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](#_Toc182737644)

[2 Teoria 6](#_Toc182737645)

[2.1 SIEM 7](#_Toc182737646)

[3 Elasticin käyttöönotto 7](#_Toc182737647)

[4 Palo Alton logien vienti SIEMiin 19](#_Toc182737648)

[5 Integraatiot 24](#_Toc182737649)

[6 Ongelmien ratkonta 32](#_Toc182737650)

[7 Hälytysten testaus 36](#_Toc182737651)

[7.1 Hälytysten testaus APT28-ryhmän hyökkäyspolun mukaisesti 40](#_Toc182737652)

[7.1.1 1. Tiedustelu 40](#_Toc182737653)

[7.1.2 Alkuperäinen pääsy 41](#_Toc182737654)

[7.1.3 Suorittaminen 42](#_Toc182737655)

[7.1.4 Pysyvyys 43](#_Toc182737656)

[7.1.5 Oikeuksien laajentaminen 44](#_Toc182737657)

[7.1.6 Suojausten kiertäminen 45](#_Toc182737658)

[7.1.7 Sivuttaisliike 47](#_Toc182737659)

[7.1.8 Tiedon keruu 49](#_Toc182737660)

[7.1.9 Komento ja ohjaus 51](#_Toc182737661)

[7.1.10 Tietojen siirtäminen, exfiltraatio 51](#_Toc182737662)

[8 Valvontanäkymät 53](#_Toc182737663)

[9 Pohdinta 55](#_Toc182737664)

[Lähteet 57](#_Toc182737665)

Kuviot

[Kuvio 1. VLE 6](#_Toc182737666)

[Kuvio 2. Kibana-palvelimen ongelma 8](#_Toc182737667)

[Kuvio 3. Vanhentunut sertifikaatti 8](#_Toc182737668)

[Kuvio 4. SSL-verifikaatio 8](#_Toc182737669)

[Kuvio 5. Elasticin aloitusnäkymä 9](#_Toc182737670)

[Kuvio 6. Valmiit säännöt ja aikajanat 10](#_Toc182737671)

[Kuvio 7. Sääntöjen käyttöönotto 10](#_Toc182737672)

[Kuvio 8. Virheilmoitus sääntöjä ladattaessa 11](#_Toc182737673)

[Kuvio 9. Fleetin määrittämisen aloitus 11](#_Toc182737674)

[Kuvio 10. Fleet-palvelimen IP-osoite 12](#_Toc182737675)

[Kuvio 11. Fleet-palvelimen asennus 12](#_Toc182737676)

[Kuvio 12. Komennon suorittaminen 13](#_Toc182737677)

[Kuvio 13. Workstations-politiikka 13](#_Toc182737678)

[Kuvio 14. Agentin asennuskomento 14](#_Toc182737679)

[Kuvio 15. Virhe agentin asennuksessa 14](#_Toc182737680)

[Kuvio 16. Onnistunut agentin asennus 15](#_Toc182737681)

[Kuvio 17. WS01 Fleetissä 15](#_Toc182737682)

[Kuvio 18. Agenttien lisääminen Fleetiin 16](#_Toc182737683)

[Kuvio 19. Palvelimet ja työasema yhdistettynä Fleetiin 17](#_Toc182737684)

[Kuvio 20. sshd\_config -tiedoston asetukset 17](#_Toc182737685)

[Kuvio 21. Agentin asennus NS01:lle. 18](#_Toc182737686)

[Kuvio 22. Kaikki agentit asennettuna 18](#_Toc182737687)

[Kuvio 23.Syslog profiili 19](#_Toc182737688)

[Kuvio 24. Yhteensopivuuslista 20](#_Toc182737689)

[Kuvio 25. Lokien välitysprofiili 20](#_Toc182737690)

[Kuvio 26. Välitysprofiilin lisääminen turvallisuuspolitiikkaan 21](#_Toc182737691)

[Kuvio 27. Syslogin arvot 21](#_Toc182737692)

[Kuvio 28. SIEM:n avoimet portit 22](#_Toc182737693)

[Kuvio 29. Datan liikkumisen varmistaminen 22](#_Toc182737694)

[Kuvio 30. Palo Alton monitori 22](#_Toc182737695)

