Harjoitustyön 1 Omaisuuksien hallinta

Ryhmä 13

Leevi Kauranen, AC7750
Samir Benjenna, AD1437
Eelis Suhonen, AA3910
Juho Eräjärvi, AD1276
Mikke Kuula, AC7806

Kyberturvallisuuden hallinta TTC6020-3007
17.10.2024
Tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

Kuviot

1 Johdanto

Ensimmäisessä kyberturvallisuuden hallinta kurssin harjoitustehtävässä oli tarkoitus tunnistaa ympäristömme, eli DefendByVirtualin omaisuuserät (assets) ja valita tarvittavat omaisuuksien hallintakeinoja tunnistettuihin omaisuuksiin. Tämän jälkeen tunnistettiin ja listattiin vielä käytössä olevat turvallisuus-/hallinta työkalut.

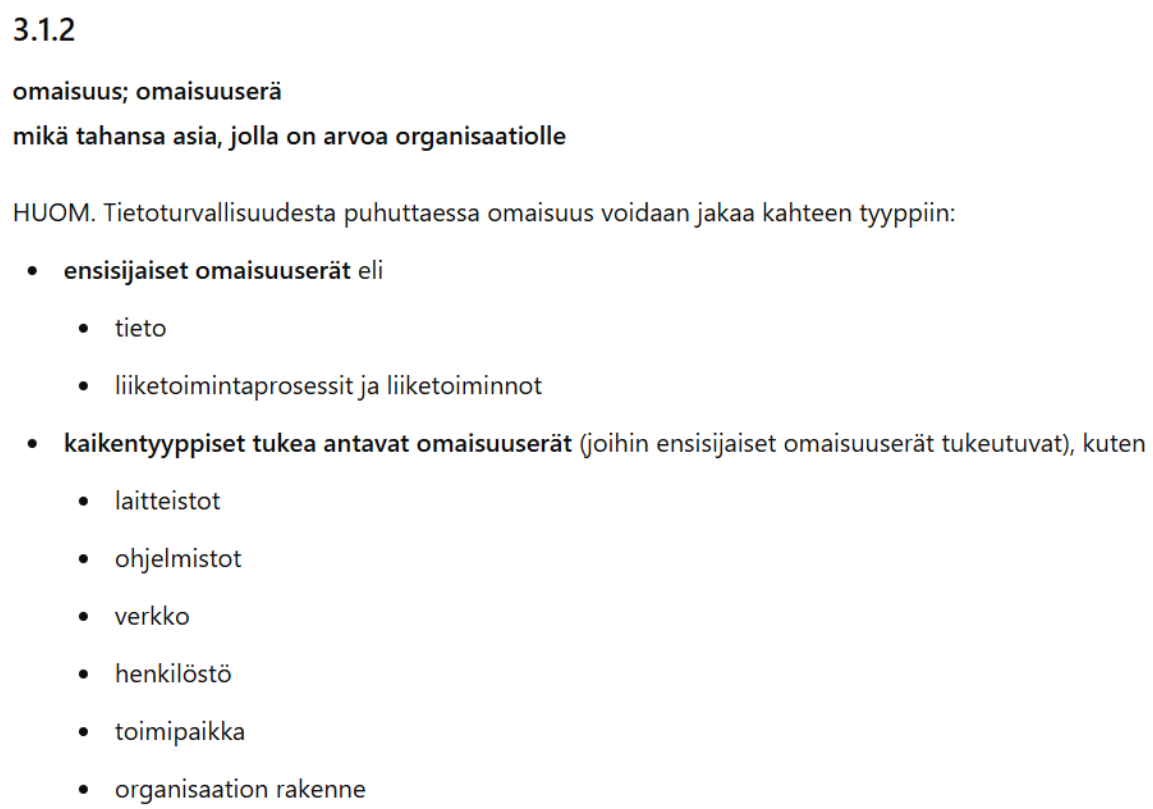
Tehtävässä tulee käyttää ISO 27001:2023 standardin taulukosta A.1 Tietoturvallisuuden hallintakeinojen viiteluettelo löytyviä käytäntöjä, joilla voidaan hallita organisaatiomme kyberturvallisuutta eri osa alueilla. Omaisuuteen kohdistuvia käytäntöjä ovat esimerkiksi ymmärrys ja dokumentointi koko omaisuuden laajuudesta ja työntekijöiden vastuista näihin liittyen, omaisuuden hyväksyttävät käyttötarkoitukset ja omaisuuserien hallinta muutoksessa. Standardia sovellettaessa omaan organisaatioon käytetään ISO 27002:2022 standardin tiettyjä hallintakeinoja, jotka kuvaavat yksityiskohtaisemmin näitä käytänteitä.

