

Jussi Tarkkonen

Windows-päätelaitteen tietoturvan kovennus ja auditoitavuus

Tekniikan ylempi ammattikorkeakoulututkinto

Kyberturvallisuuden koulutus

2024



Kaakkois-Suomen
ammattikorkeakoulu

Tutkintonimike	Insinööri (ylempi AMK)
Tekijä	Jussi Tarkkonen
Työn nimi	Windows-päätelaitteen tietoturvan kovennus ja auditoitavuus
Toimeksiantaja	Verohallinto, Turvallisuus ja Riskienhallintayksikkö
Vuosi	2024
Sivut	78 sivua, liitteitä 93 sivua
Työn ohjaajat	Kimmo Kääriäinen, Vesa Kankare

TIIVISTELMÄ

Tässä opinnäytetyössä pyrittiin selvittämään toimeksiantajan työasematurvallisuudessa kokemat ongelmat ja kehitystarpeet. Tutkimusongelma rajattiin koskemaan Windows-työaseman tietoturvan järjestelmällistä kovennusta, hyödyntäen parhaita käytäntöjä tai tietoturvakehyksiä. Lisäksi tavoitteena oli varmistaa päätelaitetietoturvan tilannekuva ja auditoitavuus, koska johdon kokema näistä oli epäselvä. Esitutkimuksessa arvioitiin myös, että tutkimusongelmaan liittyvät käsitteet ja syyt olivat organisaatiossa jäsentymättömiä ja epäselviä.

Tavoitteeksi asetettiin kirjallisen konstruktion ja intervencioehdotuksen laatiminen toimeksiantajan käyttöön. Tutkimuksen sekundäärisenä tavoitteena oli tutkia, voisiko tutkimuksen pohjalta toteuttaa työkalun, jonka avulla organisaatiot voisivat arvioda oman työasematurvallisuutensa kehityksen resurssivaatimuksia ja sidonnaisuuksia tietoturvan osa-alueisiin nähden. Tutkimusotteeksi valittiin laadullinen kehittämistutkimus, sisältäen monimenetelmällisiä toteutuskeinoja. Toimeksiantajan työasematurvallisuuden kehitykseen osallistuttiin havainnoinnin keinoin yhdeksän kuukauden jakson ajan, jonka lisäksi organisaation asiantuntijoita ja ulkopuolista tietoturva-eksperttiä haastateltiin. Työkalujen kokeilulla varmennettiin lisäksi tutkimusaineistoista nousseet havainnot.

Tutkimuksen johtopäätöksissä todettiin, että työaseman tietoturvan koventaminen on monivaiheinen ja erityistä asiantuntemusta vaativa työ. Windows-käyttöjärjestelmä ei sovellu yrityskäyttöön oletusasennuksena, vaan sen konfiguraatio täytyy koentaa, jossa apuna voidaan käyttää siihen tarkoitettuja tietoturvakehyksiä. Tietoturvakehysten käytöllä ei kuitenkaan varmisteta käytännön tietoturvallisuutta, vaan lisäksi tarvitaan uhkien ja riskien hallintaa, jatkuva testaamista ja konfiguraatiohallintaa sekä tietoturvalvontan yhteistoimintaa. Tutkimuksen perusteella aihealue vaatii merkittävästi lisäkehitystä holistisen työasematurvallisuuden mallin rakentamiseksi.

Tutkimuksen päätuotoksesta on taulukkohojainen työasematurvallisuuden käyttöönottomalli, joka sisältää toimeksiantajan intervencioehdotuksen. Ehdotusta tukee kirjallinen konstruktio, joka sisältää kattavan vertailun tietoturvakehysistä, työaseman tietoturvakovenkuksista sekä työkaluista.

Asiasanat: tietoturva, työasema, tilannekuva, auditointi, hyvät käytännöt

Degree title	Master of Engineering
Author	Jussi Tarkkonen
Thesis title	Hardening and auditability of Windows endpoint security
Commissioned by	Finnish Tax Administration, Department of Security and Risk Management
Time	2024
Pages	78 pages, 93 pages of appendices
Supervisors	Kimmo Kääriäinen, Vesa Kankare

ABSTRACT

This thesis aimed to investigate the problems and development needs experienced in the commissioner's workstation security. The scope of the study was limited to systematic hardening of Windows workstation security using best practices or security frameworks. Additionally, the objective was to examine methods to ensure endpoint security status and auditability. It was understood at the start of the study that despite external auditing of workstation security, the management's perception of endpoint security status remained unclear. The primary objective was focused on creating an intervention proposal, including a synthesized background paper for the commissioner's use. A secondary objective, not within the commissioner's scope, was to explore the possibility of designing a tool that would help organisations assess the development requirements and dependencies of their workstation security.

In this thesis, a qualitative multimethodological design-based approach was chosen. The commissioner's workstation security development was observed over a nine-month period, and interviews were conducted with in-house experts and an external cybersecurity expert. Additionally, the findings from the data were validated through tool experimentation.

The main outcomes from this study were a spreadsheet-based model for implementing workstation security, an intervention proposal for the commissioner, including a synthesized background paper containing a comprehensive comparison of security frameworks, hardening techniques, and tools.

It was concluded in the study that the Windows operating system is not suitable for enterprise use in its default configuration, and therefore it requires hardening, possibly by using a dedicated security framework and specialized expertise. However, the use of security framework alone does not ensure practical security, which in addition requires continuous testing and threat, risk and configuration management. Close collaboration with security monitoring is also necessary. Thus, organisations should prefer a holistic security model for governing workstation security.

Keywords: security, hardening, testing, auditing, frameworks, best practises

SISÄLLYS

1	JOHDANTO	7
2	TUTKIMUSASETELMA	9
2.1	Tutkimusongelma	10
2.2	Tutkimuskysymykset.....	12
2.3	Tutkimuksen tavoitteet.....	13
2.4	Tutkimusote	14
2.5	Tutkimusmenetelmät	16
2.6	Tutkimuskohde	23
3	TEOREETTINEN VIITEKEHYS.....	24
3.1	Avainkäsitteiden ja teorioiden määrittely.....	24
3.2	Käsitteiden valinta ja perustelut	30
4	TYÖN TOTEUTUS	30
4.1	Sekundäärisen aineiston haku.....	32
4.2	Teemahaastattelut, havainnointi ja kokeilut	40
4.3	Kirjallinen konstruktio ja käyttöönottomalli	41
5	TUTKIMUSTULOKSET	42
5.1	Windows-työaseman tietoturvan kovennus	42
5.2	Windows-työaseman käytännön tietoturva ja uhkat.....	49
5.3	Windows-työaseman auditointavuus ja tilannekuva.....	55
5.4	Windows-työasematurvan määrämuotoinen hallinta	58
5.5	Interventioehdotuksen esittely	62
6	JOHTOPÄÄTÖKSET	64
6.1	Analyysi Windows-työaseman tietoturvan kovennuksesta.....	64
6.2	Analyysi Windows-työaseman käytännön tietoturvasta ja uhkista	65
6.3	Analyysi Windows-työaseman auditointavuudesta ja tilannekuvasta	66
6.4	Analyysi Windows-työasematurvan määrämuotoisesta hallinnasta.....	66
7	POHDINTA	67

7.1	Luotettavuus- ja eettisyystarkastelu.....	68
7.2	Jatkotutkimusaiheet.....	69
7.3	Loppusanat.....	70
	LÄHTEET.....	71

KUVALUETTELO

TAULUKKOLUETTELO

LIITTEET

- Liite 1. Kokeilupöytäkirjat
- Liite 2. Työasematurvallisuuden teemoitellut havainnointi
- Liite 3. Haastatteluaineiston teemoittelut
- Liite 4. Tutkimustuloksissa hyödynnettyt aineistot
- Liite 5. Kirjallinen konstruktio
- Liite 6. Työasematurvallisuuden käyttöönottomalli
- Liite 7. Julkisuuslain mukaan salattu havainnointiaineisto

KÄSITTEET JA LYHENTEET

Auditointi	Järjestelmän sisäinen tai ulkopuolinen tarkastus sen varmistamiseksi, että se noudattaa vaatimuksia ja toimii tehokkaasti.
CIS	Center for Internet Security. Voittoa tavoittelematon yhteisö-pohjainen parhaiden tietoturvakäytäntöjen kehittäjä.
DISA	Defense information systems agency. Yhdysvaltain puolustusministeriön alainen virasto, joka kehittää tietoturvakehyksiä.
Kyberturvallisuus	Kokonaisvaltainen lähestyminen tietojärjestelmien suojaamiseen luvattomalta käytöltä, muutoksilta tai tuhoamiselta.
NIST	National institute of standards and technology. Yhdysvaltain liiketoimintaministeriön alainen virasto.
Päätelaite	Verkkoon liitetty tietokone tai muu laite.
Penetraatiotestaus	Teknisen testauksen muoto, jolla pyritään löytämään haavoittuvuuksia tietojärjestelmistä.
Tietoturvakehykset	Joukko ohjeita ja parhaita käytäntöjä, joita voidaan käyttää tietoturvan parantamiseksi.
Tietoturvakovennus	Prosessi, joka sisältää yksityiskohtaisia teknisiä määritlyksiä, joiden avulla pyritään vähentämään tietoturvariskejä vahvistamalla järjestelmän puolustuskykyä.
Tietoturvariski	Todennäköisyys sille, että tietoturvauhka toteutuu ja aiheuttaa vahinkoa.
Tietoturvauhka	Mahdollinen vaaratekijä, joka voi vahingoittaa tietojärjestelmiä tai tietoja.
Tilannekuva	Liittyy organisaation ymmärrykseen tietoturvauhkista ja -riskeistä sekä niihin liittyvistä suojaustoimista.
Työasema	Viittaa terminä tietokoneeseen, jota käytetään työhön.
Vaatimustenmukaisuus	Liittyy lakiin, sääntöjen tai sopimusten vaatimusten täyttämiseen.
Virhekonfiguraatio	Virheellinen määritys, joka voi vaarantaa järjestelmän tietoturvan.
Windows-ympäristö	Tarkoittaa Microsoft Windows -käyttöjärjestelmän käyttöä yritysympäristössä.

1 JOHDANTO

Organisaatioissa ja yksityiskäytössä on nykyään hyvin yleistä, että suurin osa työasemista, jopa 73 %, on Windows-pohjaisia (Dunkerley & Tumbarello 2022, 7). Yrityskäytössä suurella osalla Microsoftin teknologioita hyödyntävistä organisaatioista alkaa olla myös pitkä kokemus päätelaitteiden sekä tietoturvan hallinnasta. Käyttöjärjestelmäversioiden uudet ominaisuudet ja muutokset, protokollien ja sovellusten kehitys sekä prosessien muutokset ovat kuitenkin asioita, joita voi olla pitkällä aikavälillä vaikea hallita niiden monimutkaisuuden takia. Toisaalta myös työasemien hallinta ja tietoturvan koventaminen on muuttunut automaation ja pilvipalvelupohjaisten järjestelmien myötä. Tietoturvakehykset ja parhaat käytännöt ovat myös kehittyneet valtavasti vuosien aikana. (Mistry ym. 2018).

Ongelmia työasematurvallisuudessa saatetaan korjata pistemäisesti ja konkreettinen määrämuotoinen tapa tehdä asioita puuttuu. Usein organisaation päätelaitetietoturva on hoitanut monta eri tekijää, monilla eri tavoilla ja välineillä. Ylläpitäjät, jotka ovat jossain kehitysvaiheessa tehneet työasemamääritykset (sekä tietoturvan kovennukset), eivät enää ole käytettävissä, tai vaikka olisivatkin, ei tehdystä toimista ole vältämättä riittävä dokumentaatiota. Monissa organisaatioissa ei ole vältämättä käytössä riittävästi (osaavia) resursseja, mikä väistämättä johtaa kiireeseen, puuttuviin prosesseihin, järjestelmällisen hallintamallin puutteeseen tai perustelemattomiin sekä hätäisiin päätöksiin. Teknisen tietoturvavelan kerääntyminen alkaa johtuen em. puutteista ja pahimmillaan johtaa isoihin puutteisiin turvallisuudessa (Csoonline 2021).

Tämä opinnäytetyö pyrki löytämään toimeksiantajan käyttöön tutkimuksellisin keinoin perustellun tietopohjan, joka esittelee työasematietoturvan parhaita käytäntöjä sekä tietoturvakehyksiä, joiden avulla voitaisiin ratkaista ongelmat organisaation Windows-työaseman tietoturvallisuuden määrämuotoisen kovettamisen ja auditointivuuden kanssa. Toimeksiantajana on Verohallinnon riskienhallinta ja turvallisuusyksikkö, jonka tavoitteena on hyödyntää tutkimuksen tuloksia pohjana työasematurvallisuuden hallintamallissa (eng. governance model). Ilman tämän tutkimuksen tuloksia työasematurvallisuuden kehittämistä jouduttaisiin jatkamaan ns. artesaanityönä. Tällä hetkellä

työasematurvallisuuden tilan raportointi johdolle on hankala pirstaloituneen tiedon takia, mutta tilannekuva pyritään parantamaan hallintamallin käyttöönoton avulla. Toimeksiantaja tavoittelee hallintamallin käytöllä myös työasematurvallisuuden auditointiin tarvittavan manuaalisen tiedonkeruuvaheen minimoitria, ja sitä kautta kustannuksia.

Opinnäytetyön tekijän omana mielenkiinnon kohteena oli tutkia samalla, voidaanko työasematurvallisuuden kehitystä helpottaa jonkinlaisella yleistetyllä käyttöönottomallilla. Mallia hyödyntäen organisaatiot saisivat paremman käsityksen työasematurvallisuuden parannukseen liittyvistä osa-alueista ja vaatimuksista.

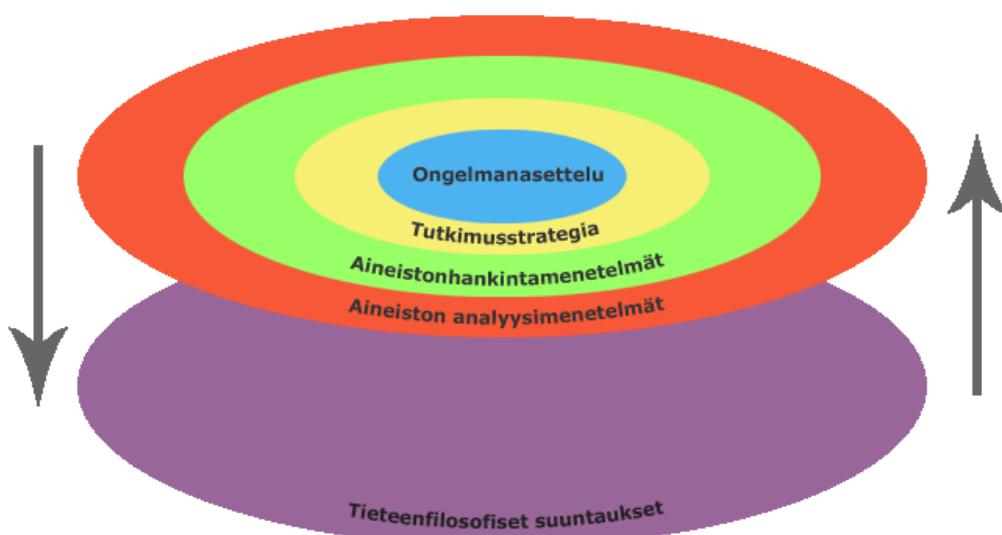
Tiedonhaku paljasti, että Suomessa tehdyt aihealueen tutkimukset ovat eri tasoisten opintojen lopputöitä (Mäntylä 2020, Clark 2020, Siik 2017), joissa sivutaan tämän työn aihealueita, mutta pääsääntöisesti keskitytään eri tasoisten ja eri tarpeista lähtevien kovennusten toteutukseen. Kansainvälisti aihealueesta löytyi runsaasti tutkimuksia ja kirjallisuutta (mm. Zamora ym. 2019; Mistry ym. 2018; Hamdani ym. 2021; Duncan & Whittington 2014), joissa vertaillaan eri kehysten käyttöä tietoturvan kovennuksissa, auditoinnissa tai tuodaan esiin näkökulmia kovennukseen kuuluvista alueista ja niiden automatisoinneista. Aiempien tutkimusten sekä ammattikirjallisuuden (mm. Redswitches 2023, Cimcor s.a, Cyphere 2021, Intel 2023 ja Beyondtrust 2023) hajanaisuus perustee tässä työssä luotavan kattavan kirjallisen konstruktion ja sen pohjalta tehtävän interventioehdotuksen, jonka avulla tutkimus voi parhaiten palvella toimeksiantoa ja toimia pohjana kehittämispäätöksille toimeksiantajan organisaatiossa.

Opinnäytteen tekijä työskentelee toimeksiantajan organisaatiossa tietoturva-arkkitehtinä, teknisissä asiantuntijatehtävissä. Toimeksiantajan tehtävänä on varmistaa Verohallinnon tietoteknisen ympäristön tietoturvallisuus. Tutkimuksen tuloksilla voidaan täten todeta olevan vähintään kansallista yhteiskunnallista merkitystä. Työaseman tietoturvan kovennus ja auditointi ovat kyberturvallisuuden osa-alueita ja tämä opinnäytetyö kuuluu kyberturvallisuuden alaan.

2 TUTKIMUSASETELMA

Tutkimusasetelman kirjoittaminen opinnäytetyön rakenteeseen kuuluu osaksi raportointia, jolla pyritään vastaamaan kysymyksiin mitä, miten ja miksi tutkimusprosessi on edennyt tietyllä tavalla. Tutkimusasetelmassa kerrotaan juuri tämän tutkimuksen tutkimusongelmasta, -kysymyksistä, -tavoitteista, -otteesta sekä -menetelmistä (Kananen 2015, 19–21; Jyväskylän yliopisto 2014). Laadullisen tutkimuksen tutkimusasetelma on joustava, joten esimerkiksi teoreettisen viitekehyn esittelemät peruskäsitteet voivat kuulua osaksi tutkimusasetelmaa. Tutkija vastaa myös tutkimuksen eettisyydestä, ts. siitä, että tutkijan ennakkoolettamat tai työhypoteesit ja tutkimuksen kulku kerrotaan läpinäkyvästi tutkimusasetelmassa. (Ronkainen ym. 2011, 63–70; Cheek 2012; Puusa & Juuti 2020, 76–77; Tuomi & Sarajärvi 2018, 18–22; Eskola & Suoranta 1998, 11–17).

Opinnäytetyö kirjoitetaan korkeakouluissa aina samaa rakennetta noudattaen, joka takaa samalla, että tieteellisyyden vaatimukset on otettu huomioon työssä. Hyvä tutkimusasetelma toimiikin siten suunnitelmana, jonka avulla itse tutkimusprosessia voidaan lähteä toteuttamaan. Tutkimusasetelmassa määritetyjen menetelmien valinta vaikuttaa koko tieteellisen tutkimuksen prosessiin. Tutkimuksen suhdetta menetelmien valintaan on havainnollistettu kuvassa 1.



Kuva 1. Tutkimusasetelma (Jyväskylän yliopisto 2014)

Tutkimusmenetelmien huolellisella valinnalla pohjustetaan myös tutkimuksen analyysivaihetta ja vältetään siinä umpikujaan ajautuminen. Ennen tutkimusasetelman kirjoittamista tutkijan pitää perehtyä aihealueen kirjallisuuteen ja tutkimuksiin sekä kartoittaa mahdollisia aineistoja. (Kananen 2015, 19–21, 85; Jyväskylän yliopisto 2014, menetelmäpolku, tutkimuksensuunnittelu; Tuomi & Sarajärvi 2018, 54–57).

2.1 Tutkimusongelma

Kanasen (2014) mukaan "tutkimusongelman tarkka määrittely on työn alussa usein vaikeaa ja on olemassa jopa tapauksia, joissa tutkimusongelma voidaan kirjoittaa viimeisenä johdannon kanssa". Tieteelliseen työhön, kuten opinnäytetyöhön kuuluu kuitenkin aina tutkimusongelma, joka täytyy määritellä erikseen. Tutkimusongelmaa selvittäessä sitä tulee rajata, muttei liian aikaisessa vaiheessa, jottei jouduta umpikujaan aiheen käsittelyn kanssa. Tutkimusongelma selviää lopulta tutkimalla kerääntyvästä aineistosta ja tekemällä selkeän valinnan mitä ilmiön osa-aluetta tutkimus tulee käsittelemään. (Kananen 2014, 32–34; Pitkäranta 2014, 59–61).

Rajaaminen helpottaa niissä valinnoissa, mitä opinnäytetyöhön kuuluu, mutta myös siinä, mitä jätetään pois, koska muutoin opinnäytetyön tutkimusaiheesta tulee helposti liian laaja. Tutkijan tulee myös asettaa ongelma niin, että se on ratkaistavissa. Rajaamisella tai fokusoinilla varmistetaan työn kannalta riittävä tiedonsaanti, joka tukee tieteellisten aineistojenkeruu- ja analyysimenetelmien käyttöä (Kananen 2015, 32–34,41; Pitkäranta 2014, 60–63).

Käytännön toimeksiantoissa tutkimuksen rajaamattomuus voi myös vaatia merkittävästi esitutkimusta aidon ongelman esiin saamisessa. Ongelmanasettelua voi lähestyä myös tavoitekuvausten kautta, ts. miettiä, millaista tietoa tutkimuksella itse asiassa haetaan. Asettamalla tavoitteita voidaan niistä johtaa myös tutkimusongelma (Kananen 2015, 45–47,51; Pitkäranta 2014, 69–71; Jyväskylän yliopisto 2014). Ongelmanasettelun tavoitteita on havainnollistettu kuvassa 2.



Kuva 2. Ongelmanasettelun tavoitteet (Jyväskylän yliopisto 2014)

Ongelmanasettelun tavoitteista tunnistettiin kolme tavoitetta, joiden kautta tutkimusongelmaa lähdettiin rajaamaan tarkemmin: **ilmiöön vaikuttavien taustojen selvittäminen, teorian muodostaminen sekä ilmiön kuvaaminen ympäristössään**. Tämän työn tutkimusongelman rajaus vaati merkittävästi esitutkimusta ja fokusoitui toimeksiantajan kanssa käytyjen iteratiivisten suunnittelupalavereiden avulla. Tutkimusongelma rajautui työasemien tietoturvakovenusten järjestelmällisen kovettamismenetelmän ja työkalujen puutteeseen sekä auditointeihin käytettävän manuaalisen tiedonkeruun resurssihaasteisiin. Toimeksiantaja esitti lisäksi huolenaiheekseen päätelaitetietoturvan tilannekuvan tai raportoinnin vajavaisuuden.

Tutkimusongelma rajattiin käymällä dokumentaatiota läpi, haastattelemalla organisaation asiantuntijoita, sekä havainnoimalla työprosesseja. Työasemien teknisen tietoturvan todettiin dokumentaation sekä edellisen auditointiraportin perusteella olevan kiitettävällä tasolla, joten päädyin rajaamaan suorat teknisten ominaisuuksien parannustoimet tutkimuksen ulkopuolelle. Tutkimusongelman lopullinen asettelu sisältää toimeksiantajan edustajan ja tutkijan ammatilliseen kokemukseen pohjautuvan työhypoteesin mahdollisesti ongelman korjaavista toimista. Puusan ja Juutin mukaan laadullisissa tutkimuksissa voidaan esittää hypoteeseja, joita tutkija testaa tulkitsemalla aineistoa analyysin, synteesin ja johtopäätösten avulla (Puusa & Juuti 2020, 76–77).

Näiden rajausten perusteella **tutkimusongelmaksi määriteltiin** Windows-työaseman tietoturvan järjestelmällinen kovennus hyödyntäen parhaita käytäntöjä ja tietoturvakehyksiä, varmistaen samalla auditoitavuus ja päätelaitetietoturvan tilannekuva. Tutkimusongelma tuntui mielenkiintoiselta, koska oma työura on pääosin rajoittunut teknisten tietoturvaominaisuksien käyttöönnottoon ja ylläpitoon.

2.2 Tutkimuskysymykset

Tutkimusongelman ratkaisemista auttaa siitä johdettavat tutkimuskysymykset, koska kysymyksiin on helpompi vastata kuin itse ongelmaan.

Tutkimuskysymykset ratkaistaan aineiston avulla. Jokaisen kysymyksen on jollain tavoin palveltava itse ongelman ratkaisua, muutoin kyseinen kysymys on turha. Opinnäytetöissä voidaan käyttää eritasoisia kysymyksiä, eri tarkoituksiin ja ne toimivatkin tutkijan työkaluina. Kysymykset voivat olla yleisluontoisia, tai yksityiskohtaisia. (Kananen 2014, 35–41; Vilkka 2023, 36–44)

Tutkimuskysymyksiä voi olla yksi tai useampia, joista osa voi toimia apukysymyksinä (metakysymykset), joilla tuotetaan tietoa varsinaiselle tutkimuskysymykselle. Hyvin määritellyt tutkimuskysymykset ohjaavat tutkimusta ja aineistonkeruuta. Apukysymykset sisältävät yleensä mitä, kuka, milloin, missä, miten -kysymystyyppejä, mutta ne eivät voi vastata tutkimuskysymykseen, jollei se itsessään ole mitä?-muotoinen. Laadullisissa tutkimuksissa, joihin tämäkin tutkimus kuuluu, voidaan hyödyntää myös teemakysymyksiä, joita hyödynnetään teemahaastatteluissa.

Teemakysymykset rakennetaan vasten tutkimusta varten asetettuja tutkimuskysymyksiä ja tutkimusongelmaa. (Kananen 2015, 55–59; Vilkka 2023, 36–44; Eskola & Suoranta 1998, 63–67)

Opinnäytetyön tutkimuskysymykset aseteltiin taulukon 1 mukaisesti.

Taulukko 1. Tutkimuskysymykset

Kysymys	Tyyppi
1. Mitkä tietoturvakehykset ja parhaat käytännöt tai niiden osat ovat soveltuivia Windows-työaseman tietoturvan koventamiseen?	Pääkysymys
2. Ovatko parhaiden käytäntöjen ja tietoturvakehysten suositukset ajantasaisia ja kattavia Windows-työaseman käytännön tietoturvan ja uhkien kannalta?	Apukysymys
3. Mahdollistaako parhaisiin käytäntöihin ja tietoturvakehykseen perustuva Windows-työaseman kovennus auditoitavuuden ja organisaatiotasoinen päätelaitetietoturvan tilannekuvaan?	Pääkysymys
4. Miten Windows-työaseman tietoturvaa ja auditoitavuutta voi hoitaa hallitusti ja määrämuotoisesti?	Apukysymys

2.3 Tutkimuksen tavoitteet

Tutkimuksen tärkeimpänä tavoitteena on tuottaa organisaatiolle tutkimuksen kautta kattava kirjallinen konstruktio ja analyysi tunnistetun ongelman ratkaisevista käsitteistä ja niiden välisistä suhteista. Tämä konstruktio ja siitä tehty analyysi muodostavat toimeksiantajalle mallin Windows-työasematurvallisuuden järjestelmälliseen kovettamiseen. Tutkimus tavoittelee sitä, että toimeksiantaja voi aloittaa tutkimuksen jälkeen tutkijan avustuksella kehittämistyön (interventio) tutkimusongelman korjaamiseksi. Tutkimuksen aikana ei ole siis tarkoitus toteuttaa lopullista kehittämistyötä, vaan intervencio esitellään ilman muutossyklia tai ongelman poistavaa

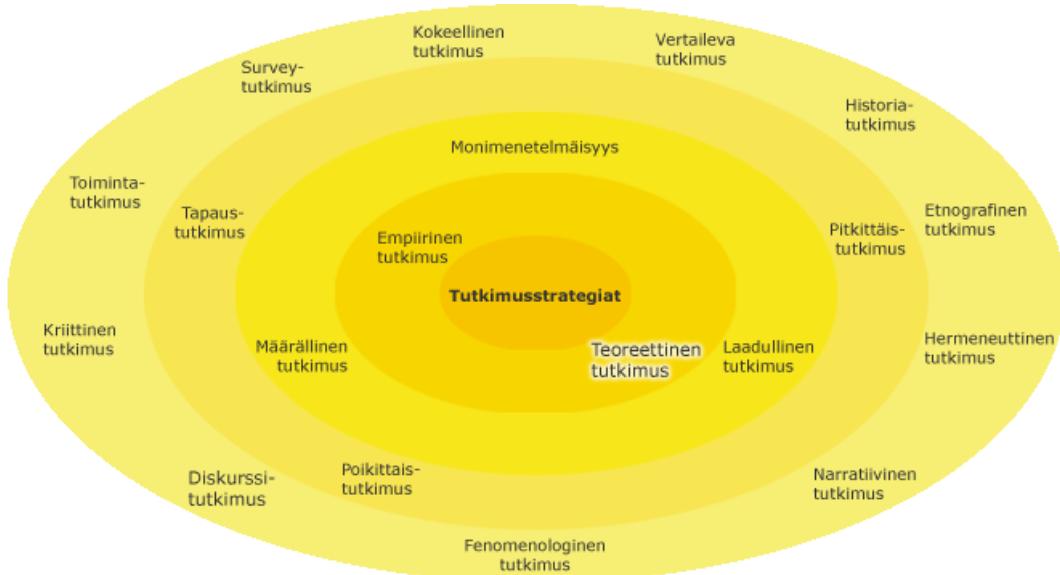
vaihetta. Tämä esiteltävä tutkimussyyklin mukainen ongelmanratkaisun interventio riittää Kanasen mukaan siihen, että voidaan todeta tutkimuksessa olevan kehittämistutkimuksen piirteitä. Kehittämistutkimuksen päätavoitteena on tuottaa toimivia käytännön ratkaisuja. (Kananen 2019, 82; Kananen 2015, 19; Puusa & Juuti 2020, 9–14).

Tavoitteen asettaminen tutkimusasetelmassa on Kanasen mukaan haasteellista, mutta se voidaan lisätä mukaan silloin, kun kyseessä on interventionistinen tutkimus (Kananen 2019, 24). Sekundäärisenä tavoitteena on tutkia voitaisiinko tutkimuksen pohjalta toteuttaa työkalu, jonka avulla eri organisaatiot voivat arvioida oman työasematurvallisuutensa kehityksen resurssivaatimuksia ja sidonnaisuuksia eri tietoturvan osa-alueisiin nähdien.

2.4 Tutkimusote

Tutkimusongelman ja kysymysten määrittelyä seuraa tutkimusotteen eli tutkimuksessa käytettävän metodologian valinta. Tutkimusongelman ratkaisuun tähtäävää kokonaisuutta voidaan nimittää myös lähestymistavaksi. Tehdyt valinnat tulee perustella, kuten tieteelliseen työhön kuuluu ja valittavan menetelmän tulee tuottaa ongelman ratkaisun kannalta oikeaa tietoa. (Kananen 2015, 63–64; Kananen 2019, 25; Pitkäranta 2014, 69–74).

Jyväskylän yliopiston (2014) menetelmäpolun ohjeistuksen mukaan ongelmanasettelu ohjaa valittavan tutkimusstrategian ja menetelmällisten ratkaisujen kokonaisuutta. Tutkimusstrategiat voidaan jakaa mm. havainnointitavan mukaan joko empiiriseksi tai teoreettiseksi tutkimukseksi. Teoreettinen tutkimus ei havainnoin tutkimuskohteita suoraan, vaan aiemman tutkimuskirjallisuuden kautta. Empiirinen tutkimus kerää tutkimustulosia konkreettisten havaintojen pohjalta ja koottu tutkimusaineisto on olennainen osa tutkimusta. Monimenetelmäisyys on myös mahdollista. Tämä tarkoittaa sitä, että tutkittavan kohteen ongelman ratkaisussa voidaan hyödyntää erilaisia aineistonkeruu ja -analysointimenetelmiä. Tutkimusstrategiat on esitelty kuvassa 3. (Jyväskylän yliopisto 2014; Puusa & Juuti 2020, 19–24).



Kuva 3. Tutkimusstrategiat (Jyväskylän yliopisto 2014)

Tutkimusotteet voidaan jakaa karkeasti kvalitatiivisiin tai kvantitatiivisiin tutkimuksiin (laadullinen tai määrellinen). Kvalitatiivinen tutkimus pyrkii ongelman ratkaisuun ilmiön ymmärtämisen kautta raamittamalla ilmiöön vaikuttavat tekijät, kun taas kvantitatiivisen tutkimuksen edellytyksenä on ilmiön tunteminen, jolloin sitä voidaan mitata kyselyn ja tilastollisten menetelmien kautta. Laadullinen tutkimus perustuu sanoihin ja lauseisiin, eikä hyödynnä tilastollisia menetelmiä tai määrellisiä keinoja. Määrellisten tutkimusten takana on yleensä aina laadullinen tutkimus, vaikkakin määrellinen tutkimus perustuu lukuihin. (Kananen 2019, 25–27; Kananen 2015, 63–73; Kananen 2012, 29–31; Eskola & Suoranta 1998, 11–17).