[Kuvio 31. GlobalProtectin lokien lähetys SIEM:iin 23](#_Toc182737696)

[Kuvio 32. Uhkalokien lähetys SIEM:iin 23](#_Toc182737697)

[Kuvio 33. Integraatioiden lisäämisen aloittaminen 24](#_Toc182737698)

[Kuvio 34. Integrointi Beatsia käyttäen 24](#_Toc182737699)

[Kuvio 35. Konfiguraatio-ohjeet 25](#_Toc182737700)

[Kuvio 36. Sormenjäljen etsiminen 25](#_Toc182737701)

[Kuvio 37. Filebeat.yml-tiedoston muokkaus 26](#_Toc182737702)

[Kuvio 38. Panw-moduulin käyttöönotto 26](#_Toc182737703)

[Kuvio 39. Panw.yml-tiedoston muokkaus 27](#_Toc182737704)

[Kuvio 40. Filebeatin asentaminen, virhe 27](#_Toc182737705)

[Kuvio 41. Filebeatin asentaminen onnistui 28](#_Toc182737706)

[Kuvio 42. Filebeatin käynnistys 28](#_Toc182737707)

[Kuvio 43. Data liikkuu 28](#_Toc182737708)

[Kuvio 44. Windows-integraatio 29](#_Toc182737709)

[Kuvio 45. Workstations-politiikan alla olevien koneiden integrointi 29](#_Toc182737710)

[Kuvio 46. Windows-integraatiot 30](#_Toc182737711)

[Kuvio 47. Endpoint and Cloud Security -integraatio 30](#_Toc182737712)

[Kuvio 48. Integroidut järjestelmät 31](#_Toc182737713)

[Kuvio 49. ElasticSearchin loki 32](#_Toc182737714)

[Kuvio 50. Metricbeat loki 32](#_Toc182737715)

[Kuvio 51. Endpoint loki 33](#_Toc182737716)

[Kuvio 52. Endpoint testi 33](#_Toc182737717)

[Kuvio 53. Kibana.yml-tiedoston Fleetin asetukset 34](#_Toc182737718)

[Kuvio 54. Fleetin outputasetukset 34](#_Toc182737719)

[Kuvio 55. Autorunsin käynnistys 36](#_Toc182737720)

[Kuvio 56. OneDriven automaattisen käynnistyksen poisto 37](#_Toc182737721)

[Kuvio 57. OneDriven automaattisen käynnistyksen poisto 2 37](#_Toc182737722)

[Kuvio 58. Analyzer 38](#_Toc182737723)

[Kuvio 59. Credential Dumping -testi 38](#_Toc182737724)

[Kuvio 60. Alerts-ikkuna 39](#_Toc182737725)

[Kuvio 61. Tietoja hälytyksestä 39](#_Toc182737726)

[Kuvio 62. T1592.001 komento 40](#_Toc182737727)

[Kuvio 63. T1566.001 komento. 41](#_Toc182737728)

[Kuvio 64. T1566.001 hälytys. 41](#_Toc182737729)

[Kuvio 65. T1204.002 komento. 42](#_Toc182737730)

[Kuvio 66. T1204.002 hälytys. 42](#_Toc182737731)

[Kuvio 67. T1547.001 komento. 43](#_Toc182737732)

[Kuvio 68. T1547.001 hälytys. 43](#_Toc182737733)

[Kuvio 69. T1547.001 analyysi. 44](#_Toc182737734)

[Kuvio 70. T1037.001 komento 44](#_Toc182737735)

[Kuvio 71. T1037.001 hälytys 45](#_Toc182737736)

[Kuvio 72. T1037.001 analyysi 45](#_Toc182737737)

[Kuvio 73. T1070.001 komento 46](#_Toc182737738)

[Kuvio 74. T1070.001 hälytys 46](#_Toc182737739)

[Kuvio 75. T1070.006 komento. 47](#_Toc182737740)

[Kuvio 76. Mimikatz:n lataus 47](#_Toc182737741)

[Kuvio 77. T1550.002 komento 48](#_Toc182737742)

[Kuvio 78. Elastic estää mimikatz:n 48](#_Toc182737743)

[Kuvio 79. T1550.002 hälytys 49](#_Toc182737744)