2 Yrityksen omaisuuserät (Assets)

Yrityksen omaisuudet koostuvat useista eri osa-alueista, jotka voidaan jakaa laitteistoihin, ohjelmistoihin ja tietoihin. Omaisuuksien tunnistaminen on keskeinen osa tietoturvallisuutta, sillä se mahdollistaa kriittisten kohteiden suojaamisen asianmukaisilla toimenpiteillä.

Kuviossa 1 on ISO 27002 dokumentin mukainen määritelmä sanalle “**Assets**”. Määritelmässä **omaisuuserät** pitää sisällään mm. Työntekijät (organisaation omaisuutta?), johtuen sanan kankeasta

suomennoksesta, mutta termi on määritelty ISO 27002 dokumenttia varten kuvaamaan organisaation mitä tahansa resurssia tai omaisuutta, jolla on sille arvoa. (SFS-EN ISO/IEC 27002:2022, 10).



3.1.2

omaisuus; omaisuuserä
mikä tahansa asia, jolla on arvoa organisaatiolle

HUOM. Tietoturvallisuudesta puhuttaessa omaisuus voidaan jakaa kahteen tyyppiin:

- **ensisijaiset omaisuuserät** eli
  - tieto
  - liiketoimintaprosessit ja liiketoiminnot
- **kaikentyyppiset tukea antavat omaisuuserät** (joihin ensisijaiset omaisuuserät tukeutuvat), kuten
  - laitteistot
  - ohjelmistot
  - verkko
  - henkilöstö
  - toimipaikka
  - organisaation rakenne

Kuvio 1. Omaisuuserien määritelmä

DefendByVirtualin omaisuuserät ovat lueteltuna liitteessä 1.

3 Omaisuuksien hallintakeinojen toteutus

Omaisuuksien hallintakeinot ovat toimenpiteitä, joilla pyritään hallitsemaan organisaation omaisuuteen liittyviä riskejä. Riskejä voidaan muuttaa, vähentää tai säilyttää, tärkeää kuitenkin on, että riskit liittyen omaisuuteen ovat organisaation tiedossa. Jos tietoturvapolitiikka on käytössä, mutta sitä ei sovelleta käytäntöön, niin riski on säilytetty, jos taas politiikkaa sovelletaan käytäntöön, riski saadaan pienennettyä. ISO 27002 dokumentissa esitetään tietoturvallisuuden hallintakeinoja perustuen yleisiin hyviin käytänteisiin ja niitä voidaan soveltaa oman organisaation omaisuuseriin. (SFS-EN ISO/IEC 27002:2022, 8).

Omaisuuksien hallintakeinojen määrittämisessä organisaatio päättää omaisuuserien laajuuden ja niihin liittyvien riskien perusteella, miten riskeihin liittyen toimitaan. Riskejä omaisuuteen liittyen voidaan vertailla esim. Omaisuuserän tärkeyden perusteella. Riskejä voidaan hyväksyä tietyin kriteerein tai katsoa, jos ne vaativat toimenpiteitä ja niiden käsittelylle voidaan luoda riskienhallintamalli. Organisaatio voi suunnitella hallintakeinonsa itse tai käyttää ulkoisia, muiden organisaatioiden malleja. Hallintakeinojen määrittämisessä tulee myös selvittää, onko mahdollinen hallintakeino järkevä perustuen siihen, miten paljon se kustantaa, verrattuna itse riskin tekemään vahinkoon. (SFS-EN ISO/IEC 27002:2022, 8).

3.1 5.9 Tietojen ja niihin liittyvien omaisuuserien luettelo

3.1.1 Hallintakeino

Olisi laadittava omaisuusluettelo tieto-omaisuudesta ja muihin niihin liittyvistä omaisuuseristä sekä tieto näiden omistajista. Luetteloa olisi ylläpidettävä. (SFS-EN ISO/IEC 27002:2022, 28).

3.1.2 Tarkoitus

Tunnistetaan organisaation tieto-omaisuus ja muut niihin liittyvät omaisuuserät, jotta voidaan ylläpitää niiden tietoturvallisuutta ja varmistua siitä, että näillä on omistajat. (SFS-EN ISO/IEC 27002:2022, 28).

3.1.3 Toteutus

Yksilöidään organisaation tiedot ja niihin liittyvät omaisuuserät, sekä määritellään tietoturvallisuutta koskeva tärkeys. Ylläpidetään dokumentaatiota tarkoitusta varten olevissa luetteloissa.

Tietoja ja niihin liittyviä omaisuuseriä koskevan omaisuusluettelon tulee olla tarkka, ajantasainen, johdonmukainen ja muiden luetteloiden kanssa yhtenevä. Varmistetaan omaisuuserien luettelon tarkkuus tietojen ja niihin liittyvien omaisuuserien säännöllisellä katselmoinnilla ja vertaamalla omaisuusluetteloon. Omaisuuserän sijainti sisälletään omaisuusluetteloon tarvittaessa.