Tutkimusotteen voi tunnistaa myös tutkijan roolin kautta, joka laadullisessa tutkimuksessa on ulkopuolinen osallistuja, kun taas määrellisessä ulkopuolinen havainnoija. Tutkimusongelma voi liittyä myös jonkin asian kehittämiseen tai muutoksen aikaansaamiseen (interventio). Tällaista tutkimusta voidaan nimittää kehittämis-, toiminta- tai konstruktiviseksi tutkimukseksi. Kehittämis- ja toimintatutkimuksen ero on hyvin pieni, varsinkin koska kummankin lopputulokset voivat jäädä toteavalle, tai suositusten tasolle ilman muutokset toteuttavaa sykliä. Toimintatutkimuksen kohteena ovat lähes aina ihmiset ja heidän toimintansa. Toimintatutkimus voidaan tunnistaa myös siitä, että tutkija on mukana testaamassa ratkaisun toimivuutta, kun taas kehittämistutkimus ei edellytä tutkijan mukanaoloa. Kehittämistutkimuksen vaiheet etenevät nykytilan kartoituksesta, ongelmatalanteen analyysiin,

synteesiin tai interventioehdotukseen, kokeiluun, arvointiin ja lopulta seurantaan. (Kananen 2019, 25–27; Kananen 2015, 63–73; Kananen 2012, 27,38–44,52–54; Tuomi & Sarajärvi 2018, 47–59).

Tutkimusongelman, kysymysten ja tavoitteenasettelun kautta tämän tutkimuksen tutkimusotteeksi valikoitui **laadullinen kehittämistutkimus**. Perusteluna valinnalle on tutkijan toimiminen aineiston kerääjänä, tutkimusaineiston monilähteisyys, tutkimuksen tapahtuminen toimeksiantajan ympäristössä sekä tavoite kokonaisvaltaisen tai holistisen näkemyksen saamiseksi tutkittavasta ilmiöstä (Kananen 2019, 76).

Työn tavoitteena ilmiön kuvauksen lisäksi on ongelman ratkaisu, joka vaatii tutkimuksen lisäksi toimintaa ja pyrkii **interventioon** eli muutokseen. Tässä tutkimuksessa on siten sekä toimintatutkimuksen että kehittämistutkimuksen piirteitä, koska tutkijan rooli vaihtelee tutkimuksen aikana itsenäisen työskentelyn ja osallistuvan havainnoinnin välillä. Tutkimuksessa on myös konstruktivisia näkökulmia, koska yhtenä tavoitteena on kirjallinen konstruktio, joka toisaalta puolataa tutkimuksen määritystä monimenetelmäiseksi tutkimukseksi. Tutkimus sisältää tutkijan havainnointia, teknistä kokeilevaa testaamista sekä menetelmällistä kehittämistä organisaation tarpeisiin. Työn tavoitteiden saavuttaminen ei edellytä määrällistä tutkimusta, vaan tutkimus sisältää käytännössä pelkästään laadullisia piirteitä.

2.5 Tutkimusmenetelmät

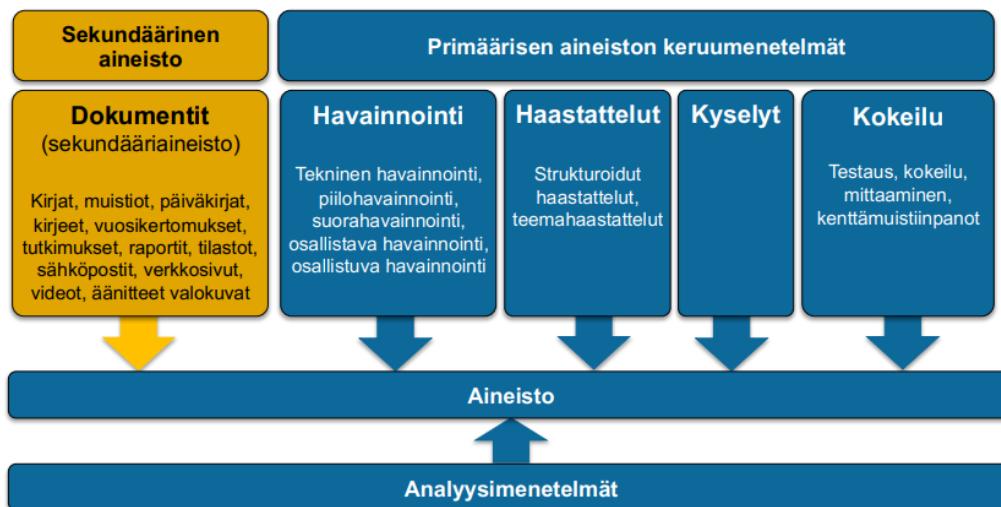
Tutkimusmenetelmien, kuten aineistonkeruu-, analyysi- ja luotettavuusmenetelmien valinta on tärkeä tehdä oikein, jotta niillä voidaan tuottaa tutkimusongelman ratkaisun kannalta relevanttia aineistoa. Tieto kerätään järjestelmällisesti ja järkiperäisesti, hyödyntäen tieteellisiä menetelmiä. Kerätty aineisto jalostetaan tiedoksi, jonka avulla tutkimusongelma ratkaistaan analyyttisellä menetelmällä varmistaen lopulta tehty työ luotettavuusmenetelmiä käyttäen (Kananen 2019, 27–30; Kananen 2015, 80–84; Salminen 2023, 7–11).

Aineistonkeruumenetelmät

Laadullisen tutkimuksen aineistonkeruumenetelmiä ovat dokumentit, havainnointi ja haastattelut. Näistä dokumentit ovat sekundääristä aineistoa, joka tarkoittaa olemassa olevaa tietoa, kuten tekstiä, kuvia, äänitteitä tai videoita. Primäärisen aineisto muodostuu havainnoinnin, haastattelujen, kyselyiden ja kokeilun avulla tutkimusta varten kerätystä tiedosta.

Dokumenttipohjainen aineisto voidaan jakaa karkeasti neljään eri tyyppiin: tutkimustieto, ammatillinen tieto, virallistieto ja yleistieto.

Aineistonkeruumenetelmiä on havainnollistettu mukautetussa kuviossa 4, joka on jaettu sekundäärisen aineiston ja primäärisen aineiston keruumenetelmiin. (Kananen 2019, 28–29; Kananen 2015, 80–82; Vilkka 2023, 17–29; Pitkäranta 2014, 90–97; Xamk s.a.a, aineiston keruu).



Kuva 4. Aineistonkeruumenetelmiä (Xamk s.a.a, mukaillen Kananen 2017; Jyväskylän yliopisto 2014)

Tämä tutkimus yhdistää empiiristä ja teoreettista tutkimusta, joka vaatii sekä sekundäärisen että primäärisen aineiston keruumenetelmiä. Valitut aineistotyypit ja niitäh vastaavat keruumenetelmät ja hypoteesi oletettavasta aineistosta on kuvattu taulukossa 2.

Taulukko 2. Tutkimuksen aineistonkeruumenetelmät

Keruumenetelmä	Tarkenne	Oletus aineistosta
Dokumentit (sekundääriinen aineisto)	Tiedonhaku Xamk:in tietokantojen avulla, google scholar, sekä vapaan verkon haut.	Tutkimukset, kirjat, verkkosivut, standardien dokumentaatiot (tekstiä). Videot.
Havainnointi (primääriinen aineisto)	Työasematurvallisuuden viikkopalavereiden osallistuva havainnointi.	Havainnointipäiväkirja, kenttämuistiinpanot
Haastattelut (primääriinen aineisto)	Organisaation omien ja ulkopuolisten työasematurvallisuuden asiantuntijoiden teemahaastattelut	Videotallenne ja litterointi. Tallennettu teksti Teams-keskusteluista.
Kokeilu (primääriinen aineisto)	Tietoturvan kovennus- tai auditoinnin työkalujen kokeilut.	Kokeilupöytäkirja.

Dokumenttien käyttö laadullisen aineiston tietolähteinä on hyödyllistä, koska ne ovat monesti kuvaauksia jo tapahtuneista asioista. Niiden kautta voidaan helpommin ymmärtää ilmiön kehittymistä nykytilaansa. Dokumenttien käytössä on oltava kuitenkin kriittinen: niiden objektiivisuus tulee tunnistaa ja tutkijan tulee aina pohtia mitä/ketä varten, miksi, milloin ja kuka dokumentin on laatinut? Onko dokumentilla ollut joku tietty tavoite, joka on ohjannut sen sisältöä? Myös dokumentista puuttuvat asiat voivat olla hyödyllisiä aineiston hyödyllisyyden arvioinnissa. Vertaisarvioidut dokumentit myös osoittavat miten aihealueen tutkimus on edistynyt tiedemaailmassa. Dokumenttien valintaan vaikuttaa myös tutkimuksen tavoitteet, joten aina vertaisarvioitu alkuperäistutkimus ei ole paras valinta aineistoksi. Joka tapauksessa valitut aineistot tulisivat olla sellaisia, jotka liittyvät olennaisesti tarkasteltavaan tutkimusongelmaan. (Kananen 2012, 88–91; Kananen 2015, 90–94; Vilkka 2023, 29–36).

Tieteessä aineistoa käytetään kirjallisuuskatsauksen tekoon. Tyypillisesti kirjallisuuskatsaus jaetaan yleensä kuvalevaan, systemaattiseen tai meta-analyysiin. **Kuvaleva katsaus** voidaan jakaa edelleen kolmeen eri tyylisiin (narratiivinen, kartoittava, integratiivinen). Kuvaleva katsaus on tyypillisin laadullisen tutkimuksen tyyppi. Sillä pyritään yleiskatsaukseen, hyödyntääne laajoja aineistoja, ilman rajaamatta aineistojen valintaa metodisilla säännöillä. Integratiivinen katsaus voi olla osa systemaattista katsausta, eikä siinä ole suurta eroa siihen, vaikka se ei seulo aineistoa yhtä tarkkaan kuin systemaattinen katsaus. **Systemaattisen katsauksen** tavoitteena on olla toistettava ja hyvin rajattu tiivistelmä tietyn aihepiirin aiempien tutkimusten olennaisista sisällöistä. Se ei anna mahdollisuutta valita tutkittavaksi muuta kuin tieteellisiä tutkimuksia. **Meta-analyysi** pyrkii metasynteesiin eli holistiseen tulkinthaan ja uuden tieteellisen tiedon muodostamiseen. Meta-analyysi voidaan tehdä laadullisena tai määrällisenä ja siinä käytetään sekundaaridataa. Metasynteesin suorittamiseen soveltuu myös ns. ei-akateeminen tutkimusaineisto. (Salminen 2023, 8–12; Vilkka 2023, 19–26).

Tässä tutkimuksessa tarvitaan kattava dokumenttiaineisto tukemaan kirjallisen konstruktion sekä **integroidun kirjallisuuskatsauksen** muodostamista. Esitutkimuksen perusteella aineisto koostuu kirjallisuudesta, tutkimuspapereista, videoleikeistä ja verkkosivuista. Aineiston keruu tehdään tutkijan itsenäisenä työnä, jolla taataan samalla tutkimuksellinen objektiivisuus. Organisaation omaa dokumentaatiota ei käytetä aineistona tietoturvasyistä.

Havainnointi on yksi vanhimmista tutkimusmenetelmistä. Havainnoinnin yhdistäminen haastatteluun on hyödyllinen tapa saada vahvistusta saatuun tietoon. Havainnoinnin avulla onkin mahdollista saada materiaalia jonkin ilmiön tai asian prosesseista tai ristiriidoista pidemmällä aikavälillä. Toisaalta havainnointi monipuolistaa saatua tietoa, koska tieto on suoraan lähteestä reaalialkaiseksi kerättyä. Havannointitapoja ovat piilo-, suora-, osallistava- ja osallistuva havainnointi. Kanasen mukaan havainnointipäiväkirja on hyvä tapa kirjata kohteen aitoa elämää. Päiväkirja voi olla lomake, jossa on valmiit kentät tilanteen ja henkilöiden toiminnan, tavoitteiden, ja tunteiden kuvaamiseen. On tärkeää, että päiväkirjassa erotetaan kontekstitieto ja havainnointi-ilmiöön liittyvät muistiinpanot. Kontekstitieto voidaan esimerkiksi tallentaa

kenttämuistiinpanoiksi, jotka toimivat tukena päiväkirjalle. Havainnot ja kenttämuistiinpanot kirjataan heti tapahtuman hetkellä. Havainnointi on suuritöinen aineistonhankintamenetelmä. (Kananen 2015, 65–70; Eskola & Suoranta 1998, 72–78; Tuomi & Sarajärvi 2018, 70–72; Puusa & Juuti 2020, 127–136).

Osallistuva havainnointi valitaan tähän tutkimukseen havannointitavaksi, jotta tutkija pääsee osaksi yhteisön elämää. Havainnointia toteutetaan koko tutkimuksen aineistonkeruujakson ajan, kuitenkaan tekemättä itse havainnoitavaan prosessiin muutoksia. Havainnoinnin kautta pyritään ymmärtämään ihmisten toiminnan ja tutkimusongelman suhdetta sekä dokumentoimaan syitä, jotka voivat liittyä tutkimusongelmaan. Havainnointipöytäkirjojen avulla todennetaan myös organisaation asiantuntijoiden teemahaastatteluissa esitettyjä väittämiä. Kenttämuistiinpanot kerättiin sovitusti anonymisoituna.

Teemahaastattelut ovat yleisiä laadullisissa tutkimuksissa. Muita haastattelutyyppejä ovat lomakehaastattelu ja syvähaastattelu. Teemahaastattelun tavoitteena on ymmärtää tutkimuksen kohteena olevaa ilmiötä ihmisten toiminnan kautta. Haastattelu etenee kahden välisenä vuorovaikutteisena keskusteluna, jonka rungon eli teeman tutkija suunnittelee ennalta. Haastattelussa edetään teemoittain yksityiskohtaisempiin kysymyksiin, kuitenkin kysyen haastateltavilta heidän kokemuksiaan ilmiöstä. Tutkijan rooli pitää olla neutraali, eikä hän saa ottaa kantaa vastauksiin. Jos tutkija vaikuttaa teemojen valinnan lisäksi keskusteluun liikaa esim. eleillään voi tällä olla vaikutusta saataviin vastauksiin. Kysymykset muotoillaan niin, että haastateltavat tuntevat aihealueen. Teemahaastattelussa voi hyödyntää myös ns. pumppaavia kysymyksiä eli entä sitten -tekniikkaa, jolla päästään syvemmälle teeman sisällä. (Kananen 2014, 70–89; Eskola & Suoranta 1998, 63–69; Tuomi & Sarajärvi 2018, 65; Puusa & Juuti 2020, 107–109).

Teemahaastattelu valittiin tämän työn haastattelumuodoksi. Perusteluna tälle oli toimeksiantajaorganisaation havainnointia tukevan aineiston kerääminen. Jokainen haastattelu oli henkilökohtainen ja tulokset anonymisoitiin. Mahdolliset täydentävät kysymykset esitettiin Teams-viestisovelluksen kautta

yksityisviesteinä. Haastattelut tallennettiin videomuotoisina(mpg-tiedostoformaatti) sekä litteroitiin.

Jyväskylän yliopisto kertoo kokeellisen aineistonhankintamenetelmän olevan mahdollinen silloin, kun halutaan tarkastella suoraan jonkin ilmiön vaikutusta toiseen ilmiöön tai todentaa syy-seuraus-suhteita. Kokeen toteuttamisessa oleellista on sen riippumattomuus, huolellinen suunnittelu ja valmistelu.

Kokeen tuloksia voidaan analysoida laadullisesti tai määrällisesti. Yleensä pyritään toistettavuuteen ja tarkkaan koeasetelman määrittelyyn. (Jyväskylän yliopisto 2014, kokeet).

Työkalujen kokeilulla pyrittiin saamaan holistinen käsitys siitä onko niiden käytännön hyödyntämisessä jotain dokumentaatiolta piilossa olevia ongelmia ja kuinka ne toimivat organisaatiossa tunnistettujen ongelmien poistamiseen. Teknisen kokeilun muistiinpanot kasattiin kokeilupöytäkirjoiksi, joiden pohjalta tehtävä analyysi toimi myös tutkimustuloksienvuotettavuutta varmistavana aineistona.

Aineiston analyysimenetelmät

Laadullisen tutkimuksen aineistojen analysointi vaatii kerätyn aineiston yhteismitallistamista eli tekstimuotoon saattamista. Tämän jälkeen aineistoa voidaan analysoida lukemalla tai erillisellä analyssiohjelmistolla. Ohjelmiston käyttö ei ole pakollista, koska johtopäätösten teko on kuitenkin tutkijan vastuulla. Aineistot analysoidaan yleensä laadullisesti tai määrällisesti. Sisältöanalyysi vaatii usein tiivistämistä, aineiston koodaamista tai luokittelua ja usein uutta tiedonhakukierrosta. Aineiston koodaaminen tarkoittaa tiivistetylle aineistolle sen sisältöä kuvaavan ilmaisun eli koodin antoa. Luokittelu tarkoittaa koodatun aineiston ryhmittelyä. Laadullisen aineiston yleisimpiä analyysimenetelmiä ovat tyypittely, teemoittelu, sisällönerittely, keskusteluanalyysi sekä diskurssianalyysi. Teemoittelussa aineistosta etsitään toistuvat keskeiset aiheet, kun taas tyypittelyssä tunnistetaan toistuvat tapahtumakulut tai merkitykset. Grounded theory -analyssia voidaan käyttää silloin kun halutaan luoda uusi näkökulma tai käsitteellistää tutkimuskohdetta laajan ja monilähteisen aineiston pohjalta. Aineistoanalyysi vaatii tutkijan intuitiota, jolla löydetään aineistosta sen olennainen viesti. Laadullisessa

tutkimuksessa voidaan löytää samasta aineistosta monia tulkintoja. (Kananen 2015, 83; Kananen 2014, 98–105, 115; Kananen 2012, 112–118; Jyväskylän yliopisto 2014, aineiston analyysimenetelmät; Eskola & Suoranta 1998, 124–132; Tuomi & Sarajärvi 2018, 78–92).

Tätä tutkimusta tuki parhaiten holistiseen käsitykseen pyrkivä laadullinen sisältöanalyysi, tai tarkemmin **aineistolähtöinen temaatinen analyysi**. Sisältöanalyysin menetelminä tässä tutkimuksessa hyödynnetään **tyypittelyä** tai **teemoittelua**, jonka avulla paikannetaan tutkimusongelmaan liittyvät tekstit sekä toistuvat teemat.

Luotettavuusmenetelmät

Opinnäytetyön luotettavuusmenetelmillä mitataan työn laatua, oikeutta, pätevyyttä(validiteetti) sekä luotettavuutta(reliabiliteetti). Tiedon luotettavuus on tieteen tärkein tekijä. Tieteellisyyden määritelmä on, että se on objektiivista, testattavissa, toistettavissa sekä julkista. Nämä tarkoittavat sitä, että mitä esitetään tieteenä, pitää olla tutkijan mielipiteistä riippumatonta, muidenkin tutkijoiden todennettavissa ja tulosten pitää olla kenen tahansa saatavilla. Lisäksi tieteen tulee olla kriittistä, riippumatonta ja edistyksellistä. Näissä kriteereissä on kuitenkin tulkinnan varaa. (Kananen 2012, 161–164; Eskola & Suoranta 1998, 151–164; Puusa & Juuti 2020, 167–190).

Opinnäytetyötä tarkastellaan tutkimustulosten pysyvyyden ja oikeiden asioiden tutkimisen näkökulmasta. Luotettavuustarkastelussa dokumentaatio on olennaista, jotta työn tuloksia voidaan arvioida, ts. onko tutkittu sitä mitä on pitänytkin alun perin tutkia. Kanasen (2012) mukaan erityisesti kehittämistutkimusten luotettavuus voidaan varmentaa helpoiten luetuttamalla aineisto ja sen tulkinta niillä, joita se koskee. Aineiston varmennukseen voidaan käyttää ns. memberchecking -menetelmää tai informantin vahvistusta. Tämä tarkoittaa sitä, että koko aineisto ja tutkijan tulkinta tai tulokset annetaan luettavaksi ja varmistettavaksi arvioijalle. Informantti voi vahvistaa tai kielää tutkijan tulkinnan ja tutkimustuloksen. Vahvistusta tutkimuksen paikkansapitävyydlle voidaan hakea myös vertaamalla sen tuloksia aiempiaan tutkimuksiin, joissa on samankaltaisia tuloksia. Kehittämistutkimuksen siirrettävyys todistaa myös sen validiteettia.

Siirrettävyys tarkoittaa tutkimusasetelman ja tutkimuskohteen tarkkaa kuvausta, jotta tulokset ovat sovellettavissa toisessa ympäristössä. Yrityskohtaisissa tutkimuksissa siirrettävyyden täyttyminen edellyttää, että toimiala, koko, liikevaihto ja työntekijämäärä ilmenevät tutkimusasetelmasta. (Kananen 2012, 161–176; Eskola & Suoranta 1998, 165–176; Puusa & Juuti 2020, 167–190).

Tämä työ on monimenetelmällinen tutkimus. Työssä käytetään teemahaastatteluja, osallistuvaa havainnointia sekä tehdään kuvalevia ja systemaattisia menetelmiä hyödyntävää kirjallisuuskatsausta. Työn sisältöanalyyseissä hyödynnetään teemoittelua ja temaatista analyysia. Monimenetelmällisyyden takia työssä hyödynnetään kattavasti triangulaatiota, joka tarkoittaa erilaisten aineistojen välistä vertailua. Triangulaation avulla voidaan saada kattava ja luotettava kuva tutkittavasta ilmiöstä sekä perustella aineistojen luotettavuutta. (Kananen 2019, 30–35; Tuomi & Sarajärvi 2018, 118–128; Vilkka 2023, 72; Puusa & Juuti 2020, 169–178).

2.6 Tutkimuskohde

Verohallinto on Suomen valtion viranomainen, joka hoitaa nykymuotoisen verotustoiminnan Suomessa. Verohallintoa ohjaa Valtiovarainministeriö, joka myös valmistelee verolait. Viranomainen muodostui vuonna 1970 perustetun verohallituksen, sekä 1974 perustetun verohallinnon tietojenkäsittelykeskuksen ja verovirastojen yhdistyessä vuonna 2008. Verohallinto on jakaantunut eri yksiköihin, kuten verotus-, asiakkuus- ja tuotehallintayksikköön. Yksiköjen toiminta on jaettu verohallinnon sisällä tuoteryhmiin, esim. henkilö-, kiinteistö- ja autoverotus. IT-toiminnot hoidetaan tuotehallintayksikössä, yhteistyössä tietoturvallisuuteen keskittyvän turvallisuus ja riskienhallintayksikön kanssa. Koko verohallinnossa työskentelee noin 5000 henkilöä ympäri Suomen. Tämä opinnäytetyö fokusoi päätelaitteiden teknisiin prosesseihin, joiden parissa työskentelee päätoimisesti 6 henkilöä ja tukemassa osa-aikaisesti tietoturvan osalta noin 10 henkilöä. (Verohallinto s.a).

3 TEOREETTINEN VIITEKEHYS

Tieteellisen työn toteutukseen kuuluu tunnetun teorian, tutkimusten ja käsittelien määrittely. Teoreettinen, viitekehys sisältää usein teorian ja empirian yhteen liimaavia osia, kuten aikaisempien tutkimusten, alan kirjallisuuden ja artikkeleiden tuloksia, väittämiä ja mittareita. Luku kolme avaa tässä tutkimuksessa oleellisia avainkäsitteitä ja teorioita sekä niiden valinnan perusteita. (Kananen 2015, 95–99, 112–115).

3.1 Avainkäsitteiden ja teorioiden määrittely

Windows-ympäristö, päätelaitteet ja työasemat

Weiss ja Solomon (2016) esittelevät työasemaluokan (eng. workstation) käsitteen. Heidän mukaansa yleisimmät ko. luokan laitteet ja komponentit ovat kannettavat tietokoneet, pöytätietokoneet, tabletit ja älypuhelimet sekä näihin liitetty lisälaitteet kuten usb-muistit. Nykyaisempana yleisterminä käytetään usein päätelaitetta, joka tarkoittaa tietoverkkoon kuten internettiin tai yritysverkkoon liitettyä tiedonkäsittelylaitetta (Weiss & Solomon 2016, 72–73, luku 9, luku 13).

Silberschatz (2018) mukaan Windows ympäristö määrittyy käyttöjärjestelmän tyypin mukaan. Koti-, ammattilais- ja yrityskäyttöön (eng. home, pro, enterprise) tarvitaan erilaisia ominaisuuksia, kuten yritysten Windows-ympäristöissä vaadittava erityinen tietoturva sekä käyttöjärjestelmäpäivitysten pitkä tuki. Yrityksille suunnatusta enterprise-versiosta löytyykin tiedon salausominaisuksien lisäksi erityisiä turvallisia käyttöoikeus-, etäkäyttö sekä suojaustekniikoita. Näiden erikoisominaisuksien käyttö voi vaatia lisäksi päätelaitteiltä erityisiä laitteisto-ominaisuksia, jotta kaikki tietoturvaominaisuudet saadaan käyttöön (Silberschatz ym. 2018, luku 21).

Dunkerley ja Tumbarello (2022) määrittelevät yritysten Windows-ympäristöön kuuluvan olennaisesti myös erilaiset hallintaohjelmistot ja automaatiot, joiden avulla työasemia ja niiden ohjelmistojen asetuksia ja tietoturvaa voidaan toteuttaa keskitetysti. Yritysten Windows-ympäristöjen sekä työasematurvallisuuden ylläpito vaatii yleensä erityisesti siihen keskittyneitä ammattilaisia (Dunkerley & Tumbarello 2022, luvut 6–8).

Windows-työaseman tietoturvakovennus ja penetraatiotestaus

Työaseman tietoturvan kovettaminen tarkoittaa Mistryn ym. (2018) mukaan yksinkertaisimillaan jatkuvaan prosessia, jolla pyritään pienentämään mahdollisuuksia hyväksikäyttää työaseman tietoturvan puutteita.

Tietoturvakovennukset tehdään karsimalla tarpeettomia teknisiä työasemaominaisuksia ja ohjelmistoja, huolehtimalla päivityksistä ja tiukentamalla tarvittavien ominaisuuksien tietoturva-asetuksia. Työasemien tietoturvaa koventamalla suojataan välillisesti niillä käsiteltävää hyvinkin sensitiivistä tietoa sekä tietojärjestelmiä. Mistryn ym. mukaan tietoturvakovennusten toteutus voidaan tehdä manuaalisesti, tarkistuslistoihin pohjautuen, tai puoli-automatisoidusti erillisiä tarkastusohjelmistoja hyödyntäen. Työaseman tietoturvariskejä eniten pienentävät kovennukset tulee priorisoida toteutuksissa. (Mistry ym. 2018).

Zamoran ym. (2019) mukaan PC-laitteiden kerroksittainen tietoturvakovennus lähtee käyttöjärjestelmän omista tietoturvaominaisuuuksista. Lisäksi poistetaan paikalliset ylläpitäjän oikeudet käyttäjiltä, sekä kovennetaan sovellusten tietoturvaa. Kovennuksia tehdään keskitetysti ja hallintajärjestelmää kuten ryhmäkäytäntöjä (eng. group policy) hyödyntäen. Tietoturvakovennusten tilaa ja voimassaoloa tulee seurata ja mitata. Hamdanin ym. mukaan käyttöjärjestelmän kovennus on monesti taiteenlaji, johon vaikuttaa erityisesti organisaation omat säännöt, resurssit sekä ylläpitäjien erikoisosaaaminen. (Zamora ym. 2019; Hamdani ym. 2021).

Dunkerley ja Tumbarellon (2022) määritelmä Windows työaseman tietoturvakovennuksista noudattelee määrämuotoista prosessia, jonka ydinperiaatteisiin kuuluu ns. perustason (eng. baseline) määrittely. Perustason määrittely aloitetaan tunnettujen tietoturvauhkien ja haavoittuvuuksien tunnistamisella. Näiden pohjalta lähdetään rakentamaan kovennettu Windows työasemakokoonpano. Sama perustason työasemakokoonpano asennetaan kaikkiin organisaation laitteisiin, varmistaen hallitu ja kovennettu tietoturvataso. Dunkerley ja Tumbarellon määrittelevät tietoturvakehysten suositusten käytön osaksi perustason määrittelyä. (Dunkerley & Tumbarellon 2022, luvut 1,2,4).

Penetraatiotestaus on tapa etsiä järjestelmistä, laitteista ja ohjelmistoista haavoittuvuuksia, väärinmäärittelyitä tai puutteita, joita hyödyntämällä voidaan aiheuttaa haittaa, varastaa informaatiota ja hyväksikäyttää kyseistä järjestelmää. Oriyanon mukaan tietoturvakovenukset ovat olennainen keino tiukentaa järjestelmien oletustasoisia tietoturvaominaisuksia. Erityisesti kaksi periaatetta kuten ehdoton kielto ja vähimmän käyttöoikeuden malli (eng. implicit deny, least privilege) ovat tärkeitä. Ehdoton kielto tarkoittaa sitä, että mikä ei ole erikseen sallittua on aina oletuksena kiellettyä. Vähimmän käyttöoikeuden malli taas tarkoittaa sitä, että tehtävän suorittamiseksi siihen myönnetään aina pienimmät mahdolliset käyttöoikeudet. (Oriyano 2017, luku 16).

Kyberturvallisuus, standardit, parhaat käytännöt ja tietoturvakehykset

Duncanin ja Whittingtonin (2014) mukaan kyberturvallisuus keskittyy tiedon käsittelyn luottavuuden, eheyden ja saavutettavuuden (eng. confidentiality, integrity, availability) turvaamiseen tietojärjestelmissä, tietoverkoissa ja laitteissa. Yleisesti ottaen em. toimet vaativat sekä teknisiä että hallinnollisia toimia, ohjeistuksia ja käyttäjien koulutusta. Tämän kokonaisuuden hallintaan on kehitetty ajan saatossa useita kilpailivia, eri käyttötarkoituksiin ja eri aloille kehitettyjä standardeja sekä tietoturvakehyksiä. Erona näillä on se, että standardit sisältävät valikoiman tarkkoja sääntöjä, ohjeita ja määrityksiä, joita noudattamalla jotain tehdään tai toteutetaan, tarkalleen standardin mukaisesti. Tietoturvakehykset sen sijaan ovat kokoelmia muokattavia ja uudelleenkäytettäviä työkaluja, perustoiminnallisuksia ja suunnitteluohejistuksia. Tietoturvakehykset sisältävät usein myös listauksia parhaista käytännöistä tai menetelmistä jonkin asian toteuttamiseen. (Duncan & Whittington 2014).

Hamdanin ym. (2021) mukaan IT-järjestelmät sisältävät niin paljon yksittäisiä tietoturvaan vaikuttavia asetuksia, että ilman kyberturvallisuusosaamista niiden huomiointi jää monesti käytön helppouden jalkoihin. Tietoturvakeysten käytöllä voidaan parantaa järjestelmien käytännön tietoturvaa, vähentäen mm. järjestelmien väärinmäärittelyitä. Hamdani ym. kertoo tietoturvakeysten käytännön hyödyntämisen olevan jopa väsyttävä prosessi, koska kehysiä on niin monta erilaista ja oikeanlaisen löytäminen vie aikaa. Kehysten

hyödyntämisessä on myös haasteita, mm. tulosten mittaaminen, työkalujen puutteet ja kehysten yhteismitallisuuden puuttuminen. (Hamdani ym. 2021).

Nichon (2018) mukaan tietoturvakehyksiä käytetään kehämisesti, siten että niitä hyödynnetään yleisestä yksityiskohtaiseen kehykseen päin, käyttäen useita eri kehysiä. IT turvallisuudessa käytännön kehykset otetaan käyttöön vasta operatiivisen turvallisuuden toteutusvaiheessa (Nicho 2018).

Malatjin ym. (2019) tutkimus painottaa erityisesti sosio-teknologisten ns. harmaiden alueiden näkökulmien huomioimista, kun käytetään joitain tietoturvakehystä. Heidän mukaansa nykyiset tietoturvakehykset eivät riittävästi painota ihmisten, prosessien ja teknologian välistä turvallisuusnäkökulmia (Malatji ym. 2019). Toisaalta Siponen ja Willison (2009) määrittelevät toisaalta tietoturvakehysten olevan geneerisiä ja validiteiltaan ongelmallisia, koska niiden taustalla tehdyn tutkimustyön prosesseja ja perusteita ei julkaista, vaan tulokset esitetään asiantuntijoiden parhaina käytäntöinä, jolloin ne eivät voi mitenkään ottaa riittävästi huomioon eri organisaatioiden eroja turvallisuusvaatimuksissa (Siponen & Willison 2009).

Dedeken ja Mastersonin (2019) mukaan uusin trendi on ollut erilaisten kansallisten tietoturvakehysten kehitys, joita kehitetään vastaamaan erityisesti tietyt maan lakeja ja säännöksiä vasten. Näissä ongelmana on, että ne eivät ole keskenään verrattavissa, koska osassa jokin kategoria on voitu jättää kokonaan pois (Dedeke & Masterson 2019).

