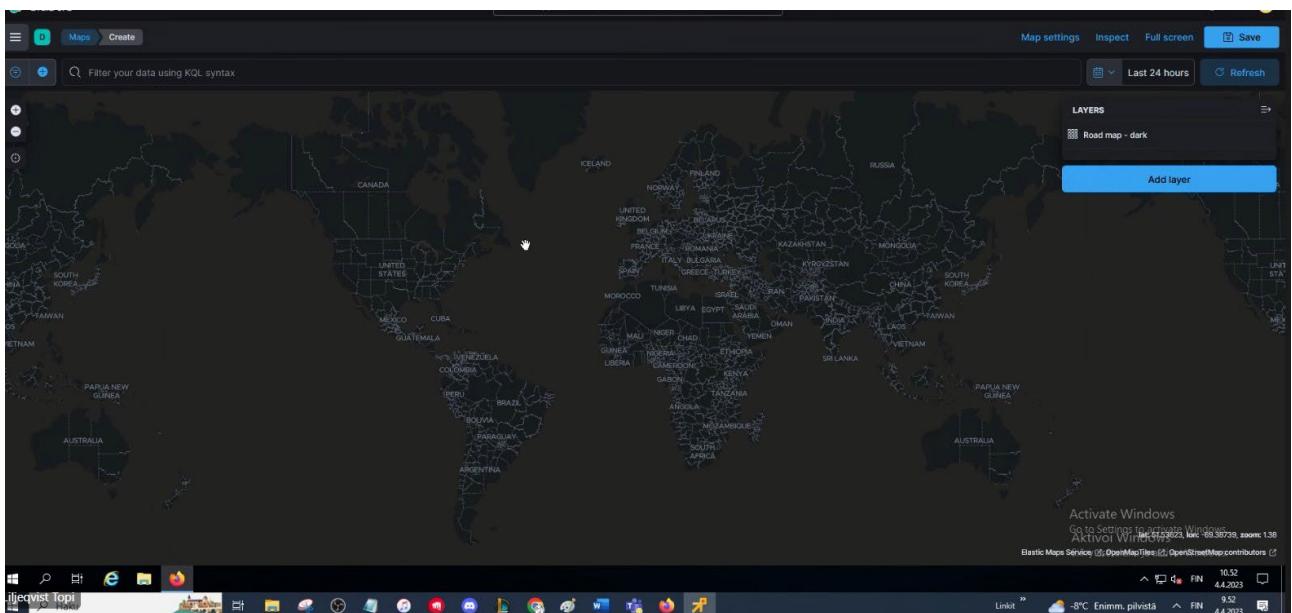
Kysymys harjoituksessa liittyen Zeek: Mikä Zeek on ja miksi se antaa niin paljon tuloksia?

Zeek on passiivinen, avoimen lähdekoodin verkkoliikenteen analysaattori. Monet operaattorit käyttävät Zeekiä verkon suojausmonitorina (NSM) epäilyttävän tai haitallisen toiminnan tutkinnan tukena. Zeek tukee myös laajaa valikoimaa tietoturva-alueen ulkopuolisista liikenteen analysointi-tehtäviä, mukaan lukien suorituskyvyn mittaus ja vianmääritys. (About Zeek 2023.)

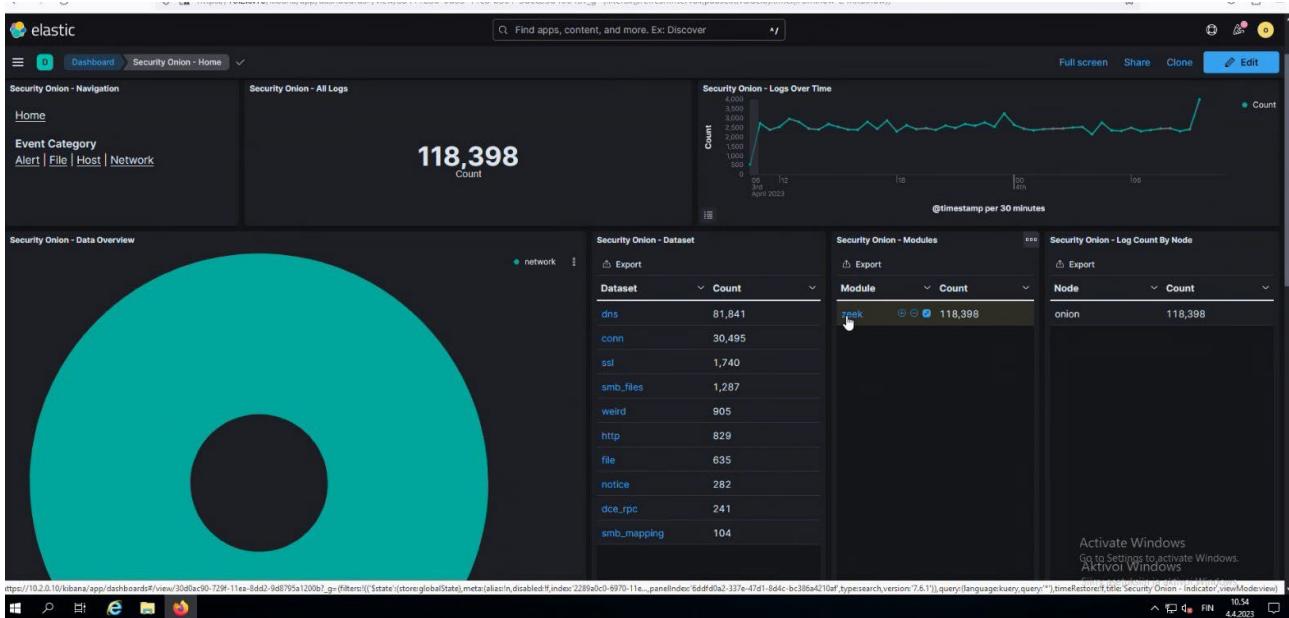
Zeek antaa paljon tuloksia koska siitä saa laajan lokisarjan, joka kuvaa verkon toimintaa. Nämä lokit sisältävät paitsi kattavan tietueen jokaisesta johdolla havaitusta yhteydestä, myös sovellustason transkriptioita. Näitä ovat kaikki HTTP-istunnnot pyydettyineen URI-tunnisteineen, avainotsikoinen, MIME-tyyppineen ja palvelinvastauksineen. DNS-pyynnöt ja vastaukset, SSL-varmenteet; SMTP-istuntojen avainsisältö ja paljon enemmän. (About Zeek 2023.)



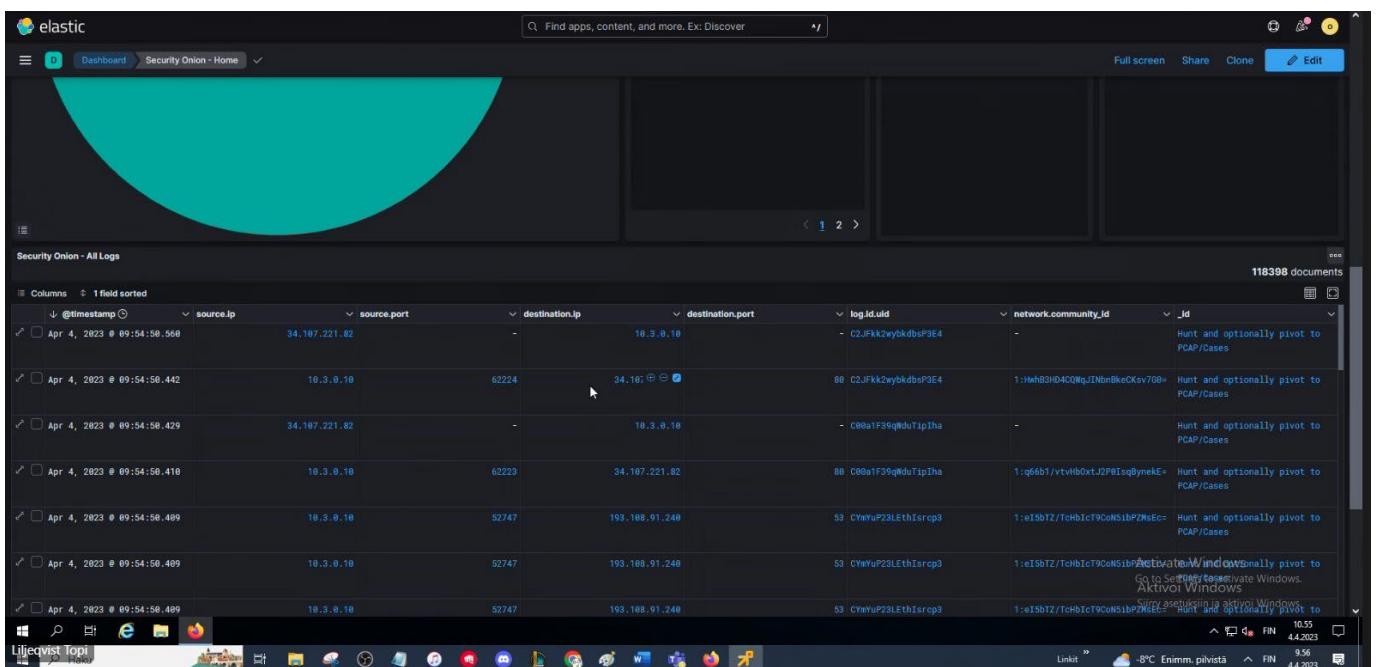
Kuva 6 Security Onion - Zeek etusivu

Kuva 7 Zeek - Discover ([www.latimes.com](http://www.latimes.com))

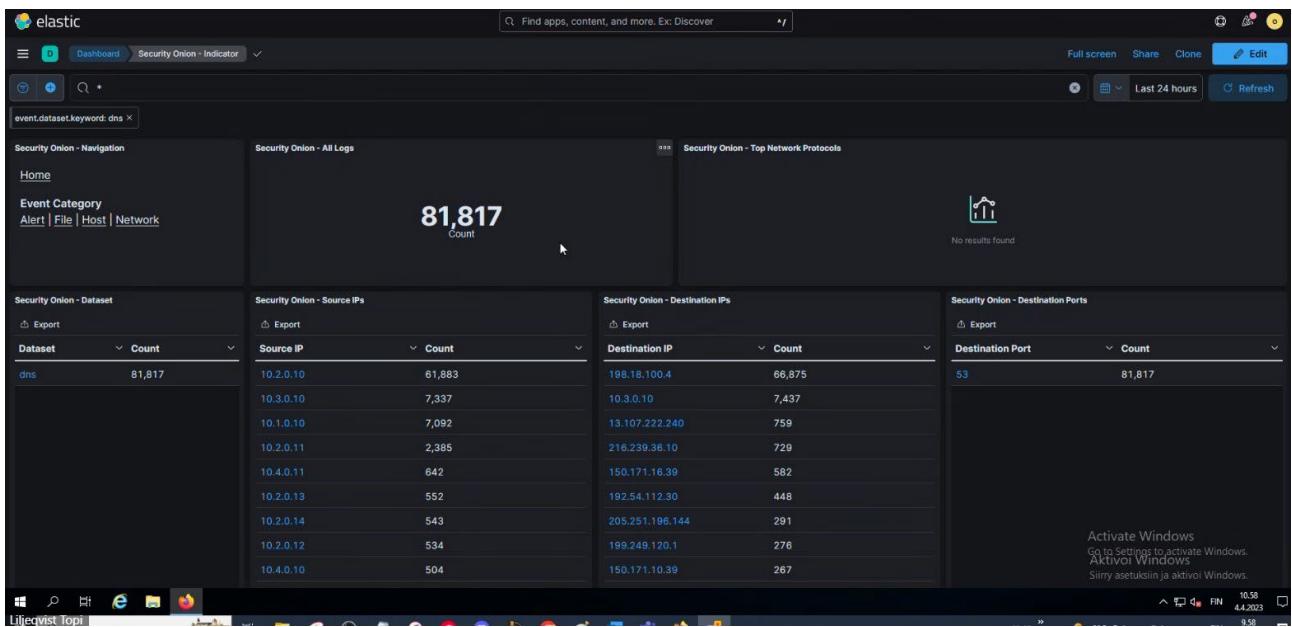
Kuva 8 Zeek - Maps



Kuva 9 Home page



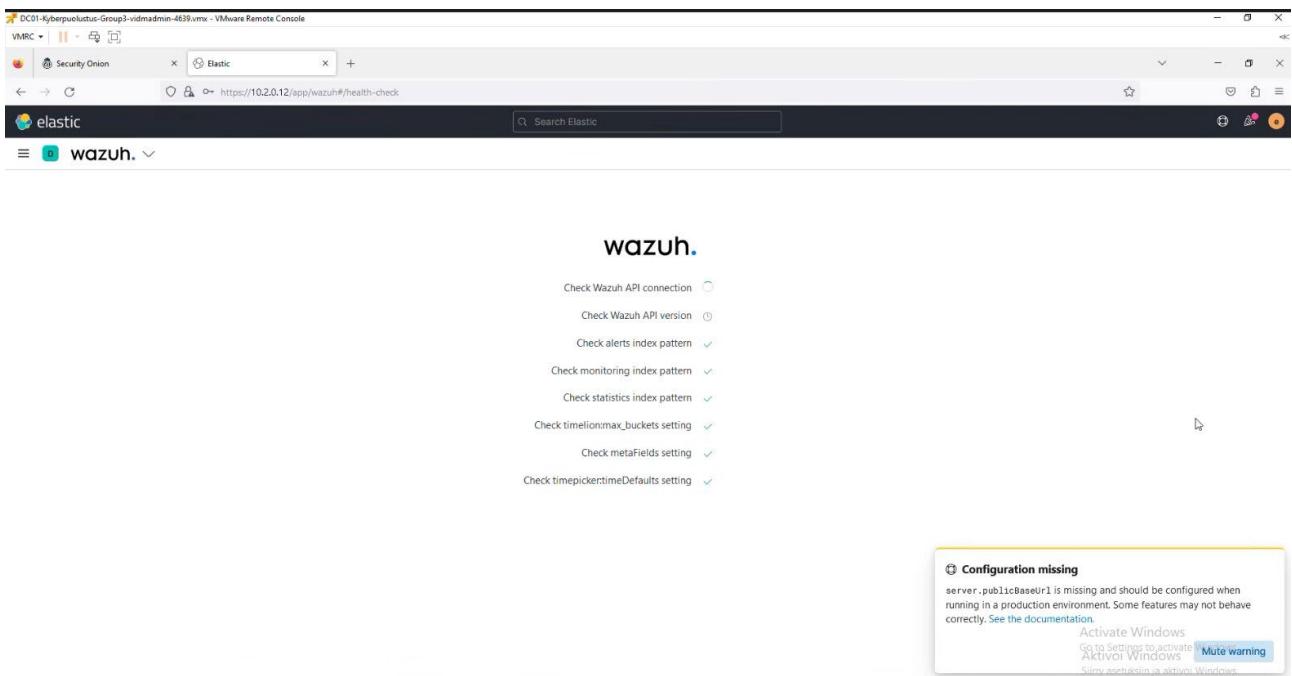
Kuva 10 All logs



Kuva 11 Indicator

### 3.3 Wazuh

Kirjauduttiin seuraavaksi Wazuhiin osoitteessa 10.2.0.12 ja siellä oli valmiiksi asetetut agentit, jotka sitten poistimme ohjeiden mukaan ja loimme ne uudestaan. Esitetty kuvissa 12,13,14,15 & 16.