Kunkin yksilöidyn tiedon ja siihen liittyvän omaisuuserän omistajuus osoitetaan nimetylle henkilölle tai ryhmälle ja sen luokitus yksilöidään kohtien 5.12 ja 5.13 mukaisesti. Toteutetaan prosessi ja varmistetaan oikea-aikaisesti tapahtuva omaisuuserän omistajuuden osoittaminen eli kun omaisuuserä luodaan tai siirretään organisaatioon ja uudelleen osoitetaan tarpeen mukaan omistajan lähdön tai työrooli muutoksen tapahtuessa.

1. Merkataan Tieto-omaisuus omaisuusluetteloon

2.Tunnistetaan tieto-omaisuuteen liittyvät omaisuuserät kuten tallennusvälineet

esim: tietokantaa säilytetään palvelimella, jonne pääsee vain tietyt työntekijät, ja se on suojattu palomuureja ja salauksella. Tässä tapauksessa tieto-omaisuus on tietokanta, omaisuuseriä ovat palvelin, palomuuri ja salaus

3. tunnistetaan tieto-omaisuuden omistaja, joka on siitä vastuussa.

1. **Omaisuusluettelon laadinta ja ylläpito:** Luodaan omaisuusluettelo, joka sisältää kaikki tietojen ja niihin liittyvien omaisuuserien yksityiskohdat. Omaisuusluettelo on pidettävä ajan tasalla. Luettelon tulee sisältää seuraavat tiedot:
    a. **Omaisuuserän nimi ja yksilöintitiedot**
    b. **Omaisuuserän sijainti (fyysinen / digitaalinen)**
    c. **Tiedon luokitus (esim. julkinen, luottamuksellinen, salainen)**
    d. **Omaisuuserän omistaja (henkilö tai ryhmä)**
    e. **Prosessi, järjestelmä tai komponentti, johon omaisuuserä liittyy**
2. **Omaisuusluettelon päivitys:** Omaisuusluetteloa on päivitettävä säännöllisesti ja aina, kun omaisuuseriin tehdään muutoksia. Päivitys voi tapahtua automaattisesti tai manuaalisesti, ja on otettava huomioon seuraavat vaihtoehdot:
    a. Säännöllinen katselmointi
    b. Automaattinen päivittäminen

3.2 5.10 Tietojen ja niihin liittyvien omaisuuserien hyväksyttävä käyttö

Tietojen ja niihin liittyvien omaisuuserien hyväksyttävän käytön säännöt ja menettelyt olisi yksilöitävä, dokumentoitava ja vietävä käytäntöön. (SFS-EN ISO/IEC 27002:2022, 29).

3.2.1 Tarkoitus

Varmistetaan, että tiedot ja niihin liittyvät omaisuuserät on suojattu asianmukaisesti ja että niitä käytetään ja käsitellään asianmukaisesti. (SFS-EN ISO/IEC 27002:2022, 30).

3.2.2 Toteutus

Laaditaan tietojen ja niihin liittyvien omaisuuserien hyväksyttävän käytön kohdennetut toimintaperiaatteet ja viestitään niistä kaikille, jotka käyttävät tai käsittelevät tietoja ja niihin liittyviä omaisuuseriä. Nämä tarjoavat selkeän ohjeistuksen siitä, mikä on hyväksyttävää käyttöä.

1. **Sallitut ja Ei-sallitut toimet tietojen käsittelyssä**
    a. **Sallitut toimet:**
        - Organisaation tietoja tulee käsitellä turvallisesti, noudattaen sovittuja käyttöoikeuksia ja tietoturvamenettelyjä
        - Tietoja saa käyttää vain niiden tarkoitusten mukaisesti, joihin oikeudet on myönnetty
    b. **Ei-Sallitut toimet:**
        - Tietojen luvaton kopiointi, siirtäminen tai jakaminen kolmansille osapuolille on kielletty.
        - Tietojen käyttö muihin kuin organisaation hyväksymiin tarkoituksiin on kielletty.

2. **Tietojen ja Omaisuuserien käyttö**
    a. **Sallittu Käyttö:**
        - Organisaation tietoja ja omaisuuseriä saa käyttää vain työtehtävään liittyvissä toiminnoissa
        - Tietojen käyttö tule tapahtua vain siihen tarkoitetuissa ympäristöissä (esim. hyväksytty järjestelmä ja laite).
    b. **Ei sallittu käyttö:**
        - Henkilökohtaisten laitteiden käyttö organisaation tietojen käsittelyssä ilman erillistä lupaa on kielletty.
        - Tietojen tallentaminen julkisiin pilvipalveluihin ilman IT-osaston hyväksyntää on kielletty.

Käytetään erilaisia valvontakeinoja tietojen käytön seurantaan. Näitä keinoja voi olla esimerkiksi. lokitietojen seuranta, verkkoliikenteen valvonta sekä laitteiden ja järjestelmien pääsynhallinta.