Auditointi, vaatimustenmukaisuus ja tarkastus

Auditointi tarkoittaa Weissin ja Solomonin (2016) mukaan joko organisaation sisäisesti tai ulkoisesti toteutettua järjestelmän teknistä tai hallinnollista määrämuotoista tarkastusta tai vaatimustenmukaisuuden (eng. audit, compliance) kuten lakien, standardien tai alan vaatimusten noudattamisen tarkastusta. Tietoturvakovenkset voidaan nähdä kuuluvan myös osaksi vaatimustenmukaisuutta, koska joillain aloilla, kuten terveydenhuollossa ja pankkisektorilla on myös omia vaatimuksia tietoturvakovenkusten suhteeseen, erilaisten lakien ja säädösten kautta. (Weiss & Solomon 2016, 22–27).

Duncanin ja Whittingtonin (2014) mukaan taas auditointi, vaatimustenmukaisuus ja varmistukset (eng. audit, compliance, assurance) menevät IT turvallisuudessa monesti sekaisin. Auditoinnilla voidaan esim. saavuttaa vaatimustenmukaisuus, mutta se ei varmista tietoturvallisuutta. Vaatimustenmukaisuuden tarkastuksessa ulkopuolin auditoija voi objektiivisesti todeta täyttävätkö esitetyt todisteet tietyn standardin tai tietoturvakehyksen vaatimukset vai ei. Toisaalta vaatimustenmukaisuus voi sisältää tietyn standardin osalta myös yrityksen toimien eettisyyden ja riskienhallintakyvyn arviontia. Vaatimustenmukaisuuden täyttäminen on säädöstellä aloilla edellytys esim. tuotteen valmistusluvalle tai palvelun myynnille. Auditointia parempi termi IT turvallisuudessa onkin varmistus, joka tarkoittaa lähes aina sisäisen tai ulkoisen tietoturvallisuusasiantuntijan itse toteuttamaa ja raportoimaa kattavaa teknistä tai hallinnollista tarkastusta valitusta kohteesta. Tarkastuksissa ei vältämättä hyödynnetä standardia tai kehystää taustalla. IT turvallisuuden auditoinnilla halutaan varmistaa suojaustoimien toimivuus ja vaikuttavuus. (Duncan & Whittington 2014).

Nichon (2018) mukaan auditointi ja vaatimustenmukaisuus kuuluvat osaksi organisaation tietoturvallisuuden jatkuvaan hallintamallia. Hallintamallin prosessiytimessä on ISO/IEC standardoinnin ensin esittelemä ns. suunnite-tee-tarkista-reagoi malli (eng. plan-do-check-act). Mallin avulla saavutetaan kehämäinen prosessi, jolla hallita auditointia, tietoturvakehyksiä ja vaatimustenmukaisuutta. Yksittäiset auditoinnit ja vaatimustenmukaisuuden tarkastus eivät yleensä Nichon mukaan johda jatkuvaan tietoturvan parantamisen maliin, vaan mukaan tarvitaan lisäksi ihmisten, prosessien ja teknologian huomioon ottavia elementtejä. (Nicho 2018).

Tietoturvauhkat, -riskit ja tilannekuva

Antonuccin (2017) mukaan tietoturvan tilannekuvan olennainen osa on käytännön tietoturvauhkiien ja -riskien tunnistaminen, analysointi ja arviointi. Uhkat ja riskit jaetaan määritykseen mukaan organisaation sisäisiin ja -ulkoisiin uhkiin ja riskeihin. Erityisesti ulkoisia uhkia voi tunnistaa ns. kyberturvallisuuden uhkatiledon kautta, joka on tyypillisesti eri tietoturvaorganisaatioiden koostamia raportteja tai uutiskirjeitä. Antonucci:n

mukaan tietoturvakehysten noudattaminen on tärkeää, mutta kyberuhkien seurannan olevan niiden volatilitetin takia vielä tärkeämpää. Jos yrityksen tietoturvan tilannekuva perustuu vain tietoturvakehysten noudattamiseen, katsotaan aina tilannetta taaksepäin. (Antonucci 2017, Luvut 7,14,15).

Goel ym. (2020) esittää nykyisten tietoturvakehysten olevan monimutkaisia ja käyttöönnottoon suuntautuneita. Määrittelyn mukaan johdon näkyvyys ja päätöksenteon perusteet eivät perustu nykyisissä kehyksissä riittävästi riskiarvioihin organisaation nyky- ja tulevaisuuden kyberuhkista. Goel ym. ehdottaa riskipohjaista PRISM metodia, joka ottaa päätöksenteossa huomioon priorisoinnin, resurssit, implementoinnin, standardisoinnin, valvonnan sekä riskiarvion. Organisaation johdon strateginen päätöksenteko ja tilannekuvan hallinta paranee, kun operatiivisen turvallisuuden osuus sisällytetään osaksi kokonaisriskienhallintaa. (Goel ym. 2020).

Atoum Ym. (2014) ehdottaa holistista hallintamallia puhuessaan tietoturvastrategian käyttöönottomallista tutkimuksessaan. Kyseinen malli ottaa huomioon organisaation tietoturvavaatimukset, joista johdon tuella priorisoiden tehdään tavoitteita, ottaen huomioon toteutus, sen mittaaminen ja raportointi. Holistista mallia hyödyntäen voidaan saavuttaa tehtyihin toimiin parempi näkyvyys ja tilannekuva (Atoum ym. 2014).

Bongiovanni ym. (2021) kertovat organisaation johdon tilannekuvaongelmien johtavan tietoturvaratkaisujen aliresursointiin. Alalle kehitetyt standardit eivät tarjoa riittävää näkyvyyttä ratkaisujen laatuun, varsinkin kun edes alalla toimivien asiantuntijoiden välillä ei ole konsensusta tietoturvaohjelmien kontrollien, menetelmien ja keinojen priorisoinnista ja riittävyydestä (Bongiovanni ym. 2021).

Virhekonfiguraatiot

Xu ja Zhou (2015) esittelevät virhekonfiguraatiot yhdeksi isoimmaksi syyksi järjestelmävoieille. Konfiguraatio tarkoittaa kokoelmaa asetuksia, joiden parametrejä voidaan muokata. Virhekonfiguraatio ei tarkoita ohjelmistovikaa, vaan yhdistelmää ylläpitäjien väärin valitsemia asetuksia, jotka kokonaisuudessaan heikentävät järjestelmän vikasietoisuutta, tietoturvaa ja

käytettävyyttä. Järjestelmien monimutkaisuus tekee virhekonfiguraatioiden tunnistamisen ja välttämisen hankalaksi (Xu & Zhou 2015). Dietrich ym. (2018) ehdottavat, että nykyään hyvin yleiset tietoturvaloukkaukset eivät ole itseasiassa useinkaan monimutkaisten hyökkäysten syytä, vaan ne mahdollistuvat yksinkertaisten tietoturvan konfiguraatiovirheiden myötä. Tietoturvan yksinkertaisimpia konfiguraatiovirheitä ovat päivittämättömät ohjelmistoviat ja julkiseen internettiin liitettyjen järjestelmien väärin määritellyt käyttöoikeudet tai pääsynhallintasäännöt (Dietrich ym. 2018).

3.2 Käsitteiden valinta ja perustelut

Esitetyjen avainkäsitteiden ja teorioiden valintaan vaikuttaneet pohdiskelut ja perusteet on kuvattu tarkemmin tutkimuksen liitteen 4 antic-taulukossa. Tutkimukset ja aineistot on valittu palvelemaan joko teoreettista viitekehystä, tutkimusta tai kumpaakin. Kaikki tutkimukseen valitut teoriat avaavat joko tutkimuskysymyksiin liittyviä perusteita tai tuovat jonkin erityisen näkökulman itse tutkimuskysymyksiin vastaamista varten. Muissa samankaltaisissa opinnäytetöissä on keskitytty tietoturvakontrollien tai kehysten käyttöönnottoon joko teknisestä tai riskienhallinnan näkökulmasta.

Omassa tutkimuksessani ei tehdä teknistä tietoturvakontrollien käyttöönottoa, vaan tutkitaan holistikesti, miten ja miksi tietoturvakehysiä pitää ja kannattaa käyttää sekä mitä niiden käyttö oikeastaan parantaa. Tutkimuksen valitut teoriat tukevat parhaiten tästä tavoitetta. Useissa tutkimuksissa taas on pyritty löytämään uusi ratkaisu kehysten käytössä tunnistettujen ongelmien korjaamiseksi. Usein tämä ratkaisu on ollut uuden mallin tai uuden kehyksen kehittäminen. Mallin kehittäminen on myös oman tutkimukseni sekundäärisenä tavoitteena.

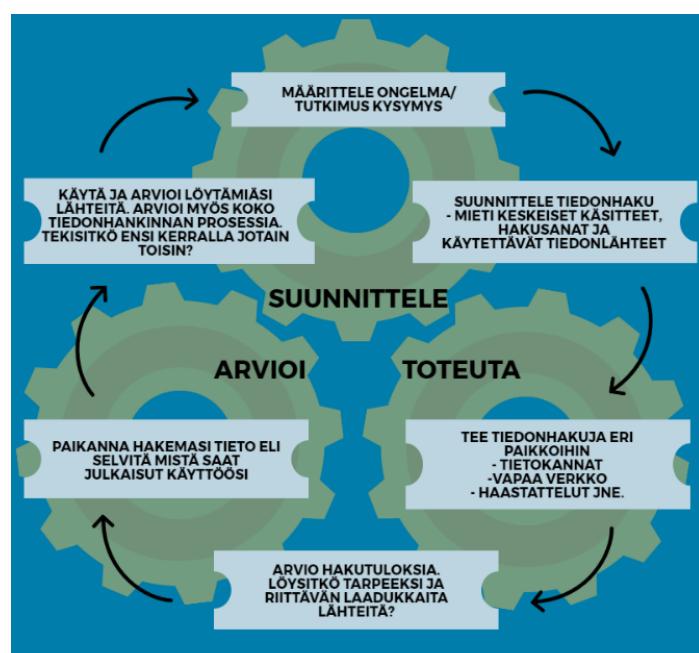
4 TYÖN TOTEUTUS

Tiedonhaku tulee olla systemaattista, kattavaa ja perusteellista, riippumatta kirjallisuuskatsauksen tyyppistä. Hakusanat, hakutavat ja aineiston valintakriteerit sekä rajoukset tulee perustella. Yksittäisten hakusanojen sijasta on tehokkaampaa yhdistellä niitä hakulausekkeiksi. Hakusanojen yhdistämisessä hyödynnetään Boolean operaattoreita AND, NOT ja OR. AND-operaattorilla voidaan rajata hakutuloksia, kun taas NOT-operaattori poistaa

hakutuloksista epätoivottuja hakusanoja sisältävät artikkelit. Hakutuloksia voidaan lisäksi rajata vuosiluvun, aineistolajin tai tieteenlajin avulla. Hakutulosten laajennus tapahtuu OR-operaattorilla, jolla hakuun otetaan mukaan molemmat määritellyt hakusanat. Boolean operaattoreita voidaan myös yhdistellä hakulausekkeissa sulkeilla, sekä hyödyntää sitaatteja useiden sanojen peräkkäisissä hauissa. Sitaattien käyttöä nimitetään myös fraasihauksi. (Oulun yliopisto, s.a. haun dokumentointi; Xamk, s.a.b, luvut 1–6; Vilkka 2023, 45–55).

Systemaattinen tiedonhaku sisältää saannin ja tarkkuuden termit, joilla on keskinäinen suhde. Mikäli hakutulosten tarkkuutta kasvatetaan suodattamalla epärelevantteja dokumentteja, voidaan menettää myös relevantteja dokumentteja, saannin pienentyessä. Tiedonhakuun kuuluu olennaisesti hakulauseiden sinnikäs testaaminen ja hakujoukon läpikäynti. Käytetyt hakulausekkeet, niissä käytetyt operaattorit sekä hakutulosten määräät tulee dokumentoida, jotta valintaprosessi voidaan kuvata läpinäkyvästi. Hakuprosessin dokumentointiin voi hyödyntää PRISMA-metodiikkaa, joka tarjoaa valmiita tarkistuslistoja sekä dokumentatiopohjia. (Oulun yliopisto, s.a. haun dokumentointi; Xamk, s.a.b, luvut 1–6; Vilkka 2023, 45–62).

Tiedonhakua voi ajatella prosessina, joka sisältää suunnittelu, toteutus ja arviontivaiheet. Näitä vaiheita on havainnollistettu kuvassa 5.



Kuva 5. Tiedonhaun prosessi (Xamk s.a.a)

Tiedonhaun apuvälineenä voi myös hyödyntää aineistojen sisältämiä asiasanoja. Näiden sanojen avulla voidaan helpommin kohdistaa hakuja aihealueeseen, eikä pelkästään artikkeleista löytyviin sanoihin. Valmiiden asiasanastojen käyttö voi olla myös hyödyllistä, koska niiden avulla voi helpommin löytää rinnakkaisermejä sekä synonyymejä. (Xamk. s.a.b, luvut 1–6; Vilkka 2023, 45–48).

4.1 Sekundäärisen aineiston haku

Kirjallisuuskatsauksen tyypin perusteella keskityin hakemaan tietoa suoraan tutkittaviin kysymyksiin. Tutkimusasetelman määrittelyiden pohjalta tein aluksi rajaamattomia hakuja sekä Xamk:n kautta saataviin tietokantoihin, että vapaan verkon aineistoihin. Hakujen sisältöjen perusteella määritettiin käytettävät tietokannat, jotka on kuvattu taulukossa 3.

Taulukko 3. Valitut tietokannat

Tietokanta	Sisältö	Perustelut ja huomiot
Kaakkuri.finna.fi	Kirjojen, artikkeleiden ja opinnyytetöiden haku	Helppo haku, jossa yksinkertaiset rajauskeinot.
Ebook Central	Laaja valikoima ulkomaisia tekniikan alan teoksia	E-kirjat saatavilla kokonaисina kirjoina lainaan.
EBSCO (Academic search elite)	Teknisen alan tutkimuksia ja artikkeleita	Haku palauttaa laajasti tietoa kohteesta, mutta itse tutkimus tai artikkeli voi olla maksumuurin takana toisessa tiedeportaalissa.

Emerald Premier	Teknisen alan tutkimustietoa	PDF saatavilla suoraan haetun artikkelin ohessa.
Sage Premier	Teknisen alan artikkeleita ja lehtiä	Hyvä hakuhistoria tehdystä hakulausekkeista.
Science direct	Teknisen alan lehtiä ja seminarijulkaisuja	Tiivistelmä ja pdf tosi helposti saatavilla.
Researchgate	Laajasti eri alojen tutkimusjulkaisuja sekä artikkeleita	Tarjoaa maksumuurienkin takana olevia tieteellisiä artikkeleita PDF-muodossa.
Google scholar	Laajasti kirjoja, tutkimusjulkaisuja sekä avoimen verkon aineistoja indeksoiva tieteellinen portaali	Avoimen verkon aineistojen kuten ammattiaineistojen ja blogikirjoitusten osalta oleellinen työkalu.

Aihesanojen muodostaminen

Tietokantoihin tutustumisen jälkeen oli hyödyllistä kasata työn tutkimuskysymisten pohjalta aihesanat, joiden avulla lähteää haarukoimaan hakuja tarkemaksi. Alla olevaan taulukkoon 4 on listattu tutkimuskysymyksistä johdetut aihesanat suomeksi ja englanniksi, sekä valikoidut englanninkieliset aihesanat.

Taulukko 4. Aihesanat suomeksi ja valikoidut aihesanat englanniksi

Tutkimuskysymys	Näkökulma	Aihesanat suomeksi	Aihesanat englanniksi
1. Mitkä tietoturvakehykset ja	Tietoturvakehykset, parhaat käytännöt,	Tietoturvakehys,	Security framework,

parhaat käytännöt tai niiden osat ovat soveltuivia Windows-työaseman tietoturvan koventamiseen?	tietoturvan kovennus	Parhaat käytännöt vertailu, Windows tietoturva kovennus	best practises, comparison, Windows security hardening, benchmark
2. Ovatko parhaiden käytäntöjen ja tietoturvakehysten suosituksset ajantasaisia ja kattavia Windows-työaseman käytännön tietoturvan ja uhkien kannalta?	Käytännön tietoturva, uhkat, riskit	Windows käytännön tietoturva, uhka, riski	Windows security risks, threats, practical security
3. Mahdollistaako parhaisiin käytäntöihin ja tietoturvakehykseen perustuva Windows-työaseman kovennus auditoitavuuden ja organisaatiotasoinen päätelaitetietoturvan tilannekuvan?	Windows kovennusten auditointi, tietoturvan tilannekuva	Windows auditointi, tietoturvan tilannekuva	Auditing Windows, security hardening, security posture, visibility, compliance
4. Miten Windows-työaseman tietoturvaa ja auditoitavuutta voi hoitaa hallitusti ja määrämuotoisesti?	Työaseman tietoturvan hallinta ja auditoitavuus prosessit ja työkalut	Windows tietoturvan hallinta, tietoturvan auditointi	Windows security management Security auditing tools

Valikoidut englanninkieliset asiasanat ja yhdistelmät:

Windows, “Operating system”, hardening, auditing, compliance, benchmarks, vulnerability, “security hardening”, “system hardening”, “security auditing”, cybersecurity +posture, +visibility, +standards, +frameworks, “practical security”, “best practises”.

Tutkimuksen edetessä ja aihealueen ymmärryksen kasvaessa, hakutulosten pohjalta pystyi tunnistamaan kiinnostavimpia ja yleisimmin hauissa esiintyviä aihesanoja. Näiden pohjalta pystyi muodostamaan sopivia hakulausekkeita, joissa hyödynnettiin Boolean logiikkaa rajoiksina. Tietokannoissa oli mahdollista tehdä tietokannan omia rajoja, joita hyödynnettiin aihealueen rajaamisessa vain tekniikan ja tietoturvan alueelle sekä tietokantojen että sisällön osalta.

Hyvin pian aineistohaun aloituksen jälkeen ilmeni, että suomenkielistä tutkimustietoa, tai vapaan verkon aineistoja oli saatavilla pääosin vain aiempien opinnäytetöiden muodossa. Tämän takia lopullisessa tutkimusaineiston keruussa käytettävät hakulausekkeet rakennettiin vain englannin kielellä. Kotimaisten lehtien ja artikkeleiden valikoimasta ei tunnistettu tutkimuksen kannalta merkittäväää tietoa, jonka takia niiden hyödyntämisestä luovuttiin.

Hakulausekkeet ja ensimmäinen hakukierros

Hakulausekkeita rakennettiin vaihdellen asiasanoja sekä Boolean rajaustermejä. Haun palauttamien aineistojen käsitteily lopetettiin ja hakulauseeketta muutettiin, jos ensimmäisen 25 aineiston otsikossa, tiivistelmässä tai asiasanoissa ei ollut tutkimuksen kysymyksiin liittyvästä tekstiä. Hakuja tehtiin käyttämällä asiasanoja sekä yksikkö- että monikkomuotoisina, joista yksikkömuoto palautti relevantimpia tuloksia. Eri tietokantojen hakujen toiminta ei ollut yhdenmukaista, vaan hakuja pitä muokata mm. boolean-rajausten järjestyksen ja asiasanojen järjestyksen suhteen. Lisäksi eri tietokantojen asiasanarajauksella tehdyt haut toimivat ristiriitaisesti, joten hakulausekkeet päätettiin kohdistaa kaikkiin sisältöihin otsikon, tiivistelmän tai asiasanojen sijaan.

Finnan ja Ebook central:n tietokantoihin kohdistettiin yksinkertaisia hakulausekkeita AND-rajauksilla. Tavoitteena oli löytää kirjallisuutta tai opinnäytetöitä, joissa olisi asiasanoja vastaavaa sisältöä. Muihin tietokantoihin kohdistuvien aineistohakujen lähtökohtana oli, että kaikkiin tietokantoihin kohdistetaan samat hakulausekkeet. Hakulausekkeet muodostettiin ensin EBSCO-tietokannan kautta. Tutkimusongelmaan ja -kysymyksiin parhaiten vastaavaa tietoa palauttivat taulukoissa 5–8 esitellyt hakulausekkeet.

Taulukko 5. Windows OR Operating system AND (security) AND (hardening) OR (auditing) OR (best practises)

Tunniste	Tietokanta	Osumat
A	Finna	65
B	Ebook Central	114
C	EBSCO	65
D	Emerald Premier	71
E	Sage Premier	91
F	Science Direct	185
G	Google Scholar	411

Taulukko 6. Security AND (frameworks) OR (standards) AND (hardening) OR (auditing)

Tunniste	Tietokanta	Osumat
A	Finna	203
B	Ebook Central	287
C	EBSCO	96
D	Emerald Premier	48
E	Sage Premier	116
F	Science Direct	564
G	Google Scholar	368

Taulukko 7. Operating system AND (compliance) OR (best practises) AND (security)

Tunniste	Tietokanta	Osumat
A	Finna	178
B	Ebook Central	312
C	EBSCO	75
D	Emerald Premier	216

E	Sage Premier	68
F	Science Direct	327
G	Google Scholar	158

Taulukko 8. Cyber security AND (posture) AND (compliance) OR (benchmarks) OR (visibility)

Tunniste	Tietokanta	Osumat
A	Finna	69
B	Ebook Central	239
C	EBSCO	59
D	Emerald Premier	42
E	Sage Premier	54
F	Science Direct	292
G	Google Scholar	211

Rajauskriteerit ja toinen hakukierros

Tutkimusaineiston hakuun piti asettaa rajauskriteereitä, koska käsiteltäviä aineistoja tuli riippuen tietokannasta kymmenistä tuhansiin. Rajauskriteereillä aineistojen määät saatiin pidettyä pääsääntöisesti kohtuullisina (n. 1–50 kpl/hakulauseke). Palautuneiden tutkimusaineistojen tietokantojen rajaussissa hyödynnettiin myös JUFO-portaalilta saatavilla laatuluokitusta (vain ylimmän 3 kriteerin tietokantatulokset hyväksytiin).

Poikkeuksia rajauskriteereihin sallittiin, jos aineisto vaikutti tutkimuksen kannalta mielenkiintoiselta. Zotero-viitteidenhallintajärjestelmää hyödynnettiin tietokantojen hakutulosten kaksoiskappaleiden poistamisessa. Toisella hakukierroksella hyödynnettiin myös laajasti NOT-Boolean termiä irrelevantteja asiasanoja sisältävien tulosten poisrajamiseen. Rajauskriteerit on kuvattu taulukossa 9.

Taulukko 9. Rajauskriteerit

Rajauskriteeri	Perustelu	Poikkeus
Tutkimusartikkeli on vertaisarvioitu	Vertaisarvointi todistaa artikkelin tieteellisyyden prosessin.	Otsikko, sisältö tai tiivistelmä vaikuttaa

		oleelliselta tutkimuksen kannalta.
Julkaisuvuosi 2013–2023	Vanhentunut tekniikka tai artikkelin sisältö vanhentunut.	Otsikko, sisältö tai tiivistelmä vastaa tutkimuskysymyksiin
Julkaisukieli suomi tai englanti	Vaara tulkita tutkimus väärin, kielen tai käänönksen väärintulkinnan myötä.	-
Kokoteksti tai artikkeli saatavilla	Ilman kokotekstiä on vaikea todeta onko artikkelin sisältö relevanttia.	Jos kiinnostava artikkeli ja löytyy avoimen verkon kautta.

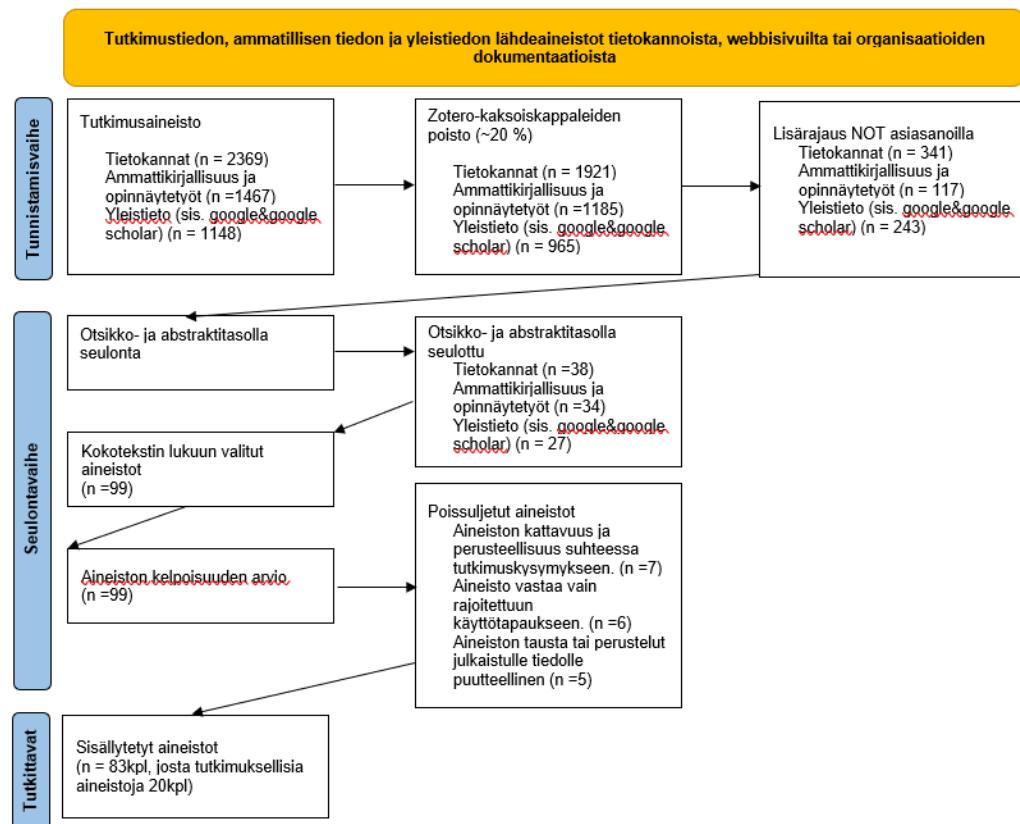
Tutkimusaineiston valinta ja laadunvarmistus

Tutkimusaineiston valintaprosessi voidaan kuvata PRISMA-kaavion avulla.

Tutkimusaineiston valinnassa on tunnistamis-, seulonta- ja tutkintavaiheet. On tärkeää edetä vaiheittain pienempään määärään tutkimusaineistoa lajitellessa, kriittisesti lukien ja tunnistaen siitä tutkimuksen kannalta oleellista ja merkittävää tietoa. Tutkija itse määrittelemien hakukriteerien lisäksi haussa tulee käyttää luovuutta, harkintaa ja omaa ajattelua. Osana laadunarviointia tehdään sekä alkuperäistutkimusten että oman tutkimuksen kirjallisuuskatsauksen arvointi. Jokainen aineisto arvioidaan erikseen tai yhtenä kokonaisuutena. Yksityiskohtainen arvointi voidaan tehdä tutkimukseen hyväksytyille aineistoille. (Oulun yliopisto s.a; Vilkka 2023, 55–64).

Alkuperäistutkimusten laadunarvioinnissa laatua voidaan arvioida myös julkaisijan tai kirjoittajien auktoriteetin perusteella, ts. kuinka tunnettuja tutkijat ovat ja kuinka paljon heidän töitään on viitattu. Laadunvarmistuksessa kannattaa pitää mielessä myös julkaisuharhan käsite. Se tarkoittaa vääristymää, joka saattaa ohjata tutkijoita julkaisemaan mieluummin sellaisia töitä, joissa on merkityksellisiä tuloksia tai ne esittävät koteen positiivisessa valossa. Tutkija on aina vastuussa lähdekriikitä ja sellaisten aineistojen käyttöä, joilla on poliittisia intressejä tai muita merkittävästi ohjaavia taustoja

on syytä harkita tarkkaan. Tämän tutkimuksen tiedonhakuprosessia on havainnollistettu kuvassa 6. (Oulun yliopisto s.a; Vilkka 2023, 74–77).



Kuva 6. Tiedonhakuprosessi. Mukailleen PRISMA 2020 Flow-kaavio (Prisma 2024)

Tiedonhaku suositellaan kuvaamaan myös muistiinpanojen kautta ja perustelemaan niiden avulla mikä on aineiston oleellinen sisältö ja miten on päätynyt tiettyyn aineistoon. ANTIC-tiedostokortti on tapa esittää valittu aineisto tiivistetynä ja perusteltuna. Tiedostokortin perusteluja voi hyödyntää myös saturaatiopisteenvaihto-tilassa, ts. kun huomataan että aihealueen teemat alkavat toistua, voidaan tiedonkeruu lopettaa (Vilkka 2023, 65–67; Tuomi & Sarajärvi 2018, 72–75). Tutkimukseen valitut tutkimukselliset aineistot perusteluineen, ANTIC-mallia mukaillen on esitelty liitteessä 4. Tutkimukseen otettiin mukaan rajauskriteerien, seulonnan ja kokotekstin luvun jälkeen 83 erityyppistä aineista. Poissulun yleisimpiä syitä oli aineiston sisältö, jossa ei ollut tutkimuksen kannalta merkittävää lisätietoa, tai aineisto ei osunut tutkimuskysymyksiin. Teknologian kehittyminen ei aiheuttanut merkittävästi aineiston hylkäämistä, koska tutkimus ei keskittynyt niinkään yksittäisiin teknisiin ominaisuuksiin. Osa tutkimuksista keskittyi vain rajalliseen

käytöömpäristöön, kuten erikoistuneeseen teollisuuslaitokseen ja nämä jätettiin yleistettävyyden takia pois.

4.2 Teemahaastattelut, havainnointi ja kokeilut

Teemahaastattelujen analyysissä hyödynnettiin tekniikkana teemoittelua.

Tämä on hyvä tapa silloin, kun halutaan löytää litteroiduista tarinoista olennaista tietoa jonkin käytännöllisen tutkimusongelman kannalta.

Semistrukturoituja teemahaastatteluja tehtiin neljä kappaletta, tutkijan tutkimuskysymyksistä esittämillä teemoilla. Valitut haastateltavat edustivat erilaisia työrooleja, erilaisilla taustoilla ja osaamisella. Yksi haastatelluista oli täysin organisaation ulkopuolin tietoturvaekspertti. Haastattelujen kulkua ohjattiin jokaisen henkilön osaamisalueisiin pohjautuen, jonka takia materiaali ja teemoittelut eivät ole jokaisen haastattelun osalta samanlaiset.

Haastatteluaineiston reliabiliteettia ei todettu, koska haastatteluja tehtiin vain yhden kerran per henkilö. Informantien kommentit on dokumentoitu teemoittelun oheen liitteeseen 3 (Hirsjärvi & Hurme 2022, 180–182, 190–195; Pitkäranta, 2014, 89–94).

Teemahaastattelujen purku tehtiin koneellisesti videotallenteesta hyödyntäen Microsoft word tekstinkäsittelyohjelman litterointiomaisuutta. Litteraattien taso muodostui yleispiirteiseksi, ts. keskusteluun liittyvät tauot, huokailut, äänenpainot tai naurahdukset jäivät automaattisesti pois. Teksti jätettiin pääsääntöisesti siihen muotoon kuin automaattinen litterointiomaisuus tuotti sen, lukuun ottamatta korjauksia formatointiin, selviin virheisiin tekstintunnistuksessa tai toistuvien tilkesanojen ketjuihin (tota, tuota, niinku, jep, joo, kylläkyllä), joita siistittiin materiaalista manuaalisesti. Kielen käyttöön, äänen painotuksiin tai elekieleen ei kiinnitetty huomiota analyysityypin takia. (Hirsjärvi & Hurme 2022, 145–155; Puusa & Juuti 2020, 121).

Havainnointia voidaan käyttää monimenetelmäisessä tutkimuksessa todentamaan miten tutkimuksessa havaitut, tai haastatteluissa kerrotut asiat toteutuvat käytännössä. Tutkijan tehtävänä on tarkkailla ilmiön suhdetta ihmisten toimintaan, kuitenkin suhtautuen siihen subjektiivisesti. Tässä tutkimuksessa hyödynnettiin tutkijan osallistuvaa havainnointia työasematurvallisuuden viikkopalavereista. Havainnointijakso tapahtui välillä

tammikuu-syyskuu 2023. Palavereista muodostui havainnointipöytäkirjoja, joiden materiaali teemoitettiin vastaavasti kuten teemahaastattelut.

Havainnointipöytäkirjat ovat työn liitteessä 7 julkisuuslain mukaisesti salattuna. Pöytäkirjat sisältävät yksityiskohtaista organisaation salaista materiaalia, joka paljastuessaan voisi aiheuttaa toimeksiantajalle merkittäviä tietoturvariskejä tai haittaa (Laki viranomaisten toiminnan julkisuudesta 21.5.1999, 6. luku 24.§ kohta 21). (Puusa & Juuti 2020, 127–137; Eskola & Suoranta 1998, 73–76).

Havainnointipöytäkirjoista teemoiteltu ja anonymisoitu aineisto löytyy liitteestä 2. Haastattelu- ja havainnointiaineistosta nousevien teemojen ja seikkojen yhteyttä toisiinsa tarkastellaan tarkemmin tutkimustulosvaiheessa.

Kokeilut toteutettiin tutkijan omalla työasemalla, jossa oli valmiina tietoturvakovennuksia, sekä erillisellä Windows-virtuaalikoneella, joka alustettiin kokeiluja varten täysin oletusasetuksille. Kokeiluista muodostui kokeilupöytäkirjoja, joihin kirjattiin huomioidut työkalujen käytöstä. Pöytäkirjat löytyvät opinnäytetyön liitteestä 1. Pöytäkirjoja ei ole teemoiteltu, koska niitä hyödynnetään työssä työkaludokumentaation käytännön validoinnissa. Kokeilujen huomioita hyödynnetään tutkimustulosten triangulaatiossa.