Kuva 12 Wazuh: 10.2.0.12

The screenshot shows the Wazuh dashboard with several sections:

- Top Metrics:** Total agents (6), Active agents (0), Disconnected agents (6), Pending agents (0), Never connected agents (0).
- SECURITY INFORMATION MANAGEMENT:**
  - Security events:** Browse through your security alerts, identifying issues and threats in your environment.
  - Integrity monitoring:** Alerts related to file changes, including permissions, content, ownership and attributes.
- AUDITING AND POLICY MONITORING:**
  - Policy monitoring:** Verify that your systems are configured according to your security policies baseline.
  - System auditing:** Audit users behavior, monitoring command execution and alerting on access to critical files.
- THREAT DETECTION AND RESPONSE:**
  - Vulnerabilities:** Discover what applications in your environment are affected by well-known vulnerabilities.
  - MITRE ATT&CK:** Security events from the knowledge base of adversary tactics and techniques based on real-world observations.
- REGULATORY COMPLIANCE:**
  - PCI DSS:** Global security standard for entities that process, store or transmit payment cardholder data.
  - TSC:** Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.
  - NIST 800-53:** National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.
  - GDPR:** General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.
  - Activate Windows:** Go to Settings to activate Windows.

Kuva 13 Wazuh etusivu

The screenshot shows the Wazuh Agents page with the following sections:

- STATUS:** Shows 0 Active, 6 Disconnected, 0 Pending, 0 Never connected, and 0.00% Agents coverage.
- DETAILS:** Last registered agent: DC01, Most active agent: -.
- EVOLUTION:** No results found in the selected time range (Last 24 hours).
- Agents (6):** A table listing agents with columns: ID, Name, IP, Group(s), OS, Cluster node, Version, Registration date, Last keep alive, Status, and Actions.

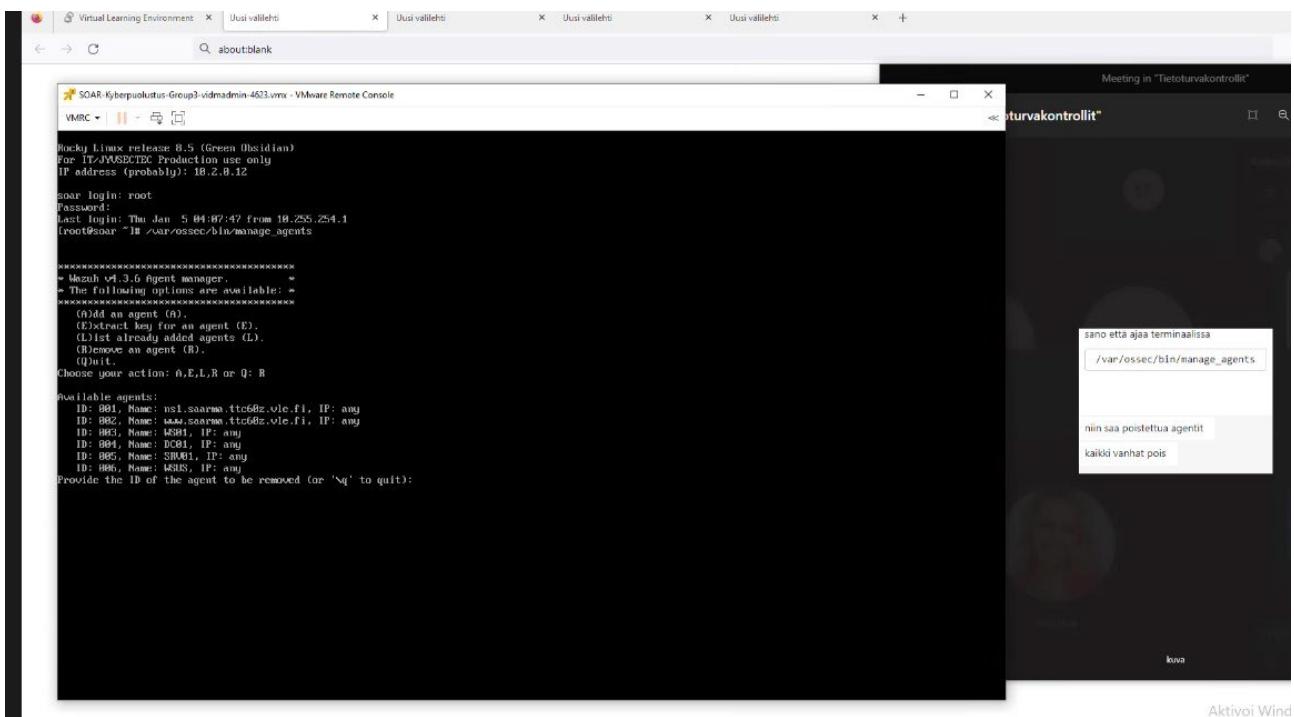
ID	Name	IP	Group(s)	OS	Cluster node	Version	Registration date	Last keep alive	Status	Actions
001	ns1.saarma.ttc60z.vle.fi	10.4.0.10	default	Rocky Linux 8.6	node01	v4.3.6	Jan 5, 2023 @ 04:0...	Jan 5, 2023 @ 05:0...	• disconnected	
002	www.saarma.ttc60z.vle.fi	10.4.0.11	default	Rocky Linux 8.5	node01	v4.3.6	Jan 5, 2023 @ 04:0...	Jan 5, 2023 @ 05:0...	• disconnected	
003	WS01	10.1.0.10	default	Microsoft Windows 11 Edu...	node01	v4.3.6	Jan 5, 2023 @ 04:0...	Jan 5, 2023 @ 05:0...	• disconnected	
004	DC01	10.3.0.10	default	Microsoft Windows Server ...	node01	v4.3.6	Jan 5, 2023 @ 04:0...	Jan 5, 2023 @ 05:0...	• disconnected	
005	SRV01	10.3.0.12	default	Microsoft Windows Server ...	node01	v4.3.6	Jan 5, 2023 @ 04:0...	Jan 5, 2023 @ 05:0...	• disconnected	
006	WSUS	10.3.0.11	default	Microsoft Windows Server ...	node01	v4.3.6	Jan 5, 2023 @ 04:0...	Jan 5, 2023 @ 05:0...	• disconnected	

Activate Windows  
Go to Settings to activate Windows.  
Aktivoi Windows

Kuva 14 Wazuh jo valmiit agentit jotka poistettiin ja luotiin uudestaan

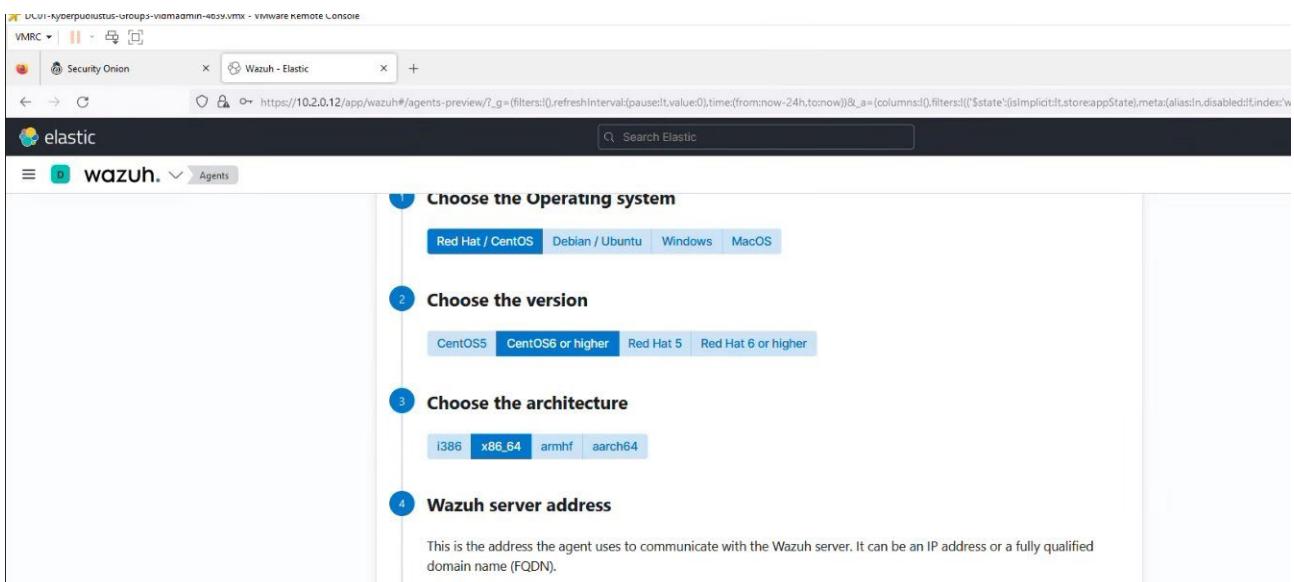
```
/var/ossec/bin/manage_agents
niin saa poistettua agentit
kaikki vanhat pois
```

Kuva 15 Ohjeistus agenttien poistoon

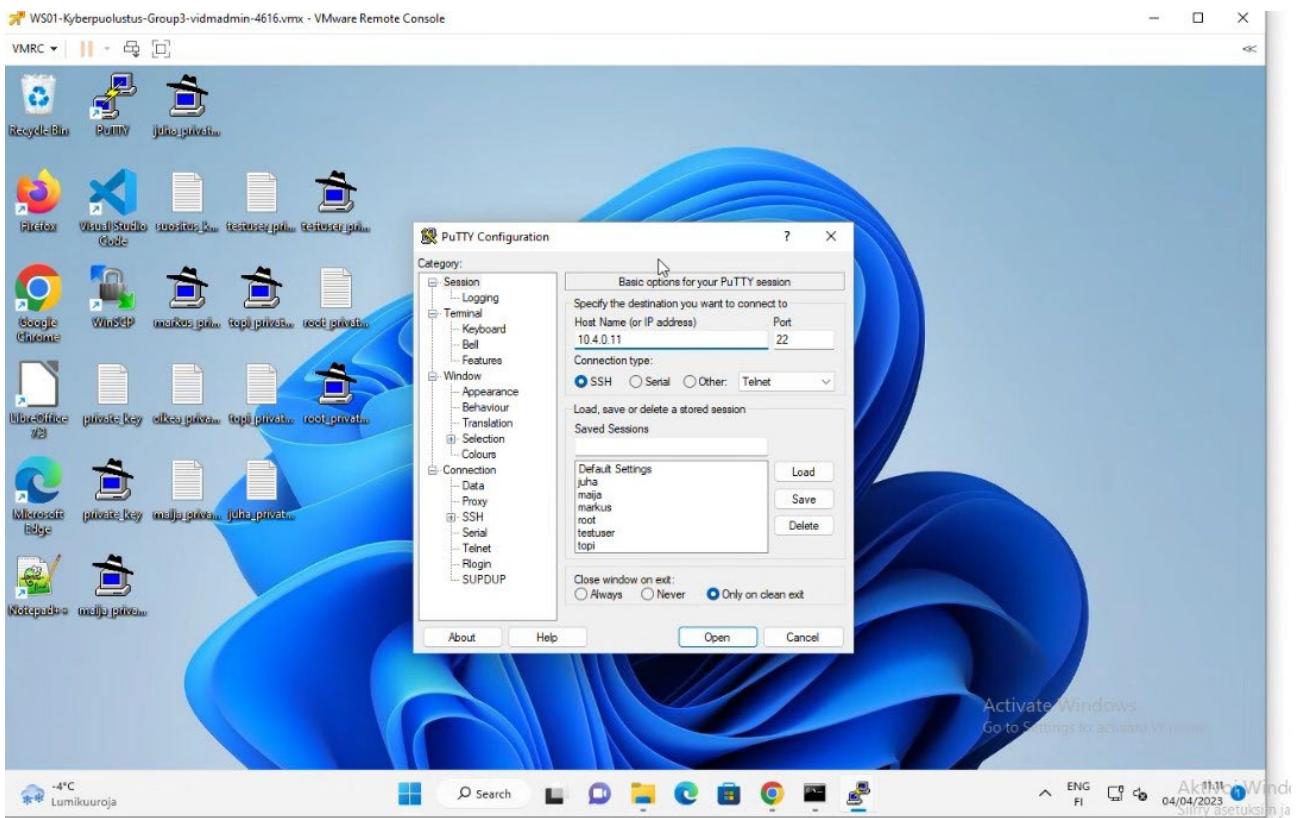


## Kuva 16 Agenttien poistoa

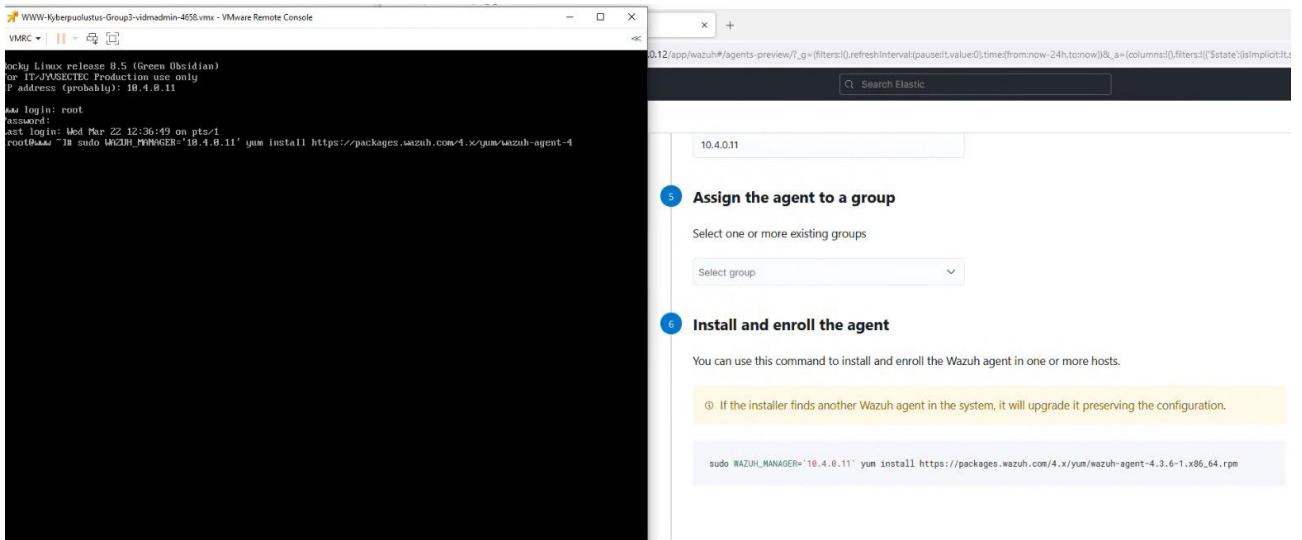
Aloitettiin agenttien lisääminen WS01:een, DC01:een, WSUS:iin, SRV01:een, NS1:een, WWW:hen aivan kuten teimme aikaisemmin toisessa harjoituksessa ElasticSIEM:n kanssa. Aluksi teimme väärällä IP osoitteella, mutta huomasimme virheen melko nopeasti ja aloitimme alusta. Esitetty kuviissa alla agentin luonti.