3. **Hyväksyttävän käytön menettelyt ja prosessit:** Hyväksyttävän käytön toimintaperiaatteet on laadittu kattamaan tietojen koko elinkaaren luokittelun ja niihin liittyvien riskien mukaisesti.

a. **Pääsyoikeudet:** Määritettiin pääsyoikeudet tietojen luokitustason mukaan. Tarkoituksena on tukea tietojen suojausvaatimuksia. Vain oikeutetut henkilöt voi käyttää tietoja ja omaisuuseriä. Pääsyoikeuksia seurataan ja hallinnoidaan tietojärjestelmien kautta
b. **Henkilöiden Oikeudet ja tietojen ylläpito:** pidetään ajan tasalla lista kaikista henkilöistä, joilla on oikeus käyttää tietoja ja niihin liittyviä omaisuuseriä.
c. **Tietojen kopioiden suojaaminen:** Kaikki tietojen kopiot, olivatpa ne väliaikaisia tai pysyviä, on suojattava samantasoisesti kuin alkuperäinen tieto.
d. **Säilytys:** Tietojen säilyttäminen noudattaa tietoturvavaatimuksia ja huolehtii siitä, että tiedot ovat aina suojattuja. Säilyttämisessä noudatetaan valmistajan tai palveluntarjoajan antamia ohjeita ja standardeja. Tämä koskee tietoja ja myös niihin liittyviä omaisuuseriä
e. **Tallenteiden ja tallennusvälineiden merkinnät:** Kaikki sähköiset ja fyysiset tallenteet sekä tallennusvälineet on merkittävä selkeästi niin, että vain käyttöön oikeutettu vastaanottaja voi tunnistaa ja käsitellä niitä.
f. **Tietojen ja omaisuuserien hävittäminen:** Hävittämisessä noudatetaan hyväksyttyä menettelytapaa. Hävitettävät tiedot ja tallennusvälineet käsitellään turvallisesti, mikä voi sisältää tietojen pysyvän poistamisen, laitteen nollauksen, tai tarvittaessa fyysisen tuhoamisen.

3.3 5.11 Omaisuuden palauttaminen

Henkilöstön ja muiden sidosryhmien olisi palautettava kaikki hallussaan oleva organisaation omaisuus työsuhteen tai sopimuksen päättyessä tai muuttuessa.

3.3.1 Tarkoitus

Organisaation omaisuuserien suojaaminen osana työsuhteen tai sopimuksen päättymis- tai muutosprosessia.

3.3.2 Toteuttaminen

Sisällytetään työsuhteen muutos- tai päättymisprosessiin kaiken aiemmin saadun organisaation tai sille luovutetun fyysisen tai sähköisen omaisuuden palauttaminen. Mikäli henkilöstö tai sidosryhmä ostaa organisaation laitteita tai käyttää henkilökohtaisia laitteita, noudatetaan menettelyjä, joilla varmistetaan tärkeän tiedon seuranta ja siirtäminen organisaatiolle ja sen turvallinen poistaminen laitteistosta.

Luodaan dokumentti, jossa määritetään palautettavat omaisuuserät tai tiedot, joita voi olla esimerkiksi:

1. **Päätelaitteet:** Tietokoneet, puhelimet ja tabletit

2. **Siirrettävät tallennusvälineet:** USB-tikut, ulkoiset kiintolevyt, muistikortit
3. **Muut välineet ja laitteet:** Työkalut, kamerat, näytöt, laitteet, jotka on annettu työsuhteen ajaksi käyttöön
4. **tunnistautumisvälineet:** tilojen ja tietojärjestelmien avaimet, älykortit, sähköiset tunnistusvälineet (esim. turvakoodit, henkilökortit)
5. **tietojen fyysiset kopiot:** Sopimukset, raportit tai muut asiakirjat

Toimenpiteet työsuhteen päättyessä:

1. **Luettelo omaisuuseristä:** Laaditaan luettelo omaisuudesta, joka on luovutettu työntekijälle tai sidosryhmälle.
2. **Palautusprosessin aloittaminen:** Työsuhteen tai sopimuksen loppuessa, palautusprosessi käynnistetään. Tämä sisältää laitteiden, tietojen ja muiden resurssien palauttamisen
3. **Tietoturva- ja poistotoimenpiteet:** Valvotaan, että kaikki tiedot poistetaan asianmukaisesti eikä organisaation dataa jää työntekijän käyttöön

3.4 5.14 Tietojen siirtäminen

Kaiken tyyppisellä organisaation sisäisellä, organisaatioiden välisellä ja sidosryhmille tapahtuvalla tietojen siirtämisellä olisi oltava säännöt, menettelyt tai sopimukset.

3.4.1 Tarkoitus

Ylläpidetään organisaation sisällä tai ulkopuolisen sidosryhmän kanssa siirretyn tiedon suojausta.

3.4.2 Toteuttaminen

Jaamme toteutuksen kolmeen osa-alueeseen: Sähköinen, fyysinen ja suullinen siirtäminen.