[Kuvio 80. T1113 komento 49](#_Toc182737745)

[Kuvio 81. Uuden hälytyssäännön luonti 50](#_Toc182737746)

[Kuvio 82. T1113 hälytys 50](#_Toc182737747)

[Kuvio 83. T1105 komento 51](#_Toc182737748)

[Kuvio 84. T1105 hälytys 51](#_Toc182737749)

[Kuvio 85. Curl:n asennus 52](#_Toc182737750)

[Kuvio 86. T1048.002 komento 52](#_Toc182737751)

[Kuvio 87. Rclonen asentaminen 52](#_Toc182737752)

[Kuvio 88. T1567.002 komento 53](#_Toc182737753)

[Kuvio 89. Kohdemaat visualisoituna 54](#_Toc182737754)

[Kuvio 90. bruteforce 54](#_Toc182737755)

[Kuvio 91. Epäonnistuneet kirjautumisyritykset 55](#_Toc182737756)

# 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)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, diagrammi, muotoilu

Kuvaus luotu automaattisesti

Kuvio 1. VLE

# Teoria

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

## 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)

# Elasticin käyttöönotto

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

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, ohjelmisto

Kuvaus luotu automaattisesti

Kuvio 2. Kibana-palvelimen ongelma

Tutkimme Kibanan lokeja, ja löysimme virheilmoituksen, joka kertoi ElasticSearchin sertifikaatin vanhenneen. Epäilimme tämän liittyvän ongelmaan, ja saimmekin siihen vastauksen labrainsseiltä. (Kuvio 3).



Kuvio 3. Vanhentunut sertifikaatti

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

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

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).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, diagrammi

Kuvaus luotu automaattisesti

Kuvio 5. Elasticin aloitusnäkymä

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).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

Kuvio 6. Valmiit säännöt ja aikajanat

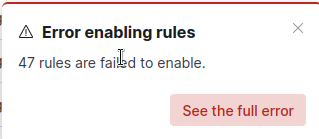
Valitsimme kaikki säännöt ja painoimme Bulk actions alta Enable, joka ottaa säännöt käyttöön. (Kuvio 7).

Kuva, joka sisältää kohteen teksti, Fontti, numero, viiva

Kuvaus luotu automaattisesti

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).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, muotoilu

Kuvaus luotu automaattisesti

Kuvio 9. Fleetin määrittämisen aloitus

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

Kuva, joka sisältää kohteen teksti, Fontti, numero, kuvakaappaus

Kuvaus luotu automaattisesti

Kuvio 10. Fleet-palvelimen IP-osoite

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

Kuva, joka sisältää kohteen teksti, Fontti, kuvakaappaus

Kuvaus luotu automaattisesti

Kuvio 11. Fleet-palvelimen asennus

Saimme komennon suoritettua ilman ongelmia. (Kuvio 12)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

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)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, ohjelmisto

Kuvaus luotu automaattisesti

Kuvio 13. Workstations-politiikka

Seuraavaksi avasimme WS01-työaseman, jolle asensimme ensimmäisen agentin.

Syötimme WS01:llä PowerShelliin kuvion 14 mukaiset komennot.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, numero

Kuvaus luotu automaattisesti

Kuvio 14. Agentin asennuskomento

Asennus ei onnistunut ja saimme virheilmoituksen. Se johtui siitä, että palomuuri esti liikenteen WS-netistä Admin-netiin. (Kuvio 15).  
Kuva, joka sisältää kohteen kuvakaappaus, teksti

Kuvaus luotu automaattisesti

Kuvio 15. Virhe agentin asennuksessa

Lisäsimme Palo Altoon turvallisuussäännön, joka sallii liikenteen WS-netistä Admin-netiin, jonka jälkeen ajoimme komennon uudestaan. Tämän jälkeen agentti asentui ongelmitta ja kuvion 16 mukaisesti Elasticissä näkyi vihreää.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, ohjelmisto

Kuvaus luotu automaattisesti

Kuvio 16. Onnistunut agentin asennus

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

Kuva, joka sisältää kohteen teksti, Fontti, numero, ohjelmisto

Kuvaus luotu automaattisesti

Kuvio 17. WS01 Fleetissä

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

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, ohjelmisto

Kuvaus luotu automaattisesti

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). Tajusimme, että DC01 ei ole palvelin, joten loimme sille myöhemmin oman politiikan Domain Controllers.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, numero, Fontti