## Kuva 17 Wazuh agenttien luomista – Operating system



Kuva 18 Kirjatuminen koneille SSH yhteyden kautta



Kuva 19 WWW agentin luomista

```

Rocky Linux release 8.5 (Green Obsidian)
For IT/JYUSECTEC Production use only
IP address (probably): 10.4.0.11

www login: root
Password:
Last login: Wed Mar 22 12:36:49 on pts/1
[root@www ~]# sudo WAZUH_MANAGER='10.4.0.11' yum install https://packages.wazuh.com/4.x/yum/wazuh-agent-4.3.6-1.x86_64.rpm
Last metadata expiration check: 1:42:51 ago on Tue 04 Apr 2023 08:33:38 AM EEST.
wazuh-agent-4.3.6-1.x86_64.rpm
Dependencies resolved.

=====
| Package           | Architecture | Version | Repository |
| ======            | ======       | ======  | ======      |
| Installing:      |              |          |             |
|   wazuh-agent    |          x86_64 | 4.3.6-1 | @commun... |
| Transaction Summary |
| ======            |              |          |             |
| Install  1 Package |
| Total size: 8.5 M
| Installed size: 24 M
| Is this ok [y/N]: y
| Downloading Packages:
| Running transaction check
| Transaction check succeeded.
| Running transaction test
| Transaction test succeeded.
| Running transaction
|   Preparing      :
|     Running scriptlet: wazuh-agent-4.3.6-1.x86_64
|   Installing      :
|     : wazuh-agent-4.3.6-1.x86_64
|     Running scriptlet: wazuh-agent-4.3.6-1.x86_64
|     Verifying      :
|       : wazuh-agent-4.3.6-1.x86_64

| Installed:
|   wazuh-agent-4.3.6-1.x86_64

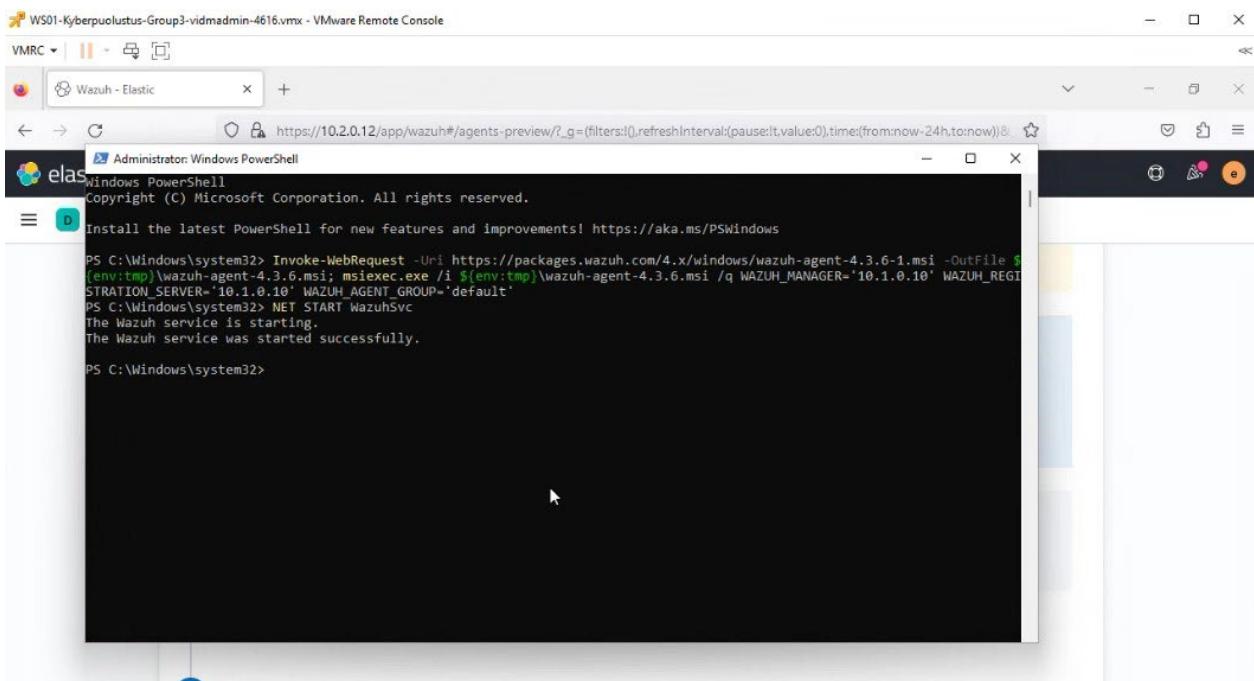
| Complete!
[root@www ~]#

```

Kuva 20 Onnistunut agentin luonti mutta väärä IP= 10.4.0.11

Systemd	SysV Init
<pre> Installing : wazuh-agent-4.3.6-1.x86_64 Running scriptlet: wazuh-agent-4.3.6-1.x86_64 Verifying   : wazuh-agent-4.3.6-1.x86_64  Installed:   wazuh-agent-4.3.6-1.x86_64  Complete! [root@www ~]# sudo systemctl daemon-reload [root@www ~]# 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@www ~]# sudo systemctl start wazuh-agent [root@www ~]# </pre>	<pre> sudo systemctl daemon-reload sudo systemctl enable wazuh-agent sudo systemctl start wazuh-agent  To verify the connection with the Wazuh server, please follow </pre>

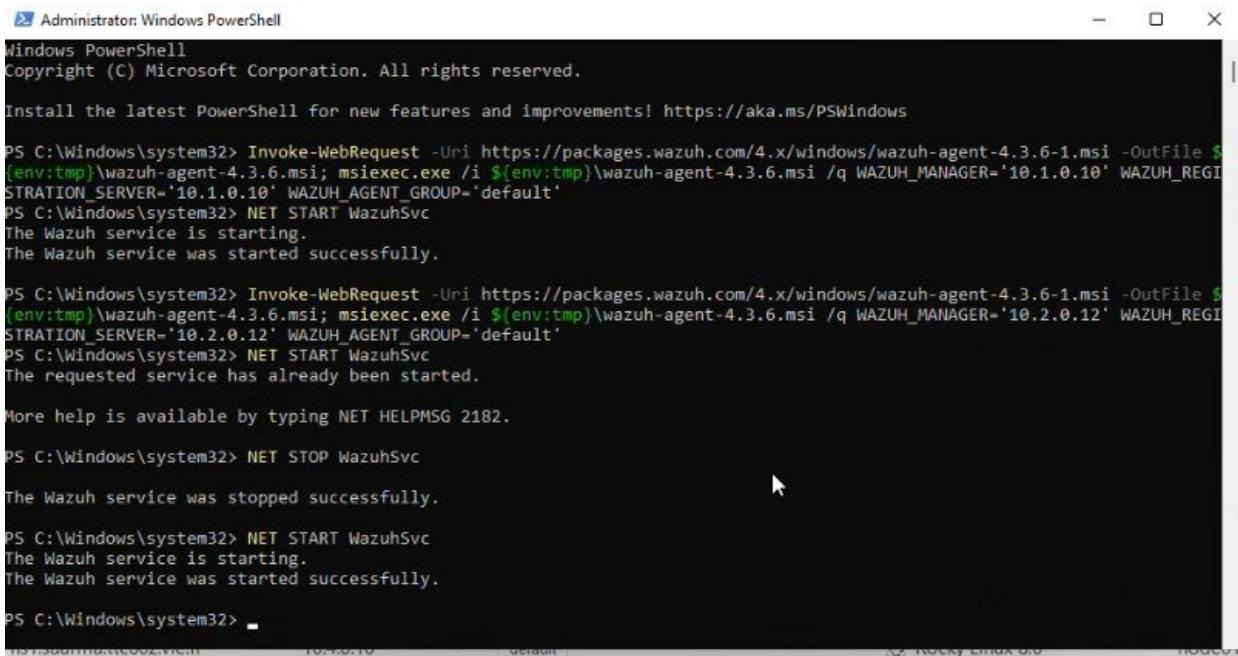
Kuva 21 start wazuh-agent komentoa



Kuva 22 WS01 , vielä väärä IP

ID	Name	IP	Group(s)	OS	Cluster node	Version	Registration date
007	WS01	10.1.0.10	default	Microsoft Windows 11 Education 10.0...	node01	v4.3.6	Apr 4, 2023 @ 11:22:22

Kuva 23 Wazuh väärä IP (WS01)



```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> 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; msiexec.exe /i $env:tmp\wazuh-agent-4.3.6.msi /q WAZUH_MANAGER='10.1.0.10' WAZUH_REGISTRATION_SERVER='10.1.0.10' 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> 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; msiexec.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 requested service has already been started.

More help is available by typing NET HELPMSG 2182.

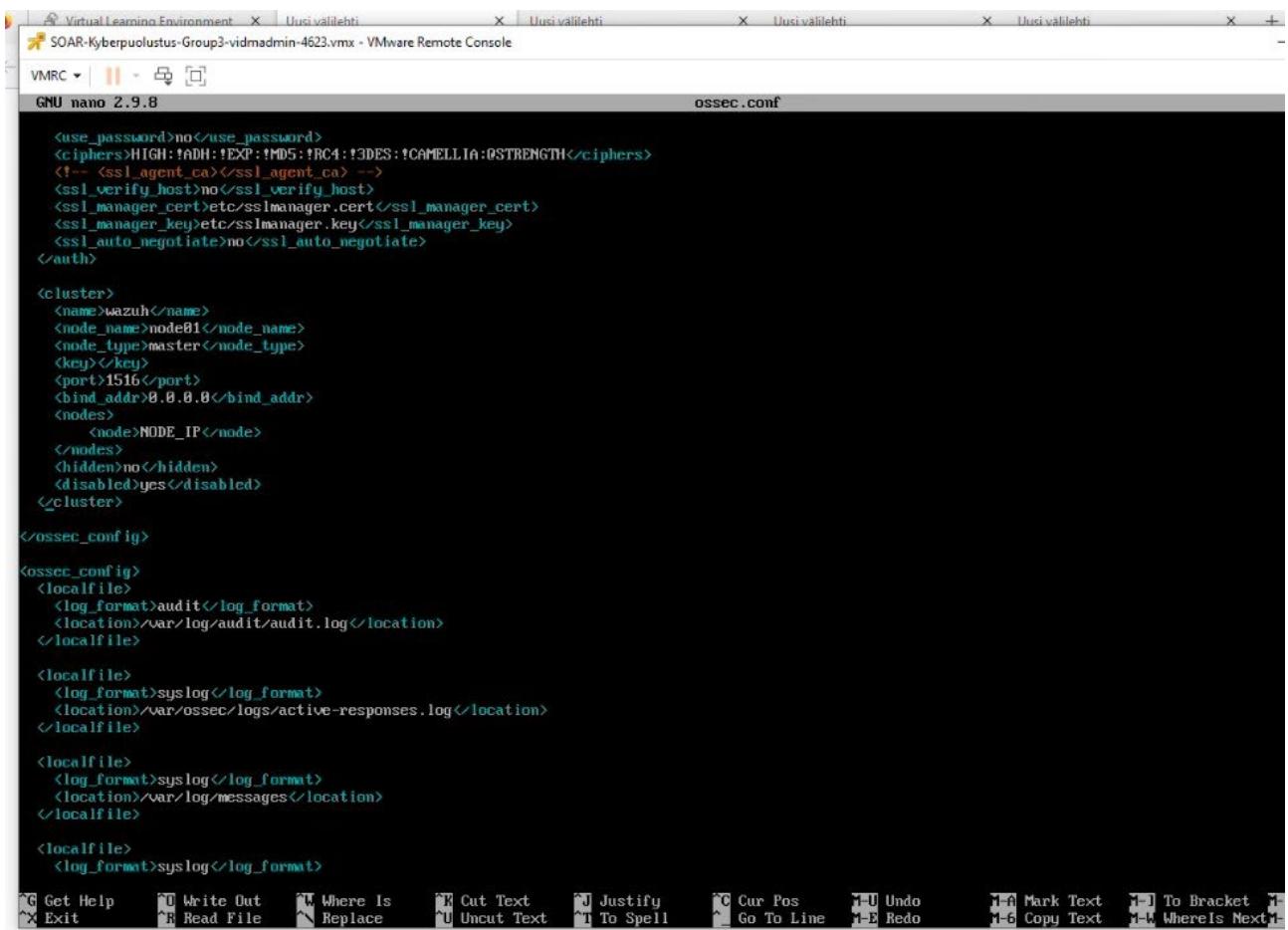
PS C:\Windows\system32> NET STOP WazuhSvc
The Wazuh service was stopped successfully.

PS C:\Windows\system32> NET START WazuhSvc
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\Windows\system32>