4.3 Kirjallinen konstruktio ja käyttöönottomalli

Tutkimuksen aineiston ja teoreettisen viitekehyn selvitessä kattavan kirjallisen konstruktion tarve tutkimusongelman käsitteiden ja taustojen kuvaamiseksi organisaation intervencioehdotuksen tueksi tuli entistä selvemmäksi. Tutkimuksen liitteessä 5 on tutkimuksen toimeksiantajalle suunnattu kattava vertaileva kirjallinen konstruktio. Kokonaisuus sisältää vertailua eri tietoturvastandardeista ja kehysistä, käytäntötason standardeista sekä järjestelmäkovennuksen ja auditoinnin näkökulmista että työkaluista. Konstruktio on koostettu ilman tutkimuksellisia artikkeleita ja se koostuu vain julkisesti saatavilla olevista tietoturvakehysten dokumentaatioista, ammattiaineistoista sekä vapaan verkon aineistoista.

Konstruktioita voidaan hyödyntää itsenäisenä ja yleistetynä tietoturvakehysten ja työasemajärjestelmäkovenヌsten koulutus- tai pohjamateriaalina. Konstruktion lisäksi työasematieturva kehittävä organisaatio voi saada

apua yleistetystä taulukkolaskentamallista, joka luotiin esittelemään työasematurvallisudessa tarvittavia elementtejä, niiden resurssivaateita, sekä tietoturvakehysten suhdetta tarvittaviin resursseihin. Taulukkolaskentatyökirja löytyy tutkimuksen liitteestä 6.

5 TUTKIMUSTULOKSET

Tutkimustulokset esitetään vastauksina työlle asetetuille tutkimuskysymyksille ja niiden teemoille. Tulokset perustuvat kerättyihin aineistoihin, kuten tutkimusartikkeleihin, ammattikirjallisuuteen, sekä havainnoinnin, teemahaastattelujen ja kokeilupöytäkirjojen aineistoihin. Lisäksi tuloksia verrataan tutkimuksen aikana luotuun kirjalliseen konstruktioon.

Tutkimusartikkeleissa oli käytetty useita eri tutkimusmenetelmiä, kuten kyselytutkimuksia, kirjallisuuskatsauksia ja kehittämistutkimuksia. Aineistoa analysoidessa oli mukava huomata, kuinka hyvin primääriaineistosta nousseet teemat tukivat sekundaarisen aineiston, kuten tutkimusartikkeleiden, tuloksia ja päinvastoin. Kummankin aineistotyypin käyttö oli kuitenkin perusteltua, koska pienet vivahde-erot toivat erilaista näkökulmaa samaan teemaan. Eri lähteisten aineistojen toisiaan tukevat huomiot antavat niille luotettavuutta. Tutkimustulokset on jaettu tutkimuskysymysten ja aineiston teemoittelun mukaisesti eri alaotsikoiden alle.

5.1 Windows-työaseman tietoturvan kovennus

Alaotsikko vastaa tutkimuskysymykseen 1: mitkä tietoturvakehykset ja parhaat käytännöt tai niiden osat ovat soveltuivia Windows-työaseman tietoturvan koventamiseen?

Tietoturvakehykset, standardit ja parhaat käytännöt

Maailmalla on käytössä useita kilpailevia, eri käyttötarkoituksiin tehtyjä tietoturvakehyksiä ja standardeja. Tietoturvakehyksiä ja standardeja laativat yleensä asiantuntijaorganisaatiot kuten ISO/IEC, CIS, NIST, DISA sekä tietyt valtiot ja viranomaiset. Tietoturvakehykset sisältävät ohjeistuksia tietoturvaan parantavista parhaista käytännöistä, kun taas standardit antavat tarkan vaatimuksen tietyn asian toteuttamiseksi. Kehysten ja standardien lisäksi

kansalliset lait ja regulaatiovaatimukset, kuten GDPR voivat asettaa tietoturvavaatimuksia organisaatioille. (Duncan & Whittington 2014; Trustcloud s.a.).

Organisaation erilaisista tarpeista ja lähtökohdista johtuen voi olla vaikea valita sopivaa tietoturvakehystä. Kehykset eivät ole myöskään yhteismitallisia, vaikkakin osaa kontolleista on mahdollista verrata ristiin. Tietoturvakehysten käyttöönotto koetaan monesti haasteelliseksi, niiden geneerisyyden takia. Vuonna 2018 julkaistun HIMSS:n kyselyn mukaan NIST:n ja CIS:n tietoturvakehysten käytön yleisyys kattaa yhteensä 85 % kaikista kyselyyn vastanneista (Hamdani ym. 2021). Tietoturvakehysten sisältämien parhaiden käytäntöjen käyttöönotto vaatii asiantuntemusta, aikaa ja resursseja, varsinkin koska niiden suositusten lähteitä ja perusteluita ei aina ole tuotu ilmi (Siponen & Willison 2009). Ihmisten, prosessien ja teknologian välistä yhteistoimintaa ei myös usein oteta tarpeeksi huomioon tietoturvakehysten parhaissa käytännöissä (Malatji & Marnewick 2019).

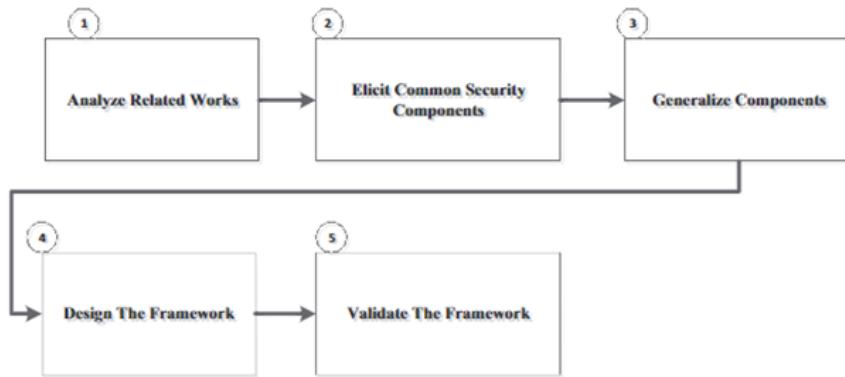
Uusien tietoturvakehysten kehittäminen onkin nousussa kansallisten toimijoiden ja tutkijoiden toimesta, johtuen nykyisten tietoturvakehysten puutteesta (Dedeke & Masterson 2019). Tutkimusten mukaan organisaatiot käyttävät tietoturvakehyksiä kehämisestä, niiden sisältämien päällekkäisten suositusten takia (Nicho 2018). Uudet kehitetyt mallit kattavat yleensä vain minimivaatimukset tietyn asian, kuten käyttöjärjestelmän kovennuksen toteuttamiseksi (Hamdani ym. 2021). Toisaalta nykyisiä kehyksiä voidaan hyödyntää tekemällä tietoturvakovenusten kartoitus niitä vasten (eng. mapping) ja onpa osa kehysten valmistajista, kuten CIS tehty myös kehysten välille vastaavan kartoituksen. Osa tietoturvakehyksistä on myös jättänyt täysin osan tietoturvakategorioista määrittelemättä, ja viittaa niissä suoraan toiseen laajempaan keykseen, kuten ISO:on tai NIST:n (Clark 2020; CIS s.a.a; Di Giulio ym. 2017).

Erityisesti Windows-työaseman kovennukseen keskittyneitä kehyksiä ei ole montaa. Yleisimpiä käytäntötason tietoturvakehyksiä on vertailtu tutkimuksen liitteessä 5 olevassa kirjallisessa konstruktiossa, joista on tunnistettavissa kaksi laadukkainta Windows-tietoturvaan keskittyväät tietoturvakehystä: CIS benchmark ja DISA STIG. Kokeilupöytäkirjojen ja kehysten dokumentaation

perusteella näiden kahden kehyksen käyttöön löytyy kattavasti ohjeistuksia ja laadukkaita työkaluja. Microsoft Seccon ei oikein ole valmis, vaan jäännyt kehitysasteelle, vaikkakin se tarjoaa tarkemman mallin työasemien segmentointiin, kuin kaksi muuta kehystä. CIS ja DISA STIG mallien etuna on, että ne rakennetaan aina tiettyä käyttöjärjestelmäversiota varten, jolloin uudet ominaisuudet ja muutokset tulevat huomioiduksi. Toisekseen niiden rakenne on yksityiskohtainen ja määrämuotoinen. Kumpikin näistä kehyksistä noudattelee hyvin samankaltaista rakennetta, jossa on kategoria, kontrolli, kontrollin tarkoitus, kuvaus, vaikuttavuus ja kontrollin käyttöönotto-ohjeistus. (Liite 5, Käytäntötason kehykset ja tietoturvakovenus; Liite 1).

Sami Laihon (Liite 3) mukaan Microsoftin itse koostama security baseline tai CIS ovat kumpikin hyviä tietoturvakehyksiä työaseman tietoturvan parantamiseen. Niillä saavutetaan työasemaan perustason tietoturvasuojauskset, koska yrityskäytössä on oltava jonkinlaiset peruskäytännöt joka tapauksessa. Kehysten käytöllä ei kuitenkaan ratkaista sitä, joutuuko yritys tietomurron kohteeksi, mutta niillä päästään alkuun suojausten kanssa. (Liite 3, TMH1).

Haastateltavan 2 (Liite 3) mukaan toisaalta työasematietoturva voidaan tehdä myös ilman tietoturvakehyksiä, ainakin teknisestä näkökulmasta katsottuna. Työaseman tietoturvatoteutukseen voi vaikuttaa kulloisenkin lainsäädännön vaatimukset, mutta ongelma näissä on usein, että niitä ei ole organisaatiossa dokumentoitu, vaan otettu vaan käyttöön. Organisaatiolle itse laadittu kustomoitu vaatimuskehys on haastateltavan mukaan helpompi kartoittaa julkisesti tunnettuihin kehyksiin kuin toisinpäin. (Liite 3, TMH2). Haastateltavan kustomointiajatusta tukee kuvassa 7 Atoum ym. (2022) esittelemä malli, jossa rakennetaan holistinen tietoturvakehys. Mallin rakennuksessa edetään vaiheittain tutustuen ensin olemassa oleviin kehyksiin, tunnistamalla ja yleistämällä niistä yhteiset komponentit, jonka jälkeen kehys suunnitellaan ja validoidaan (Atoum ym. 2022).



Kuva 7. Holistisen tietoturvamallin rakennus (Atoum ym. 2020)

Haastatteluissa tuli ilmi, että yksinkertaistenkin työasematioturvakaytosten käyttö vaatii ylläpidolta aikaa, kouluttautumista, testaamista, tiedottamista ja määritysten hallittua jakelua. Näillä toimilla varmistetaan ylläpidettävyys ja työasemaylläpidon kuormituksen hallinta. Ylläpito voi kokeilla tietoturvakaytosten käyttöä itsekin, mutta ideaalililanteessa tietoturvakaytosten hyödyntämiseen olisi hyvä olla erillinen resurssi, joka voisi keskittyä vain siihen työhön (Liite 3, TMH3, TMH4).

Havainnointipöytäkirjojen perusteella työasemien tietoturvaominaisuksien hallinta tapahtuu jo täällä hetkellä toimeksiantajan organisaatiossa hyvin testaten, tiedottaen ja hallittua jakelua hyödyntäen. Tietoturvakayksiä ei kuitenkaan hyödynnetä millään tasolla työasematurvallisuudessa (Liite 2).

Havainnollistan tutkimuksen kirjallisessa konstruktiossa käsiteltyjen tietoturvakaytosten luokittelua itse luomallani hypoteettisella mallilla kuvassa 8. Esitän että luokittelumalli tukisi tietoturvakaytosten käyttöä suunnittelevien organisaatioiden päätöstentekoa ja ymmärrystä suunnitellun kehyksen käytön vaatimuksista ja tuotoksista. Taulukkomuotoinen luokittelumalli on osa työaseman tietoturvan käyttöönottomallia, jossa myös havainnollistetaan tarvittavia resursseja, sidonnaisuuksia ja esitetään hypoteettinen käyttöönottomalli (Liite 6)

Kehyksen tai standardin nimi	Luokka			
SABSA Security architecture	Tietoturva-arkkitehtuurimalli			
NIST Cybersecurity Framework	Ylätason tietoturvakehys/hallintamalli			
NIST Security and Privacy Controls for Information Systems	Ylätason tietoturvakehys/hallintamalli			
Digitaalisen turvallisuuden arkkitehtuuri (Dtark)	Ylätason kansallinen tietoturvakehys			
Funktioaalisen turvallisuuden malli	Uhka- ja riskipohjainen tietoturvamalli			
CIS Critical security controls	Uhka- ja riskipohjainen tietoturvamalli			
Mitre att&ck ja d3fend	Uhka- ja riskipohjainen tietoturvamalli			
DISA Security Technical Implementation Guide	Käytännön työasematioturvakehys			
CIS Benchmarks	Käytännön työasematioturvakehys			
Windows security baselines	Käytännön työasematioturvakehys			
Microsoft SecCon	Käytännön työasematioturvakehys			
Kehyksen tai standardin nimi	Luokka	Avaliressursit Käyttöönnoton resurssivaatimus	Yläpidon resurssivaatimus	Ydinisästä
SABSA Security architecture	Tietoturva-arkkitehtuurimalli	Suur	Keskisuur	Kyberturvallisuuden hallintamalli, laatu, määrimuotoisuus, mitattavuus
NIST Cybersecurity Framework	Ylätason tietoturvakehys/hallintamalli	Keskisuur	Keskisuur	Organisaation kyberturvallisuuden lähtökohtainen riskienhallintaohjeisto
NIST Security and Privacy Controls for Information Systems	Ylätason tietoturvakehys/hallintamalli	Keskisuur	Keskisuur	Kattava kyberturvallisuuskontrollien käytönotto-ohjeisto, myös vasteimustenmukaisus
Digitaalisen turvallisuuden arkkitehtuuri (Dtark)	Ylätason kansallinen tietoturvakehys	Keskisuur	Keskisuur	Nist cybersecurity framework, rikastettuna suomalailla standardilla ja lain vasteimukaisilla
Funktioaalisen turvallisuuden malli	Uhka- ja riskipohjainen tietoturvamalli	Suur	Keskisuur	Ulkailtahtinen metodologia tietoturvakontrollien asettamiseen, hallintamalli, vaikuttaa prosesseihin
CIS Critical security controls	Uhka- ja riskipohjainen tietoturvamalli	Suur	Keskisuur	Uhkapohjainen tietoturvamalli työasematuorvaan
Mitre attack ja d3fend	Uhka- ja riskipohjainen tietoturvamalli	Suur	Keskisuur	Uhkapohjainen tietoturvamalli työasematuorvaan
DISA Security Technical Implementation Guide	Käytämön työasematioturvakehys	Keskisuur	Pieni	Yritystasoisem tekevän työasematioturvaviran käytöönotto
CIS Benchmarks	Käytämön työasematioturvakehys	Keskisuur	Pieni	Yritystasoisem tekevän työasematioturvaviran käytöönotto
Windows security baselines	Käytämön työasematioturvakehys	Pieni	Pieni	Yritystasoisem tekevän työasematioturvaviran käytöönotto
Microsoft SecCon	Käytämön työasematioturvakehys	Pieni	Pieni	Malli yritystasoisesta noillepäihien työasemamallin rakennuksen avaksi
Selitteet				
Käyttöönnoton resurssivaatimukset				
Pieni	Muutamaa kuukausia, jos käytössä sopiva osaaminen			
Keskisuur	Useampia kuukausia-vuosi, jos käytössä sopiva osaaminen			
Suuri	Puhutaan koko organisaation läpitemppuavasta käyttöönnotosta, projektiltaa voi hyvin olla useampi vuosi			
Yläpidon resurssivaatimukset				
Pieni	Hyvin tehtävässä yhden tilinin sisäisesti, ilman merkittävää sidonaisuuksia			
Keskisuur	Vasta useaman tilinin yhteyttäminä, organisaation tukia sekä tilapäisesti ulkopuolista apua			
Suuri	Jos ylätaso muuttuu suurtoiseksi, on ehkä paikallaan tarkoitus jo käyttöönottaa ja pyrkii saamaan resurssivaatimukset pienemmäksi.			
Värien merkitys				
	Työasemayläpidon resurssit			
	Työasematioturvan resurssit			
	Hallintolisen tietoturvan erityisosamoinen			
	Teknisen tietoturvan erityisosamoinen			
	Ulkotilointi			

Kuva 8. Ehdotus tietoturvakehysten luokittelumallista (Tarkkonen 2024a)

Tietoturvakovennukset

Tietoturva-alalla puhutaan usein kerroksellisesta tietoturvasta ja suojausten syvyydestä (eng. layered defense, defense in depth). Näitä termejä käytetään usein synonyymeinä toisilleen, koska niiden keinot ja tavoitteet ovat osittain samoja. Lähtökohta kerroksellisessa tietoturvassa on, että kasaamalla monta erilaista puolustuskeinoa tai metodia järjestelmää uhkaavan vaaran eteen, saavutetaan niiden yhteisvaikutuksella tietoturvallinen järjestelmä.

Esimerkkinä kerroksellisesta tietoturvasta on turvallisuustuote, joka sisältää antivirustuotteen, palomuurin, antispm suojan, sekä yksityisyysensuojaksen. Analogiana näille suojauksille voi ajatella keskiaikaisen linnan eri tyypisiä suojausmuotoja, kuten vallihautoja, muureja, jousimiehiä ja ansoja. Kerroksellinen tietoturva määrittelee suojaukset karkeasti kolmeen eri kerrokseen; fyysiset suojaukset, ihmisten osuus ja teknisten kontrollien kerros. Defense in depth on enemmänkin strategia, jonka idea on, että yksittäiset tietoturvakerrokset ovat vain tapa hidastaa ja

vaikeuttaa hyökkääjää, kunnes hyökkääjä joko turhautuu tai hyökkäys havaitaan ja se voidaan torjua lisätoimien avulla. Strategiassa otetaankin huomioon monitorointi, havainnointi, ihmisten aktiviteettien seuranta, toipumiskyky, sekä raportointi ja analysointi. (Techrepublic 2008; Medium 2016; Dataprot 2023; Liite 5, kpl 1.7).

Käyttöjärjestelmän täytyy pystyä takaamaan sen päällä toimiville sovelluksille ja käyttäjille turvallinen tiedonkäsittely-ympäristö. Yleiskäytöisen käyttöjärjestelmän, kuten Windowsin tapauksessa tämä on erityisen vaikeaa, koska sovellukset jakavat käyttöjärjestelmän käyttämän laitteiston, jolloin myös sovellusten pääsy toistensa käyttämiin muistialueisiin, tallennustilaan ja suoritusympäristöön täytyy suojata. Täydellinen turvallisuus onkin lähes mahdottomus, mutta siihen voidaan pyrkiä toteuttamalla käyttöjärjestelmään tietoturvakovenkuksia (Silberschatz ym. 2018, luku 16).

Laihon (Liite 3) mukaan Windows on lähtökohtaisesti huonosti suojattu yrityskäytöön. Oleellisimmat periaatteet yritystason tietoturvakovenkuksissa ovat vähimmän käyttöoikeuden periaate, ylläpitökäyttöoikeuksien poisto tai rajoukset vain turvallisille laitteille, sovellustason pääsylistat (eng. application whitelisting) sekä päätelaitopalomuurit. Laihon mukaan sovellustason pääsylistojen hallinta ja merkitys ymmärretään monesti vasta auditoinnin jälkeen (Liite 3, TMH1).

Työaseman tietoturvan kovettaminen vaatii jatkuvan prosessin, jolla valittujen keinojen efektiivisyyttä seurataan ja tarkistellaan. Kokonaisuutta määrittelevänä terminä voidaan käyttää konfiguraationhallintaa. Tietoturvakovenkuiset voidaan karkeasti jakaa vaiheittain käyttöjärjestelmän asennuksen aikaisiin valintoihin sekä elinkaaren aikaiseen muutostenhallintaan. Elinkaarenhallintaan kuuluu päivitystenhallinta ja ohjelmistojen versiomuutokset. Käyttöjärjestelmään kohdistettavat asennuksen aikaiset toimet tehdään yksittäisiä parametrejä tai asetuskokonaisuuksia määrittelemällä. Asetusten määrittelyyn kuuluu myös sovellus- ja käyttöoikeuksien määrittelyt. Tämän lisäksi karsitaan tarpeettomia teknisiä työasemaominaisuksia. protokollia ja ohjelmistoja. Tästä kokonaisuudesta syntyy ns. perustaso, jonka pohjalta rakennettu Windows

työasemakokooppano on kovennettu. (Mistry ym. 2018; Zamora ym. 2019; Hamdani ym. 2021; Dunkerley & Tumbarello 2022).

Oriyanon (2017) mukaan olennaisinta tietoturvakovennuksissa on, että ne tiukentavat järjestelmän oletustasoisia tietoturvaominaisuksia. Erityisesti vähimmän käyttöoikeuden periaate ja ehdoton kielto ovat hyviä periaatteita. Nämä tarkoittavat sitä, että riippumatta järjestelmän ominaisuudesta, sen käytämiseen myönnetään vähimmät käyttöoikeudet. Ehdoton kielto on voimassa aina oletuksena, jollei joku ole erikseen sallittua. Oriyano kertoo myös kattavasti penetraatiotestaamisesta, jonka avulla voidaan etsiä väärinmäärittelyitä ja haavoittuvuuksia, sekä suosittelee sen käyttöä aina tietoturvakovenusten todennuksessa. (Oriyano 2017)

Työasemien tietoturvakovenusten kokonaisuuteen liittyviä asioita selittää erittäin hyvin Ibor:n & Obidinnu:n (2015) kasaama kuva 9. Pelkästään koventamalla tietoturvapolitiikkoja esim. kehysten suositusten mukaan ei saavuteta suojattua laitteistokokooppanoa, vaan kovennekset pitää toteuttaa kerroksittain, ottaen huomioon kaikki kokonaisuuteen kuuluva. (Ibor & Obidinnu 2015)

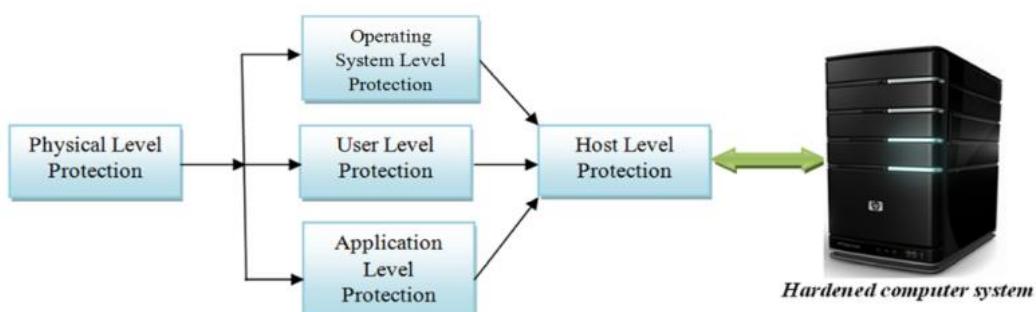


Figure 1: System hardening architecture for safer access to critical business data

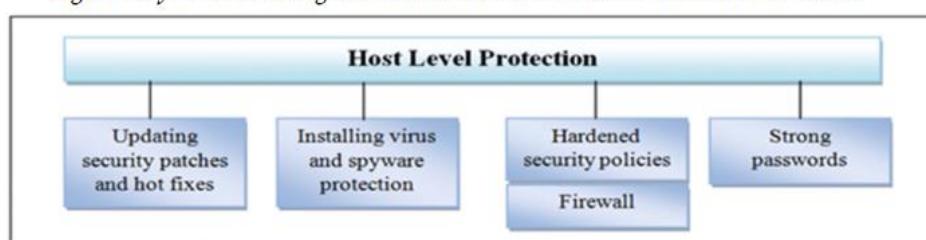


Figure 2: Host level protection for systems hardening

Kuva 9. Järjestelmän tietoturvakovenusten kokonaisuus (Ibor ym. 2015)

Haastateltavan 3 ja 4 mukaan tietoturvakovennuksia toteutetaan organisaatiossa lukien teknisiä dokumentteja ja niiden suosituksia

asiantuntijatiimilla, jonka jälkeen kovennukset testataan ja toteutetaan vaiheittain. Toteutuksessa ollaan siirtymässä pilvipohjaisten työkalujen käyttöön, joissa on kuitenkin havaittavissa ongelmia asetusmuutosten kohdistumisen kanssa. Erityisen hankalaa on, ettei ylläpitäjä aina tiedä milloin uudet jaellut asetukset lopulta aktivoituvat työasemajoukkoon (Liite 3, TMH3 & TMH4).

Havainnointipöytäkirjat vahvistavat asiantuntijatiimin työmetodin. Oli kiinnostava huomata, että huolellinenkaan tietoturva-asetusten testaaminen ei aina auta, koska joskus ongelmat tietoturvakovennusten kanssa tulevat esii vasta tuotantoon jaeltujen muutosten jälkeen. Toinen mielenkiintoinen seikka tietoturvakovennusten suhteen oli, että pitkällä havainnointijaksolla ei kertaakaan arvioitu tai muutettu asiantuntijatiimilla käyttöjärjestelmän peruskokoonpanon määritystä, vaan kaikki muutokset kohdistuivat uusiin ominaisuuksiin. Syynä tälle on valittu kovennustapa, jossa uuden käyttöjärjestelmän alustavan peruskokoonpanon jälkeen se siirtyy ylläpitotilaan, jolloin perusteisiin ei kosketa, ennen seuraavaa määrämuotoista alustatarkastusta (Liite 2)

5.2 Windows-työaseman käytännön tietoturva ja uhkat

Alaotsikko vastaa tutkimuskysymyksen 2 teemaan: ovatko parhaiden käytäntöjen ja tietoturvakehysten suositukset ajantasaisia ja kattavia Windows-työaseman käytännön tietoturvan ja uhkien kannalta?

Haavoittuvuushallinta

Laihon (Liite 3) mukaan käytännön työasematietoturva on käännyttänyt tilastojen mukaan haavoittuvuuksien korjaamiseen phishing-estojen sijaan.

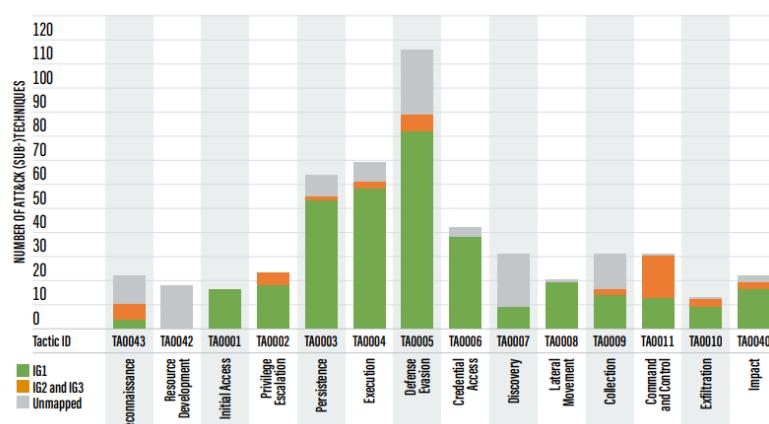
Ransomwarehyökkäykset alkoivat useammin työaseman takaporttien kautta, kuin ihmisen huolimattomuuden takia. Tietoturvakehysten suositusten ohilausee koko ajan uusia haavoja, joten niitä noudattamalla ei pelkästään ratkaista työaseman tietoturvaa. Haavoittuvuushallintaan löytyy valtavasti työkaluja, mutta haavojen korjaaminen vaatii tiedon yhdistelyä ja ammattitaitoa, ml. korjausten priorisointi, joten pelkästään työkaluilla ei voi ratkota ongelmia (Liite 3, TMH1).

Uhkapohjaisen tietoturvakehyksen hyödyntäminen

Laihon (Liite 3) mukaan Mitre (att&ck) on hyvä tapa ilmaista haavoittuvuuksia ja niiden käyttötapoja, mutta se toimii hyvin vain isomissa ympäristöissä, joissa on riittävät resurssit sen hyödyntämiseen. Mitre:n mallia on esitelty tutkimuksen liitteessä 5 (Liite 5, kpl 1.6; Liite 3, TMH1).

Haastateltavan 2 mukaan käytännön tietoturva toteutuu parhaiten tekemällä organisaatiolle omat vaatimukset, joita vasten voidaan katsoa esim. uhkatieloon pohjautuvan tietoturvakehyksen avulla vastaavatko ne omat vaatimukset ulkoista kehystä. Työaseman turvaaminen voidaan aloittaa tutkimalla ensin yleisimmät uhkat, riskit ja haavoittuvuudet. Näistä voidaan tunnistaa vaatimukset ja niitä vasten parhaat käytännöt kehysten kautta. (Liite 3, TMH2)

CIS on kehittänyt uhkapohjaisen community defense mallin. Mallin tarkoituksena on kartoittaa CIS:n kontrollien vastaavuus Mitre att&ck:n, esittämiin uhkapolkuihin ja taktiikoihin sekä raportoida samalla kontrollien efektiivisyys tietyn tyypisiä hyökkäyksiä vasten. Kartoituksia on havainnollistettu kuvassa 10.



TACTIC ID	TA0043	TA0042	TA0001	TA0002	TA0003	TA0004	TA0005	TA0006	TA0007	TA0008	TA0009	TA0010	TA0011	TA0040
	45%	0%	100%	100%	86%	88%	77%	90%	29%	95%	52%	92%	97%	86%
ATTACK TYPE	% OF ATT&CK (SUB-)TECHNIQUES DEFENDED AGAINST BY I61 CIS SAFEGUARDS										% OF ATT&CK (SUB-)TECHNIQUES DEFENDED AGAINST BY CIS SAFEGUARDS			
Malware	77%										94%			
Ransomware	78%										92%			
Web Application Hacking	86%										98%			
Insider and Privilege Misuse	86%										90%			
Targeted Intrusions	83%										95%			

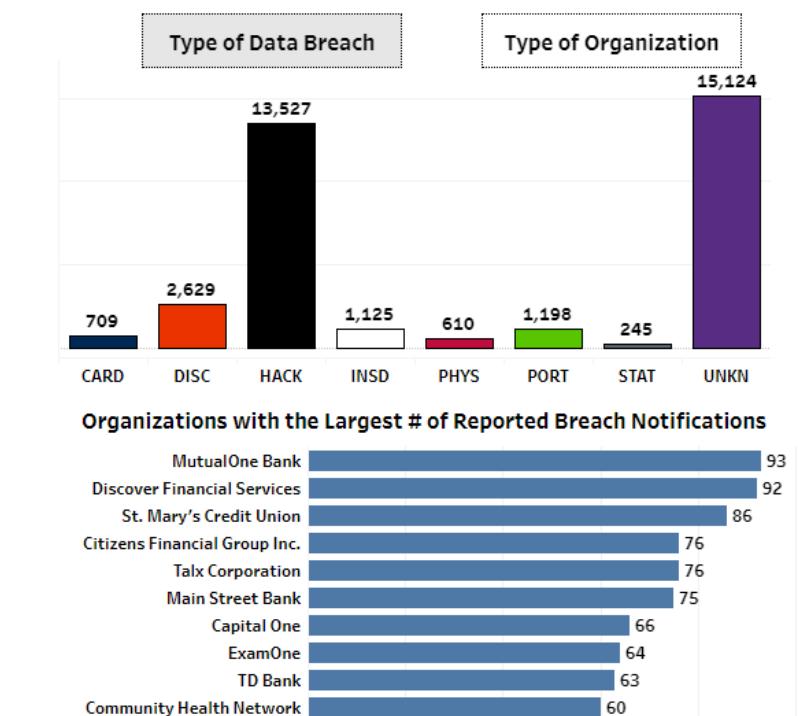
Kuva 10. CIS community defense malli (CIS 2022)

Mallin pohjana on tietoturvayhteisön työ, kuten Verizon DBIR-raportti ja MS-ISAC:n tiedot tärkeimmistä hyökkäyksistä. (CIS 2022; Liite 5, kpl 1.5)

Uhkatieto ja riskiarviot

Antonucci (2017) painottaa kyberuhkien seurantaa ja riskiarvioiden tekemistä, sekä sisäisten että ulkoisten uhkien ja riskien osalta. Uhkatiedolla tarkoitetaan kyberturvallisuusalan koostamia raportteja, uutiskirjeitä ja statistiikkaa uusimmista hyökkäystavoista tai toimijoista. Riskiarviot hyödyntävät uhkatietoa pohjana arvioitaessa tietoturvatoimien nykytilan riittävyyttä organisaatiossa. Yrityksen tietoturva ei tulisi perustua pelkästään tietoturvakehysten noudattamiseen, koska tällöin katsotaan aina tilannetta taaksepäin. (Antonucci 2017, Luvut 7,14,15).