1. **Sähköinen siirtäminen**: Kun tietoa siirretään sähköisesti esim. sähköpostilla, varmistetaan seuraavat asiat:
    a. **Salaus:** Arkaluontoinen tieto, kuten liitteet tai henkilötiedot tulee suojata salauksella, erityisesti kun niitä siirretään julkisessa verkossa.
    b. **Haittaohjelmien torjunta:** Estetään haittaohjelmien leviämistä sähköpostin kautta erilaisilla työkaluilla.
    c. **Osoitteiden tarkistus:** Estetään väärien vastaanottajien tai sähköpostiosoitteiden käyttö esimerkiksi automaattisilla varmistusprosesseilla
    d. **Käyttäjien tunnistus:** Käytetään kaksivaiheista tunnistautumista.
    e. **Ohjeistaminen:** Ohjeistetaan henkilöstöä ja muita sidosryhmiä kriittisten tietojen oikeasta viestimisestä. Esimerkkinä, että kriittisiä tietoja ei lähetettäisi teksti- tai pikaviesteissä.

f. **Julkisten palveluiden hyväksyntä**: määritellään selkeät käyttöehdot ja rajoituksen ennen ulkoisen julkisen palvelun käyttöä. Näitä voi olla esim. pikaviestis, sosiaalinen verkosto, pilvitallennus.

2. **Fyysinen siirtäminen:** Kun tietoa siirretään fyysisillä tallennusvälineillä (kuten paperilla tai USB-tikuilla), seuraavat asiat tulisi ottaa huomioon:
    a. **Vastuuhenkilöt:** Nimetään vastuuhenkilöt siirtojen hallinnasta ja ilmoittamisesta
    b. **Pakkaus:** Pakataan tallennusvälineet suojaten ne ympäristövaurioilta kuten kuumuudelta, kosteudelta tai sähkömagneettisilta häiriöiltä
    c. **Siirron seuranta:** luodaan lokit, joista käy ilmi siirrettävästä tiedosta ja vastaanotosta vastaava henkilö.
    d. **Hyväksytyt kuljetuspalvelut:** Hyväksytään vain tietyt, turvalliset kuljetuspalvelut ja pidetään niistä kirjaa.

3. **Suullinen siirtäminen:** Suullisessa tiedon siirrossa (esim. puhelin, kasvotusten), huomioidaan seuraavat seikat:
    a. **Keskustelutilan suojaaminen:** Huolehditaan siitä, että keskustelutila on suojattu sivullisilta, kun kyseessä on luottamuksellinen keskustelu. (esim. äänieristetty huone, suljettu ovi)
    b. **Ääniviestien käyttö:** Luottamuksellista tietoa ei saa jättää puhelinvastaajiin tai jakaa ääniviesteinä. Ääniviestit altistavat tiedon päätymistä ulkopuolisille.
    c. **Keskustelun aloittaminen:** Arkaluontoiset keskustelut aloitetaan informoimalla kuuntelijoita tiedon luokitustasosta ja tietojen käsittelyrajoituksista.

3.5 5.33 Tallenteiden suojaaminen

Tallenteet suojataan katoamiselta, tuhoutumiselta, väärentämiseltä, luvattomalta käytöltä ja levittämiseltä. (SFS-EN ISO/IEC 27002:2022, 65).

3.5.1 Tarkoitus

Varmistetaan, että tallenteiden suojaamista ja saatavuutta koskevien lakien, asetusten, viranomaisten ja sopimusten asettamia vaatimuksia sekä niihin liittyviä yleisiä ja yhteiskunnan odotuksia noudatetaan. (SFS-EN ISO/IEC 27002:2022, 56).

3.5.2 Toteuttaminen

Julkaistiin tallenteiden hallussapitoketjua ja hävittämistä koskevat ohjeistukset, joihin sisältyy tallenteiden luvattoman muokkauksen estäminen. Laadittiin myös arkistosuunnitelma, jossa yksilöidään arkistoitu tallenne sekä säilytysaika.

Tallennus- ja käsittelyjärjestelmällä varmistetaan, että tallenteet ja niiden säilytysjaksojen pituuden määrittelemisessä otetaan huomioon kansalliset tai alueelliset lait ja viranomaismääräyksen sekä yleiset ja yhteiskunnan odotukset. Järjestelmä sallii tallenteiden hävittämisen säilytysajan loputtua, mikäli tallennetta ei enää tarvita.

Tallenteiden suojaamisessa otetaan huomioon tallenteen tiedon luokitus luokittelujärjestelmässämme. Luokitellaan tallenteet myös tallenne tyyppeihin kuten kirjanpidon tallenteet tai sopimuksiin liittyvät tallenteet ja määritetään kullekin tallenne tyypille säilytysaika ja sallittu tallennusväline (fyysinen tai sähköinen).