Kuvaus luotu automaattisesti

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).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

Kuvio 20. sshd\_config -tiedoston asetukset

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

Kuva, joka sisältää kohteen teksti, kuvakaappaus

Kuvaus luotu automaattisesti

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).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, numero, Fontti

Kuvaus luotu automaattisesti

Kuvio 22. Kaikki agentit asennettuna

# Palo Alton logien vienti SIEMiin

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

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

Kuva, joka sisältää kohteen teksti, kuvakaappaus, tietokone, ohjelmisto

Kuvaus luotu automaattisesti

Kuvio 23.Syslog profiili

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

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, näyttö

Kuvaus luotu automaattisesti

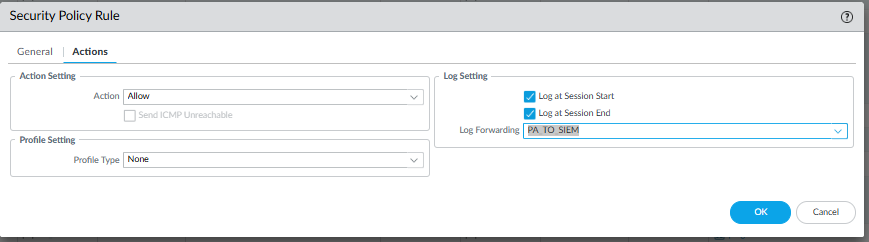
Kuvio 24. Yhteensopivuuslista

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Tietokonekuvake

Kuvaus luotu automaattisesti

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.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, numero

Kuvaus luotu automaattisesti

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.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, ohjelmisto

Kuvaus luotu automaattisesti

Kuvio 28. SIEM:n avoimet portit

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

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

Kuvio 29. Datan liikkumisen varmistaminen

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



Kuvio 30. Palo Alton monitori

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

Kuva, joka sisältää kohteen kuvakaappaus, teksti, ohjelmisto, Tietokonekuvake

Kuvaus luotu automaattisesti

Kuvio 31. GlobalProtectin lokien lähetys SIEM:iin

Teimme uhkalokien lähettämistä varten uusi yhteensopivuuslista aiemmin tehtyyn lokienvälitysprofiiliin. (Kuvio 32).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, näyttö

Kuvaus luotu automaattisesti

Kuvio 32. Uhkalokien lähetys SIEM:iin

# Integraatiot

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

Kuva, joka sisältää kohteen teksti, Fontti, diagrammi, kuvakaappaus

Kuvaus luotu automaattisesti

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)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, numero

Kuvaus luotu automaattisesti

Kuvio 34. Integrointi Beatsia käyttäen

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

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Verkkosivusto

Kuvaus luotu automaattisesti

Kuvio 35. Konfiguraatio-ohjeet

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

Kuva, joka sisältää kohteen teksti, ohjelmisto, Tietokonekuvake, Verkkosivusto

Kuvaus luotu automaattisesti

Kuvio 36. Sormenjäljen etsiminen

Muokkasimme filebeat.yml-tiedostoa kuvion 37 mukaisesti.  
Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

Kuvio 37. Filebeat.yml-tiedoston muokkaus

Seuraavaksi laitoimme panw moduulin käyttöön kuvion 38-mukaisesti



Kuvio 38. Panw-moduulin käyttöönotto

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

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, tietokone

Kuvaus luotu automaattisesti

Kuvio 39. Panw.yml-tiedoston muokkaus

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



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).

Kuva, joka sisältää kohteen teksti, Fontti, kuvakaappaus

Kuvaus luotu automaattisesti

Kuvio 41. Filebeatin asentaminen onnistui

Seuraavaksi käynnistimme filebeatin kuvion 42 mukaisesti.



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).