Uhkatieto voi olla esimerkiksi statistiikkaa tapahtuneista tietomurroista, kuten privacyrights:n julkisista lähteistä kerätty tietomurtotietokanta. Raportti esittää tietomurtotyypit, kuten hakkeroinnit ja laitteiden häviämiseen johtaneet tapahtumat (eng. hack, port). Statistiikkaa voi myös filtteroida organisaatiotyypin ja aikajanan mukaan (kuva 11). Tietokanta sisältää myös jokaisen tietomurron osalta siitä julkaistun informaation. (Privacyrights s.a)



Kuva 11. Tietomurtotietokanta. (Privacyrights s.a)

Toisaalta uhkatieto voi olla hyvinkin holistisesti koostettua. Verizon on rakentanut oman avoimen uhkatietoturvakehyksensä veris:n. Tämä uhkatietokehys pyrkii yhdistämään tiedot uhkatoimijoista, toimista, resursseista, hyökkäystavoista, sekä organisaatiotypeistä. Veris on kartoitettu vasten Mitren att&ck- sekä CIS:n Critical Security Controls tietoturvakehystä. Verizon julkaisee uhkatietokehyksen avulla kartoitettua tietoa tietomurto (eng. data breach) raportin muodossa. Havaintojen kooste kertoo mielenkiintoisia faktuja: 83 % murroista tapahtui ulkopuolisen toimijan toimesta ja 73 % näistä tapahtumista sisälsi ihmiselementin.

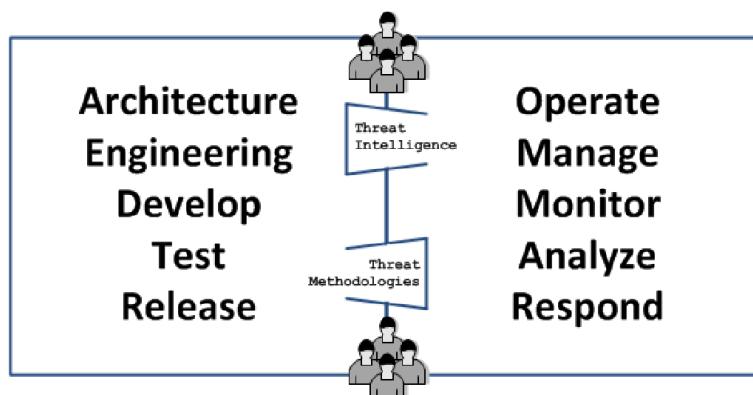
Hyödynnettyjä metodeja olivat käyttöoikeuksien väärinkäyttö, varastetut käyttöoikeudet, virheet, sosiaalinen hakkerointi tai haavoittuvuuksien hyväksikäyttö. Raportti myös suosittelee tiettyjä CIS:n mukaisia tietoturvakontrolleja havaintoja korjaaviksi toimiksi. Verizon tarjoaa raportin lisäksi kehyksen avulla kartoitetusta tiedosta mittavan avoimen tietokannan työkaluineen GitHub sivullaan. (Verizon s.a; Verizon s.a.b).

Havainnointipöytäkirjan perusteella uhkamallinnusta hyödynnetään organisaatiossa ainakin uusien käyttöjärjestelmäversioiden käyttöönottoissa. Mallinnuksella pyritään tunnistamaan tietoturvaheikkouksia työpajatyöskentelynä. (Liite 2)

Funktionaalisen tietoturvan hallintamalli

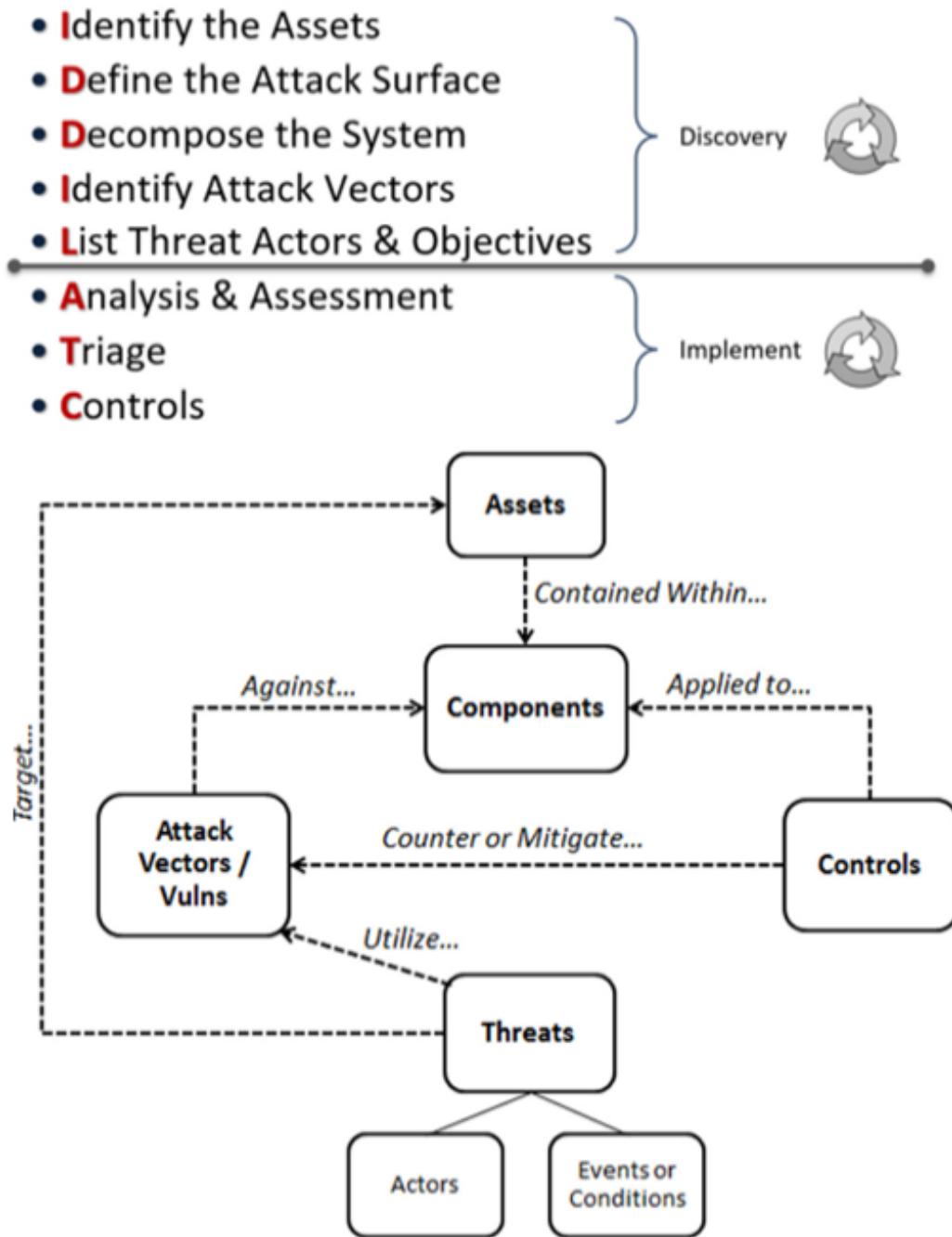
Muckin ja Fitch (2019) esittävät nykyisten riskienhallintakeinojen keskittyyvän liikaa vaatimustenmukaisuuden täyttämiseen tietoturvakehysten tai standardien avulla, joka pakottaa organisaation keskittymään turvallisuuskontolleihin ja haavoittuvuuksiin. Tämä vääristymä pakottaa organisaatiot jättämään uhkien tarkastelun sivuseikaksi. Lisäksi kyberturvallisuuden funktiot ovat segmentoituneet eri tiimeihin, kuten arkkitehtuuriin, ylläpitoon, suunnittelun ja valvontaan. Näiden välillä ei kulje riittävästi tietoa käytännön ongelmista ja uhkista, jonka takia tekeminen on kankeaa. Ongelman korjaamiseksi esitetään funktionaaliseksi integroitua tietoturvaorganisaatiota, joka sijoittaa uhkat, uhka-analyysin ja uhkatiedon ensimmäiseksi portaaksi järjestelmien kehitys ja operointimalleja.

Organisaatiomalli mahdollistaa tietoturvakontrollien arvioinnin, käyttöönnoton ja mukauttamisen aina sen hetkisiä tärkeimpää uhkia ja hyökkäyskeinoja varten. Organisaatiomallissa uhkatieto ja käytännön ongelmat tulevat syötteenä suunnittelusta ja tietoturvateknoloista vastaaville, jotka kehittävät niihin ratkaisuja. Tällainen malli parantaa organisaation tietoturvalilaa ketterästi. Kuvassa 12 on esitetty mallin mukaisesti toimivan organisaation uhkakäsittely. (Muckin & Fitch 2019).



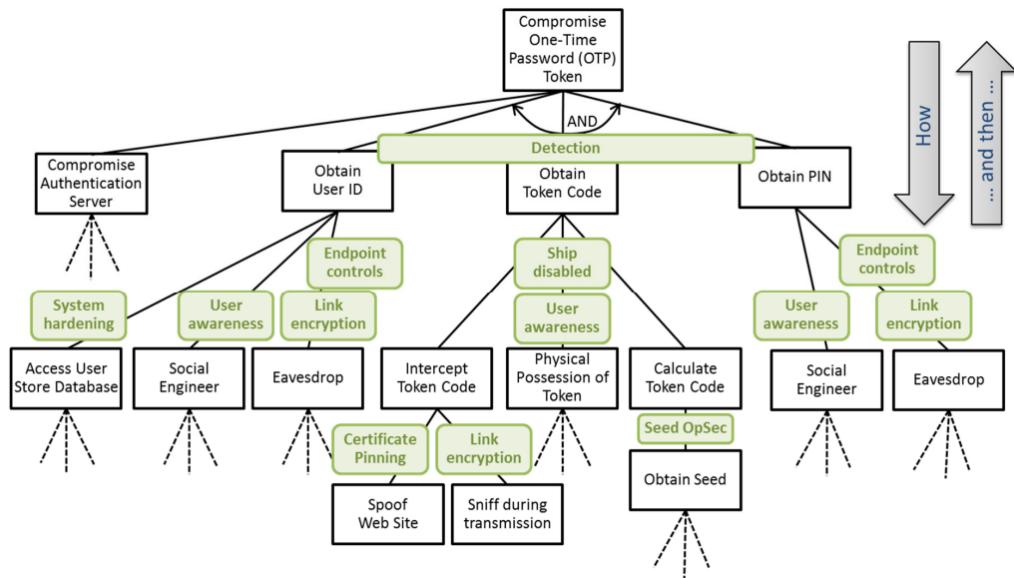
Kuva 12. Funktionaalisen turvallisuuden organisaatiomalli (Muckin & Fitch 2019)

Muckin ja Fitch (2019) kertovat kannattavansa luotettavuuteen pohjautuvia kehitysmalleja, kuten FMEA/FMECA, joiden periaate on, että korkeaa laatua noudatteleva kehitys johtaa myös korkeaan tietoturvallisuuteen. Nämä mallit eivät kuitenkaan palvele tietoturvallisuutta ja siksi kirjoittajat esittelevät kuvassa 13 jatkuvaan kehitykseen tarkoitettun IDDIL/ATC-metodologian, sekä sitä tukevan käsitemallin, jonka avulla organisaatio voi toteuttaa uhkapohjaista tietoturvaa.



Kuva 13. Mukautettu kuva. Iddil/ATC-metodologia sekä käsitemalli. (Muckin & Fitch 2019)

Yksinkertaisimillaan tällaisella mallinnuksella saadaan aikaiseksi tietoturvinventaario uhkista, hyökkäyskeinoista, kohteista ja niihin liittyvistä korjaavista kontrollleista. Organisaatio voi toki hyödyntää mallinnuksen apuna muitakin malleja, kuten esimerkiksi Microsoft:n stride-lm:ää tai hyökkäyspuita. Hyökkäyspuurakennetta on havainnollistettu kuvassa 14.



Kuva 14. Hyökkäyspuurakenne (Muckin & Fitch 2019)

Lopputuloksena näillä mallinnuksilla on ns. uhkatiedon hallintajärjestelmä. Järjestelmä kattaa kategorisoidut uhkat, funktioaalisten tietoturvakkontrollien katalogin, kontrollien efektiivisyysmittariston, sekä arkkitehtuurilliset kuvat kokonaisuudesta. (Muckin & Fitch 2019).

5.3 Windows-työaseman auditoitavuus ja tilannekuva

Alaosikko vastaa tutkimuskysymyksen 3 teemaan: mahdollistaako parhaisiin käytäntöihin ja tietoturvakehykseen perustuva Windows-työaseman kovennus auditoitavuuden ja organisaatiotasoinen päätelaitetietoturvan tilannekuva?

Auditoitavuus, vaatimustenmukaisuus ja tarkastus

Auditoitavuuden toteutuminen riippuu siitä mitä sillä haetaan. Weiss:n ja Solomon:n (2015) mukaan vaatimustenmukaisuuden auditoinnissa taustalla on jokin laki, standardi tai alan vaatimus. Tällöin tietoturvakkovenusten toteuttaminen tietoturvakehyksen avulla helpottaa ja nopeuttaa tietenkin itse auditointiprosessia, koska auditoijan kysymyksiin on näyttää valmis kovennettu kokoonpano. Toisaalta Duncan:n ja Whittington:n (2014) mukaan IT-turvallisuudessa voidaan puhua varmistuksesta, joka tarkoittaa suojaustoimien toimivuuden ja vaikuttavuuden tarkastusta. Nicho:n (2018) mukaan käytännössä yksittäiset auditoinnit ja vaatimustenmukaisuuden tarkastus eivät johda jatkuvaan tietoturvan parantumiseen. Jotta auditoinnilla

saavutetaan merkittäväyttä, tulee yksittäisten auditointien liittyä osaksi jonkinlaista jatkuvaa hallintamallia. (Weiss & Solomon 2015; Duncan & Whittington 2014; Nicho 2018)

Laihon mukaan ”tietoturvakehykset ovat soveltuivia auditointiin, ainakin siinä mielessä, että voidaan mitata onko yritys ymmärtänyt, että Windows pitää konfiguroida eri lailla yrityskäytöön kuin kotikäytöön”. Kehysten käytön voidaankin ajatella parantavan perus tietoturvan tilannekuvaan. (Liite 3, TMH1)

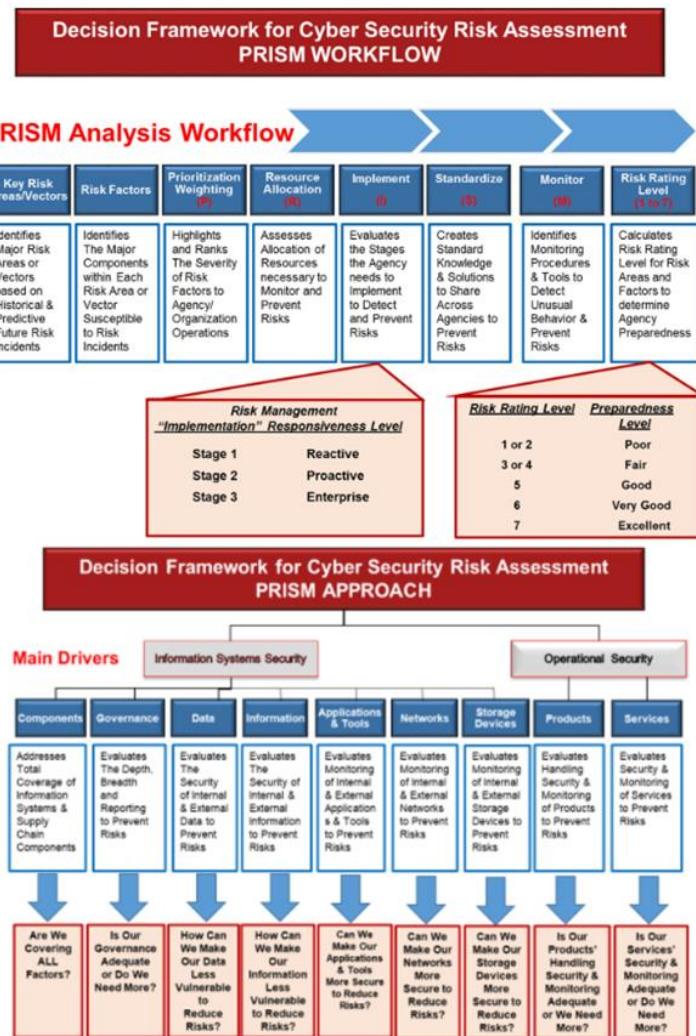
Auditointia mahdollistaa haastateltavan 2 mukaan se, että on olemassa yksinkertaiset suorituskykyvaatimukset, jotka pysyvät muuttumattomina. Esimerkiksi tekninen toteutus voi muuttua, mutta alkuperäinen vaatimus pysyy. Johdolle suojausvaatimuksen toteutuminen on tärkeämpi kuin sen takana oleva tekniikka. Haastateltavan mukaan työasematurvallisuuden uhkamaailman seurannalla ja ulkopuolisilla auditoinneilla voidaan korvata jopa jatkuva tietoturvakehyksiin pohjautuva omavalvonta (Liite 3, TMH2).

Havainnointipöytäkirjan ja haastateltavan 3 ja 4 mukaan organisaatio toimii tällä hetkellä juuri em. auditointiprosessin varassa, jota kutsutaan ns. alustatarkastukseksi. Auditoinnin havaintojen perusteella korjataan ja parannetaan tietoturvan tilaa työasemissa. Auditointia tukee organisaatiossa raportti, joka sisältää ylätason kuvaukset käytetyistä tietoturvakontrolleista (Liite 3 TMH3, TMH4; Liite 2).

Tilannekuva

Haastateltavan 2 mukaan organisaation dokumentointikäytännöt ovat puutteellisia. Ajatusta tukevia kommentteja on tunnistettavissa myös haastateltavan 3 ja 4 haastatteluiden pohjalta. Tilannekuva muodostuu haastateltavan 2 mukaan valvonnan ja reagoinnin yhteistyöstä. Jollei dokumentaatio ole ajantasaisista tämä yhteistyö kärsii. Ilmentymänä puutteellisesta dokumentaatiosta on ajantasainen käyttötapauskuvaus (tietoturvan näkökulmasta) erilaisista työasemien käyttötapaiksista, esim. etäkäyttölinjaukset tai laitteiden käyttö julkisisissa tiloissa ja verkoissa. (Liite 3, TMH2, TMH3, TMH4).

Goel ym. (2020) kertovat että johdon näkyvyys ja päätöksenteon perusteet tulevat pohjautua riskiarvioihin organisaation kyberuhkista. Tilannekuvan heikkous organisaatiossa johtuu siitä, että johdolla ei ole riittävää näkyvyyttä priorisointiin, resursseihin, implementointiin, standardisointiin, valvontaan ja riskiarvioihin. Bongiovanni ym. (2022) kertoo tilannekuvaongelmien johtavan tietoturvaratkaisujen aliresursointiin. Goel ym. (2020) ehdottavat toteuttamaansa holistista prism-riskimallia ratkaisuksi tilannekuvan parantamiseen. Kuvassa 15 on havainnollistettu mallin sisältämiä kategorisoitun riskivaiheiden käsitteilyä ja niiden sidontaa käytännön prosesseihin. (Goel ym. 2020).



Kuva 15. Riskipohjainen päätösmalli, mukautettu kuva. (Goel ym. 2020)

Tuomalla mallin kautta sekä tietoturvan että operatiivisen tietoturvan komponentit näkyviksi riskipohjaisen päätösmallin alle, johdon tilannekuva organisaation tietoturvaratkaisuista paranee. Malli ottaa huomioon kaikki IT:n ja tietoturvan osa-alueet (Goel ym. 2020).

5.4 Windows-työasematurvan määrämuotoinen hallinta

Alaosikko vastaa tutkimuskysymyksen 4 teemaan: miten Windows-työaseman tietoturvaa ja auditoitavuutta voi hoitaa hallitusti ja määrämuotoisesti?

Automaatio ja työkalut

Muita työasemien tietoturvakovenkuksiin keskittyviä opinnäytetöitä ja tutkimusaineistoja analysoitaessa ilmeni selkeästi yksi toistuva havainto: tietoturvakehysten suositusten käyttöönottoon ei ole automaatiota. Leppäsen (2017) toteutus tietoturvakovenkuksista vaati ryhmäkäytäntöjen (eng. group policy) hyödyntämistä. Joissain yksittäistapauksissa voidaan tehdä käyttöönottoja komentoriviskriptejä tai -käskyjä hyödyntäen, mutta vain pienessä skaalassa. Clark (2020) oli yritynyt toteuttaa automaatiota ansible konfiguraationhallintatuotteella, mutta sekin joutui tukeutumaan skriptipohjaisiin itse rakennettuihin komentoihin. Jögi:n (2017) toteutus koski linux-järjestelmää, mutta päätyi samaan lopputulokseen, jossa tietoturvakehyksen suosittelemien kovenヌusten toteutus tehtiin manuaalisesti tai konfiguraationhallintatuotteella. (Jögi 2017; Leppänen 2017; Clark 2020)

Stöckle ym. (2020) toteavat, että vaikka DISA:n pohjat ovat xml pohjaisia, ne eivät ole silti koneluettavassa muodossa. Ilman automatisointia pohjien käyttöönotto on virheherkkää. Tämän takia tutkijat toteuttivat kunnianhimoisen tutkimuksen, jossa DISA STIG-scap-pohjaisista Windows 10 tietoturvamallipohjista pyrittiin luonnollisen kielimallityökalun avulla irrottamaan suositusten käyttöönnottopolut ja komennot. Näitä irrotettuja metodeja verrattiin Windows:n oman turvallisuusmallin sisältämiin konfiguraatiopolkuihin automaation mahdollistamiseksi. Tämä tavoite toteutui 83 %:sti, mutta vaati silti powershell komentokielen avulla tehdyn moottorin hyödyntämistä, sekä puuttuvien osien manuaalista asettamista (Stöckle et.al 2020).

Kokeilupöytäkirjat vahvistavat automaation puutteen siinä mielessä, että tietoturvakovenustyökalut kuten CIS-CAT ja SCAP compliance checker tarkastavat nykyisen konfiguraation vasten valittua kovenヌusmallia, mutta eivät tee käyttöönottoja. Työkaluja voi kylläkin hyödyntää määrämuotoisessa

dokumentaatiossa. Testattu haavoittuvuushallinnan työkalu viittasi yleisiin CVE määritysten löytämiensä haavojen osalta, joka on varmasti helpottaa korjausten suunnittelua. Työkaluilla on helppo raportoida ja testata nykytilanne. (Liite 1)

Työkaluja testiin etsiessä havaittiin, että kaupallisesti on olemassa työkaluja, kuten steelcloud configOS, joka tuotekuvauksen mukaan tukee sekä CIS että STIG pohjaisten tietoturvakovenusten automaattista käyttöönottoa. Tätä nimenomaista työkalua ei kuitenkaan päästy testaamaan ajanpuutteen ja työkalun maksullisuuden takia (steelcloud s.a.).

Useat aiemmissa tutkimuksissa viitatuin Microsoftin omat työkalut oli ajettu alas niiden vanhentumisen takia (mm. mbsa, security baseline analyzer). Erityisesti tietoturvakovennuksiin keskittyvän työkalun sijaan Microsoft suosittelee nykyään hyödyntämään powershell skriptauskielen mukana tulevaa hallittavan konfiguraation moduulia (eng. desired state configuration).

Microsoft on itse toteuttanut moduulia hyödyntävän DSC environment analyzer työkalun. Työkalun ytimessä on referenssitiedosto, jonka ylläpito voi itse rakentaa. Tätä tiedostoa vasten voidaan tarkistaa nykykonfiguraation tilanne tai asettaa konfiguraatio sitä vastaavaksi. Microsoft ei kuitenkaan itse tarjoa esim. CIS:iä vastaavia referenssitiedostoja, mutta yhteisöpohjaisesti kehitettyjä malleja löytyy, kuten NVISOsecurity:n posh-dsc hardening projektin. (Microsoft s.a; Nvisosecurity s.a).

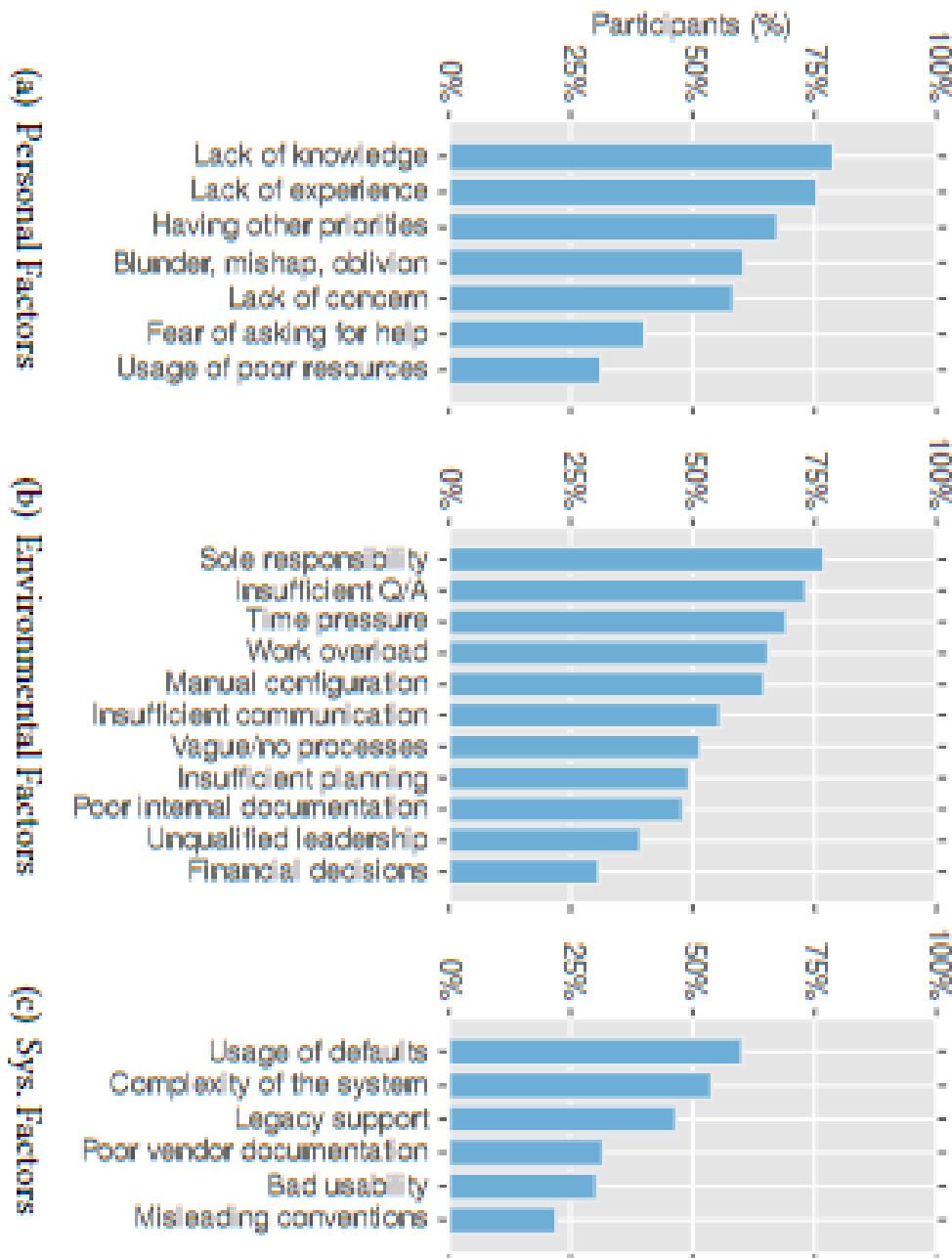
Virhekonfiguraatiot ja kiire

Haastateltavan 4 mukaan organisaatiossa on reagoitu ulkopuolelta tulleenseen uhka- tai haavoittuvuustietoon nopeastikin, ohittaen muutoshallinta, joka on aiheuttanut myös ongelmia. Tiedotus tehdyistä muutoksista saattaa olla kiireessä myös puutteellista. Virhekonfiguraatiot johtuvat nykyään myös toimittajan puolelta tulevan dokumentaation ylimalkaisuudesta tai jopa puutteellisuudesta. Välillä dokumentaatiot voivat olla virheellisiä tai vanhentuneita, ja näitä ei sitten kiireessä keretä tarkistamaan, joka johtaa testausvaiheessa väärin havaintoihin.

Kiire johtaa myös teknisen muutosvelan kertymiseen, joka taas aiheuttaa ongelmia muutostilanteissa, kun kaikkea ei keretä varmistamaan. Tyypillinen prosessiongelma haastateltavan mukaan on myös tietoturvakontrollien hajautuneisuus eri tuotteisiin ja eri tiimien hallintaan. Työasematiimi ei enää pysty muodostamaan niistä kokonaiskuvaaa. (Liite 3, TMH4).

Xu ja Zhou (2015) kertovat järjestelmien monimutkaisuuden vaikeuttavan virhekonfiguraatioiden tunnistamista ja vältämistä. Dietrich ym. (2018) tutkimus ja sen kyselyt ja haastattelut olivat kohdistettu erityisesti järjestelmälläpitäjille. Tutkimus pystyi osoittamaan, että tietomurtoihin ja tietoturvatapahtumiin johtaneet syyt ovat olleet merkittävästi ihmisten tekemiin virheisiin liittyviä. Esimerkiksi päivitysten puutteet, oletusmääritysten käyttö, tietoturvakovenusten puute ja järjestelmien käyttöoikeus- ja pääsynestojen puutteet olivat yleisiä syitä.

Näillä virheillä on tutkimuksen mukaan yhteistä se, että ne tapahtuvat järjestelmän jo ollessa käytössä, kehitysvaiheen sijaan. Syt virheisiin olivat henkilökohtaisia, ympäristöstä johtuvia tai järjestelmiin liittyviä. Erityisesti ylläpitäjät painottivat virheiden väältämisessä prosessipohjaisuutta, suunnitelmallisuutta ja organisaation johdon tukea toteutettavan tehtävän laadun varmistukseen. Organisaation johdon tuki mainittiin myös budjetin, resurssien ja aikapaineiden osalta. Myös ylläpidon osaaminen tai sen puute, järjestelmien monimutkaisuus ja vastuiden epäselvyys koettiin ongelmiksi. Näitä syitä on havainnollistettu kuvassa 16. (Dietrich ym 2018).



Kuva 16. Virhemäärittelyt (Dietrich ym 2018)

Tutkimuksen mukaan jopa 76 % vastanneista oli tehnyt virhekonfiguraatioita ja jopa 30 % näistä virhekonfiguraatioista oli johtanut tietoturvatapahtumaan. Osasyynä virhekonfiguraatioille on tutkimuksen mukaan se, että uuden järjestelmän käyttöönnotossa tärkeämpänä pidetään järjestelmän toimivaksi saamista kuin sitä, mitkä asetukset ja niiden yhdistelmät tekevät siitä samalla turvallisen. Haastateltavat myönsivät myös, että tietoturvan virhekonfiguraatiot ovat todennäköisesti yleisempiä kuin niistä tehdyt ilmoitukset. Tähän syynä on ylläpitäjien häpeä ja pelko syytöksistä, kuten kävi esim. equifax:n laajassa

tietovuodossa, jossa koko tapahtuman syyksi osoitettiin työntekijän vastuulla olleen järjestelmän päivittämättömyys. Mielenkiintoista oli, tietoturvaongelmaan johtaneet virhemääritykset nostivat hetkellisesti organisaation tietoturvahuomiota merkittävästi. Valitettavasti tämä ei useasti johtanut kuitenkaan jatkuvaan tietoturvan parantumiseen, vaan vanhat prosessit ja tavat palasivat hetken päästä takaisin. Tutkijat esittävät muutaman merkittävän virhemääritynsä korjaavan toimen: automaation hyödyntäminen, valmiusharjoittelu, neutraali jälkipurku virhetilanteille, dokumentaation ajantasaisuus ja muutoshallinta. (Dietrich ym. 2018).

Prosessit

Haastateltavan 2 mukaan työasematurvallisuus pitäisi kuulua työasemaylläpidosta vastaaville, osana työaseman laadunvarmistusta. Yksi perustelu tälle on, että työasematiimin pitää osata määritellä ja vaatia työasematurvallisuuden valvontaa, jonka organisaation tietoturvalvonta hoitaa, ei toisinpäin. Toisaalta ainoastaan työasematiimi voi varmistaa työaseman toimivuuden, joka on yhtä tärkeä tietoturvaperiaate kuin tiedon suojaaminen (Liite 3, TMH2).