3.6 Dokumentoidut toimintaohjeet

Tietojenkäsittelypalveluita koskevat toimintaohjeet dokumentoidaan ja niiden on oltava niitä tarvitsevien henkilöstön jäsenien saatavilla. (SFS-EN ISO/IEC 27002:2022, 66).

3.6.1 Tarkoitus

Varmistetaan tietojenkäsittelypalveluiden oikea ja turvallinen toiminta. (SFS-EN ISO/IEC 27002:2022, 66).

3.6.2 Toteuttaminen

Laaditaan toimintaohjeen organisaation tietoturvallisuuteen liittyville toiminnoille. Ohjeistuksen avulla turvataan oikea toiminta tapa esimerkiksi varmuuskopiointiin, kriisinkestävyyteen, tallennusvälineiden käsittelyyn, huoltoon, vastuussa oleville henkilöille, toiminnon siirrossa, kun toiminto on uusi tai sitä suoritetaan harvoin.

Dokumentoituja toimintaohjeita katselmoidaan ja päivitetään tarpeen mukaan ja niihin tehtävät muutokset valtuutetaan.

4 Turvallisuus- ja hallintatyökalut

DefendByVirtual-ympäristössä on käytössä useita kehittyneitä tietoturva- ja hallintatyökaluja, jotka tukevat omaisuuksien hallintaa, valvontaa sekä tietoturvaan liittyvien poikkeamien käsittelyä. Nämä työkalut varmistavat, että ympäristön keskeiset omaisuudet ovat suojattuina ja hallittavissa.

4.1 Palo Alto (PA-VM)

- **Käyttötarkoitus**: Virtuaalinen palomuuri, joka suojaa tietokoneverkkoja luvattomalta pääsyltä ja haitalliselta liikenteeltä. Sen pääasiallinen käyttötarkoitus on valvoa ja hallita saapuvaa ja lähtevää verkon liikennettä ennalta määriteltyjen turvallisuussääntöjen perusteella. Näin estetään epäluotettavan tai vaarallisen liikenteen pääsyn verkkoon tai sieltä ulos.

- **Miksi työkalu on ympäristössä:** Tärkein puolustuslinja VLE-ympäristön ja ulkoisen verkon välillä. Se valvoo ja rajoittaa liikennettä varmistaakseen, että vain valtuutetut käyttäjät ja palvelut pääsevät verkkoon.

- **Yhteydet:** Yhteydessä kaikkiin verkkoihin (WS-net, Admin-net, Servers-net, DMZ) ja suojaa VLE-ympäristöä ulkoisilta uhkilta.

- **Versio:** PAN-OS 10.1

4.2 Security Onion

- **Käyttötarkoitus:** Tietoturva-alusta, joka keskittyy tunkeutumisen havaitsemiseen (IDS), tapahtumien monitorointiin ja lokien analysointiin.

- **Miksi työkalu on ympäristössä:** Security Onion auttaa havaitsemaan mahdollisia tietoturvapoikkeamia analysoimalla verkon liikennettä ja lokitietoja. Se toimii keskeisenä työkaluna verkon valvonnassa ja poikkeamien havaitsemisessa.

- **Yhteydet:** Yhteydessä Admin-netin kautta muihin verkkoihin ja kerää lokitietoja palvelimista, työasemista ja verkkolaitteista.

- **Versio:** SecurityOnion 2.3.140

4.3 ElasticSIEM

- **Käyttötarkoitus:** Tietoturvainformaatioiden ja tapahtumien hallinta (SIEM). Kerää ja analysoi tapahtumalokeja eri järjestelmistä, sekä käyttää analytiikkaa ja poikkeavuuksien havaitsemista tunnistaakseen epäilyttävää toimintaa ja mahdollisia tietomurtoja reaaliaikaisesti.

- **Miksi työkalu on ympäristössä:** Keskitetty tapa seurata tietoturvatapahtumia eri järjestelmistä. ElasticSIEM tarjoaa tilannekuvan ympäristön tietoturvasta ja auttaa tunnistamaan epäilyttävän toiminnan.

- **Yhteydet:** Yhteydessä kaikkiin verkkoihin (Admin-net, WS-net, Servers-net, DMZ) keräten lokitietoja ja tapahtumia analysoitavaksi.

- **Versio:** Elastic 8.3.3

4.4 Wazuh

- **Käyttötarkoitus:** Avoimen lähdekoodin tietoturva-agentti, joka tarjoaa uhkien havainnointia ja reaaliaikaista valvontaa. On keskeinen osa SOAR-ympäristöjä. Kerää ja analysoi lokitietoja reaaliajassa.

- **Miksi työkalu on ympäristössä:** Wazuh auttaa seuraamaan omaisuuksien turvallisuutta, tunnistamaan uhkia, haavoittuvuuksia ja konfiguraatioon liittyviä ongelmia. Pystyy tunnistamaan ajankohtaisia hyökkäystekniikoita ympäristön komponenteissa.