```

Kuva 24 WS01 korjaus, oikea IP 10.2.0.12



```

Virtual Learning Environment | Ulusi välilehti | + |
SOAR-Kyberpuolustus-Group3-vidmadmin-4623.vmx - VMware Remote Console
VMRC | || - □
GNU nano 2.9.8 ossec.conf

<use_password>no</use_password>
<ciphers>HIGH:!ADH:!EXP:!MD5:!RC4:!3DES:!CAMELLIA:@STRENGTH</ciphers>
<!-- <ssl_agent_ca><ssl_agent_ca> -->
<ssl_verify_host>no</ssl_verify_host>
<ssl_manager_cert>etc/sslmanager.cert</ssl_manager_cert>
<ssl_manager_key>etc/sslmanager.key</ssl_manager_key>
<ssl_auto_negotiate>no</ssl_auto_negotiate>
</auth>

<cluster>
  <name>wazuh</name>
  <node_name>node81</node_name>
  <node_type>master</node_type>
  <key></key>
  <port>1516</port>
  <bind_addr>0.0.0.0</bind_addr>
  <nodes>
    <node>NODE_IP</node>
  </nodes>
  <hidden>no</hidden>
  <disabled>yes</disabled>
</cluster>

</ossec_config>

<ossec_config>
  <localfile>
    <log_format>audit</log_format>
    <location>/var/log/audit/audit.log</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/ossec/logs/active-responses.log</location>
  </localfile>

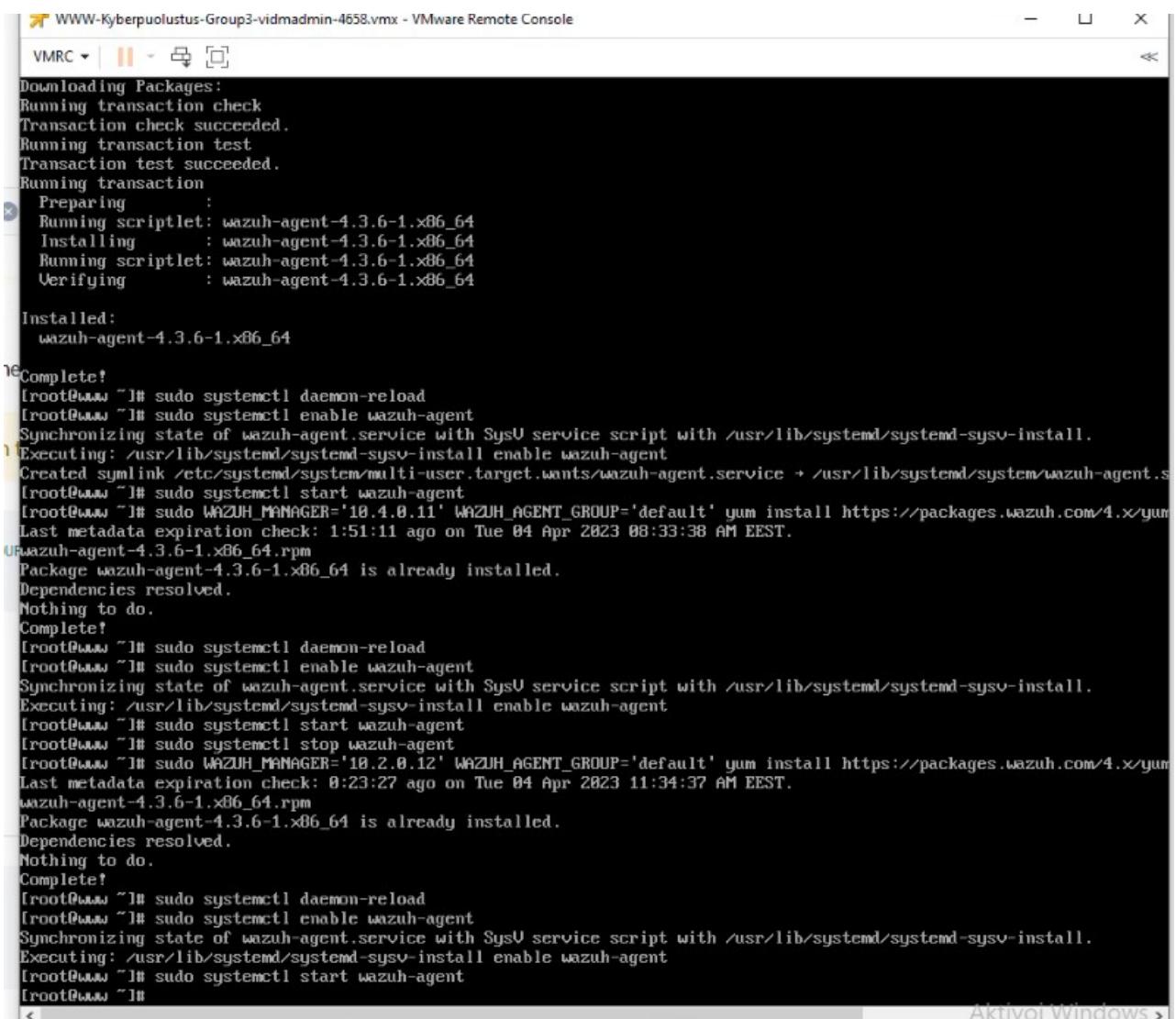
  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/messages</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
  </localfile>
</ossec_config>

G Get Help   W Write Out   F Where Is   K Cut Text   J Justify   C Cur Pos   M-U Undo   M-A Mark Text   M-J To Bracket   M-W Whereis Next
X Exit   R Read File   R Replace   U Uncut Text   T To Spell   G Go To Line   M-E Redo   M-B Copy Text   M-N Whereis Prev

```

Kuva 25 Tarkistusta



WWW-Kyberpuolustus-Group3-vidmadmin-4658.vmx - VMware Remote Console

```

VMRC ▾ | ||| ▾ □ ▾
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing : 
Running scriptlet: wazuh-agent-4.3.6-1.x86_64
Installing   : wazuh-agent-4.3.6-1.x86_64
Running scriptlet: wazuh-agent-4.3.6-1.x86_64
Verifying    : wazuh-agent-4.3.6-1.x86_64

Installed:
wazuh-agent-4.3.6-1.x86_64

Complete!
[root@www ~]# sudo systemctl daemon-reload
[root@www ~]# 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@www ~]# sudo systemctl start wazuh-agent
[root@www ~]# sudo WAZUH_MANAGER='10.4.0.11' WAZUH_AGENT_GROUP='default' yum install https://packages.wazuh.com/4.x/yum
Last metadata expiration check: 1:51:11 ago on Tue 04 Apr 2023 08:33:38 AM EEST.
wazuh-agent-4.3.6-1.x86_64.rpm
Package wazuh-agent-4.3.6-1.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@www ~]# sudo systemctl daemon-reload
[root@www ~]# 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
[root@www ~]# sudo systemctl start wazuh-agent
[root@www ~]# sudo WAZUH_MANAGER='10.2.0.12' WAZUH_AGENT_GROUP='default' yum install https://packages.wazuh.com/4.x/yum
Last metadata expiration check: 0:23:27 ago on Tue 04 Apr 2023 11:34:37 AM EEST.
wazuh-agent-4.3.6-1.x86_64.rpm
Package wazuh-agent-4.3.6-1.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@www ~]# sudo systemctl daemon-reload
[root@www ~]# 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
[root@www ~]# sudo systemctl start wazuh-agent
[root@www ~]#

```

Aktivointi Windows >

Kuva 26 Uudestaan Wazuh agentin starttaamista, oikealla IP:llä.

Kun saimme oikealla IP:llä tehtyä ja startattua agentin oikein, siirryimme eteenpäin luomisessa.

Seuraavana NS01, DC01, SRV01 ja lopuksi esitetti kaikki luodut agentit onnistuneesti Wazuhissa.

Esitetty kuvissa 27, 28, 29 & 30.

```

root@ns1:~#
Install 1 Package
=====
Install 1 Package

Total size: 8.5 M
Installed size: 24 M
Is this ok [y/N]: y
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing : 1/1
Running scriptlet: wazuh-agent-4.3.6-1.x86_64 1/1
Installing : wazuh-agent-4.3.6-1.x86_64 1/1
Running scriptlet: wazuh-agent-4.3.6-1.x86_64 1/1
Running scriptlet: wazuh-agent-4.3.6-1.x86_64 1/1
Verifying : wazuh-agent-4.3.6-1.x86_64 1/1

Installed:
wazuh-agent-4.3.6-1.x86_64

Complete!
[root@ns1 ~]# sudo systemctl daemon-reload
[root@ns1 ~]# sudo systemctl enable wazuh-agent

```

Kuva 27 Agentin luontin, NS01

```

Administrator: Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> 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; 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:\Users\Administrator> sudo systemctl daemon-reload
sudo : The term 'sudo' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ sudo systemctl daemon-reload
+ ~~~
    + CategoryInfo          : ObjectNotFound: (sudo:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

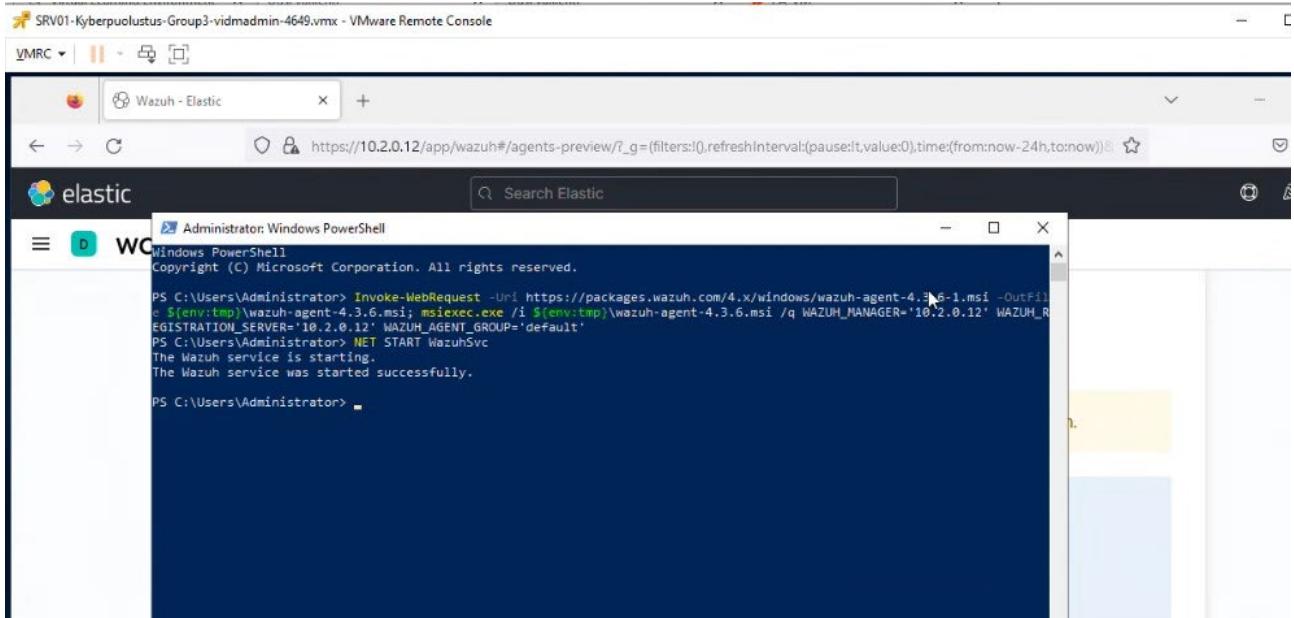
PS C:\Users\Administrator> sudo systemctl enable wazuh-agent
sudo : The term 'sudo' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ sudo systemctl enable wazuh-agent
+ ~~~
    + CategoryInfo          : ObjectNotFound: (sudo:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\Administrator> NET START WazuhSvc
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\Users\Administrator>

```

Kuva 28 NET start WazuhSvc - Powershell



Kuva 29 SRV01 Wazuh start

Agents (6)

ID	Name	IP	Group(s)	OS	Cluster node	Ver...	Registration ...	Last keep alive	Status	Action
007	WS01	10.1.0.10	default	Microsoft Win...	node01	v4....	Apr 4, 202...	Apr 4, 202...	● active	
008	DC01	10.3.0.10	default	Microsoft Win...	node01	v4....	Apr 4, 202...	Apr 4, 202...	● active	
009	www.group3.ttc60...	10.4.0.11	default	Rocky Linux 8.5	node01	v4....	Apr 4, 202...	Apr 4, 202...	● active	
010	ns1.group3.ttc60z...	10.4.0.10	default	Rocky Linux 8.6	node01	v4....	Apr 4, 202...	Apr 4, 202...	● active	
011	WSUS	10.3.0.11	default	Microsoft Win...	node01	v4....	Apr 4, 202...	Apr 4, 202...	● active	
012	SRV01	10.3.0.12	default	Microsoft Win...	node01	v4....	Apr 4, 202...	Apr 4, 202...	● active	

Kuva 30 Onnistuneesti luodut agentit Wazuh (status: active)

### 3.4 Testausta

Seuraavaksi ajoimme Kalilla test\_script.sh skriptin, jonka avulla pystyimme seuraamaan Security Onioniin nousseita hälytyksiä. Filtreröimme myös hälytyksiä ilman WS01 (agent 007) sekä tutkimme yksittäisten koneiden ja servereiden hälytyksiä. Esitetty testausta kuvissa 31-58 alla.

```
#!/bin/bash

# Host and port scanning
timestamp=$(date +%d-%m-%Y\ %H:%M:%S)
echo "Starting Nmap ICMP scan at $timestamp" >> log.txt
echo "root66" | sudo -S nmap -sn 10.3.0.10 10.3.0.12 10.4.0.11 10.3.0.11
# sleep 120

timestamp=$(date +%d-%m-%Y\ %H:%M:%S)
echo "Starting Nmap port and service scan at $timestamp" >> log.txt
echo "root66" | sudo -S nmap -sV -o 10.3.0.10 10.3.0.12 10.4.0.11 10.3.0.11
# sleep 300

# Web scanning
timestamp=$(date +%d-%m-%Y\ %H:%M:%S)
echo "Starting Nikto scan at $timestamp" >> log.txt
nikto -h https://10.4.0.11
# sleep 30

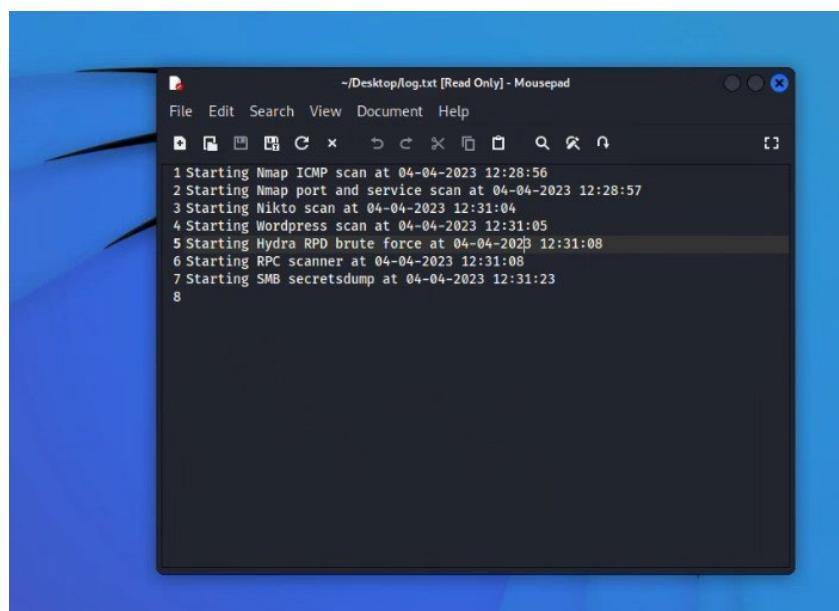
timestamp=$(date +%d-%m-%Y\ %H:%M:%S)
echo "Starting Wordpress scan at $timestamp" >> log.txt
wpscan --url https://10.4.0.11
# sleep 600

# Service scanning
timestamp=$(date +%d-%m-%Y\ %H:%M:%S)
echo "Starting Hydra RPD brute force at $timestamp" >> log.txt
hydra -L misc/users.txt -P misc/pass.txt rdp://10.3.0.11
# sleep 800

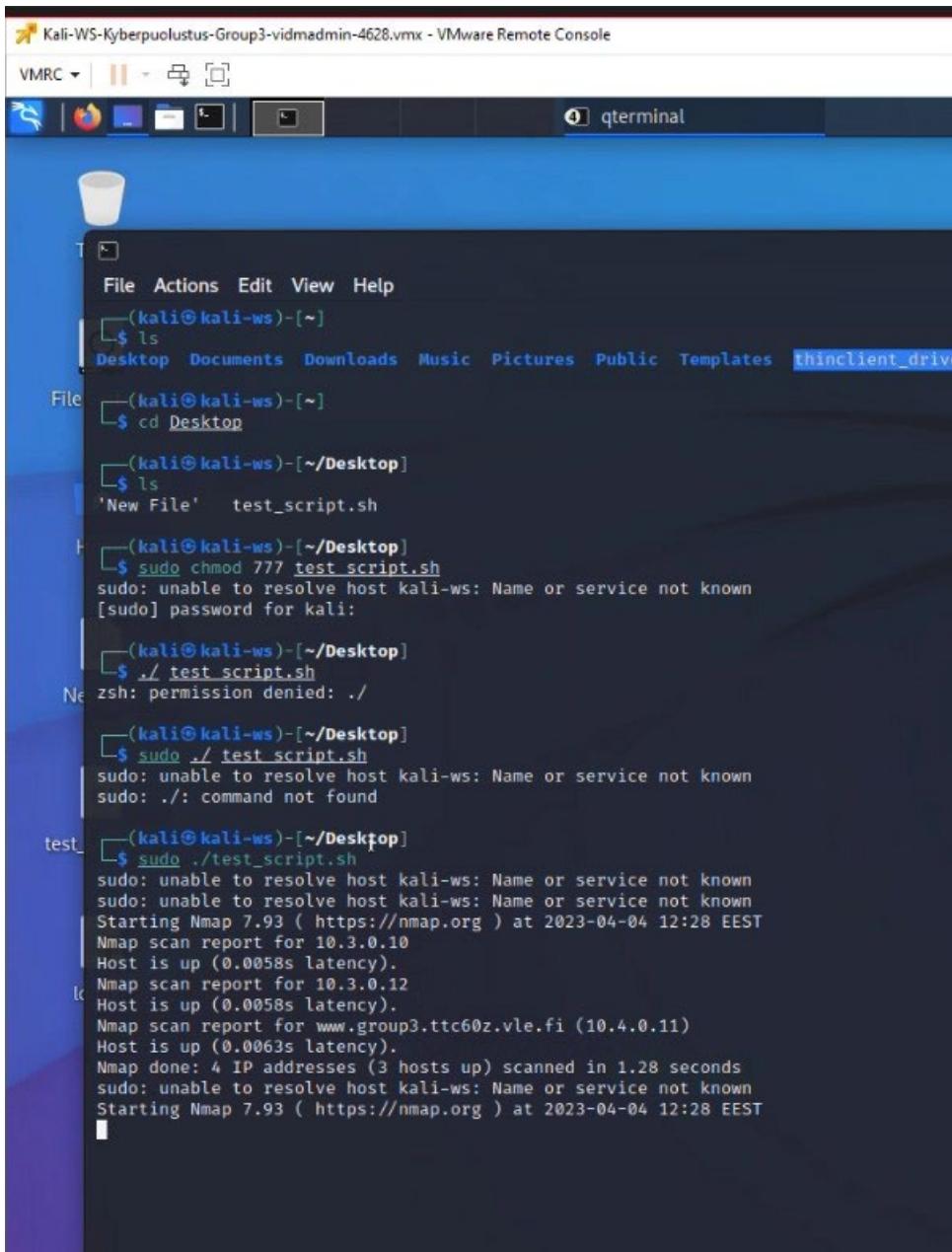
timestamp=$(date +%d-%m-%Y\ %H:%M:%S)
echo "Starting RPC scanner at $timestamp" >> log.txt
msfconsole -x "use auxiliary/scanner/dcerpc/endpoint_mapper; set RHOSTS 10.3.0.12; run; exit;"
# sleep 100

timestamp=$(date +%d-%m-%Y\ %H:%M:%S)
echo "Starting SMB secretsdump at $timestamp" >> log.txt
msfconsole -x "use auxiliary/scanner/smb/impacket/secretsdump; set SMBPass Root-66; set SMBUser Administrator; set RHOSTS 10.3.0.11; run; exit;"
```