Kuva, joka sisältää kohteen teksti, Fontti, kuvakaappaus

Kuvaus luotu automaattisesti

Kuvio 43. Data liikkuu

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

Etsimme Windowsin Elasticin Integrations-välilehdeltä. (Kuvio 44)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, numero

Kuvaus luotu automaattisesti

Kuvio 44. Windows-integraatio

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

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto

Kuvaus luotu automaattisesti

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)

Kuva, joka sisältää kohteen teksti, Fontti, numero, viiva

Kuvaus luotu automaattisesti

Kuvio 46. Windows-integraatiot

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

Kuva, joka sisältää kohteen teksti, Fontti, viiva, ohjelmisto

Kuvaus luotu automaattisesti

Kuvio 47. Endpoint and Cloud Security -integraatio

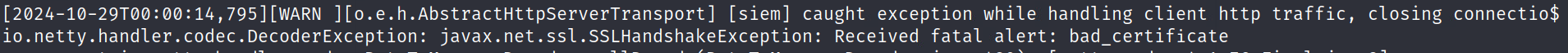
Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, numero

Kuvaus luotu automaattisesti

Kuvio 48. Integroidut järjestelmät

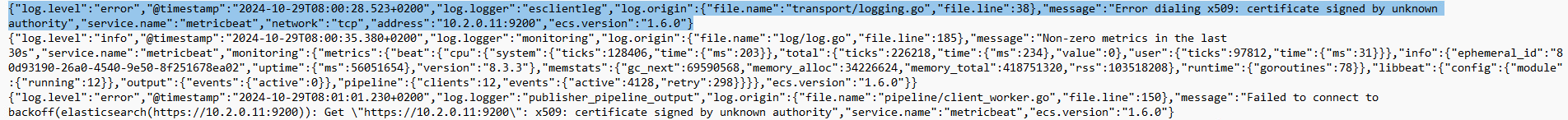
# Ongelmien ratkonta

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



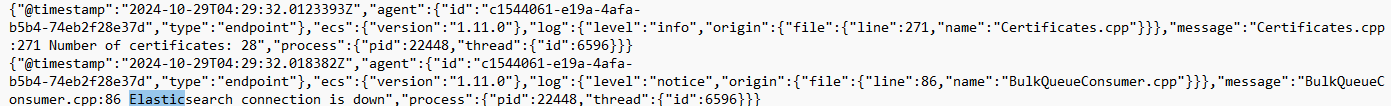
Kuvio 49. ElasticSearchin loki

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



Kuvio 50. Metricbeat loki

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

Kuvio 51. Endpoint loki

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

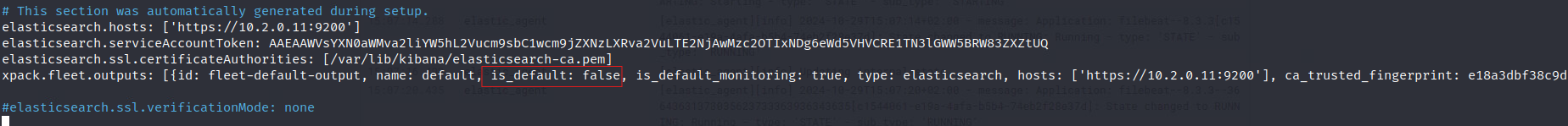
Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

Kuvio 52. Endpoint testi

Päädyimme tulokseen, että ongelman täytyy liittyä sertifikaatteihin, joten halusimme jotenkin ohittaa sertifikaattien käsittelyn. Muistimme, että meillä oli harjoitustyön alussa myös sertifikaattiongelma, 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)



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.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, numero

Kuvaus luotu automaattisesti

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 sertifikaatin elasticsearch-ca.pem, jossa oli eri sormenjälki (fingerprint), kuin alkuperäisessä sertifikaatissa. Muokkasimme uuden sertifikaatin mukaisen sormenjäljen kibana.yml ja filebeat.yml tiedostoihin sekä fleetin output -asetuksiin vanhan sormenjäljen tilalle. Otimme myös kaikista edellä mainituista tiedostoista ssl.verifiactionmode: none asetuksen pois.