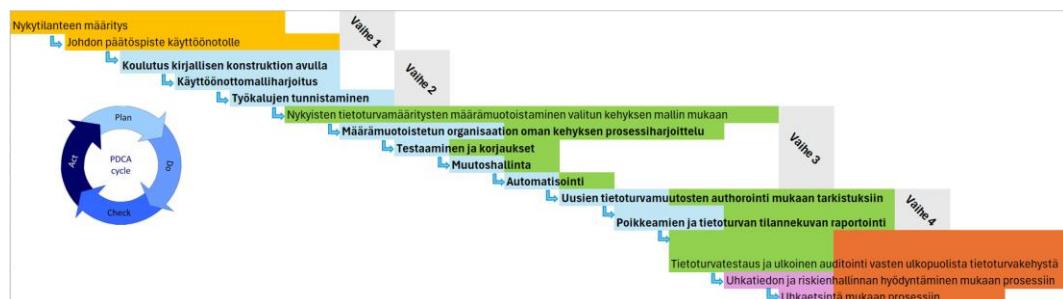
Haastateltavien 3 ja 4 mukaan tietoturvapäivitysten jakelu ja poikkeamahallinta tehdään määrämuotoisesti ja hallitusti. Toimittajan järjestämiin tietoturvakokouksiin osallistutaan, josta saadaan syötteitä tietoturvaongelmista. Poikkeamaraportit tehdään, jos käyttäjille koituu näkyviä ongelmia tietoturvatapahtumista. Haastateltavat ehdottivat säännöllisin välein tilattavaa tietoturvakontrollit tarkastavaa lisäresurssia keinoksi parantaa toimintaa. Määrämuotoisen prosessin toimivuudesta saatuiin vahvistus havainnointipöytäkirjojen kautta. (Liite 3, TMH3, TMH4; Liite 2)

5.5 Interventioehdotuksen esittely

Organisaation teemahaastattelut ja havainnointi kertovat selkeästi, että monta tutkimuksessa esiin tullutta asiaa on hyvällä mallilla tälläkin hetkellä. Tutkimustulosten hyödynnettävyys interventioehdotuksena olisi helpompaa, jos organisaatio olisi aloittamassa työasematurvallisuuden kehittämistä puhtaalta pöydältä. Tällöin interventioehdotuksen ytimessä olisi

tutkimustulosten perusteella uhka/riskipohjainen metodologia, joka hyödyntää uhkapohjaista tietoturvakehystä tietoturvakovenkuksia ohjaavan kehyksen lisäksi. Toimivan resursoinnin ja prosessien rakentaminen olisi myös merkittävästi helpompaa, kuin olemassa olevien muuttaminen.

Tämän tutkimuksen ytimessä oli kuitenkin toimeksiantajan nykyinen organisaatio ja sen tarve löytää parhaat käytännöt erityisesti Windows-työaseman järjestelmälliseen koventamiseen, auditointavuuteen ja tilannekuvaan. Interventioehdotus on tämän takia vaiheistettu, koska kokonaisuus on liian laaja toteuttaa mille tahansa organisaatiolle yhtenä isona muutoksesta. Järjestelmällisen kovenkuksen vaiheet 1–4 voidaan toteuttaa PDCA-mallin mukaan kokonaisuuden toteutuksesta riippumatta. Projekti toteuttaa työasematiimi, jonka tukena toimii opinnäytetyön tekijä. Vaiheesta kolme eteenpäin tarvitaan myös erityisesti työasematurvallisuuteen keskittyvä resurssia, tai työasematuen uudelleenresursointia, jolla taataan riittävä osaaminen ja ajankäyttö tekemiselle. Intervention vaiheistusta on havainnollistettu kuvassa 17.



Kuva 17. Interventioehdotuksen vaiheistus (Liite 6)

Työn liitteenä (Liite 6) olevassa käyttöönottomallissa voidaan mallintaa myös resursointia ja työn priorisointia. Käyttöönottomallin harjoittelu kuuluu vaiheeseen 2. Vaiheet ja kehitysaskeleet on priorisoitu käyttöönottomallissa. Muut vaiheet vaativat myös merkittävästi suunnittelua ja/tai mahdollisuksia tehdä muutoksia organisaation IT:n ja tietoturvan prosesseihin ja toimintaan. Vaikeustason kasvua suhteessa kehitysaskeleisiin on myös kuvattu käyttöönottomallissa.

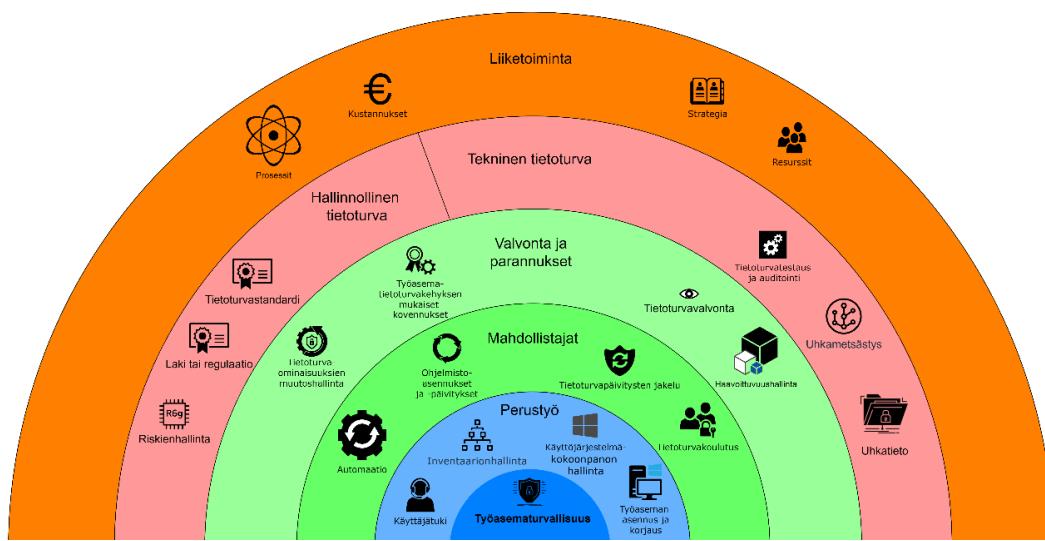
Opinnäytetyön tutkimus tukee erityisesti vaiheita 1–4. Näiden vaiheiden käyttöönotto parantaa merkittävästi työaseman tietoturvan järjestelmällistä

kovennusta hyödyntäen parhaita käytäntöjä ja tietoturvakehyksiä.

Auditointavuus paranee, koska organisaatio voi tarkastaa tai varmistaa itse määritysten paikkansapitävyyden vasten asetettua kokoonpanoa. Tällöin ulkopuolin tarkastus tai auditointi voi keskittyä peruskokoonpanoasetusten sijaan vaikeammin havaittaviin tietoturvaongelmiin, mahdollisesti hyödyntäen uhkametsästystä tai penetraatiotestausta. Päätelaitetietoturvan tilannekuva paranee vasta vaiheesta 4 eteenpäin, jolloin otetaan mukaan funktionaalisten tietoturvakkontrollien katalogi sekä niiden efektiivisyyttä mittaava malli.

6 JOHTOPÄÄTÖKSET

Tutkimusta tehdessä selvisi, että tutkimusongelmaan sisältyvät asiat ja ongelman korjaavat toimet ovat erittäin monimutkaisia. Niihin vaikuttaa sekä ihmisten, teknologian että prosessien suhde toisiinsa. Havainnollistan kuvassa 18 työasematurvallisuuden osa-alueita ja toimintoja sekä niiden suhdetta toisiinsa. Osa-alueiden käyttöönnoton priorisointia on ehdotettu liitteen 6 käyttöönottomallissa perustuen tarvittavaan osaamiseen, resurssien määrään ja tarvittavaan aikaan.



Kuva 18. Työasematurvallisuuden sidonnaisuudet. (Tarkkonen 2024b)

6.1 Analyysi Windows-työaseman tietoturvan kovennuksesta

Tutkimustuloksissa ja kirjallisessa konstruktiossa tuli hyvin ilmi tietoturvakehyksiin liittyvät sidonnaisuudet, joista olennaisimpana on niiden kehämäisyys, limittyminen ja eri käyttötarkoitukset. Ylätason tietoturvakehyksiä hyödynnetään riskienhallintänäkökulmasta tai

vaatimustenmukaisuuden näyttämiseen. Lisäksi voidaan hyödyntää uhkapohjaista tietoturvakehystä, ennen työaseman tietoturvan kovennuksessa käytettävän kehyksen valintaa. Useiden kehysten käyttöä ei voi oikein edes välttää koska osa niiden sisällöistä on lain vaatimuksia, kuten GDPR tai suomalainen tiedonhallintalaki.

Työaseman käytännön tietoturvakehyksen valinta tehdään pääsääntöisesti CIS:n ja DISA:n kehysten välillä. CIS:n kehyksen jatkuva hyödyntäminen vaatii käytännössä maksullisen pro palvelun hankinnan, heikon perusversion raportoinnin takia. Näiden kahden kehyksen sisällöissä ei ole suuria eroja, mutta DISA:n formaatti vaikuttaa kustomoitavuuden kannalta paremmalta vaihtoehdolta. Erittäin hieno ominaisuus DISA:n pohjassa on sen xml-pohjaisuus, jonka ansiosta organisaatio voi itse kehittää DISA:n formaatin pohjalta oman kustomoidun tietoturvakontrollit sisältävän kehyksen.

Työaseman tietoturvakehykset ottavat hyvin huomioon käyttöjärjestelmän peruspohjan tietoturvakovennukset. Tietoturvakehysten käyttö parantaa laatua ja poistaa virhekonfiguraatioiden mahdollisuksia, erityisesti jos konfiguraatioita valvotaan tai tarkastellaan jatkuvasti sitä varten tehdynillä työkalulla. Käyttöjärjestelmän päälle asennettujen sovellusten tietoturva täytyy myös koventaa. Joihinkin yleisimpiin selaimiin tai sovelluksiin löytyy parhaita käytäntöjä, mutta usein sovellustason tietoturva vaatii erityisasiantuntemusta. Jopa käyttöjärjestelmän omista ominaisuuksista kuten PowerShell-komentotulkista löytyy tietoturvan kannalta kovennettavia asioita, joiden kovennukseen toimittaja antaa omat ohjeistuksensa tietoturvayhteisön ja ammattilaisten lisäksi.

6.2 Analyysi Windows-työaseman käytännön tietoturvasta ja uhkista

Haastatteluiden, kirjallisen konstruktion, havaintojen ja tutkimustulosten perusteella työasematurvallisuus kannattaisi rakentaa uhkapohjaa hyödyntäen. Uhkapohjaisuus tuli ylitsevuotavan paljon eteen sekä tutkimustiedon, haastattelujen että havaintojen tasolla. Uhkapohjaisuudella saavutettaisiin valittujen tietoturvakontrollien parempi kohdistuvuus käytännön uhkia vastaan. Tämä tapa parantaisi myös merkittävästi tietoturvavalvonnan ja työasemakonfiguraatioista vastaavien yhteistoimintaa. Uhkapohjaisesti

toimiessa kaikki osapuolet ymmärtäisivät mitä, miksi ja miten tiettyä tietoturvauhkaa torjutaan milläkin tietoturvan kerroksella.

Tietoturvan kerroksellisuus ja vähimpien oikeuksien periaatteet korostuvat tutkimuksessa, joita noudattamalla moni käytännön tietoturvauhka on jo suoraan estettävissä. Käytännön tietoturvaa voidaan tarkastaa ja todentaa hyödyntämällä valvontaa, haavoittuvuushallintaa ja uhkametsästystä. Lisäksi käytännön tietoturvaa voidaan parantaa seuraamalla ja ottamalla tietoturvan uhkatiedon käsittely mukaan.

6.3 Analyysi Windows-työaseman auditoitavuudesta ja tilannekuvasta

Windows-työaseman auditoitavuus tarkoittaa käytännön tasolla tarkastusta, jolla voidaan varmistua käyttöjärjestelmäkonfiguraation tietoturvan ja kontrollien efektiivisyydestä. Tutkimuksen perusteella tietoturvakehyksen käyttöönotto vähentäisi auditoinnissa tarvittavaa aikaa, joka toimeksiantajan organisaatiossa kuluu käspelin tehtävään tietoturvatakastukseen.

Auditoitavuus toteutuu toimeksiantajan organisaatiossa mutta se tapahtuu haastattelujen perusteella niin harvoin, että väliaikoina konfiguraatiomuutokset voivat johtaa tietoturvaongelmiin. Jatkuva tietoturvakehykseen sidottu automatisoitunut tarkastus parantaisi suoraan organisaation tilannekuvaan työasematurvan tasosta. Tilannekuva paranisi samalla kehyksen tarkastuksesta muodostuvan automaattisen dokumentaation myötä ja vapauttaisi aikaa tehdä esim. työaseman käyttötapaustestauksia.

6.4 Analyysi Windows-työasematurvan määrämuotoisesta hallinnasta

Windows-työasematurvallisuuden hallintaan vaikuttaa luotettavasti toimivien käyttöönotto/automaatioratkaisujen puutteet. Vaikuttaa siltä, että organisaatio joutuu investoimaan joko rahaa erillisen automaatiotyökalun hankintaan, tai merkittävästi aikaa ottaakseen kustomoidun työkalun kuten Microsoft-dsc:n käyttöön. Vaikka konfiguraationhallintatyökalut eivät toimi täydellisesti ja niiden käyttö lisää ylläpitotaakkaa ainakin hetkellisesti, poistaa niiden käyttö kuitenkin virhekonfiguraatioita ja lopulta kiirettä, parantaen myös tehtyjen tietoturvamääritysten laatua. Prosessinäkökulma työasematietoturvan osalta olisi todennäköisesti korjattavissa esim. tutkimuksessa ehdotetulla funktionaalisen tietoturvan mallilla. Samalla koko organisaation tietoturva tulisi

hallittavammaksi, mutta organisaatiomuutokset ovat toki vaativia ja aikaa vieviä.

7 POHDINTA

Tutkimuksen tavoitteena oli tuottaa organisaatiolle tutkimuksen kautta kattava kirjallinen konstruktio ja analyysi tunnistetun ongelman ratkaisevista käsitteistä ja niiden välisistä suhteista. Tämän kokonaisuuden avulla oli tarkoitus tehdä interventioehdotus ongelman ratkaisuun. Sekundäärisenä tavoitteena oli tutkia voitaisiinko tutkimuksen pohjalta toteuttaa työkalu, jonka avulla eri organisaatiot voisivat arvioida oman työasematurvallisuutensa kehityksen resurssivaatimuksia ja sidonnaisuuksia.

Kaikki tavoitteet saavutettiin laadukkaasti ja täydessä laajuudessaan. Kaikkiin tutkimusongelman sisältämiin osa-alueisiin löytyi tutkimuksessa ratkaisu, joka koostuu tutkimustuloksista, interventio-ehdotuksesta, käyttöönottomallista sekä kirjallisesta konstruktiossa. Intervention toteuttaminen tutkimuksen jälkeen tapahtuu organisaation toimesta. Auditoitavuus ja päätelaitetietoturvan tilannekuva vaativat merkittävästi lisätyötä, jota on havainnollistettu käyttöönottomallissa. Voidaan varmasti sanoa, että tutkimus oli onnistunut.

Oma arvioni tutkimuksesta kokonaisuutena on hieman kahtiajakautunut. Toisaalta olen tyytyväinen, että kaikki asetetut tavoitteet täyttyivät ja tutkimustulokset olivat kattavat, mutta tutkimusmenetelmien käyttö olisi voinut olla holistikempaa. Havaitsin toisten tutkijoiden tutkimuksissa erittäin hyviä metodeja tämän tyypisen tutkimuksen toteuttamiseen, kuten meta-analyysi tai sanapari-yhteyksien etsintä. Toisaalta tutkimukseni oli käytännön ratkaisua etsivä, jolloin kyseiset metodit olisivat ennenminkin luoneet vain uutta teoriaa. Keräämäni primääriaineisto on sinänsä mielenkiintoinen verrokki-aineisto muita tutkimuksia vasten. Tämä vertailu olisi kuitenkin vaatinut merkittävästi enemmän aikaa tutkimuksen toteuttamiseen. Tutkimuksen kannalta työn aiheen rajaaminen oli onnistunut, vaikkakin monimenetelmäisyyys paisutti työmäärään ja työn laajuutta.

7.1 Luotettavuus- ja eettisyystarkastelu

Tutkimustulokset on saavutettu työn tutkimusasetelmassa kuvattujen menetelmien avulla. Työ oli monimenetelmällinen ja kaikki työssä käytetyt sekundääriset aineistot on haettu julkisista lähteistä tai tieteellisistä tietokannoista. Hakumenetelmät ja työn toteutus on kuvattu ja dokumentoitu kattavasti ja läpinäkyvästi. Primääriaineistoista havainnointimenetelmän pöytäkirjat on liitetty työhön teemoitettuna, joka valitettavasti heikentää niiden läpinäkyvyttä. Alkuperäiset pöytäkirjat sisälsivät liikaa organisaation sensitiivistä tietoa, jonka takia ne salattiin. Kokeilupöytäkirjat sisältävät sanalliset havainnot kuvien lisäksi.

Teemahaastattelun raakalitteroinnit on toimitettu oppilaitoksen nähtäville, mutta työssä ne ovat teemoitettuna liitteenä. Teemahaastattelujen tutkimustulkinnat on arvioitettu (eng. memberchecking) haastateltavilla, joka varmentaa niiden luotettavuutta. Tutkimustulokset ovat pääosin objektiivisia, lukuun ottamatta interventioehdotusta, joka tutkimusotteen mukaisesti vaati tutkijan tulkintaa ja tuotti laadukkaan julkisesti tarjolla olevan tieteelliseen tietoon pohjautuvan edistyksellisen työkalun osana tutkimustuloksia. Muutamassa tutkimustulosten kohdassa on nähtävissä opinnäytetyön tekijän toteama, joka perustuu havaintoon, eikä sinänsä ole tutkijan mielipide.

Tutkimustyö on toteutettu luotettavasti, koska kaikki aineistot ja niistä saadut tulokset on dokumentoitu, lähteet ovat julkisia ja kuka tahansa voi todentaa aineistoista tehdyt päätelmät ja tiivistelmät vertaamalla niitä julkisiin dokumentteihin. Hyödynnetyt statistiikat ja raportit ovat julkisia ja kenen tahansa saatavilla. Teemahaastattelujen henkilötieto on anonymisoitu, kuten useassa muussakin tutkimuksessa. Työ on toteutettu puolueettomasti, ilman oletuksia tai tutkimusvinoumaa, jota todistaa työssä käytetyt monimuotoiset materiaalit ja ympäri maailmaa tehdyt tieteelliset tutkimukset.

Teemahaastattelut ja työkalujen kokeilujen tulokset todentavat muissa tutkimuksissa ja sekundääriaineistoissa esitettyjä kohtia, joten aineistojen triangulaation kannalta tutkimus on todettavissa luotettavaksi. Työn voidaan myös sanoa olevan eettisesti hyvin toteutettu mm. kattavan dokumentaation vuoksi.

Työssäni tuodaan holistikesti esille tietoturvakehysten hyödyntämiseen työasematurvallisudessa liittyviä käsitteitä sekä ongelmia ja näiden välisiä

suhteita. Vaikka alalla on tehty paljon tutkimusta ja opinnäytetöitä, on niissä keskitytty vain yksittäisten tietoturvakehysten ongelmallisten osa-alueiden parannuksiin, tai teknisten ominaisuuksien käyttöönottoon. Ammattikirjallisuus avaa työni tapaan käsitteiden taustoja sekä perustelee miten joku asia pitää toteuttaa. Olen kuitenkin sitä mieltä, että missään näkemässäni kirjallisessa materialissa ei ole käyty tietoturvakehysten käyttöä suhteessa käytännön tietoturvan toteuttamiseen yhtä holistikesti läpi kuin tutkimuksessani.

Esittelemäni luokittelumalli tietoturvakehyksille on mahdollisesti ensimmäinen, jossa julkisille tietoturvakehyksille esitetään kategorisointia osana niiden hyödyntämistä. En ole myös löytänyt työasematurvallisuuteen keskittynytä tutkimusta, jonka osana olisi tehty työasematurvallisuuden käyttöönottomalliehdotus.

7.2 Jatkotutkimusaiheet

Yleinen kyselytutkimus suomalaisten organisaatioiden kokemista ongelmista työasematurvallisuudessa voisi olla hyvin mielenkiintoinen tutkimus.

Dietrichin ym. (2018) tutkimus oli samankaltainen, mutta tässä voitaisiin erityisesti pureutua suomalaisten organisaatioiden erityispiirteisiin. Toisaalta mielenkiintoista voisi olla myös selvittää kuinka tietoturvaresurssien käyttö suomalaisissa organisaatioissa jakaantuu. Pitäkö esim. esittämäni hypoteettinen käyttöönottomalli paikkaansa, vai puuttuuko siitä jotain osa-alueita? Onko malli täydennettäväissä lisätutkimuksen mukaisella tarkalla tiedolla? Ehkä voisi myös tutkia organisaatioiden käytössä olevien uhkatietolähteiden käyttöä ja niiden hyödyntämistä työasematurvallisuuden apuna? Yleisesti työasematurvallisuuden tilannekuvan parantamiseen liittyvä tutkimus voisi olla myös erityisesti tämän tutkimuksen jatkona hyvä.

Teknisestä turvallisuudesta kiinnostuneelle automaatoratkaisun kehittäminen CIS tai DISA tietoturvakehysten pohjalta, hyödyntäen Microsoft DSC työkalua voisi olla hyvin mielenkiintoinen tehtävä. Tutkimusongelma olisi automaatoratkaisun kehitys tietoturvakontrollien hallintaan. Tässä jatkotutkimuksessa voitaisiin tutkia tarkemmin onko sekä tietoturvakontrollien käyttöönotto, konfiguraationhallinta, testaus, raportointi ja mittaaminen tehtävissä yhdellä työkalulla. Tutkimuksen taustoituksesta on omassa tutkimuksessani ilmi tulleet tietoturvakehysten automaatoratkaisujen puutteet, työkalujen hajanaisuus ja holistisen ratkaisun puute.

Hallinnollisen turvallisuuden parantamiseen tähtäävä jatkotutkimusaihe voisi olla haastatteluissa ilmi tullut zero trust käyttöönnotto. Tässä kulmana voisi olla ristiin kartoituksen teko CIS ja DISA käytännön tietoturvakehysten ja zero trust ideologian välillä. Tutkimus voisi keskittyä löytämään vastauksen ainakin kysymykseen ”voidaanko zero trust ideologialla korvata tietoturvakehysten käyttö” (työasemien tietoturvassa). Tutkimukseni haastatteluissa ilmi tulleet näkökulmat siitä, että työasematurvallisuutta voi tehdä myös ilman tietoturvakehyksiä olisi hyvä koettaa zero trust ideologiaa vasten.

7.3 Loppusanat

Tahdon vielä lopuksi kiittää muutamia henkilöitä, joilla oli suuri vaikutus opinnäytetyöni valmistumiseen:

- Opinnäytetyön ohjaajaani Kimmo Kääriäistä, jonka asiantuntevalla avulla pääsin opinnäytetyön eri vaiheissa ilmenneiden haasteiden kanssa eteenpäin.
- Tietoturva-ekspertti Sami Laihoa, jonka haastattelusta saadut ajantasaiset mielipiteet ja tieto auttoivat merkittävästi tutkimustulosten vertailussa.
- Työnantajaani Verohallintoa, joka tuki ja järjesti hienosti opintovapaita työn toteutusta varten.
- Toimeksiantajan ohjaavaa henkilöä valtavan hienoista keskusteluista tutkimuksen ympärillä.
- Henkilöitä, jotka antoivat arvionsa opinnäytetyön tulosten luotettavuudesta.
- Viimeisenä mutta ei vähäisimpänä vaimoani, joka muiden kiireidensä lisäksi kuljetti jatkuvasti lapsiamme harrastuksiin, jotta pystyin tekemään työtä.

LÄHTEET

- Airaksinen, J. 2011. Teoksessa Jaana Vuori (toim.) Laadullisen tutkimuksen verkkokäsikirja. Tampere: Yhteiskuntatieteellinen tietoarkisto. WWW-artikkeli. Saatavissa: <https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus> [viitattu 28.11.2023].
- Antonucci, D. 2017. The cyber risk handbook, creating and measuring effective cybersecurity capabilities. E-kirja. Saatavissa: <https://kaakkuri.finna.fi> [viitattu 16.10.2023].
- Anttila, P. 2014. Tutkimisen-taito-ja-tiedon-hankinta. WWW-dokumentti. Saatavissa: <https://metodix.fi/2014/05/17/anttila-pirkko-tutkimisen-taito-ja-tiedon-hankinta/> [viitattu 23.08.2023].
- Atoum, I., Otoom, A., Abu, A. 2014. Holistic cyber security implementation framework. Saatavissa: <https://doi.org/10.1108/IMCS-02-2013-0014> [viitattu 18.09.2023].
- Beyondtrust. s.a. Systems hardening. WWW-dokumentti. Saatavissa: <https://www.beyondtrust.com/resources/glossary/systems-hardening> [viitattu 23.08.2023].
- Bongiovanni, I., Renaud, K., Brydon, H., Blignaut, R., Cavallo, A. 2022. A quantification mechanism for assessing adherence to information security governance guidelines. PDF-dokumentti. Saatavissa: <https://doi.org/10.1108/ICS-08-2021-0112> [viitattu 19.11.2023].
- Cimcor s.a. What is System Hardening? WWW-dokumentti. Saatavissa: <https://www.cimcor.com/system-hardening#system-hardening-is> [viitattu 15.10.2023].
- CIS. 2022. CIS Community Defense Model 2.0. WWW-dokumentti. Saatavissa: <https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0> [viitattu 18.01.2024].
- CIS. s.a. CIS mapping and compliance. WWW-dokumentti. Saatavissa: <https://www.cisecurity.org/cybersecurity-tools/mapping-compliance> [viitattu 17.11.2023].
- Clark, R. 2020. Security Automation for Windows Hosts: Hardening of Windows 10 Password Policy. PDF-dokumentti. Saatavissa: https://www.theseus.fi/bitstream/handle/10024/343383/Ronald_Clark_Thesis.pdf?sequence=2 [viitattu 25.12.2023].
- Csoonline. 2021. Seven Ways Technical Debt increases security risk. WWW-dokumentti. Saatavissa: <https://www.csoonline.com/article/570851/7-ways-technical-debt-increases-security-risk.html> [viitattu 23.8.2023].
- Cyphere. s.a. How to reduce your attack surface with system hardening in 2021. WWW-dokumentti. Saatavissa: <https://thecyphere.com/blog/system-hardening/> [viitattu 26.10.2023].

- Dataprof. 2023. The Onion Theory of Data Security Layers. WWW-dokumentti. Saatavissa: <https://dataprof.net/articles/data-security-layers/> [viitattu 22.2.2024].
- Dedeke, A., Masterson, K. 2019. Contrasting cybersecurity implementation frameworks (CIF) from three countries. PDF-dokumentti. Saatavissa: <https://doi.org/10.1108/ICS-10-2018-0122> [viitattu 05.01.2024].
- Dietrich, C., Krombholz, K., Borgolte, K., Fiebig, T. 2018. Investigating System Operators' Perspective on Security Misconfigurations. PDF-dokumentti. Saatavissa: <https://doi.org/10.1145/3243734.3243794> [viitattu 01.12.2023].
- Di Giulio, C., Kamhoya, C., Campbell, R., Spraberry, R., Kwiat, K., Bashir M. 2017. IT Security and Privacy Standards in Comparison: Improving FedRAMP Authorization for Cloud Service Providers. PDF-dokumentti. Saatavissa: <https://doi.org/10.1109/CCGRID.2017.137> [viitattu 12.03.2024].
- Dunkerley, M., Tumbarello, M. 2022. Mastering-windows-security-and-hardening-second-edition. Packt publishing. PDF-dokumentti. Saatavissa: <https://www.packtpub.com/product/mastering-windows-security-and-hardening-second-edition/9781803236544> [viitattu 23.08.2023].
- Duncan, B., Whittington, Mark. 2014. Compliance with standards, assurance and audit: Does this equal security? Acm digital library. PDF-dokumentti. Saatavissa: <http://dx.doi.org/10.1145/2659651.2659711> [viitattu 27.12.2023].
- Eskola, J., Suoranta, J. 1998. Johdatus Iaadulliseen tutkimukseen. Tampere: Vastapaino. E-Kirja. Saatavissa: <https://kaakkuri.finna.fi> [viitattu 23.08.2023].
- Goel, R., Kumar, A., Haddow, J. 2020. PRISM: a strategic decision framework for cybersecurity risk assessment. PDF-dokumentti. Saatavissa: <https://doi.org/10.1108/ICS-11-2018-0131> [viitattu 02.11.2023].
- Hamdani, S., Abbas, H., Janjua, A., Shahid, W. 2021. Cybersecurity Standards in the Context of Operating System: Practical Aspects, Analysis, and Comparisons. ACM Computing Surveys, Vol. 54, No. 3, Article 57. PDF-dokumentti. Saatavissa: <http://dx.doi.org/10.1145/3442480> [viitattu 29.12.2023].
- HIMSS. 2019. Cybersecurity frameworks explained. WWW-dokumentti. Saatavissa: <https://www.himss.org/resources/cybersecurity-frameworks-explained> [viitattu 13.10.2023].
- Hirsjärvi, S., Hurme, H. 2022. Tutkimushaastattelu, teemahaastattelun teoria ja käytäntö. E-Kirja. Saatavissa: <https://kaakkuri.finna.fi> [viitattu 23.8.2023].
- Ibor, A., Obidinnu. J. 2015. System Hardening Architecture for Safer Access to Critical Business Data. PDF-dokumentti. Saatavissa: <https://www.ajol.info/index.php/njt/article/view/124044> [viitattu 20.10.2023].
- Intel. s.a. System hardening. WWW-dokumentti. Saatavissa: <https://www.intel.com/content/www/us/en/business/enterprise-computers/resources/system-hardening.html> [viitattu 23.08.2023].

Jyväskylän yliopisto. 2015. Menetelmäpolku. WWW-dokumentti. Saatavissa: <https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/> [viitattu 23.8.2023].

Jõgi, M. 2017. Establishing, Implementing and Auditing Linux Operating System Hardening Standard for Security Compliance. PDF-dokumentti. Saatavissa: <https://core.ac.uk/download/pdf/237084282.pdf> [viitattu 30.02.2024].

Kananen, J. 2012. Kehittämistutkimus opinnäytetyönä. Jyväskylä: Jyväskylän ammattikorkeakoulu. E-Kirja. Saatavissa: <https://kaakkuri.finna.fi> [viitattu 23.8.2023].

Kananen, J. 2014. Toimintatutkimus kehittämistutkimuksen muotona: Miten kirjoitan toimintatutkimuksen opinnäytetyönä? Jyväskylä: Jyväskylän ammattikorkeakoulu. E-Kirja. Saatavissa: <https://kaakkuri.finna.fi/> [viitattu 24.7.2023].

Kananen, J. 2015. Opinnäytetyön kirjoittajan opas, näin kirjoitan opinnäytetyön tai pro gradun alusta loppuun. Jyväskylä: Jyväskylän ammattikorkeakoulu. E-kirja. Saatavissa: <https://kaakkuri.finna.fi> [viitattu 23.8.2023].

Kananen, J. 2017. Laadullinen tutkimus pro graduna ja opinnäytetyönä. Jyväskylä: Jyväskylän ammattikorkeakoulu. E-kirja. Saatavissa: <https://kaakkuri.finna.fi/> [viitattu 7.2.2022].

Kananen, J. 2019. Opinnäytetyön ja pro gradun pikaopas: Avain opinnäytetyön ja pro gradun kirjoittamiseen. Jyväskylä: Jyväskylän ammattikorkeakoulu. E-kirja. Saatavissa: <https://kaakkuri.finna.fi/> [viitattu 14.2.2022].

Leppänen T. 2017. Practical implementation of Windows end-point security controls : Facing the KATAKRI requirements. PDF-dokumentti. Saatavissa: <http://www.theseus.fi/handle/10024/139806> [viitattu 31.01.2024].

Malatji, M., Von, S., Marnewick, A. 2019. Socio-technical systems cybersecurity framework. PDF-dokumentti. Saatavissa: <https://doi.org/10.1108/ICS-03-2018-0031> [viitattu 18.12.2023].

Medium. 2016. Defence in Depth: The medieval castle approach to internet security. WWW-dokumentti. Saatavissa: <https://medium.com/@sbwoodside/defence-in-depth-the-medieval-castle-approach-to-internet-security-6c8225dec294> [viitattu 18.02.2024].

Microsoft. s.a. DSCEA-DSC Environment Analyzer. WWW-dokumentti. Saatavissa: <https://microsoft.github.io/DSCEA/index.html> [viitattu 11.11.2023].

Mistry, S., Lalwani, P., Potdar, M. 2018. Endpoint Protection through Windows Operating System Hardening. International Journal of Computer Applications Technology and Research. PDF-dokumentti. Saatavissa: <https://doi.org/10.7753/IJCATR0702.1005> [viitattu 28.12.2023].