Kuva 31 Kali - test\_script.sh



Kuva 32 Kali skriptin sisältö(skannaukset)



Kali-WS-Kyberpuolustus-Group3-vidmadmin-4628.vmx - VMware Remote Console

VMRC | qterminal

```
File Actions Edit View Help
(kali㉿kali-ws)~
$ ls
Desktop Documents Downloads Music Pictures Public Templates thinclient_drive
File (kali㉿kali-ws)~
$ cd Desktop

(kali㉿kali-ws)~/Desktop
$ ls
'New File' test_script.sh

(kali㉿kali-ws)~/Desktop
$ sudo chmod 777 test_script.sh
sudo: unable to resolve host kali-ws: Name or service not known
[sudo] password for kali:

(kali㉿kali-ws)~/Desktop
$ ./test_script.sh
zsh: permission denied: ./

(kali㉿kali-ws)~/Desktop
$ sudo ./test_script.sh
sudo: unable to resolve host kali-ws: Name or service not known
sudo: ./: command not found

(kali㉿kali-ws)~/Desktop
$ sudo ./test_script.sh
sudo: unable to resolve host kali-ws: Name or service not known
sudo: unable to resolve host kali-ws: Name or service not known
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-04 12:28 EEST
Nmap scan report for 10.3.0.10
Host is up (0.0058s latency).
Nmap scan report for 10.3.0.12
Host is up (0.0058s latency).
Nmap scan report for www.group3.ttc60z.vle.fi (10.4.0.11)
Host is up (0.0063s latency).
Nmap done: 4 IP addresses (3 hosts up) scanned in 1.28 seconds
sudo: unable to resolve host kali-ws: Name or service not known
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-04 12:28 EEST
```

Kuva 33 Kali Nmap skan report

W501-Kyberpuolustus-Group3-vidadmin-4616.vmx - VMware Remote Console

VMRC | Wazuh - Elastic | Wazuh - Elastic | Security Onion - Alerts - Group | +

https://10.2.0.10/#/alerts?q=\* | groupby rule.name.event.module.event.severity.label&t=2023%2F04%2F03 01%3A32%3A10 PM - 2023%2F04%2F04 01%3A32%3A15 PM&z=Europe%2FHelsinki&el=500&gl=500

Last 24 hours REFRESH

Group By Name, Module

Count rule.name event.module event.severity\_label

141	ET SCAN Potential SSH Scan OUTBOUND	suricata	medium
72	ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent	suricata	low
15	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium
15	ET INFO DYNAMIC_DNS Query to a * cloudns.net Domain	suricata	medium
14	System Audit event.	ossec	low
10	ET SCAN Suspicious inbound to MySQL port 3306	suricata	medium
10	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium
10	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium
9	ET DOS Microsoft Remote Desktop (RDP) Sync then Reset 30 Second DoS Attempt	suricata	medium
5	ET SCAN Potential SSH Scan	suricata	medium
3	ET SCAN Potential VNC Scan 5900-5920	suricata	medium
3	ET SCAN Potential VNC Scan 5800-5820	suricata	medium
3	ET SCAN Behavioral Unusual Port 445 traffic Potential Scan or Infection	suricata	low
1	Host-based anomaly detection event (notcheck).	ossec	low
1	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	suricata	low
1	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	suricata	Activate Windows Go to Settings to activate Windows. Aktivoi Windows Siirry asetuksiin ja aktivoi Windows.

Version: 2.3.140 © 2023 Security Onion Solutions, LLC

ENGLISH FINNISH

Kuva 34 Security Onion Kalilla ajetun skriptin jälkeen

W501-Kyberpuolustus-Group3-vidadmin-4616.vmx - VMware Remote Console

VMRC | Wazuh - Elastic | Wazuh - Elastic | Security Onion - Alerts - Group | +

https://10.2.0.10/#/alerts?q=\* | groupby rule.name.event.module.event.severity.label&t=2023%2F04%2F03 01%3A34%3A15 PM - 2023%2F04%2F04 01%3A34%3A15 PM&z=Europe%2FHelsinki&el=500&gl=500

Last 24 hours REFRESH

Total Found: 334

Group By Name, Module

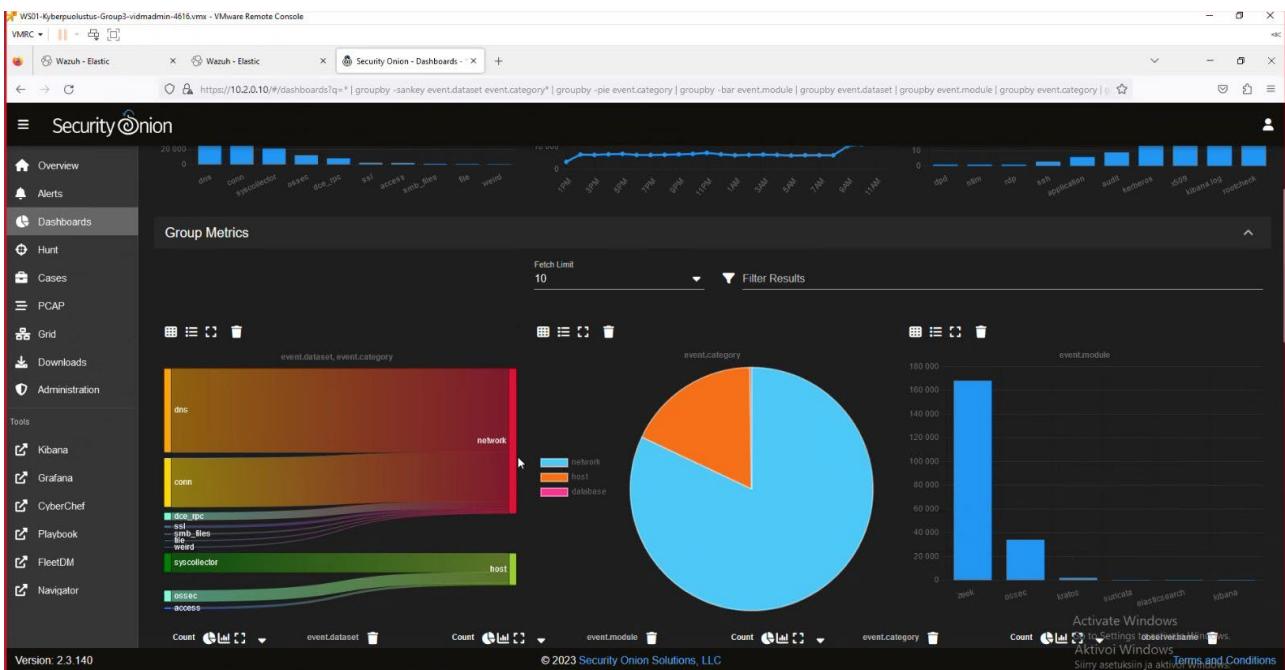
Count rule.name event.module event.severity\_label

120	ET SCAN NMP OS Detection Probe	suricata	medium
72	ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent	suricata	low
15	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium
15	ET INFO DYNAMIC_DNS Query to a * cloudns.net Domain	suricata	medium
14	System Audit event.	ossec	low
10	ET SCAN Suspicious inbound to MySQL port 3306	suricata	medium
10	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium
10	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium
9	ET DOS Microsoft Remote Desktop (RDP) Sync then Reset 30 Second DoS Attempt	suricata	medium
8	ET POLICY RDP connection confirm	suricata	low
5	ET SCAN Potential VNC Scan 5900-5920	suricata	medium
5	ET SCAN Potential SSH Scan	suricata	medium
5	ET SCAN MS Terminal Server Traffic on Non-standard Port	suricata	Activate Windows Go to Settings to activate Windows. Aktivoi Windows Siirry asetuksiin ja aktivoi Windows.