# 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).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Tietokonekuvake

Kuvaus luotu automaattisesti

Kuvio 55. Autorunsin käynnistys

Siirryimme logon välilehdelle ja poistimme valinnat onedriveen liittyvistä toiminnoista.  
Tämä poistaa onedriven käynnistyksen kirjautumisen yhteydessä. (Kuvio 56)

Kuva, joka sisältää kohteen teksti, ohjelmisto, Tietokonekuvake, Verkkosivusto

Kuvaus luotu automaattisesti

Kuvio 56. OneDriven automaattisen käynnistyksen poisto

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

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, numero

Kuvaus luotu automaattisesti

Kuvio 57. OneDriven automaattisen käynnistyksen poisto 2

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

Kuva, joka sisältää kohteen teksti, ohjelmisto, Verkkosivusto, Tietokonekuvake

Kuvaus luotu automaattisesti

Kuvio 58. Analyzer

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



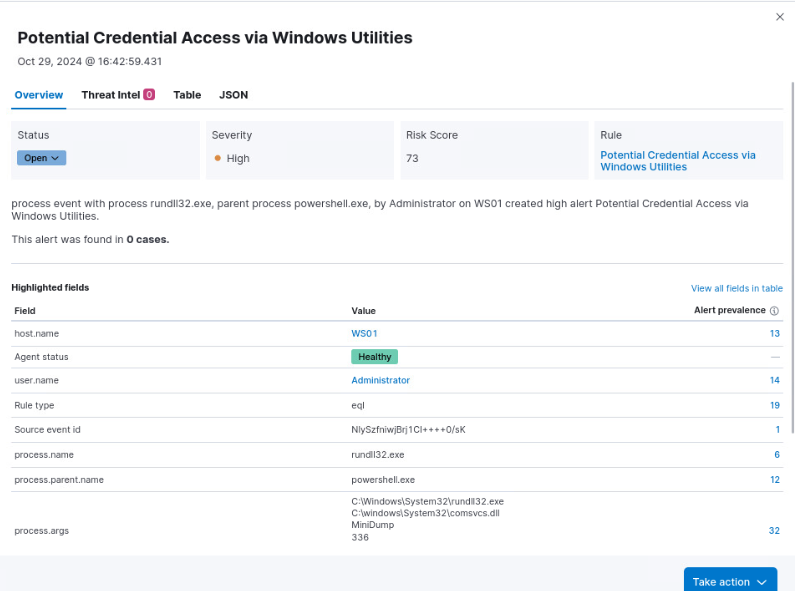
Kuvio 59. Credential Dumping -testi

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

Kuva, joka sisältää kohteen teksti, kuvakaappaus, viiva, numero

Kuvaus luotu automaattisesti

Kuvio 60. Alerts-ikkuna



Kuvio 61. Tietoja hälytyksestä

## Hälytysten testaus APT28-ryhmän hyökkäyspolun mukaisesti

Seuraavaksi testaamme tehtävänannon mukaisesti jonkin tunnetun APT ryhmän hyökkäyspolkua ja tarkkailemme, että saammeko suoritetuista toimenpiteistä hälytyksiä SIEM-järjestelmään. Valitsemme 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.

### 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 luetteloi tietokoneisiin liitetyt kamerat ja niiden tiedot. Se mahdollistaa kameroiden tunnistamisen ja sitä kautta tiedon keräämisen.

Ajoimme PowerShellillä kuvion mukaisen komennon.