- Muckin, M., Fitch, S. 2019. A Threat-Driven Approach to Cyber Security. Lockheed Martin Corporation. PDF-dokumentti. Saatavissa: <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Threat-Driven-Approach.pdf> [viitattu 12.12.2023].
- Mäntylä. 2020. Windows 10- ja Debian 10 -käyttöjärjestelmien tietoturvallisuus taktisissa päätelitteissä. PDF-dokumentti. Saatavissa: <https://urn.fi/URN:NBN:fi-fe2020073147854> [viitattu 26.12.2023].
- Nicho, M. 2018. A process model for implementing information systems security governance. PDF-dokumentti. Saatavissa: <https://doi.org/10.1108/ICS-07-2016-0061> [viitattu 08.12.2023].
- NVISOsecurity. s.a. Windows Server Hardening with PowerShell DSC. WWW-dokumentti. Saatavissa: <https://blog.nviso.eu/2020/03/03/windows-server-hardening-with-powershell-dsc/> [viitattu 13.2.2024].
- Oriyano, S-P. 2017. Penetration testing essentials. John Wiley&Sons. E-kirja. Saatavissa: <https://kaakkuri.finna.fi/> [viitattu 23.10.2023].
- Oulun yliopisto. s.a. Systemaattinen tiedonhaku. WWW-dokumentti. Saatavissa: https://libguides.oulu.fi/systemaattinen_tiedonhaku [viitattu 14.10.2023].
- Pernaa, J. (2013). Kehittämistutkimus tutkimusmenetelmänä. PDF-dokumentti Helda-Helsingin yliopiston digitaalinen arkisto. Helsingin yliopisto. Saatavissa: https://helda.helsinki.fi/bitstream/handle/10138/317958/2013_Pernaa_KT_tutkimusmenetelmana_KT_kirja.pdf [viitattu 23.8.2023].
- Prisma. 2024. Prisma Flow Diagram. PDF-dokumentti. Saatavissa: <http://www.prisma-statement.org/PRISMAStatement/FlowDiagram.aspx> [viitattu 10.09.2023].
- Pitkäranta, A. 2014. Laadullinen tutkimus opinnäytetyönä. E-kirja. Saatavissa: <https://kaakkuri.finna.fi/> [viitattu 26.8.2023].
- Puusa, A., Juuti. P. 2020. Laadullisen tutkimuksen näkökulmat ja menetelmät. E-kirja. Gaudeamus. Saatavissa: <https://kaakkuri.finna.fi/> [viitattu 26.8.2023].
- Redswitches. 2023. What's System Hardening and How It Works: A 5-Phase Process. WWW-dokumentti. Saatavissa: <https://www.redswitches.com/blog/system-hardening/> [viitattu 15.10.2023].
- Ronkainen ym. 2011; Cheek 2012. Teoksessa Jaana Vuori (toim.) Laadullisen tutkimuksen verkkokäsikirja. Tampere: Yhteiskuntatieteellinen tietoarkisto. Saatavissa: <https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus> [viitattu 28.11.2023].
- Salminen, A. 2023. Mikä kirjallisuuskatsaus. PDF-dokumentti. Vaasan yliopisto. Saatavissa: <https://urn.fi/URN:ISBN:978-952-395-082-5> [viitattu 23.8.2023].

Silberschatz, A., Galvin, P., Gagne, G. 2018. Operating system concepts, 10th edition. E-kirja. Saatavissa: <https://www.wiley.com/en-us/Operating+System+Concepts%2C+10th+Edition-p-9781119320913> [viitattu 19.01.2024].

Siponen, M., Willison, R. 2009. Information security management standards: Problems and solutions. PDF-dokumentti. Saatavissa: <https://www.sciencedirect.com/science/article/pii/S0378720609000561> [viitattu 06.01.2024].

Steelcloud. s.a. ConfigOS MPO Suite enables Continuous Compliance at Scale. WWW-dokumentti. Saatavissa: <https://www.steelcloud.com/configos-mpo/> [viitattu 18.2.2024].

Tarkkonen, J. 2024a. Tietoturvakayhysten luokittelumalli. Kuva. Saatavissa: <https://github.com/KarlSynsed/Masters/blob/main/TyoasemaTurvanKayttoonotToMalli.xlsx> [viitattu 02.04.2024].

Tarkkonen, J. 2024b. Työasematurvakaasitusistö. Kuva. Saatavissa: <https://github.com/KarlSynsed/Masters/blob/main/Tyoasematurvakaasitusisto.png> [viitattu 02.04.2024].

Techrepublic. 2008. Understanding layered security and defense in depth. WWW-dokumentti. Saatavissa: <https://www.techrepublic.com/article/understanding-layered-security-and-defense-in-depth/> [viitattu 13.01.2024].

Trustcloud. s.a. Standard vs Framework vs Laws vs Regulations. WWW-dokumentti. Saatavissa: <https://community.trustcloud.ai/docs/grc-launchpad/grc-101/compliance/standard-vs-framework-vs-laws-vs-regulations/> [02.11.2023].

Tuomi, J., Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi. E-kirja. Saatavissa: <https://kaakkuri.finna.fi/> [viitattu 26.11.2023].

Verohallinto. s.a. Verotuksen historiaa Suomessa. Verohallinnon julkaisu 381.09. PDF-dokumentti. Saatavissa: https://www.vero.fi/globalassets/tietoa-verohallinnosta/esitys--ja-opetusmateriaalit/381v09_verotuksen_historiaa.pdf [viitattu 07.01.2023].

Verizon. s.a. VERIS the vocabulary for event recording and incident sharing. WWW-dokumentti. Saatavissa: <https://verisframework.org/index.html> [viitattu 11.02.2024].

Verizon. s.a.b. The VERIS Community Database. WWW-dokumentti. Saatavissa: <https://github.com/vz-risk/VCDB> [viitattu 23.03.2024].

Vilkka, H. 2023. Kirjallisuuskatsaus metodina, opinnäytetyön osana ja tekstilajina. Art House Oy. E-kirja. Saatavissa: <https://kaakkuri.finna.fi> [viitattu 23.10.2023].

Weiss, M., Solomon, M. 2016. Auditing IT infrastructures for Compliance. E-kirja. Saatavissa: <https://www.oreilly.com/library/view/auditing-it-infrastructures/9781284090703/> [viitattu 27.12.2023].

Xamk, s.a.a. Mukailen teoksista Kananen 2017 & Jyväskylän yliopisto Koppa. Menetelmäosaamisen materiaalit. Saatavissa: <https://learn.xamk.fi/course/view.php?id=12153§ion=8#tabs-tree-start> [viitattu 28.11.2023].

Xamk, s.a.b. Tiedonhankinnan opas. Kaakkois-Suomen ammattikorkeakoulu, kirjastopalvelut. WWW-dokumentti. Saatavissa: <https://libguides.xamk.fi/tiedonhankinta/opas> [viitattu 22.11.2023].

Xu, T., Zhou, Y. 2015. Systems Approaches to Tackling Configuration Errors: A Survey. PDF-dokumentti. Saatavissa: <https://doi.org/10.1145/2791577> [viitattu 24.11.2023].

Zamora, P., Kwiatek, M., Bippus, V., Elejalde, E. 2019. Increasing Windows security by hardening PC configurations. EDP sciences. PDF-dokumentti. Saatavissa: https://www.epj-conferences.org/articles/epjconf/pdf/2019/19/epjconf_chep2018_08019.pdf [viitattu 30.12.2023].

KUVALUETTELO

- Kuva 1. Tutkimusasetelma
- Kuva 2. Ongelmanasettelun tavoitteet
- Kuva 3. Tutkimusstrategiat
- Kuva 4. Aineistonkeruumenetelmä
- Kuva 5. Tiedonhaun prosessi
- Kuva 6. Tiedonhakuprosessi.
- Kuva 7. Holistisen tietoturvamallin rakennus
- Kuva 8. Ehdotus tietoturvakehysten luokittelumallista
- Kuva 9. Järjestelmän tietoturvakovenusten kokonaisuus
- Kuva 10. CIS community defense malli
- Kuva 11. Tietomurtotietokanta
- Kuva 12. Funktionaalisen turvallisuuden organisaatiomalli
- Kuva 13. Iddil/atc-metodologia sekä käsitemalli
- Kuva 14. Hyökkäyspuurakenne
- Kuva 15. Riskipohjainen päätösmalli
- Kuva 16. Virhemäärittelyt
- Kuva 17. Interventioehdotuksen vaiheistus
- Kuva 12. Työasematurvallisuuden käsitteistö

TAULUKKOLUETTELO

Taulukko 1. Tutkimuskysymykset

Taulukko 2. Tutkimuksen aineistonkeruumenetelmät

Taulukko 3. Valitut tietokannat

Taulukko 4. Aihesanat suomeksi ja valikoidut aihesanat englanniksi

Taulukko 5. Windows OR Operating system AND (security) AND (hardening)
OR (auditing) OR (best practises)

Taulukko 6. Security AND (frameworks) OR (standards) AND (hardening) OR
(auditing)

Taulukko 7. Operating system AND (compliance) OR (best practises) AND
(security)

Taulukko 8. Cyber security AND (posture) AND (compliance) OR
(benchmarks) OR (visibility)

Taulukko 9. Rajauskriteerit

Kokeilupöytäkirjat

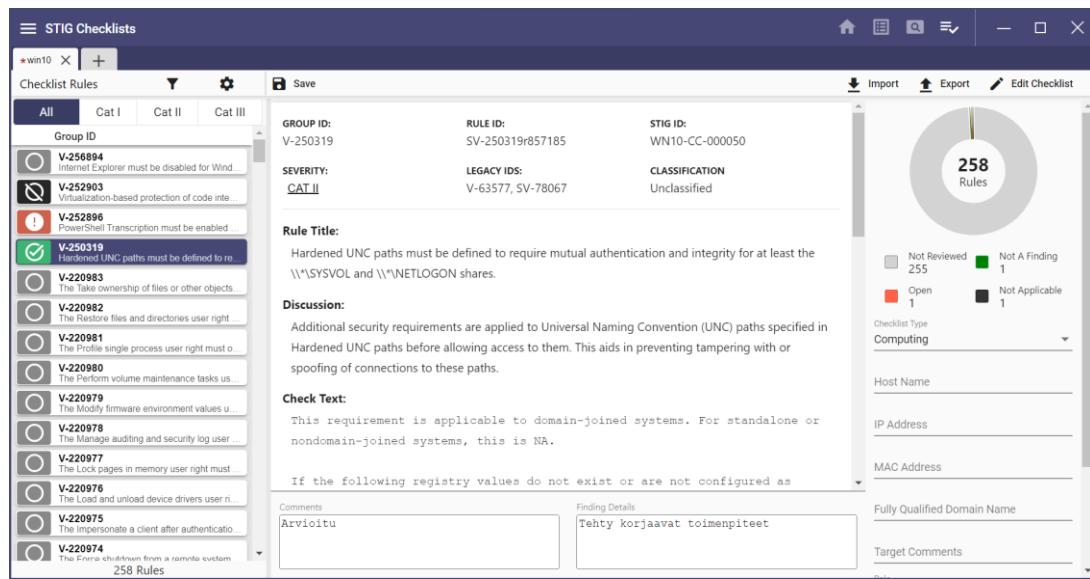
Kokeilupöytäkirja 1) Disa stig viewer

Mitä testattu	20.9.2023
Arvio työkalun hyödyllisyystestä	Toimii hyvin valitun kokoonpanon arvointiin ja dokumentointiin. Dokumentaation siirrettävyyss, filtreointi, yms. On todella helppoa!
Työkaluhuomiot	
Ilmainen tuote. Ei erillistä maksullista versiota.	

Kuvakaappaukset ja dokumentaatio työkalun koekäytöstä:

The screenshot shows the STIG Viewer 3 interface for Microsoft Windows 10. The left sidebar lists 'STIG Rules' under 'Microsoft Windows 10' with several items expanded, such as 'Overview', 'Read Me', and various V-xxxxxx rule entries. The main pane displays 'Microsoft Windows 10' details: GROUP ID: V-220700, RULE ID: SV-220700r569187, STIG ID: WN10-00-000020; SEVERITY: CAT III, LEGACY IDS: SV-91781, V-77065, CLASSIFICATION: Unclassified. Below this, sections include 'Rule Title', 'Discussion', 'Check Text', 'Fix Text', and 'References'. The 'Check Text' section for rule V-220700 states: 'Secure Boot must be enabled on Windows 10 systems.' The 'Fix Text' section states: 'Enable Secure Boot in the system firmware.'

Kuvassa on havainnollistettu stig viewerillä Windows 10 stig-pohjan tarkastelua. Jokainen yksittäinen suojaus on rikastettu kategoriatasolla, keskustelutekstillä, tarkistustekstillä, korjaustekstillä sekä viitteillä. Keskusteluteksti esittelee yksittäisen kontrollin ja tarkistusteksti kertoo tavan tarkistaa kontrollin nykytilan. Viitetekstissä tukeudutaan hyvin yleisesti NIST SP 800-53 -kontrolleihin.



Kuvassa STIG viewer checklist käyttöliittymä. Tosi näppärä, pystyy väreillä/markkereilla merkkaamaan miten tietty kontrolli on täyttynyt tai ei.

Kokeilupöytäkirja 2) CIS CAT PRO assessor (Lite)

Mitä testattu	20.9.2023
Arvio työkalun hyödyllisydestä	Erittäin fiksu, mutta tarkoituksella rajoitettu. Jatkuvuus ei oikein toteudu, koska rapsan saa vain html:änä ulos. Pro-versio sisältää tietokannat yms.
Työkaluhuomiot	Maksullisen tuotteen lite-versio. Tarkistaa kyllä tehokkaasti automaattisesti kehystä vasten tilanteen ja tarjoaa remedointivaihtoehdot suoraan.



Voi skannata paikallisesti tai etänä järjestelmiä

Benchmarks

Available

Benchmark

- CIS Controls Assessment Module - Implementation Group 1 for Windows 10 v1.0.3
- CIS Controls Assessment Module - Implementation Group 1 for Windows Server v1.0.0
- CIS Google Chrome Benchmark v2.1.0
- CIS Microsoft Windows 10 Enterprise Benchmark v2.0.0**
- CIS Microsoft Windows 10 Stand-alone Benchmark v2.0.0
- CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.1

Profile

- Level 1 (L1) - Corporate/Enterprise Environment (general use)**
- Level 1 (L1) + BitLocker (BL)
- Level 1 (L1) + Next Generation Windows Security (NG)
- Level 1 (L1) + BitLocker (BL) + Next Generation Windows Security (NG)
- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)
- Level 2 (L2) + BitLocker (BL)
- Level 2 (L2) + Next Generation Windows Security (NG)
- Level 2 (L2) + BitLocker (BL) + Next Generation Windows Security (NG)
- BitLocker (BL) - optional add-on for when BitLocker is deployed
- Next Generation Windows Security (NG) - optional add-on for use in the newest hardware and config

Add

Saatavilla useita implementation group vaihtoehtoja, sekä eri benchmarkkeja, Pienellä ruudulla painikkeet jäävät "piiloon".

Report Output Options

Format

HTML

CSV

Text

ARF XML

JSON

Lite-versiossa rajoitus: raportin saa ulos vain html-muodossa.

Summary

Description	Tests						Scoring		
	Pass	Fail	Error	Unkn.	Man.	Exc.	Score	Max	Percent
1 Account Policies	4	6	0	0	1	0	4.0	10.0	40%
1.1 Password Policy	2	5	0	0	0	0	2.0	7.0	29%
1.2 Account Lockout Policy	2	1	0	0	1	0	2.0	3.0	67%
2 Local Policies	53	44	0	0	1	0	53.0	97.0	55%
2.1 Audit Policy	0	0	0	0	0	0	0.0	0.0	0%
2.2 User Rights Assignment	22	15	0	0	0	0	22.0	37.0	59%
2.3 Security Options	31	29	0	0	1	0	31.0	60.0	52%
2.3.1 Accounts	2	3	0	0	0	0	2.0	5.0	40%
2.3.2 Audit	1	1	0	0	0	0	1.0	2.0	50%
2.3.3 DCOM	0	0	0	0	0	0	0.0	0.0	0%
2.3.4 Devices	0	1	0	0	0	0	0.0	1.0	0%
2.3.5 Domain controller	0	0	0	0	0	0	0.0	0.0	0%

Raportti kertoo testikohtaisesti onnistumiset ja summaa ne prosentteina.

More		Benchmark Item	Result
1 Account Policies			
1.1 Password Policy			
1.0 1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'			Fail
1.0 1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)'			Fail
1.0 1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)'			Fail
1.0 1.1.5 (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled'			Fail
1.0 1.1.6 (L1) Ensure 'Relax minimum password length limits' is set to 'Enabled'			Fail
1.2 Account Lockout Policy			
1.0 1.2.2 (L1) Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'			Fail
2 Local Policies			
2.1 Audit Policy			
2.2 User Rights Assignment			

Raportin voi filiteroida vain failanneisiin. Kertoo jokaisen yksityiskohtaisen kontrolli-itemin tasolla miten kävi.

Klikkaamalla auki, saa kontrollikortin auki, jossa selosteet.

1.1 Password Policy

This section contains recommendations for password policy.

1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)' [Fail](#)

Description:

This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value for stand-alone systems is 0 passwords, but the default setting when joined to a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password.

The recommended state for this setting is: 24 or more password(s).

Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Note #2: As of the publication of this benchmark, Microsoft currently has a maximum limit of 24 saved passwords. For more information, please visit [Enforce password history \(Windows 10\) - Windows security | Microsoft Docs](#)

Rationale:

The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced.

If you specify a low number for this policy setting, users will be able to use the same small number of passwords repeatedly. If you do not also configure the Minimum password age setting, users might repeatedly change their passwords until they can reuse their original password.

Remediation:

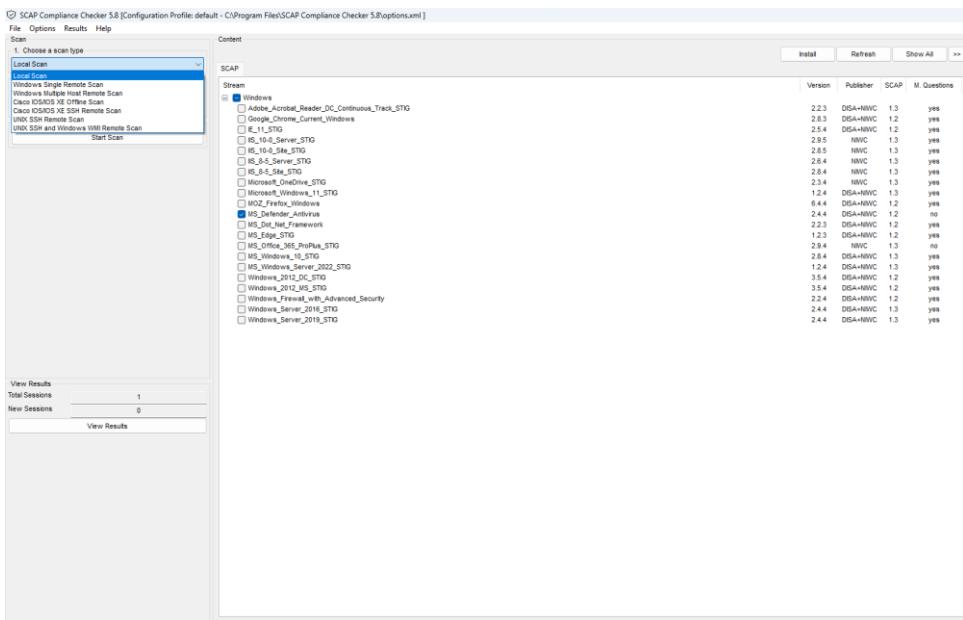
To establish the recommended configuration via GP, set the following UI path to 24 or more password(s):

Ja lisäksi automaattisesti kerätty todiste:

Assessment:				
Hide Assessment Evidence				
Complex Check				
Criterion: Ensure 'Password Hist Len' Is 'Greater Than Or Equal' to '24'				
Existence Check: At Least One Exists				
Item Check: All				
Result: Fail				
Passwordpolicy Item				
AND	Name	Type	Status	Value
	Max Passwd Age	Int	Exists	3628800
	Min Passwd Age	Int	Exists	0
	Min Passwd Len	Int	Exists	0
	Password Hist Len	Int	Exists	0
	Password Complexity	Boolean	Exists	0
	Reversible Encryption	Boolean	Exists	0

Kokeilupöytäkirja 3) SCAP compliance checker

Mitä testattu	20.9.2023
Arvio työkalun hyödyllisyystestä	Erittäin hyödyllinen kampe jatkuvaan tarkistustoimintaan. Kustomoitavissa omilla temploilla ym.
Työkaluhuomiot	
	No on hitokseen monipuolinen. Tää et tää on scap-pohjanen, tarkottaa et voidaan itsekin tehdä tarkistustempoja! Tuottaa lisäksi xml pohjasta sekä tekstimuotosta rapsaa html lisäksi, joten voidaan viedä havaintoja, vaikka powerbi-rapsoihin tms.

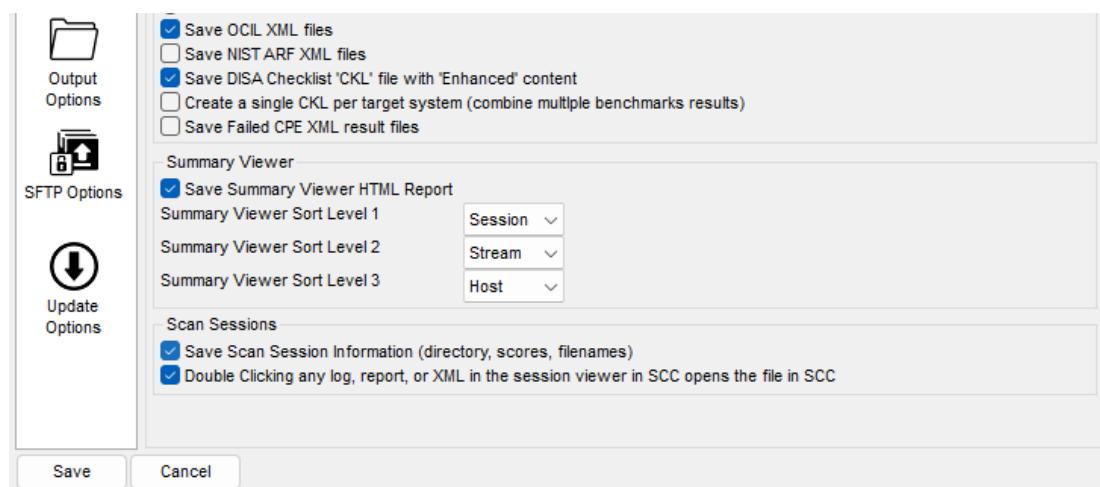


Aloitusvalikossa näkyvillä ladatut scap-pohjaiset templatet

Skannaustyypin valinnassa paikallinen, etä- windows ja unixlaitteet sekä cisco.



Raportinluonti mahdollista html ja text.



Ajetut sessiot jäävät talteen, niistä voi myöhemmin tehdä uudelleen raportin.

Ajo käyntiin.



Tulee kiva rapsa, joka antaa ensimmäisenä compliance scoren ja statuksen.

Results: High Severity (CAT I)

Automated Checks

- V-253263 - Windows 11 systems must be maintained at a supported servicing level. - Pass
- V-253265 - Local volumes must be formatted using NTFS. - Pass
- V-253275 - Internet Information System (IIS) or its subcomponents must not be installed on a workstation. - Pass
- V-253283 - Data Execution Prevention (DEP) must be configured to at least OptOut. - Fail
- V-253284 - Structured Exception Handling Override Protection (SEHOP) must be enabled. - Fail
- V-253305 - Reversible password encryption must be disabled. - Pass
- V-253382 - Solicited Remote Assistance must not be allowed. - Fail
- V-253386 - Autoplay must be turned off for non-volume devices. - Fail
- V-253387 - The default autorun behavior must be configured to prevent autorun commands. - Fail
- V-253388 - Autoplay must be disabled for all drives. - Fail
- V-253411 - The Windows Installer feature "Always install with elevated privileges" must be disabled. - Fail
- V-253416 - The Windows Remote Management (WinRM) client must not use Basic authentication. - Fail
- V-253418 - The Windows Remote Management (WinRM) service must not use Basic authentication. - Fail
- V-253452 - Anonymous SID/Name translation must not be allowed. - Pass
- V-253453 - Anonymous enumeration of SAM accounts must not be allowed. - Pass
- V-253454 - Anonymous enumeration of shares must be restricted. - Fail
- V-253456 - Anonymous access to Named Pipes and Shares must be restricted. - Pass
- V-253461 - The system must be configured to prevent the storage of the LAN Manager hash of passwords. - Pass
- V-253462 - The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM. - Fail
- V-253481 - The "Act as part of the operating system" user right must not be assigned to any groups or accounts. - Pass
- V-253486 - The "Create a token object" user right must not be assigned to any groups or accounts. - Pass
- V-253490 - The "Debug programs" user right must only be assigned to the Administrators group. - Pass

Manual Checks

- V-253264 - The Windows 11 system must use an antivirus program. - Not Checked
- V-253269 - Only accounts responsible for the administration of a system must have Administrator rights on the system. - Not Checked
- V-253294 - Administrative accounts must not be used with applications that access the internet, such as web browsers, or with potential internet sources, such as email. - Not Checked
- V-253370 - Credential Guard must be running on Windows 11 domain-joined systems. - Not Checked

Results: Medium Severity (CAT II)

Automated Checks

- V-253259 - Windows 11 information systems must use BitLocker to encrypt all disks to protect the confidentiality and integrity of all information at rest. - Pass
- V-253260 - Windows 11 systems must use a BitLocker PIN for pre-boot authentication. - Fail
- V-253261 - Windows 11 systems must use a BitLocker PIN with a minimum length of six digits for pre-boot authentication. - Fail
- V-253276 - Simple Network Management Protocol (SNMP) must not be installed on the system. - Pass
- V-253277 - Simple TCP/IP Services must not be installed on the system. - Pass
- V-253278 - The Telnet Client must not be installed on the system. - Pass
- V-253279 - The TFTP Client must not be installed on the system. - Pass
- V-253285 - The Windows PowerShell 2.0 feature must be disabled on the system. - Fail
- V-253286 - The Server Message Block (SMB) v1 protocol must be disabled on the system. - Pass
- V-253287 - The Server Message Block (SMB) v1 protocol must be disabled on the SMB server. - Pass
- V-253288 - The Server Message Block (SMB) v1 protocol must be disabled on the SMB client. - Pass
- V-253289 - The Secondary Logon service must be disabled on Windows 11. - Fail
- V-253297 - Windows 11 account lockout duration must be configured to 15 minutes or greater. - Fail
- V-253298 - The number of allowed bad logon attempts must be configured to three or less. - Fail
- V-253299 - The period of time before the bad logon counter is reset must be configured to 15 minutes. - Fail
- V-253300 - The password history must be configured to 24 passwords remembered. - Fail
- V-253301 - The maximum password age must be configured to 60 days or less. - Pass
- V-253302 - The minimum password age must be configured to at least 1 day. - Fail
- V-253303 - Passwords must, at a minimum, be 14 characters. - Fail

Automatisoitujen tarkistusten havainnot jaettu high, medium, low.

V-253284 - Structured Exception Handling Overwrite Protection (SEHOP) must be enabled.

Rule ID:	xccdf_mil.disa.stig_rule_SV-253284r828936_rule
Test Type:	Automated
Result:	Fail
Version:	WN11-00-000150
Identities:	CCI-002824 (NIST SP 800-53 Rev 4: SI-16; NIST SP 800-53 Rev 5: SI-16)
Description:	Attackers are constantly looking for vulnerabilities in systems and applications. Structured Exception Handling Overwrite Protection (SEHOP) blocks exploits that use the
Fix Text:	Configure the policy value for Computer Configuration >> Administrative Templates >> MS Security Guide >> "Enable Structured Exception Handling Overwrite Protection". This policy setting requires the installation of the SecGuide custom templates included with the STIG package. "SecGuide.admx" and "SecGuide.adml" must be copied to
Severity:	high
Weight:	10.0
Reference:	<p>Title: DPMS Target Microsoft Windows 11 Publisher: DISA Type: DPMS Target Subject: Microsoft Windows 11 Identifier: 5471</p>
Definitions:	<p>Definition ID: oval:mil:disa.stig.windows11:def:253284 Rule ID: oval:mil:disa.stig.win:st:25328400 (registry_test) Result: false Title: SEHOP is turned on and properly configured Check Existence: All collected items must exist. Check: All collected items must match the given state(s). Object ID: oval:mil:disa.stig.win:obj:25328400 (registry_object) Object Requirements:<ul style="list-style-type: none">• key must be equal to 'SYSTEM\CurrentControlSet\Control\Session Manager\kernel'• name must be equal to 'DisableExceptionChainValidation' State ID: oval:mil:disa.stig.win:ste:20000000 (registry_state) State Requirements:<ul style="list-style-type: none">• check_existence = 'at_Least_one_exists', type must be equal to 'req_dword'• check_existence = 'at_Least_one_exists', value must be equal to '0' Additional Information: Check existence requirement not met.</p>
Tests:	<p>Test ID: oval:mil:disa.stig.win:st:25328400 (registry_test) Result: false Title: SEHOP is turned on and properly configured Check Existence: All collected items must exist. Check: All collected items must match the given state(s). Object ID: oval:mil:disa.stig.win:obj:25328400 (registry_object) Object Requirements:<ul style="list-style-type: none">• key must be equal to 'SYSTEM\CurrentControlSet\Control\Session Manager\kernel'• name must be equal to 'DisableExceptionChainValidation' State ID: oval:mil:disa.stig.win:ste:20000000 (registry_state) State Requirements:<ul style="list-style-type: none">• check_existence = 'at_Least_one_exists', type must be equal to 'req_dword'• check_existence = 'at_Least_one_exists', value must be equal to '0' Additional Information: Check existence requirement not met.</p>

Tarkemmat havainnot, selosteet ja kuvaukset löytyvät klikkaamalla yksittäisiä

Osa tarkistuksista on manuaalisia, niiden tarkistamiseen on ohjeistus samassa raportissa.

V-253296 - The Windows 11 time service must synchronize with an appropriate DoD time source.

Rule ID:	xccdf_mil.disa.stig_rule_SV-253296r877038_rule
Test Type:	Manual
Result:	Not Checked
Version:	WN11-00-000260
Identities:	CCI-001891 (NIST SP 800-53 Rev 4: AU-8 (1)(a))
Description:	The Windows Time Service controls time synchronization settings. Time synchronization is essential for authentication and auditing purposes. If the Windows Time Service synchronizes with domain controllers. If an NTP server is configured, it must synchronize with a secure, authorized time source.
Fix Text:	<p>Configure the system to synchronize time with an appropriate DoD time source.</p> <p>Domain-joined systems use NT5DS to synchronize time from other systems in the domain by default.</p> <p>If the system needs to be configured to an NTP server, configure the system to point to an authorized time server by setting the policy value for Computer Configuration >> Adminstrative Templates >> "NtpServer", and configure the "NtpServer" field to point to an appropriate DoD time server.</p> <p>The US Naval Observatory operates stratum 1 time servers, identified at http://tycho.usno.navy.mil/ntp.html. Time synchronization will occur through a hierarchy of time servers.</p>
Severity:	low
Weight:	10.0
Reference:	<p>Title: DPMS Target Microsoft Windows 11 Publisher: DISA Type: DPMS Target Subject: Microsoft Windows 11 Identifier: 5471</p>
Questionnaires:	<p>Description: The Windows Time Service controls time synchronization settings. Time synchronization is essential for authentication and auditing purposes. If the Windows Time Service is configured to synchronize with domain controllers. If an NTP server is configured, it must synchronize with a secure, authorized time source.</p> <p>Questionnaire ID: ocl:nay.navwar.niwcatlantic.scc.windows11:questionnaire:841 Result: NOT_TESTED Title: The Windows 11 time service must synchronize with an appropriate DoD time source. Test Actions: • NOT_TESTED (All child checks must be true.) ○ NOT_TESTED (CAT III, V-253296, SV-253296r877038, SRG-OS-000355-GPOS-00143)</p>
Test Actions:	<p>Title: CAT III, V-253296, SV-253296r877038, SRG-OS-000355-GPOS-00143 Test Action ID: ocl:nay.navwar.niwcatlantic.scc.windows11:testaction:841 Question: Review the Windows time service configuration.</p> <p>Open an elevated "Command Prompt" (run as administrator).</p> <p>Enter "W32tm /query /configuration".</p> <p>Domain-joined systems (excluding the domain controller with the PDC emulator role):</p> <p>If the value for "Type" under "NTP Client" is not "NT5DS", this is a finding.</p> <p>References: CCI-001891 Result: NOT_TESTED</p>

Kokeilupöytäkirja 4) Opsiwat metadefender

Mitä testattu	20.9.2023
Arvio työkalun hyödyllisyystä	Toimii hyvin valitun kokoonpanon ohjelmistojen päivitystilanteen ja sovellusten haavoittuvuusinformaation selvittämiseen.
Työkaluhuomiot	
Ilmainen tuote, yrityskäyttöön oma versio.	

Kuvakaappaukset ja dokumentaatio työkalun koekäytöstä:

OPSWAT.
MetaDefender
IT-OT Access

[Install MetaDefender Endpoint](#) [Scan Device](#) [Device Report](#)

Connect your first device

Welcome Jussi Tarkkonen.
Start by downloading and installing the MetaDefender Endpoint, it will automatically connect to MetaDefender IT-OT Access, then you can access your device report in MetaDefender IT-OT Access.