Version: 2.3.140 © 2023 Security Onion Solutions, LLC

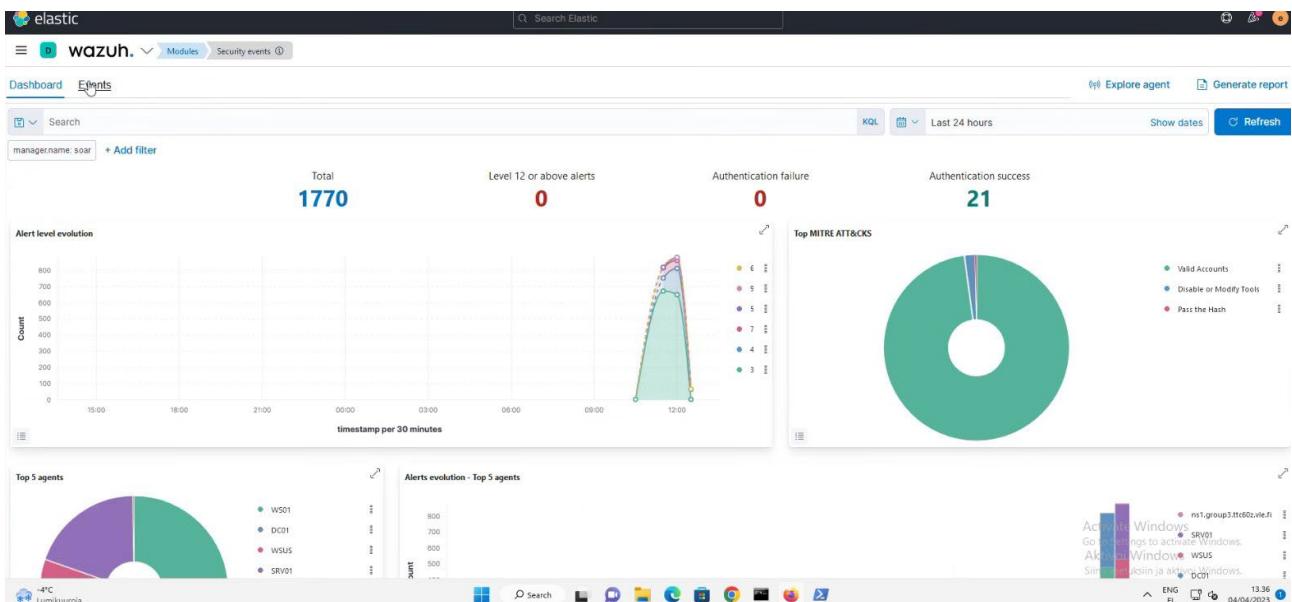
ENGLISH FINNISH

Kuva 35 Security Onion - Alerts

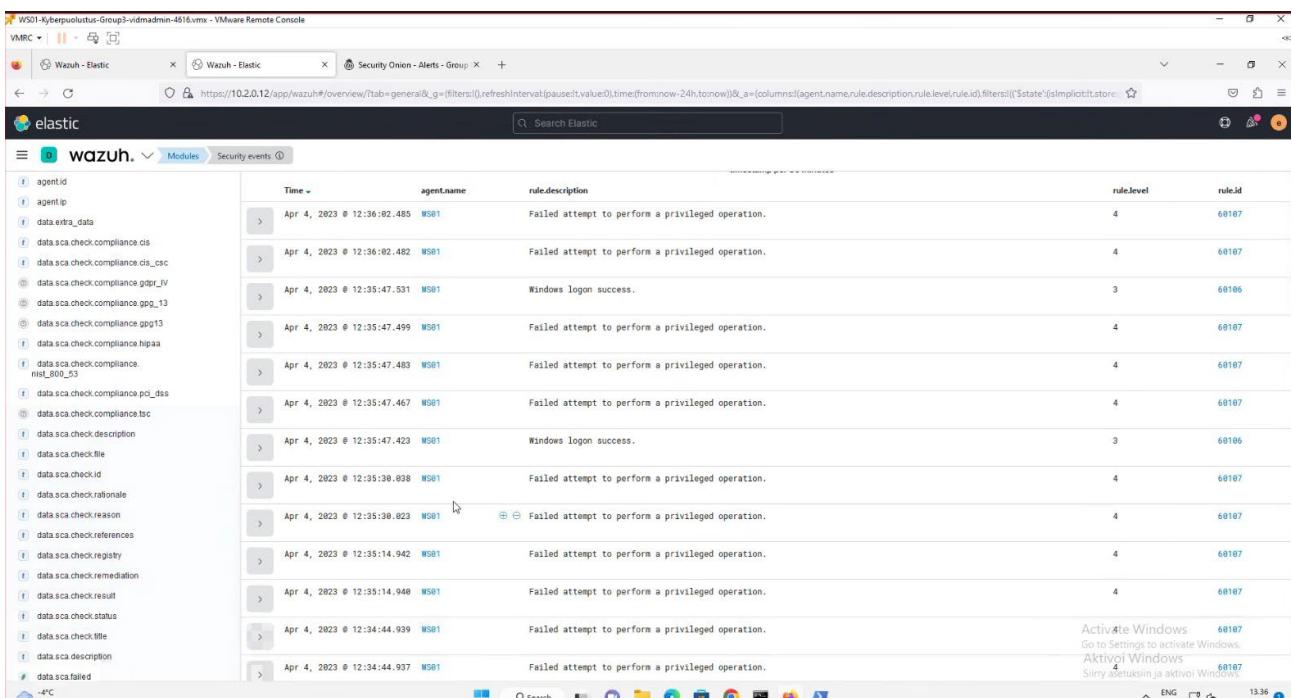


Kuva 36 Security Onion - Dashboard

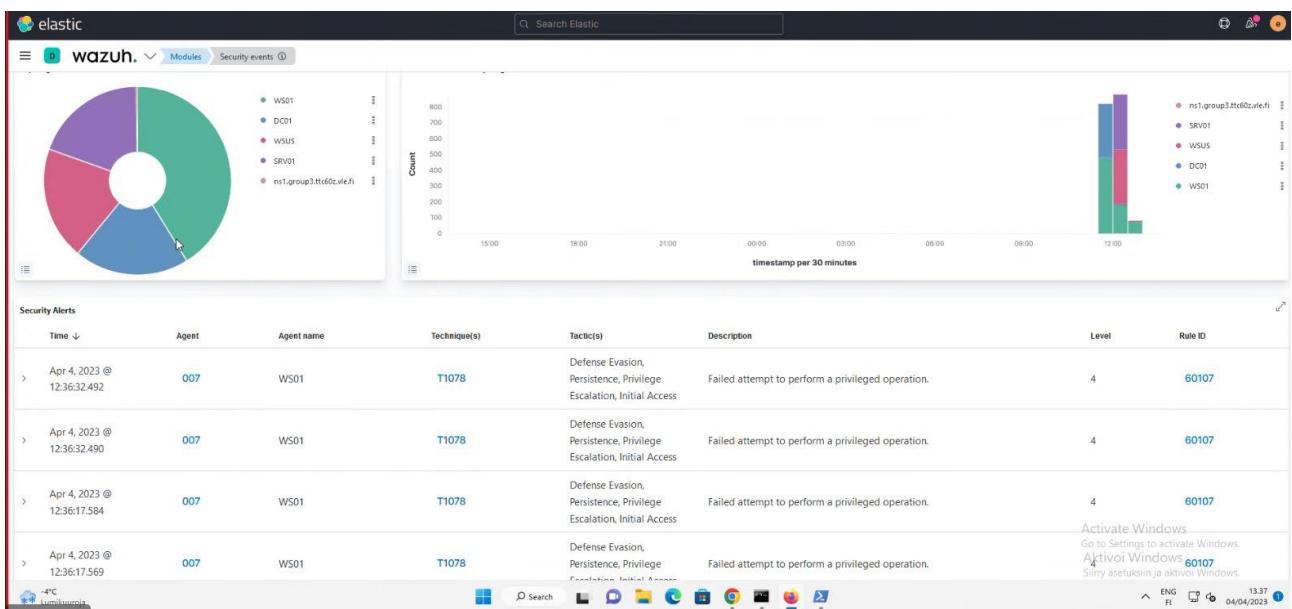
### Kuva 37 Kali ajetun skriptin tarkastelua



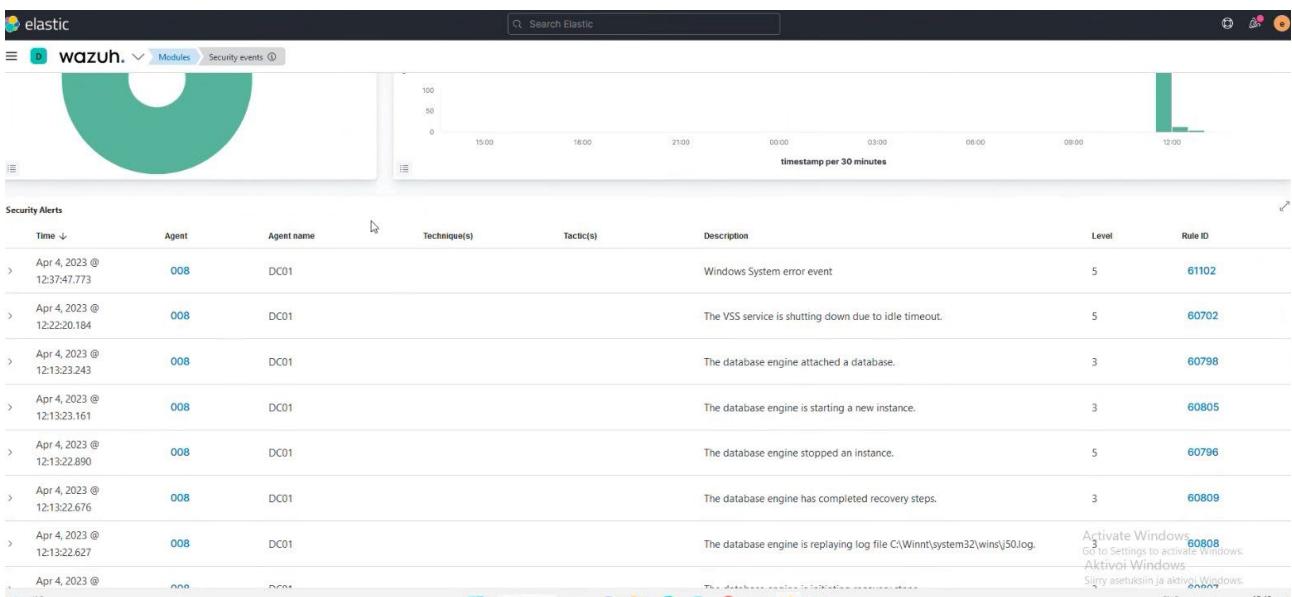
Kuva 38 Wazuh - Kalilla ajetun skriptin aiheuttamat Events



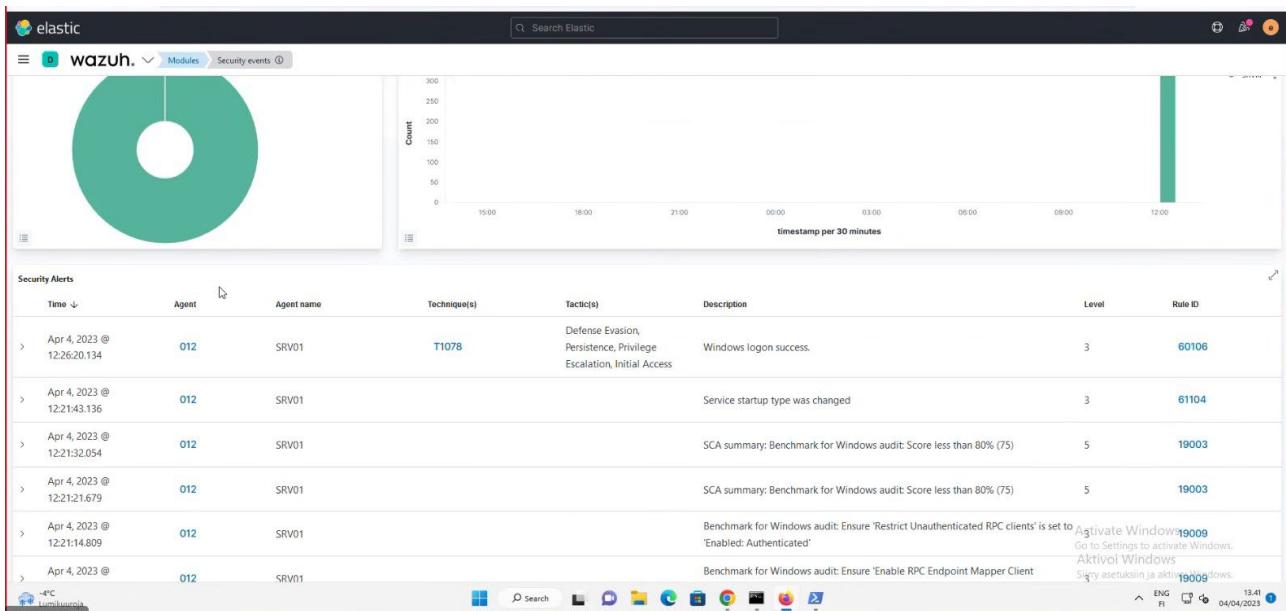
Kuva 39 Wazuh Security events



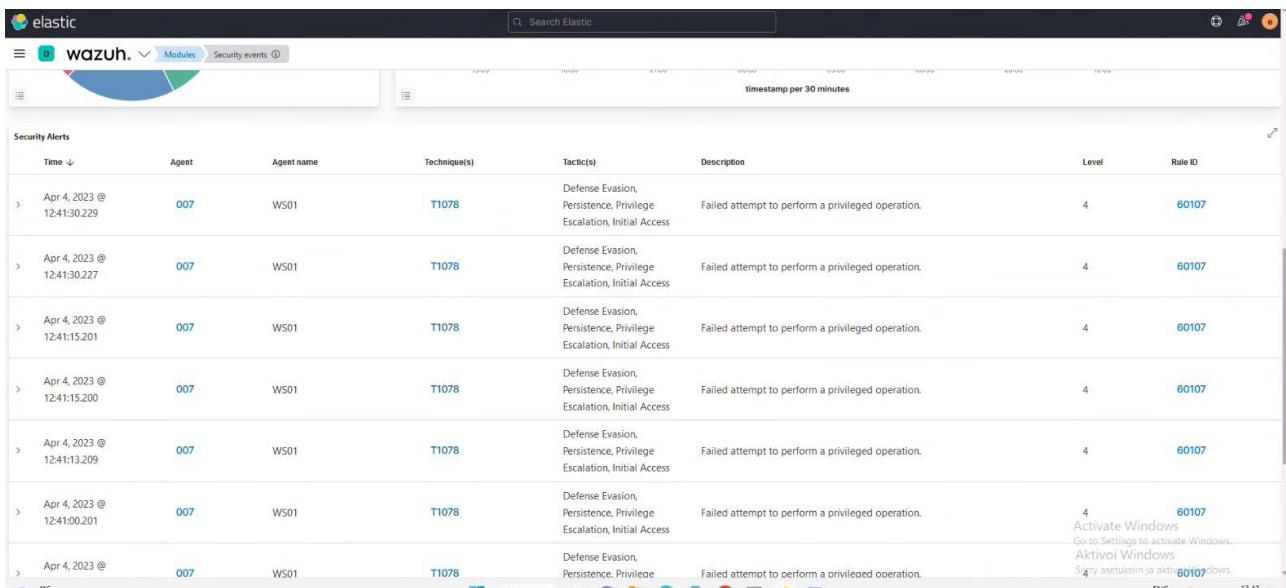
## Kuva 40 Wazuh Security Alerts – WS01



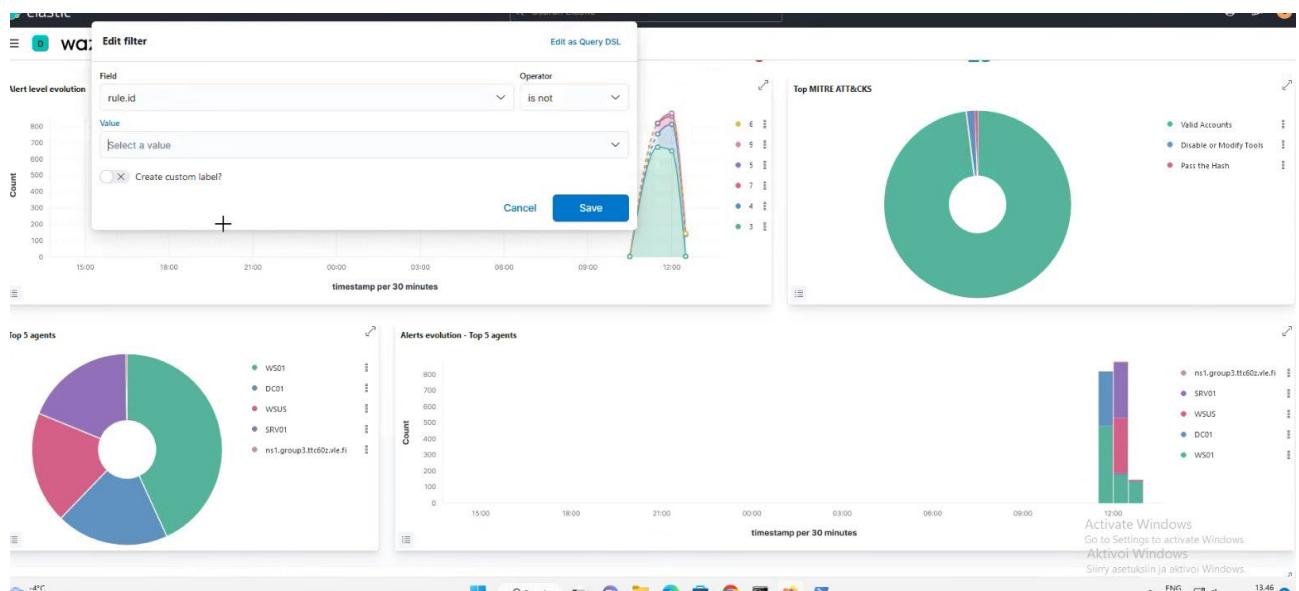
## Kuva 41 Wazuh Security Alerts - DC01



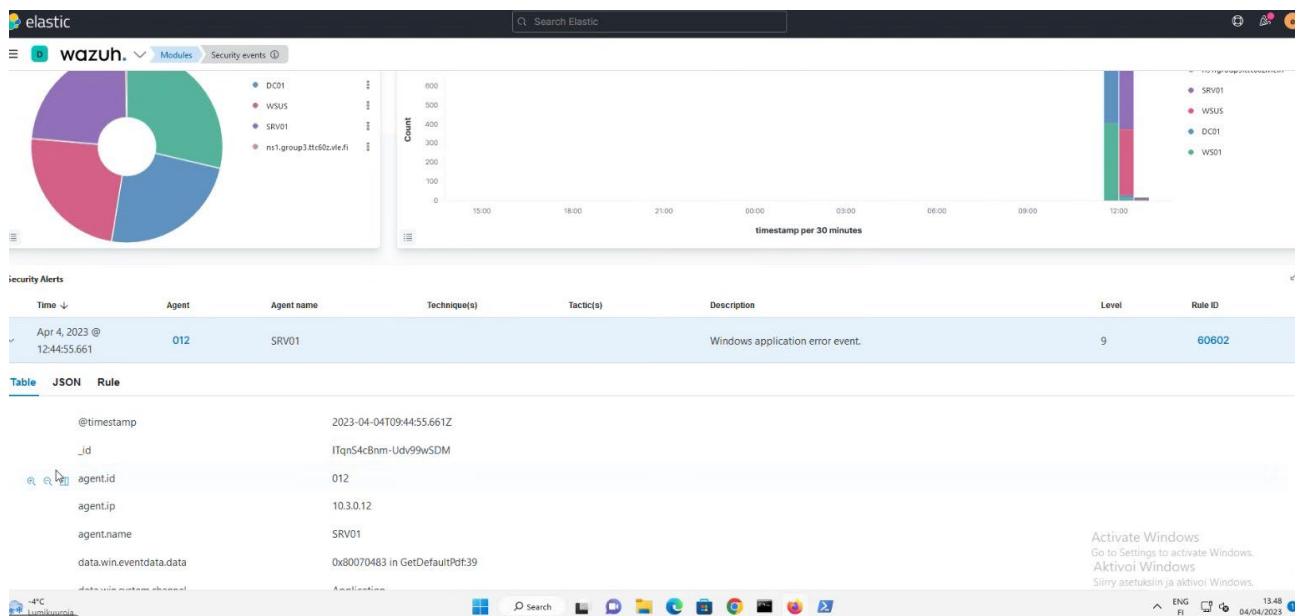
Kuva 42 Wazuh security alerts SRV01



Kuva 43 Wazuh security Alerts - WS01



Kuva 44 Wazuh alerttien filtteröintiä



Kuva 45 Wazuh filtteröidyn alertin tietojen tarkastelua

Kali-WS-Kyberpuolustus-Group3-vidmadmin-4628.vmx - VMware Remote Console

VMRC | ~ /Desktop/log.txt [Read ...] qterminal

kali㉿kali-ws: ~/Desktop

File Actions Edit View Help

GNU nano 7.1 test\_script.sh \*

#!/bin/bash

# Host and port scanning

timestamp=\$(date +%d-%m-%Y\ %H:%M:%S)

echo "Starting Nmap ICMP scan at \$timestamp" >> log.txt

echo "root66" | sudo -S nmap -sn 10.3.0.10 10.3.0.12 10.4.0.11 10.3.0.11

# sleep 120

#timestamp=\$(date +%d-%m-%Y\ %H:%M:%S)