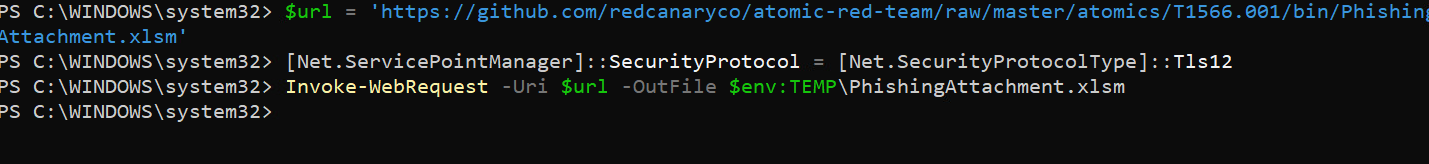
Kuvio 62. T1592.001 komento

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

### Alkuperäinen pääsy

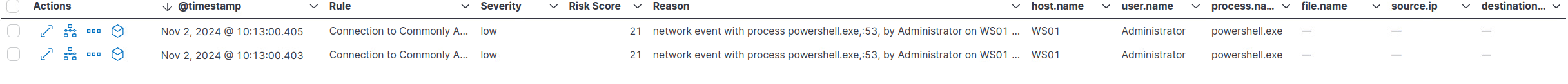
Kun tietoa on saatu, APT28 pyrkii hankkimaan ensimmäisen pääsyn organisaation verkkoon. Tämä tehdään yleensä kohdennetuilla kehittyneillä kalastelukampanjoilla tai käyttämällä hyväksi haavoittuvuuksia ulospäin näkyvissä järjestelmissä. Valitsimme tekniikan T1566.001: Liitteiden ja linkkien kautta tapahtuva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

Ajoimme PowerShellillä kuvion 63 komennot.



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 haittaohjelmasivustoon on otettu yhteys.

****

Kuvio 64. T1566.001 hälytys.

### 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

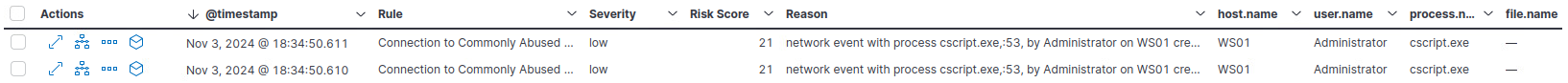
Suoritimme kuvion mukaisen komennon WS01:llä cmd:llä. (Kuvio 65)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, musta

Kuvaus luotu automaattisesti

Kuvio 65. T1204.002 komento.

Tästä aiheutui hälytys SIEM:iin. Hälytys koskee, kuten edellisessäkin kohdassa, yhteydenottoa tunnettuun haittaohjelmasivustoon. (Kuvio 66)



Kuvio 66. T1204.002 hälytys.

### 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.



Kuvio 67. T1547.001 komento.

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

****

Kuvio 68. T1547.001 hälytys.

Elasticin Analyzer-työkalulla voi analysoida hälytyksiä. Kuviossa 69 on analysoitu edellistä hälytystä ja sieltä näkee mitä rekisteriavainta on muutettu.  
Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto

Kuvaus luotu automaattisesti

Kuvio 69. T1547.001 analyysi.

### Oikeuksien laajentaminen

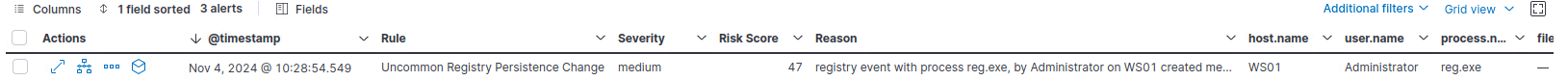
Päästyään verkkoon APT28 yrittää hankkia korkeammat oikeudet, jotta he voivat hallita järjestelmää tai muita käyttäjätiliä. Valitsimme testiin tekniikan T1037.001: Sisäänkirjautumisskriptat. Näiden avulla hyökkääjä voi käynnistyksen yhteydessä tai käyttäjän kirjautuessa sisään ajaa skriptoja, joilla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

Ajoimme cmd:llä kuvion 70 mukaisen komennon

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, musta

Kuvaus luotu automaattisesti

Kuvio 70. T1037.001 komento

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


Kuvio 71. T1037.001 hälytys

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

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Käyttöjärjestelmä

Kuvaus luotu automaattisesti

Kuvio 72. T1037.001 analyysi

### 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.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, ohjelmisto

Kuvaus luotu automaattisesti

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.  
Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, numero

Kuvaus luotu automaattisesti

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. Vaihdoimme ajan takaisin heti testin jälkeen.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

Kuvio 75. T1070.006 komento.

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

### Sivuttaisliike

APT28 käyttää hyväkseen hankittuja tunnistetietoja liikkuakseen verkossa kohti kohdejärjestelmiä, kuten tietokantoja tai palvelimia, joissa on arvokasta tietoa. Testasimme tekniikkaa T1550.002: Pass the Hash, jossa hyökkääjä yrittää varastaa salasanahashej, 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 käyttöömme. Saimme sen ladattua kuvion 76 mukaisella PowerShell komennolla.

**Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti**

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.