- **Yhteydet:** Yhteydessä palvelimiin ja työasemiin, kuten WS-netiin ja Servers-netiin, joissa se toimii valvonta-agenttina. Toimii myös osana Admin-nettiä ja on yhteydessä esimerkiksi SIEMiin ja Kali-WS. Analysoi julkisten palvelimien tietoturvauhkia DMZ-verkossa. Voi olla

yhteydessä myös Palo Alto –palomuuriin, jossa se valvoo verkkoliikennettä ja havaitsee haitallisia toimia.

- **Versio:** Wazuh 4.3.6

4.5 Greenbone

- **Käyttötarkoitus:** Haavoittuvuuksien tarkistus- ja arviointityökalu. Skannaa verkkoa, järjestelmiä ja palvelimia löytääkseen tietoturva-aukkoja. Pystyy arvioimaan tietoturvariskien tasoa. Raportoi ja seuraa skannauksia, joista kertoo löydetyt haavoittuvuudet, korjaustoimenpiteet ja riskianalyysit

- **Miksi työkalu on ympäristössä:** Ympäristön haavoittuvuuksien säännöllinen tarkastus on olennainen osa tietoturvaa. Greenbone tarkistaa kaikki ympäristön palvelimet ja verkkolaitteet mahdollisten haavoittuvuuksien varalta. Parantaa seurantaa ja varmistaa, että uudet riskit ja haavoittuvuudet tunnistetaan ja korjataan nopeasti.

- **Yhteydet:** Yhteydessä pääasiassa Servers-net- ja DMZ-verkkoihin, joissa se tarkistaa palvelimia (DC01, WSUS, SRV01, WWW). On asennettu myös Admin-netin Kali virtuaalikoneeseen. Greenbone voi olla yhteydessä esimerkiksi SIEMiin ja SOARiin.

- **Versio:** GVM 21.4.3

4.6 Shuffle

- **Käyttötarkoitus:** Tietoturvatoimintojen automaatioalusta, joka yhdistää eri työkalut ja järjestelmät toisiinsa ja luo automaattisia työnkulkuja tietoturvapoikkeamien käsittelyyn. Mahdollistaa tietoturvatapahtumien toistuvat tehtävät tapahtumien käsittelyssä. Havaitsemisien jälkeen pystyy suorittaa ennalta määriteltyjä vastatoimia.

- **Miksi työkalu on ympäristössä:** Shuffle nopeuttaa tietoturvatoimintoja ja vähentää manuaalista työtä poikkeamien käsittelyssä yhdistämällä SIEMin, SOARin ja muut järjestelmät automaattisiksi työnkuluiksi. Sen avulla yhdistetään eri tietoturvajärjestelmät, kuten

TheHive, Cortex, SIEM ja MISP, jolloin voidaan automatisoida monimutkaisia prosesseja ja parantaa koko ympäristön tehokkuutta.

- **Yhteydet:** Yhteydessä ElasticSIEMiin, SOARiin ja muihin tietoturvatyökaluihin hallintaverkossa (Admin-net).

- **Versio:** Shuffle 1.0

4.7 iTop

- **Käyttötarkoitus:** IT-palveluhallintajärjestelmä (ITSM), joka hallitsee konfiguraatioita ja omaisuuksia. Käytetään IT-infrastruktuurin hallintaan. Tukee palvelupyyntöjen ja tapahtumien hallintaa. Mahdollistaa myös järjestelmien ja laitteiden dokumentoinnin. Pystytään myös hallita ympäristön muutoksia, kuten ohjelmistopäivityksiä.

- **Miksi työkalu on ympäristössä:** iTopin avulla voidaan hallita ympäristön laitteita, ohjelmistoja, konfiguraatioita ja niihin liittyviä tapahtumia. Se antaa näkyvyyden IT-resursseihin ja tukee muutoksenhallintaa. Helpottaa ratkaisemaan ympäristössä ilmeneviä ongelmia.

- **Yhteydet:** Yhteydessä kaikkiin verkkoihin omaisuuden ja konfiguraatioiden hallinnan kautta.

- **Versio:** iTop 3.0.1

4.8 TheHive

- **Käyttötarkoitus:** Tietoturva-analyytikoiden käyttämä tapausten hallinta-alusta, joka käsittelee uhkailmoituksia ja tietoturvapoikkeamia. Mahdollistaa tietoturvapoikkeamien hallinnan ja dokumentoinnin. The Hive on suunniteltu tukemaan tietoturvapoikkeamien käsittelyä ja vastausta järjestelmällisesti ja tehokkaasti.

- **Miksi työkalu on ympäristössä:** Kriittinen työkalu poikkeamien hallinnassa. Se kokoaa ja hallitsee uhkatapahtumia, jolloin tietoturvatiimi voi tehokkaasti tutkia ja reagoida poikkeamiin. Helpottaa tapausten käsittelyä ja dokumentointia. TheHive tarjoaa yhden alustan, jolla pystyy hallita ja reagoida kaikkea verkossa tapahtuvia tietoturvatapahtumia. Se yksinkertaistaa ja vähentää manuaalista työtä.