#echo "Starting Nmap port and service scan at \$timestamp" >> log.txt

#echo "root66" | sudo -S nmap -sv 10.3.0.10 10.3.0.12 10.4.0.11 10.3.0.11

# sleep 300

# Web scanning

timestamp=\$(date +%d-%m-%Y\ %H:%M:%S)

#echo "Starting Nikto scan at \$timestamp" >> log.txt

#nikto -r https://10.4.0.11

# sleep 30

#timestamp=\$(date +%d-%m-%Y\ %H:%M:%S)

#echo "Starting Wordpress scan at \$timestamp" >> log.txt

wpSCAN --url https://10.4.0.11

# sleep 600

# Service scanning

timestamp=\$(date +%d-%m-%Y\ %H:%M:%S)

#echo "Starting Hydra RPD brute force at \$timestamp" >> log.txt

#hydra -L misc/users.txt -P misc/pass.txt rdp://10.3.0.11

# sleep 800

#timestamp=\$(date +%d-%m-%Y\ %H:%M:%S)

#echo "Starting RPC scanner at \$timestamp" >> log.txt

#msfconsole -x "use auxiliary/scanner/dcerpc/endpoint\_mapper; set RHOSTS 10.3.0.12; run; exit;"

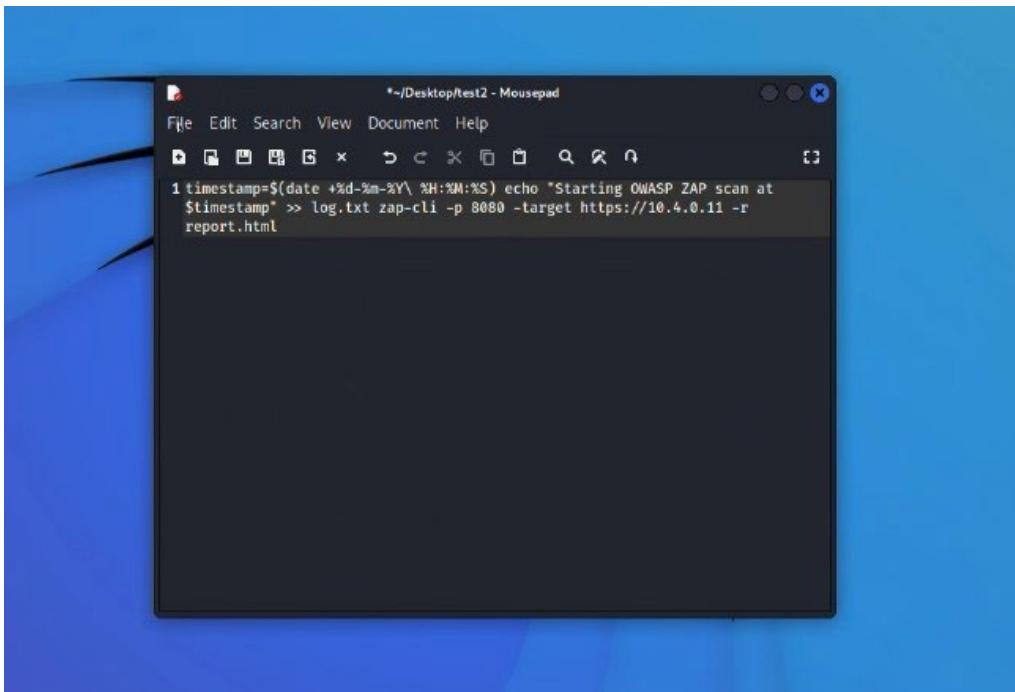
# sleep 100

#timestamp=\$(date +%d-%m-%Y\ %H:%M:%S)

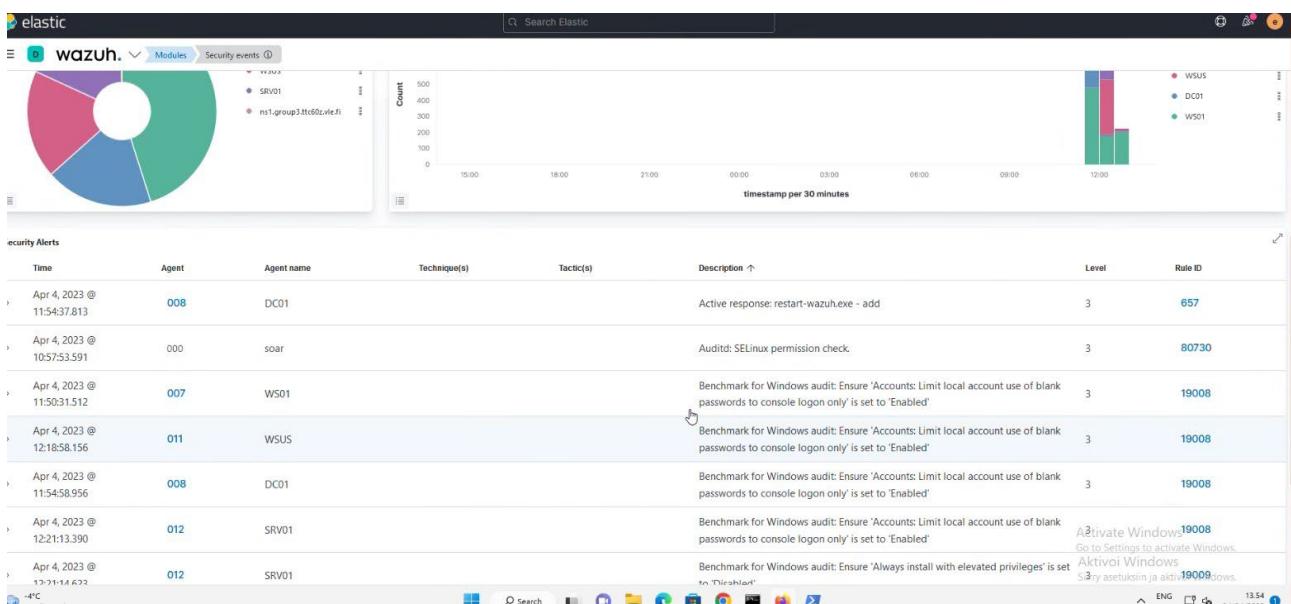
#echo "Starting SMB secretsdump at \$timestamp" >> log.txt

#msfconsole -x "use auxiliary/scanner/smb/impacket/secretsdump; set SMBPass Root-66; set SMBUser Administrator; set RHOSTS 10.3.0.11; run; exit;"

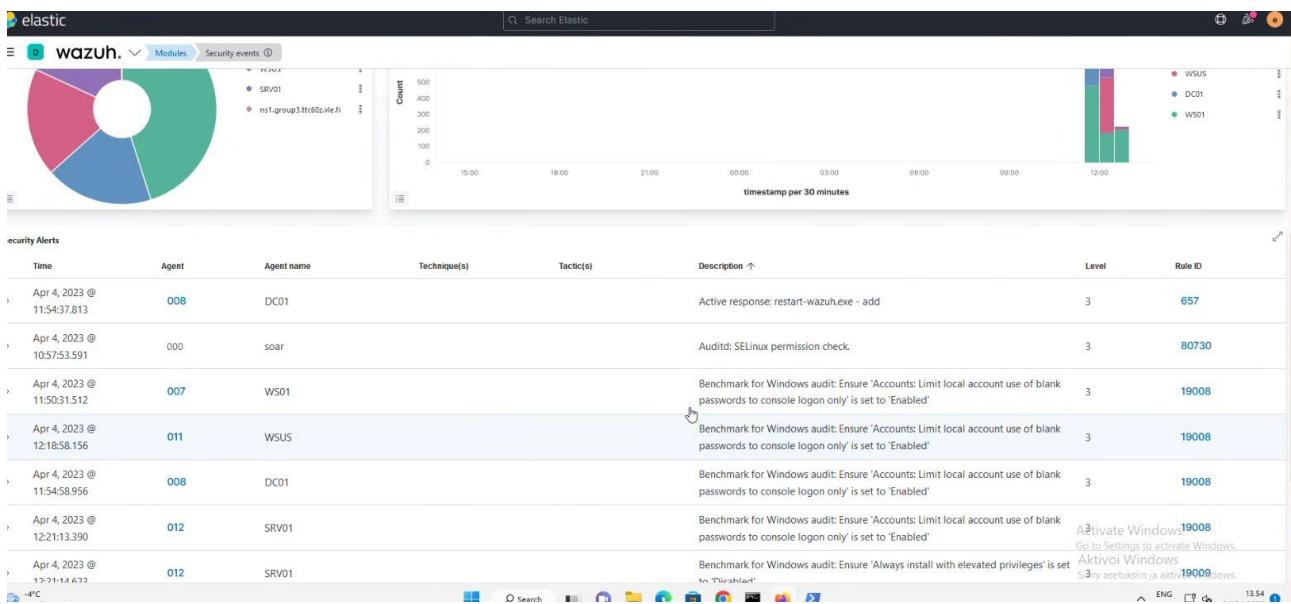
## Kuva 46 Kalin skriptin muokkausta



Kuva 47 Kali - Oma skripti



Kuva 48 Ajettiin uudestaan Kalilla muokattu skripti, Wazuh alerts



Kuva 49 Wazuh - Kaikki agentit alerts

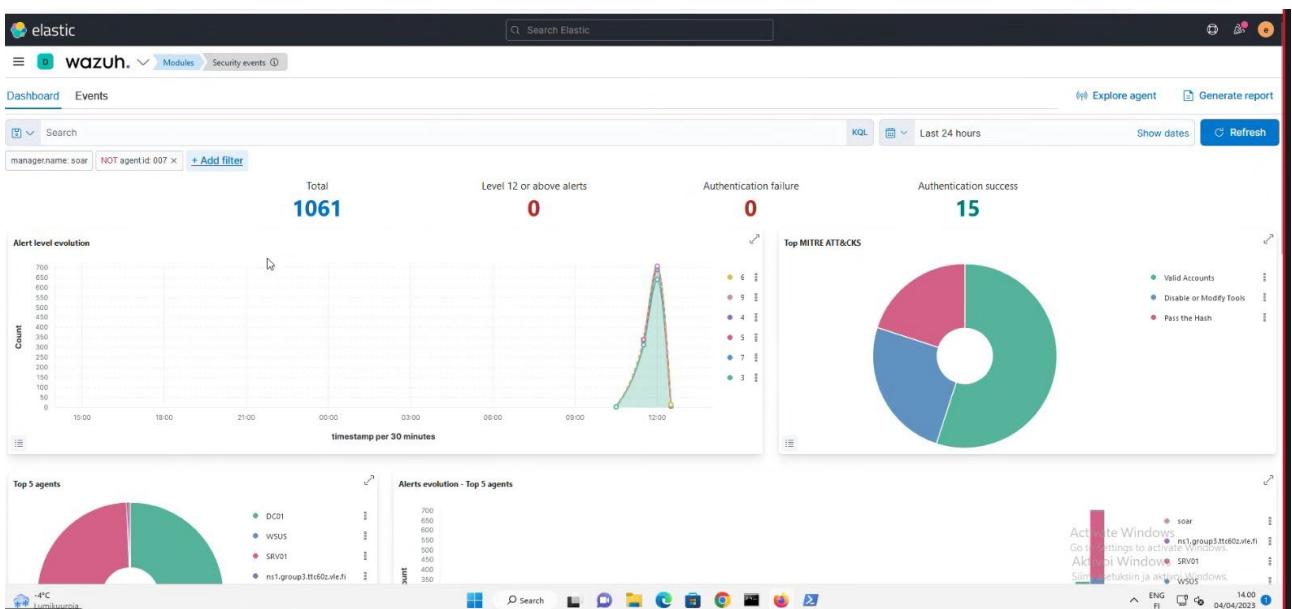
Total Found: 1 184

Count	rule.name	event.module	event.severity_label
552	ET SCAN NMAP OS Detection Probe	suricata	medium
72	ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent	suricata	low
72	ET SCAN MS Terminal Server Traffic on Non-standard Port	suricata	medium
72	ET POLICY Outbound MSSQL Connection to Non-Standard Port - Likely Malware	suricata	medium
72	ET POLICY GOPN/OP Request Outbound	suricata	high
36	ET POLICY RMI Request Outbound	suricata	high
30	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium
28	ET POLICY RDP connection confirm	suricata	low
25	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium
24	ET DOS Microsoft Remote Desktop (RDP) Syn then Reset 30 Second Dos Attempt	suricata	medium
22	ET SCAN Potential SSH Scan OUTBOUND	suricata	medium
20	ET SCAN Suspicious inbound to mySQL port 3306	suricata	medium
20	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium

Kuva 50 Security Onion uudestaan ajetun skriptin jälkeen (Alerts)

Timestamp	agent.name	message	log.level	metadata.version	metadata.pipeline	event.dataset
2023-04-04 02:59:56.421 +03:00	onion	updated role [limited-analyst]	INFO	8.3.2	filebeat-8.3.2-elasticsearch-server-pipeline	elasticsearch.server
2023-04-04 02:59:56.186 +03:00	onion	updated role [analyst]	INFO	8.3.2	filebeat-8.3.2-elasticsearch-server-pipeline	elasticsearch.server
2023-04-04 01:29:57.392 +03:00	onion	updated role [limited-auditor]	INFO	8.3.2	filebeat-8.3.2-elasticsearch-server-pipeline	elasticsearch.server