Kuvio 77. T1550.002 komento

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

Kuva, joka sisältää kohteen teksti, ohjelmisto, Tietokonekuvake, Verkkosivusto

Kuvaus luotu automaattisesti

Kuvio 78. Elastic estää mimikatz:n

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

Kuva, joka sisältää kohteen teksti, diagrammi, viiva, Fontti

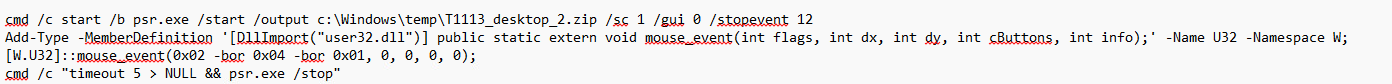
Kuvaus luotu automaattisesti

Kuvio 79. T1550.002 hälytys

### 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.



Kuvio 80. T1113 komento

Tämä ei aluksi aiheuttanut hälytystä mutta loimme uuden hälytyssäännön, joka huomaa, kun psr.exe ajetaan. (Kuvio 81)Kuva, joka sisältää kohteen teksti, kuvakaappaus, viiva, Fontti

Kuvaus luotu automaattisesti

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.

Kuva, joka sisältää kohteen teksti, diagrammi, viiva, Fontti

Kuvaus luotu automaattisesti

Kuvio 82. T1113 hälytys

### 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.exeksi sekä siirtää sen c asemalle. Komento myös tekee tekstitiedoston, jolla voidaan seurata komennon toimivuutta. (Kuvio 83).

Kuva, joka sisältää kohteen teksti, Fontti, kuvakaappaus, Grafiikka

Kuvaus luotu automaattisesti

Kuvio 83. T1105 komento

Tästä aiheutui hälytys. (Kuvio 84).



Kuvio 84. T1105 hälytys

### Tietojen siirtäminen, exfiltraatio

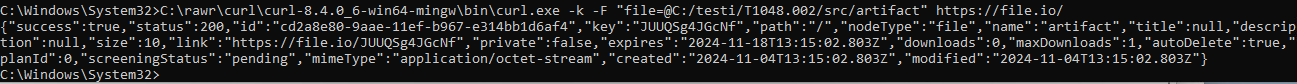
Hyökkääjä siirtää tärkeät tiedot organisaation ulkopuolelle, yleensä käyttämällä C2-yhteyttä. Tieto saatetaan pakata ja salata ennen siirtoa. Testasimme tekniikkaa T1048.002: Tietojen siirtäminen HTTPS-kanavan kautta.

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



Kuvio 85. Curl:n asennus

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



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.

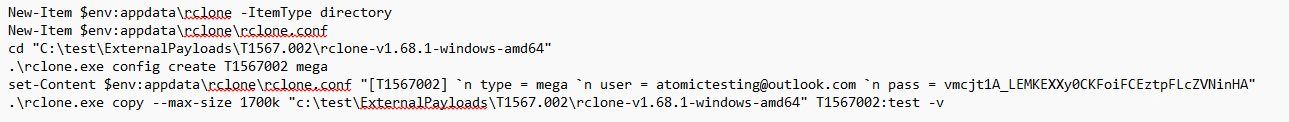
Aloitimme asentamalla rclone-sovelluksen WS01:lle. (Kuvio 87).

**Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Fontti

Kuvaus luotu automaattisesti**

Kuvio 87. Rclonen asentaminen

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



Kuvio 88. T1567.002 komento

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

# 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.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Tietokonekuvake

Kuvaus luotu automaattisesti

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 märitetylle käyttäjille, käyttäen rockyou.txt tiedostoa salasanojen kokeiluun



Kuvio 90. bruteforce

Visualisointiin tuli näkyviin epäonnistuneita kirjautumisyrityksiä. (Kuvio 91).

Kuva, joka sisältää kohteen teksti, viiva, kuvakaappaus, numero

Kuvaus luotu automaattisesti

Kuvio 91. Epäonnistuneet kirjautumisyritykset

# 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](https://mitre-attack.github.io/attack-navigator/%23layerURL=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 -verkkojulkaisu. Viitattu 7.11.2024. <https://medium.com/@joseruizsec/soc-analyst-level-2-tryhackme-log-analysis-intro-to-logs-b7b2bfbc66b5>