- **Yhteydet:** Yhteydessä Cortexiin ja muihin uhkatietojärjestelmiin, kuten MISP, hallintaverkossa. Pystyy esimerkiksi integroitumaan Cortex ja MISP kanssa. Voi toimia myös yhdessä SOAR-alustan kanssa.

- **Versio:** TheHive X

4.9 Cortex

- **Käyttötarkoitus:** Automatisoitu tietoturvatietojen analysointialusta, joka suorittaa analyysejä ja tekee johtopäätöksiä. Tekee analyysejä esimerkiksi IP-osoitteille, hash-arvoille ja verkkotunnuksille. Cortex vähentää huomattavasti manuaalista työtä. Cortex käyttää analysoijia “analyzers”, jotka tekevät esimerkiksi virustarkistuksia sekä DNS-tarkistuksia.

- **Miksi työkalu on ympäristössä:** Cortex tekee TheHive-järjestelmän kanssa yhteistyötä ja tarjoaa syvällistä analyysiä tietoturvatapahtumista sekä automatisoi tietojen analysoinnin uhkatietojen perusteella. Cortexin sijainti voidaan määrittää Admin-net verkkoon TheHive:n ja SOAR:n yhteyteen.

- **Yhteydet:** On yhteydessä tiiviisti TheHiveen ja MISP:iin sekä muihin tietoturva-analyysejä tekeviin järjestelmiin, erityisesti hallintaverkossa (Admin-net). Cortex voi integroitua SIEM-järjestelmään.

- **Versio:** 3.1.6-1

4.10 MISP (Malware Information Sharing Platform)

- **Käyttötarkoitus:** Uhkatiedon jakelualusta, joka mahdollistaa tiedon jakamisen, keräämisen ja analysoinnin haittaohjelmista ja tietoturvauhkista. MISP:n avulla uhkatiedon jakaminen keskenään on turvallista ja hallittua. MISP:iä käyttää esimerkiksi viranomaiset, yksityiset yritykset sekä tutkimusyhteisöt. Lisäksi MISP käyttö on täysin ilmaista.

- **Miksi työkalu on ympäristössä:** Tarjoaa mahdollisuuden jakaa ja vastaanottaa ajankohtaista tietoa uusista haittaohjelmista ja uhkista, mikä auttaa suojautumaan ajankohtaisilta uhilta. MISP:n avulla voidaan ennakoida ja estää mahdollisia hyökkäyksiä aikaisessa vaiheessa. MISP on todella yksinkertainen, joten sillä saa helposti kaiken tiedon irti ilman liiallista monimutkaisuutta. Eli tiimimme pysyy tämän avulla ajan tasalla uusista uhista sekä pystymme hallitsemaan tietoturvaan liittyviä haasteita tehokkaammin.

- **Yhteydet:** MISP on integroitu muihin ympäristön järjestelmiin kuten SIEM- ja SOAR-alustoihin. Se mahdollistaa uhkatiedon automaattisen jakamisen näiden palvelujen välillä. MISP on yhteydessä myös TheHive:n ja Cortex:n kanssa. Yhdessä ne tukevat uhkien tutkintaa ja incident management -prosesseja, jolloin uhkiin pystytään reagoimaan nopeasti.

- **Versio:** MISP 2.4.161

5 Pohdinta

Harjoitustyössä tutustuimme ISO 27001 ja ISO 27002 -standardien käyttöön ja soveltamiseen. Opimme laajasti omaisuuksien hallinnasta sekä sen tärkeydestä ja toteutuksesta. Harjoitusta tehdessä syvennyimme entistä enemmän ympäristömme toimintaan ja sen sisältämiin työkaluihin sekä omaisuuksien hallinnan tärkeyteen.

Tehtävä oli hyvä ensikosketus standardien käyttöön ja olennaisuuteen. Aluksi oli vaikea hahmottaa tehtävänantoa ja kokonaiskuvaa, tämä kuitenkin selvisi, kun jaksoi syventyä tehtävään. Standardien laajuus myös loi epävarmuutta aluksi, mutta kun jakoi kokonaisuuden sopiviksi palasiksi, niin homma alkoi sujua mutkitta. Jatkossa kyseiset tehtävät on varmasti helpompi ymmärtää ja lähteä toteuttamaan.

Lähteet

SFS-EN ISO/IEC 27001:2023. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 4.8.2023. Viitattu 8.10.2024. https://janet.finna.fi/, SFS online

SFS-EN ISO/IEC 27002:2022, Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 18.11.2022. Viitattu 8.10.2024. https://janet.finna.fi/, SFS online

Liitteet

Liite 1. Omaisuuserät

AssetManagement