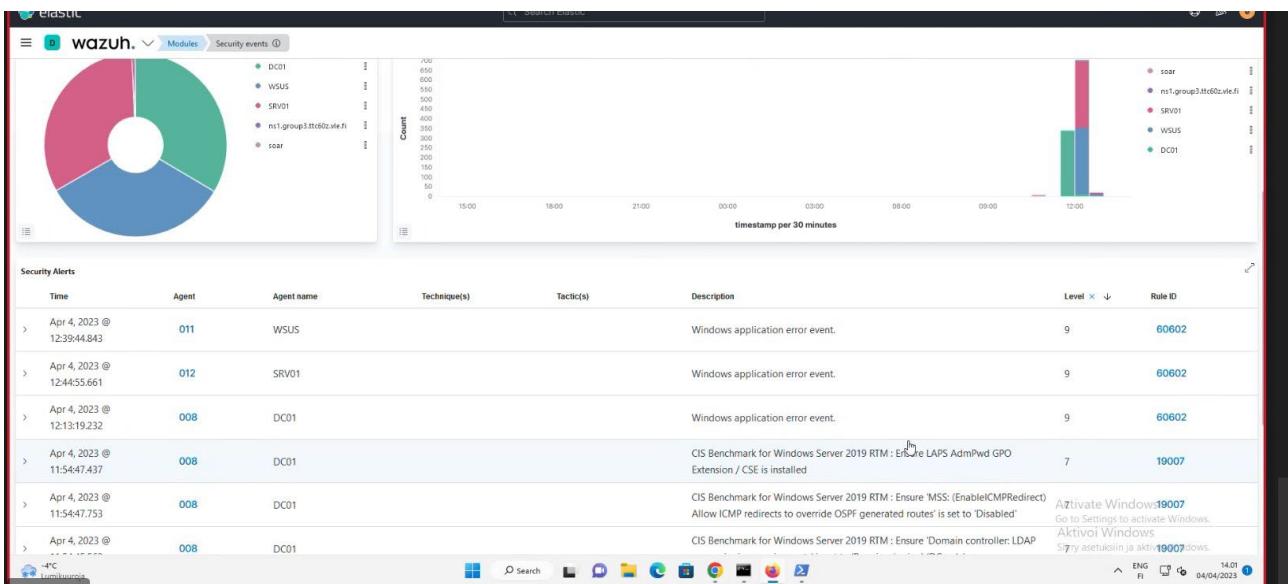
Kuva 51 Security Onion - Events (round 2)



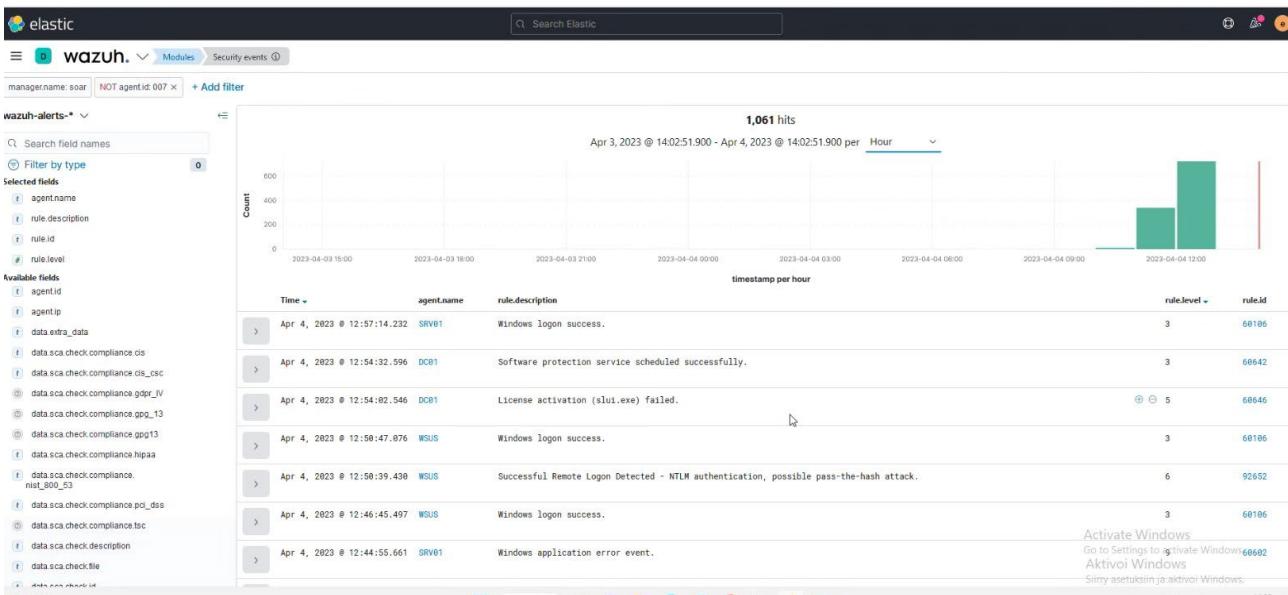
Kuva 52 Wazuh dashboard – 1061 total ILMAN 007 (ws01)

Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Apr 4, 2023 @ 12:57:14.232	012	SRV01	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Apr 4, 2023 @ 12:54:32.596	008	DC01			Software protection service scheduled successfully.	3	60642
Apr 4, 2023 @ 12:54:02.546	008	DC01			License activation (slui.exe) failed.	5	60646
Apr 4, 2023 @ 12:50:47.076	011	WSUS	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Apr 4, 2023 @ 12:50:39.430	011	WSUS	T1550.002	Defense Evasion, Lateral Movement	Successful Remote Logon Detected - NTLM authentication, possible pass-the-hash attack.	6	92652
Apr 4, 2023 @ 12:46:45.497	011	WSUS	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Apr 4, 2023 @ 12:45:55.661	012	SRV01			Windows application error event.	9	80602
Apr 4, 2023 @ 12:44:54.232	011	WSUS	T1550.002	Defense Evasion, Lateral Movement	Successful Remote Logon Detected - NTLM authentication, possible pass-the-hash attack.	6	92652
Apr 4, 2023 @ ...	...	...					

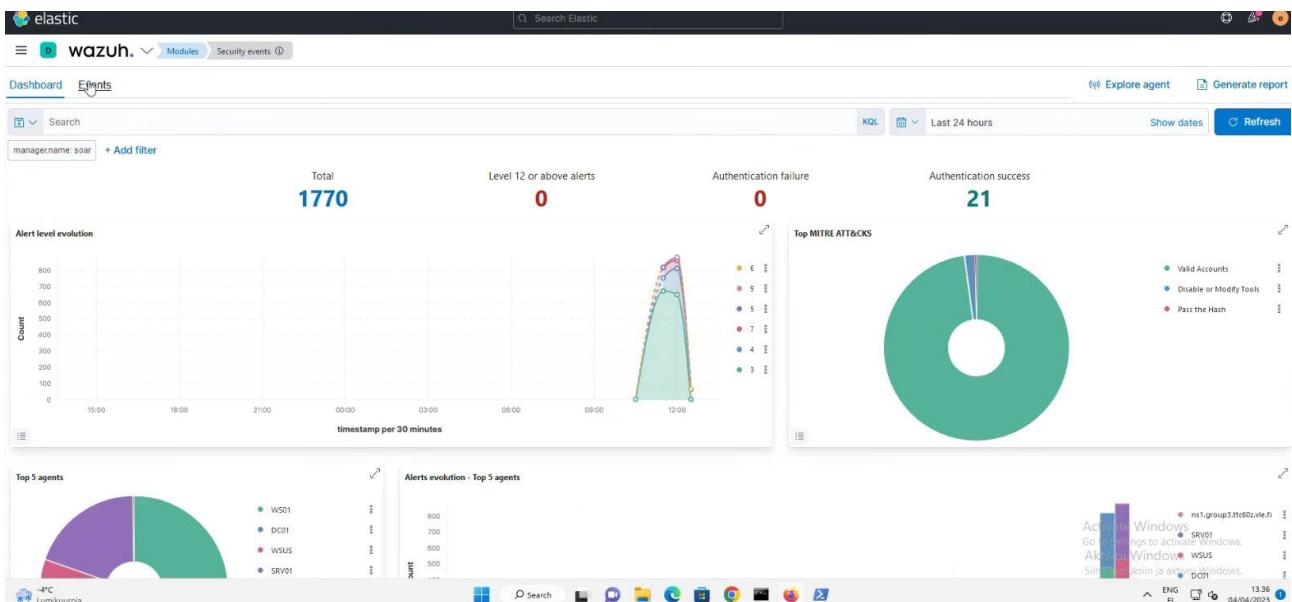
Kuva 53 Wazuh kaikki agentit Alerts



Kuva 54 Wazuh security alerts – Win application error event



Kuva 55 Wazuh filter ilman 007 agent (WS01)



Kuva 56 Wazuh Dashboard - 1770 total vielä uudestaan (Kaikki agentit)

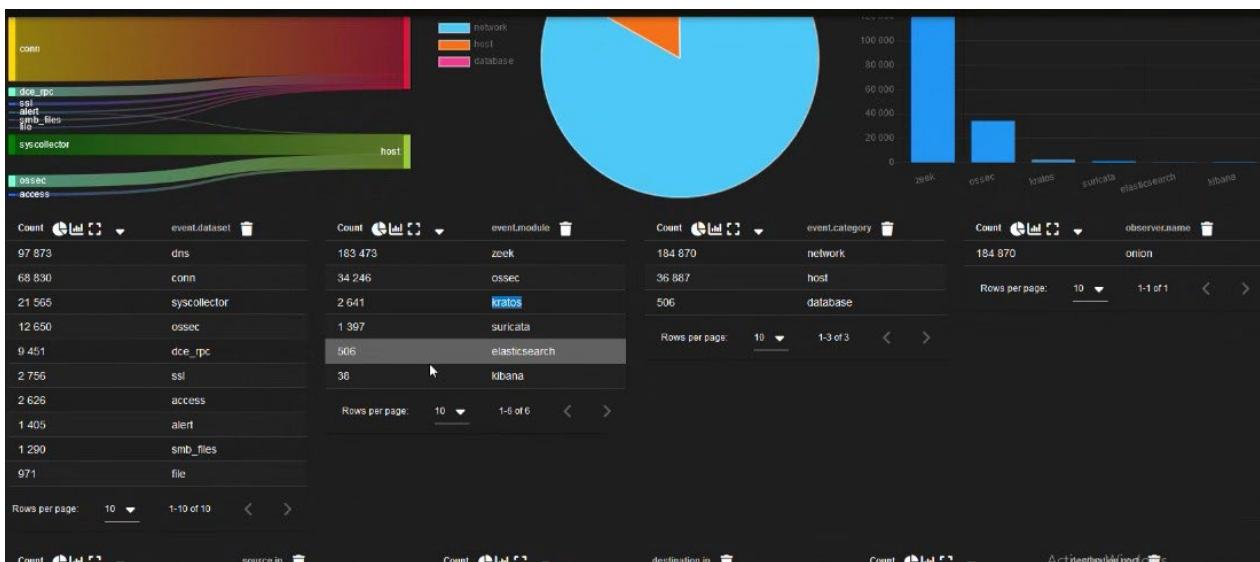
The table displays the following information for the alert:

	Value
_index	wazuh-alerts-4.x-2023.04.04
agent.id	012
agent.ip	10.3.0.12
agent.name	SRV01
data.sca.description	This document provides a way of ensuring the security of the Windows systems.
data.sca.failed	8
data.sca.file	sca_win_audit.yml
data.sca.invalid	38
data.sca.passed	25
data.sca.policy	Benchmark for Windows audit
data.sca.policy_id	sca_win_audit
data.sca.scan_id	390236342

Details for the alert:

- SCA summary: Benchmark for Windows audit: Score less than 80% (75)
- Actions: Activate Windows, Go to Settings to activate Windows, Aktivoi Windows, Siirry asetuksin ja aktivoi Windows.
- Language: ENG FI
- Date: 04/04/2023

Kuva 57 Wazuh alert table information – SRV01



Kuva 58 Total alerts

## 4 Pohdinta

Harjoituksessa tutustuttiin Security Onionin ominaisuuksiin, asennettiin Wazuhin agentit työasemille ja palvelimille, ja tutkittiin Wazuhin ominaisuuksia tarkemmin. Harjoitustyössä dokumentoitiin kaikki tehdyt toimenpiteet ja testaukset. Lisäksi käytettiin läpi IDS- ja IPS-teoriaa sekä Security Onionista, Zeekistä ja Wazuhista.

IDS tarkoittaa tunkeutumisen havaitsemisjärjestelmää ja IPS tunkeutumisenestojärjestelmää. Järjestelmien pääasiallinen ero on siinä, että IDS sisältää seurantajärjestelmiä ja IPS kontrollointijärjestelmiä. IDS ei muuta verkkoliikennettä, kun taas IPS estää pakettien liikkumisen riippuen niiden sisällöstä, palomuurin tapaan. IDS-järjestelmät luokitellaan yleisesti kahteen tyyppiin: Network Intrusion Detection System (NIDS) ja Host-based Intrusion Detection System (HIDS). IPS sovellukset keskittyvät mahdollisen haitallisen toiminnan tunnistamiseen, tietojen kirjaamiseen, raportointiin ja estämiseen.

Tehtävä sujui melkein ongelmissa, ainoaksi ongelmaksi osoittautui aluksi pistämämme väärä IP osoite, joka ei vaihtunut automaattisesti oikeaksi, vaikka ajoimme komennon uudestaan käyttämällä oikeaa ip osoitetta. Ratkaisu ongelmaan oli käydä vaihtamassa oikea IP manuaalisesti. Ajanhallinnallisesti harjoituksen tekeminen oli nopeaa ja ongelmanratkaisu IP osoitteeseen ongelman kanssa tehokasta. Lisäksi dokumentaation lopussa esitetty testaus oli mielenkiintoista.

## Lähteet

About Zeek. 2023. Zeek.org verkkosivu. Viitattu 16.4.2023. <https://docs.zeek.org/en/master/about.html>

Meena, R. N.d. What is Security Onion? How Powerful Security Onion Actually is?. Viitattu 16.4.2023. <https://luminisindia.com/cybersecurity-prism/323-what-is-security-onion-how-powerful-security-onion-actually-is>

Särkisaari, T. 2020. Wazuh SOC-ympäristössä Linux-näkyvyyden lisäämiseen. Opinnäytetyö, AMK Jyväskylän Ammattikorkeakoulu, Tieto- ja viestintätekniikan tutkinto-ohjelma. Viitattu 16.4.2023. [https://www.theseus.fi/bitstream/handle/10024/334217/Opinn%C3%A4ytety%C3%B6\\_tomi\\_sarkisaari.pdf?sequence=2&isAllowed=y](https://www.theseus.fi/bitstream/handle/10024/334217/Opinn%C3%A4ytety%C3%B6_tomi_sarkisaari.pdf?sequence=2&isAllowed=y)

Tunggal, A. 12.4.2023. IDS vs. IPS: What is the Difference?. Viitattu 17.4.2023. <https://www.upguard.com/blog/ids-vs-ips>