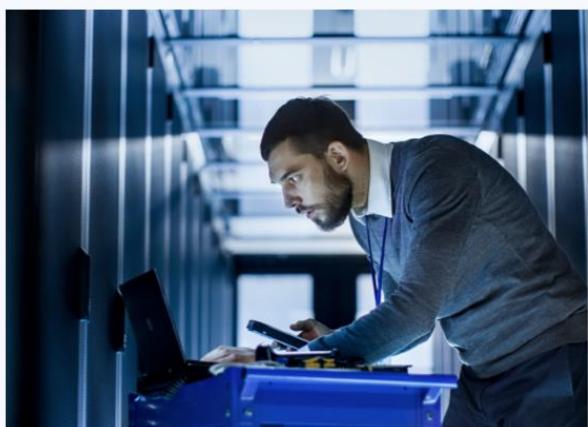
Windows

[Download MetaDefender Endpoint for Windows](#)

SHA256 2579747a957eaccbe97f48e2... 

*The download is uniquely configured for your account, to function correctly it requires you not to change the file name.

If you have the Free Client already installed - choose "Free Client" from the menu dropdown and it will connect the MetaDefender Endpoint directly to MetaDefender IT-OT Access.



Asennus vaatii erillisen clientin.

OPSWAT.
MetaDefender
IT-OT Access

① Install MetaDefender Endpoint ② Scan Device ③ Device Report

Scanning your device

When you have installed the MetaDefender Endpoint, this page monitors the connection between your device and MetaDefender IT-OT Access.

- Your device will connect with MetaDefender IT-OT Access
- The device is scanned and analyzed
- MetaDefender IT-OT Access creates the Device Report

First-time device scanning can take between 3-5 minutes. You can view and explore MetaDefender IT-OT Access while the device is processed.

[Open MetaDefender IT-OT Access](#)

Processing device

Palvelun pää odottaa clientin yhdistämistä

Privacy & security > Location

Windows can use your device's capabilities to determine your location. Microsoft might use location data to improve the accuracy of its location services. Some desktop apps might not appear on this page or be affected by these settings. [Learn more about location](#)



Lokaatiopalvelut pitää laittaa päälle

Installation Complete

The dashboard displays various metrics and a success message:

- Device Information: 265 Critical Issues, 372 Warnings
- Advanced Malware Detection: 1223 Devices
- Devices with 3rd-Party Vulnerabilities: 1306 Devices
- Devices at Risk: 1322 Devices
- Congratulations message: "Congratulations, you have installed your first device, it is now connected to MetaDefender IT-OT Access."
- View your Device Report button
- Explore many more features from the Device Details page including Policy Management, Secure Access, Vulnerabilities, and more.

Asennus onnistunut, laite liitetty palveluun

Issues 1

CVEs 23

Non-Compliant

[See Rule #2](#)
[View remediation page](#)

Compliance Details Device severity was warning in 1 consecutive data report(s)

System Information

Events

Detailed device information

All Categories	Vulnerabilities	Patch Management	Missing Patches	CVEs	Deep Compliance	Application Control	System	Other Apps
<input type="text" value="Search by CVE ID, product, KB number"/> Export ▼								
Severity ↓	CVE ID	Summary	Updated At	Associated Apps	Associated OS Patches	CVSS 3.0 Score	Allowlist Status	
Critical	CVE-2023-47359	Videolan VLC prior to version 3.0.20 contains an incorrect offset read...	Dec 01, 2023 2:15:00 AM	VLC media player (x86) - 3.0.11	N/A	9.8	▼	
Critical	CVE-2021-24112	.NET Core Remote Code Execution Vulnerability This CVE ID is unique fr...	Jul 07, 2021 7:34:00 PM	Microsoft .NET Core Runtime 3.1 (x64) - 3.1.3	N/A	9.8	▼	
Critical	CVE-2021-26701	.NET Core Remote Code Execution Vulnerability This CVE ID is unique fr...	Nov 07, 2023 3:31:00 AM	Microsoft .NET Core Runtime 3.1 (x64) - 3.1.3	N/A	9.8	▼	
High	CVE-2021-25801	A buffer overflow vulnerability in the __Parse_idx component of Video...	May 03, 2022 4:04:00 PM	VLC media player (x86) - 3.0.11	N/A	7.1	▼	
High	CVE-2020-26684	A vulnerability in EbmlTypeDispatcher::send in VideoLAN VLC media play...	Feb 03, 2023 6:49:00 PM	VLC media player (x86) - 3.0.11	N/A	7.8	▼	
High	CVE-2021-25803	A buffer overflow vulnerability in the vlc_input_attachment_New compon...	May 03, 2022 4:04:00 PM	VLC media player (x86) - 3.0.11	N/A	7.1	▼	
High	CVE-2021-25802	A buffer overflow vulnerability in the AVI_ExtractSubtitle component o...	May 03, 2022 4:04:00 PM	VLC media player (x86) - 3.0.11	N/A	7.1	▼	

Kiva rapsa asennettujen ohjelmistojen haavoittuvuuksista.

Patch Management 1 product

Windows Update Agent
Version 1023.1221.1202.0

Patch management agent is enabled
Critical, important, moderate patches have been missing for more than 1 day(s).

Anti-Malware 2 products ▾

Windows Defender
Version 4.18.24020.7

Real-time protection is enabled
Signature definitions were updated 1 day(s) ago
No successful scan recently

Encryption 1 product

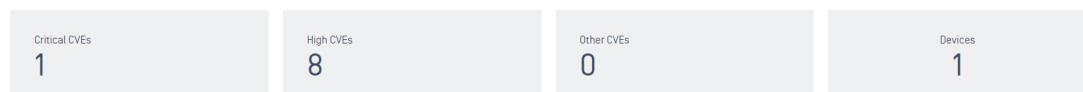
BitLocker Drive Encryption
Version 10.0.22621.1

System volume C is encrypted

Kertoo yleisesti päällä olevien tietoturvaominaisuksien tilasta.

Applications VLC media player [x86]

Version 3.0.11, VideoLAN



Severity	CVE ID	Summary	Updated At	CVSS 3.0 Score
▼ Critical	CVE-2023-47359	Videolan VLC prior to version 3.0.20 contains an incorrect offset read that lead...	Dec 01, 2023 2:15:00 AM	9.8
▼ High	CVE-2020-26684	A vulnerability in EbmTypeDispatcher::send in VideoLAN VLC media player 3.0.11 ...	Feb 03, 2023 6:49:00 PM	7.8
▼ High	CVE-2022-41325	An integer overflow in the VNC module in VideoLAN VLC Media Player through 3.0.1...	Dec 08, 2022 4:44:00 PM	7.8
▼ High	CVE-2023-46814	A binary hijacking vulnerability exists within the VideoLAN VLC media player bef...	Nov 29, 2023 6:54:00 PM	7.8
▼ High	CVE-2023-47380	Videolan VLC prior to version 3.0.20 contains an Integer underflow that leads to...	Dec 01, 2023 2:15:00 AM	7.5
▼ High	CVE-2021-25804	A NULL-pointer dereference in "Open" in avi.c of VideoLAN VLC Media Player 3.0.1...	Aug 04, 2021 2:11:00 AM	7.5
▼ High	CVE-2021-25801	A buffer overflow vulnerability in the __Parse_idx component of VideoLAN VLC Me...	May 03, 2022 4:04:00 PM	7.1
▼ High	CVE-2021-25802	A buffer overflow vulnerability in the AVI_ExtractSubtitle component of VideoLAN...	May 03, 2022 4:04:00 PM	7.1

Toinen näkymä, missä ohjelmisto kerrallaan asennusten haavoittuvuustilanne, ja mitä laitteita ongelmat koskevat.

Browser Extensions FadBlock: Friendly Adblock for Youtube™

Browser: [Google Chrome](#) | Extension ID: [mdadjffmjhfcbgfhfjbailljplkkbfc](#)

Installed Devices Installed Versions

Version Installed devices ↑

2.7	1
-----	---

Sama homma browser extensiot

Events								
Detailed device information								
All Categories	Vulnerabilities	Patch Management	Missing Patches	CVEs	Deep Compliance	Application Control	System	Other Apps
Last information updated Mar 20, 2024 4:52:51 PM								
Category	KB Number	Title			Release Date	Patch Severity	CVE	Required Status
definition_update	2287602	Security Intelligence Update for Microsoft Defender Antivirus - KB2287602 (Version 1.407.578.0) - Current Channel [Broad]			Mar 20, 2024 12:00:00 AM	Important	0	Yes
security_update	2538243	Security Update for Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package [KB2538243]			Apr 05, 2012 12:00:00 AM	Important	0	Yes
driver	Unknown	Dell Inc. - Bus Controllers and Ports, Display, Storage - Dell 2709W[HDMI]			Sep 10, 2018 12:00:00 AM	Unknown	0	
driver	Unknown	Evoluent - Mouse - 12/22/2015 12:00:00 AM - 5.7.0.0			Aug 27, 2018 12:00:00 AM	Unknown	0	
driver	Unknown	Intel - Net - 12.19.2.50			Jul 15, 2023 12:00:00 AM	Unknown	0	
driver	Unknown	Intel Corporation - System - 4/2/2019 12:00:00 AM - 30.100.1914.3			Aug 10, 2019 12:00:00 AM	Unknown	0	
driver	Unknown	Realtek Semiconductor Corp. - MEDIA - 2/28/2019 12:00:00 AM - 6.0.1.8644			Jul 21, 2019 12:00:00 AM	Unknown	0	
driver	Unknown	FUJITSU CLIENT COMPUTING LIMITED - System - 5/14/2018 12:00:00 AM - 4.0.2.6			Nov 09, 2018 12:00:00 AM	Unknown	0	
driver	Unknown	Intel - System - 2013.14.0.1529			Sep 14, 2020 12:00:00 AM	Unknown	0	

Laitteen käyttöjärjestelmän, tai ohjelmistojen puuttuvat pätsit ja ajuripäivitykset

Työasematurvallisuuden teemoitellut havainnointipöytäkirjat

Taulukko 1. havainnointipöytäkirjat Tammi-Syyskuu 2023

Aineisto	Sitaatit	Tutkimustulkinta	Teema
Tammikuu/23a	<p>"Keväällä/kesällä toteutettuja suojakontolleja kaikille työasemille, päättetty että ei edistetä toistaiseksi n.n ominaisuutta. 8 GB muistilla olevia työasemia on vielä käytössä, näissä liian hidat."</p> <p>"N.n suojautuminen testissä, ei vaikuta hyvältä Veron ympäristöön"</p> <p>"Kesällä tehtiin kaksi blokkaavaa sääntöä ja todettiin toimivan. - suunniteltava miten tästä edistetään ja kuka hoitaa."</p>	Haastatteluissa esille tullut tapa testata uudet tietoturvaominaisuudet vaiheistetusti ja keskustellen asiantuntijaporukalla pitää paikkansa.	Työaseman tietoturvan kovennus
Helmikuu/23a	<p>"Työasematakastus käynnistynyt, yleinen käyttö fokusena (withsecure)"</p> <p>" Edellisen alustatarkastuksen viimeiset kovennekset jaossa, yksittäinen virhetilanne tuli ja korjattu"</p>	Ulkoista auditointia hyödynnetään työasematurvallisuuden tarkastuksissa ja haastatteluissa kerrottu tapa koventaa työaseman tilaa sitä kautta pitää paikkansa.	Auditointivuus ja tilannekuva
Helmikuu/23b	<p>"Otettu käyttöön erilliset työasemaympäristön hallinnointitunnukset. Vastaavasti intra-tiimin asiantuntijoilla ei ole jatkossa admininoikeuksia kaikkiin työasemiin"</p>	Työasematurvallisuudessa hyödynnetään parhaita käytäntöjä, tässä "least privilege" esim.	Työaseman tietoturvan kovennus

Maaliskuu/23a	"Selvitetty alerttien ja blockkien lukumäärät, ta-voitteena edelleen kiristää n.n:ää siten että yhä useampi havainto johtaa blokkiin"	Käytöönnotettuja tie-toturvaominaisuuk-sia ylläpidetään ja kehitetään aktiivi-esti	Työasema- turvalli-suuden prosessit
Maaliskuu/23b	"Työasematiimiltä puuttuu edelleen oikeuksia n.n hal-lintajärjestelmään (kaikki näkymät eivät toimi)"	Haastatteluissa ilmi-tulleet ongelmat prosesseissa tulevat ilmi puuttuvien yllä-pito-oikeuksien osalta.	Työasema- turvalli-suuden prosessit
Huhtikuu/23a	"Haavoittuvuushallinta-tuote ja sen ominaisuus y. Voitaisiinko saada testin kautta käyttöön?"	Työasematurvalli-suutta haluttaisiin ar-vioida myös itse, sii-hen tehdyn valmiin tietoturvakehyshal-linta-työkalun avulla.	Työasema- turvalli-suuden prosessit
Huhtikuu/23b	"Microsoftin N.N tietoturva-ominaisuuden häiriöti-lanne. Tehty poikkeamara-portti ja ongelman aiheut-tanut policy vaihdettu Au-dit-tilaan"	Työasemahallinta ei voi ennakoida kaik-kaa muutoksia, var-sinkin kun ongelma liittyy järjestelmän toimitajan omaan vi-katilanteeseen. On-igelmaan joudutaan reagoimaan len-nossa, ilman toimin-taohjeita.	Työasema-turvalli-suuden prosessit
Huhtikuu/23c	"Läpikäyti uudet ominai-suudet MS:n kanssa. Osa uusista ominaisuuksista ovat vaillinaisia ja/tai kes-keneräisiä. Hyödyllisiä kui-tenkin."	Työasematurvalli-suuden kehittämä- sessä hyödynnetään järjestelmätoimittä-jan asiantuntijoita, kuten haastatte-luissa kerrottiin.	Työasema-turvalli-suuden prosessit
Toukokuu/23a	"Kriittinen haavoittuvuus Microsoft Outlookissa, n.n:ällä estetty Outlookin ajo hallintatyöasemilla"	Yleisiin haavoittu-vuksiin reagoidaan nopeasti tekemällä mitigaatiotoimet kä-yttävissä olevin kei-noin.	Työasema-turvalli-suuden prosessit
Toukokuu/23b	"Win11 uhkamallinnustyö-paja varattu 13.4."	Ainakin uusien käyt-töjärjestelmäversioi-den käyttöönnotoissa hyödynnetään myös uhkamallinnusta yh-tenä keinona tunnis-taa mahdollisia tieto-turvaheikkouksia.	Työasema-turvalli-suuden prosessit

Toukokuu/23c	"Win11 uudet turvominaisuudet tutkinnassa ja testissä: n.n ei toimi Windows x.x kanssa. N.n on kuluttajatuote, ei käyttöön. N.n tuote ei toimi n.n ympäristössä"	Palavereissa puhutaan paljon uusien ominaisuuksien testaamisesta, tutkinnasta ja käyttöönottoista. Perustelut ominaisuuksien käytölle/käyttämättömyydelle ovat hyvin ohuet tai niitä ei ole ollenkaan. Tutkijan kysyessä tarkennukset päätosten perusteisiin, niitä ei ole esittää kirjallisesti. Tästä voi ehkä vetää johtopäätöksen, että dokumentaatiota ei ole.	Työasema-turvallisuuden prosessit
Elokuu/23a	"Työaseman uhkamallinnustyöpaja pidetty 13.4. loppuraportin läpi-käynti 16.5. Loppuraportti käty läpi ja hyviä nostoja/korjaustoimenpiteitä, esim: -pakollinen koulutus etätyöskentelyyn -ohjeistuksen tarkentaminen -N.n-ratkaisujen käyttötarkoitusten uudelleenarvointi -selaimet -kehitysvälaineiden kontrollit -tallennuksen esto "pilvilevylle" kuten esim. Dropbox, iCloud"	Uhkamallinnuksen tuloksina voi olla teknisten parannustoi-mien lisäksi proses-sien tai käyttäjien tietoturvaymmärryk-ken lisäämiseen täh-täviä suosituksia.	Työasema-turvallisuuden prosessit
Syyskuu/23a	"N.n ominaisuus otettu uudelleen testaukseen: hidastuminen on nyt siedettävä ja pyritään ottaamaan käyttöön laajasti koska estää n.n tiedon vuotamisen"	Aiemmin toimimatto-man asetuksen tai ominaisuuden käytötönnotoa voidaan arvioida uudelleen myöhemmin tilan-teen tai ympäristön muuttuessa.	Työaseman tietoturvan kovennus

Haastatteluaineiston teemoittelut

Taulukko 1. Teemoiteltu haastatteluaineisto

Teemahaastattelu: TMH1			
Haastattelija: Mies 46 Oulu, Tietoturva-arkkitehti Haastateltava: Mies 44 Helsinki, Työasematietoturvan guru Haastattelun toteutus: kahdenkeskinen, Teams-videoneuvottelu.			
Aineisto	Sitaatti	Tutkimustulkinta	Teema
Litterointi TMH1	"Windows työaseman tietoturvan määrittämisessä suurin haaste on todellisuudessa se, että Microsoft tekee yhtä Windows versiota, jota myydään sekä kuluttajille että yrityksille. Vielä ehkä hämmentäväintä yrityksille on se, että jos sä ostat Enterprise lisenssin, niin siinä on aina koti Windowsin tietoturva asetukset alla, jolloin voidaan siis todeta, että Suomessakin 80 % asiakkaista ajaa yrityskäytössä Windowsia oletuksena kotiasetuksilla."	Windows on lähtökohtaisesti huonosti suojattu yrityskäyttöön.	Työaseman tietoturvan kovennus
Litterointi TMH1	"Microsoftin Security baselinet ja CIS:n eri tietoturvamallit on varmasti niitä mitä eniten käytetään siihen, että saadaan tavallaan se semmoinen perustaso, jossa voidaan todeta, että	Microsoft security baseline ja CIS hyviä tietoturvakehyksiä perustason suojausten saavuttamiseksi.	Tietoturvakeysten käytännön hyödynnettävyys

	<p>ollaan siirrytty kotikäytöstä yrityskäyttöön. CIS on vähän kattavampi, koska sen valmistelee tietoturvayhteisö, joka päättää yhdessä mitkä olisivat hyvät käytännöt. Microsoft baselinen hyvä puoli on taas se, että microsoft täysin sataprosenttisesti tukee niitä, eli koskaan ei tule sitä kysymystä, ettetkö sää olis tuetulla konfiguraatiolla ”</p>		
Litterointi TMH1	"Mä oon itse sanonut asiakkaille, että oli se CIS, NIST tai microsoft security baseline niin joku pitää olla, jotta päästään siitä, että ei olla koti Windows asetuksilla."	Jonkinlainen baseline on oltava yrityskäytössä.	Tietoturvakehysten käytännön hyödynnettävyys
Litterointi TMH1	"Jos siellä on 500 asetusta niin se että miten nää asetukset nyt on niin kun yksitellen laitettu, niin sillä ei ratkaista sitä, että joudutaanko kyber murron kohteksi vai ei."	Kehysten käyttö ei pelkästään ratkaise käytännön turvallisuutta.	Tietoturvakehysten käytännön hyödynnettävyys
Litterointi TMH1	"Tietoturvakehykset on soveltuivia (auditointiin) siinä mielessä, että me pystytään mittamaan ainakin se, onko yritys ymmärtänyt, että Windows pitää konfiguroida eri lailla yrityskäyttöön kuin kotikäyttöön."	Kehysten käytön voidaan ajatella parantavan perus tietoturvan tilannekuva.	Auditointivuus ja tilannekuva

Litterointi TMH1	"Näkisin, että on 5–6 kantavaa (tietoturvan kovennus) konseptia, jotka täytyy olla käytössä: least privilege, onko admin oikkia vai ei, onko domain admin tai global admin tunnusten käyttö rajattu vain turvallisille laitteille, allowlisting tai whitelisting ja hostkohtaiset palomuurit"	Oleellisimmat näkökulmat työaseman tietoturvakovennukseen voidaan summata viiteen tärkeimpään periaatteeseen.	Työaseman tietoturvan kovennus
Litterointi TMH1	"Työasemasta usein alkaa tietoturvaloukkaukset. 2021 tilastojen mukaan haavoittuvuuksien kautta alkoi useammin ransomware kuin phishing hyökkäysten kautta. Nyt tullaan useammin takaporttien kautta. Erottelu siitä, että on normaali työasema tai pawi tai sawi niin se on tärkeintä."	Työasematietoturva käännynty haavoittuvuuksien korjaamiseen, phishingin sijasta. Työaseman roolitus on tärkeää.	Työaseman tietoturvan kovennus
Litterointi TMH1	"Ne ei tätä asiaa ratkaise, kun siellä on niinku 500 pikku asetusta, jotka menee kohdalleen ja se on vähän kuin paikaksi 500 vulnerabilitya että niitä toisiaan sitten tulee koko ajan uusia. Se ei riitä yksinään."	Kehyksen suositusten ohi tulee koko ajan uusia haavoja, joten niitä noudattamalla ei pelkästään ratkaista työaseman tietoturvaa.	Tietoturvakehysten käytännön hyödynnettävyys
Litterointi TMH1	"(Mitre) on mun miehestä hyvä tapa ilmaista niitä vulnerabilityjä ja niiden käyttötapoja ja se on hyvä malli, kun esim. tehdään OT ympäristöjen suojaa, niin ne aika lailla kokoajan peilaa kaiken siihen mitreen. Se on kyllä työllistävä, että melkein noita isompia korporaatioita ja niissä on sitten kyllä isoja tiimejä."	Mitre toimii hyvin isommissa ympäristöissä, joissa on riittävät resurssit.	Tietoturvakehysten käytännön hyödynnettävyys

Litterointi TMH1	<p>"Elikkä meidän maailma on täynnä työkaluja, jotka kertoo sun työasemasta että mitkä ne sun vulnerabilityt on, mutta ongelma on että asiakkaat ei ymmärrä mitä ja miten päästää. Työkaluja ja mittareita on, mutta miten haavoittuvuuksien korjausen priorisointi, se on ihmisiä yllyttävienkin."</p>	<p>Haavoittuvuuksien korjaaminen vaatii tiedon yhdistelyä ja ammattitaitoa. Pelkästään työkaluilla ei voi ratkota ongelmia.</p>	Työasematurvallisuuden prosessit
Litterointi TMH1	<p>"Tietoturvan 2 tärkeintä kontrollia on ajantasalla oleva rauta- ja softainventaario, muuten sä et voi suojata jos sä et tiedä mitä suojata."</p>	<p>Tietoturvan perustana laite ja ohjelmistoinventaarion pitää olla kunnossa.</p>	Tietoturvakehysten käytännön hyödynnettävyys
Litterointi TMH1	<p>"On tehty auditti, ja sieltä on nostettu, että nämä asiat pitää korjata ja yksi näistä on binäärin hallinta niinku on se sitten millä nimellä hyvänsä"</p>	<p>Ohjelmistobinäärien hallinta ymmärretään monesti vasta auditin jälkeen.</p>	Työaseman tietoturvan kovennus
Litterointi TMH1	<p>"Suurin osa pyytää sitä wdaccia sen takia, että se puree myös admineihin. mutta sä oot jo rikkonut rikkomattoman säännön, se ei anna anteeksi sitä, että saatkin käyttää liikaa oikeuksia".</p>	<p>Ominaisuuksien käyttöönnotolla ei voida korjata tietoturvan peruskäsitteiden sivuuttamista.</p>	Työaseman tietoturvan kovennus
Memberchecking Kommentit TMH1	<p>29.1.2024 Pyydetty tarkistamaan sitaattien mukaiset tutkimustulkinnat:</p> <p>"Kyllä nämä ihan oikein on! 👍"</p> <p>-Sami Laiho</p>		

Teemahaastattelu: TMH2			
Haastattelija: Mies 46 Oulu, Tietoturva-arkkitehti Haastateltava: Mies 49 Helsinki, Kyber turvallisuuspäällikkö/Apulaisjohtaja Haastattelun toteutus: kahdenkeskinen, Teams-videoneuvottelu.			
Aineisto	Sitaatti	Tutkimustulkinta	Teema
Litterointi TMH2	"Jos pelkäään katsotaan työasemaa teknisenä entiteettinä, niin minun mielestäni sen tietokoneen teknistä kyvykkyyttä vastata organisaation vaatimuksiin tai tunnnettuihin ongelmiin pystytään tekemään ilman hirvittävää hallinnollista showta ympärillä."	Työasematietoturvaa voi tehdä ilman tietoturvakehyksiäkin.	Tietoturvakehysten käytännön hyödynnettävyys
Litterointi TMH2	"Pitää olla joku yksittäinen suorituskykyvaatimus, johon voi olla esimerkki -teknilinen toteutus, mutta se tekninen toteutus voi muuttua, mutta se alkuperäinen suorituskyky vaatimukseen vaatimus olisi olemassa."	Yksinkertainen suorituskykyvaatimus, joka pysyy muuttumattomana, on tärkeä perusta.	Auditointivuus ja tilannekuva
Litterointi TMH2	Johtoa kiinnostaa, että suojaus tai suorituskyvyn vaatimus on siellä takana. Ei esimerkiksi työaseman kovalevyn salaus, että millä tuotteilla tai teknologialla se on tehty."	Johdolle suojausvaatimukset tärkeämpiä kuin teknologiavalinnat.	Auditointivuus ja tilannekuva

Litterointi TMH2	"Ei ole dokumentoitu, että tämä tekninen kyvykkys toteutettuna tavalla x vastaa tähän lakisääteiseen ja tähän hyvään käytäntöön. Valtionhallinnon milloinkin voimassa oleva ismi on määrännyt joitain asioita kuten esimerkiksi tiedon salaamiseen tai säilyttämiseen työasemilla liittyvää vaatimus taitaa tulla nykyään jopa lainsääädännöstä."	Organisaation dokumentointikäytännöt ovat puutteellisia.	Auditointivuus ja tilannekuva
Litterointi TMH2	"Otetaan vaikka katakrin päätelaitte osuus arvioinnin/ auditoinnin näkökulmasta. Uskon sellaiseen complianceen, eli ensin tehdään organisaatiolle tärkeät vaatimukset, tunnetaan ympäristö ja teknologia ja vaikka mitre attack vektorit. Tehdään organisaatiolle ne vaatimukset ja sen jälkeen ne organisaation vaatimukset mäpätään näihin muihin julkisesti tunnettuihin käytäntöihin ja todennäköisesti ne omat vaatimukset on paremmat kuin mikä tahansa ismi/best practise. Eli kyllä se pitäisi lähteä ammattitaidosta ja sitten todistetaan ulkoista kehystä vasten, että kyllä me näitäkin asioita huolehditaan."	Organisaatiolle itse laadittu kustomoitu vaatimuskehys on helpompi mäpätä julkisesti tunnettuihin kehysiin, kuin toisinpäin.	Tietoturvakehysten käytännön hyödynnettävyys

Litterointi TMH2	"Mä itse tykkäään lähtee yksinkertaisesta mallista, joka laajennetaan eli otetaan vaikka joku. Gartnerin tai mitre tai jonkun hakkerifirman yleisimmät tavat miten työasemaa on vahingoitettu ja lähdetään sieltä purkamaan sitä auki ja ups. Kohta huomataan, että sehän laajenee ihan järkeviin vaatimuksiin ja sitten siellä suositellaan, että ottakaa muuten sitten best practice ja tarkastakaan vielä nää pari kohtaa."	Työaseman turvaamisen voi aloittaa tutkimalla ensin yleisimmät uhkat, riskit ja haavoittuvuudet. Näistä voidaan tunnistaa vaatimukset ja niitä vasten parhaat käytännöt kehysten kautta.	Tietoturvakehysten käytännön hyödynnettävyys
Litterointi TMH2	"On hyvä esimerkki, että ei standardit yleensä pyydä, että sinulla on virustarkastusohjelmisto. asennettu vaan se pyytää, että sinulla on kyky suojauttaa haitallista koodia vastaan ja senhän voi tehdä myös koventamalla. Jos käyttötapaus on tosi rajoittunut, ei tarvitse olla sitä virus skanneria siellä. Tätä mä tarkoitan suorituskyky määrittelyllä ja sitten valitaan vasta teknologiaa"	Riippuu käyttötapauksesta, kuinka standardin vaatimus toteutetaan. Ensimmäisenä ei tarvitse valita teknologiaa.	Työaseman tietoturvan kovennus
Litterointi TMH2	"Epäilen että se teettää töitä ensimmäisellä kerralla, mutta varsinkin jos se on sitten automaattisesti koko ajan ajettavissa, vaikka joka päivä. Saatetaan päästä myös semmoiseen omavalvontaan, joka kouluttaa sitten niitä vastuullisiakin, että pitäisikö tuota miettiä	Tietoturvakehysten hyödyntäminen käytännön työssä vaatii jatkuvan prosessin, mutta ensimmäisen ison työn jälkeen parantaa tilannekuva merkittävästi.	Auditointivuus ja tilannekuva

	kun edelleen se teknologinen viitekehys viisastelee meille tuosta, että meillä on tuo ja tuo palvelu pääällä ja se on konfiguroitu vähän huonosti"		
Litterointi TMH2	"Toinen vaihtoehto on laittaa hallinta prosessiin uhkamallinnukset ja vastuutetaan teknologian omistajia seuraamaan oman alansa uhka maailman kehitymistä. Tai sitten jos siihen ei pysty tai kykene niin sitten teetää määräaikaisia arvointeja sillä eli avoimesti. Pyytää ulkopuolisen auditoinnin katsositteko ulkoisesta näkökulmasta uskaltaako meidän työkoneilla tehää näitä juttuja näissä työskentely olosuhteissa?"	Työasematurvallisuuden uhkamaailman seurannalla ja ulkopuolisilla auditoinneilla voidaan korvata jatkuva tietoturvakehyksiin pohjautuva omavalvonta.	Auditointivuus ja tilannekuva
Litterointi TMH2	"Sovitetaan se mitä me tiedetään meidän ympäristöstämme ja nyt vaikka 15. yleisintä hyökkäys vektoria ja sitten varmistetaan, että meillä on niihin valvontatoiminnallisuutta ja reagoointi toiminnallisuutta niin sen perään rasi malli"	Työasematurvallisuuden tilannekuvaa voidaan parantaa valvonnan ja reagoinnin yhteistyöllä.	Auditointivuus ja tilannekuva
Litterointi TMH2	"Yhdessä luotujen periaatteiden perusteella se työasema ylläpitävä tiimi katsoo samalla automaattisesti, että meneehän se valvontaan ja onhan siinä päivitysprosessi kunnossa ja muuta vastaavaa. Elikkä mun mielestä tietoturvan ylläpito ja sen ylläpito konfiguraation tarkastaminen on ihan samanlaista laatua kuin sen jakelu paketin tekeminen"	Työasematurvallisuus pitäisi kuulua työasemaylläpidosta vastaaville, osana työaseman laadunvarmistusta.	Työasematurvallisuuden prosessit

Litterointi TMH2	"Että se pitää olla se tietoturva osaaminen sen tiimin sisällä, joka vastaa sitä infrastruktuurista ja käyttöjärjestelmästä. Se ei tule sivusta annettuna. Socci on enemmänkin operaattori. Se ajattelu pitäisi kään்டää itseasiassa toisinpäin, että ei soci määräää mitä valvotaan vaan työasema tiimi määräää mitä soci valvoo ja millä threshold rajoilla."	Työasematiimin pitää osata määritellä ja vaatia työasematurvallisuuden valvontaa, jonka soc hoitaa, ei toisinpäin.	Työasematurvallisuuden prosessit
Litterointi TMH2	"Turvallisuudessa yleensä tehdään se virhe, että sitä nähdään vaan ainoastaan sen luottamuksellisuuden suojaamisen näkökulmasta, kun tietoturvallisuudessa on yleensä aspekteja: käytettävyys, jopa helppokäyttöisyys on turvallisuuden aspekti, koska silloin ihmiset eivät etsi keinotekoista väylää sivusta tehdä niitä työnantajan asioita. "	Työaseman toimivuus ja käyttökelpoisuus on yhtä tärkeää tietoturvan periaate kuin tiedon suojaaminen.	Työasematurvallisuuden prosessit
Litterointi TMH2	"Minä en pysty johdolle kertomaan tällä hetkellä sitä, että minkälainen riskitaso minulla on, kun minä käytän työasemaa omissa tiloissa, kun minä käytän sitä kotona ADSL:N kautta erilaisten salaus ratkaisujen kautta, kun minä käytän sitä VR junaa verkossa ilman tai edellä mainittuja suojaeinoja.	Työasematurvallisuuden kannalta eri käyttötapausten kuvaaminen ja riskitason ylläpito on tärkeää johdon ja organisaation tilannekuvan ja ymmäryksen kannalta.	Auditointivuus ja tilannekuva

	Uskallanko minä ottaa työaseman ulkomaille mukaan ystävällismielisiä tai vihamielisiin maihin? ICT työaseman ylläpitäjät voisivat kehittää konetta tosi vapautuneesti, mutta ihan milloin vaan he voi kertoa, että onko riskitaso noussut vai laskenut esim. käyttö tapauksessa - käytän konetta suomessa VR junaa verkossa.”		
Litterointi TMH2	"Mä lähdetään ideologiasta, ettei mä en luota miinkään enkä kehinkään en työasemiin en identiteettiin enkä muuhun, mutta niillä hallinta toimenpiteillä siihen saadaan jonkunlaista uskottavuutta niin eikö zero trustin ideologia pitäisi myös implementoida päätelaitteeseen ja sen jälkeen päätelaitteen käyttäjään ja päätelaitteessa oleviin softiin?"	Tietoturvakovenkuksien hallintatoimista pitäisi päästä seuraavassa vaiheessa zero-trust ideologian kanssa eteenpäin.	Työaseman tietoturvan kovennus
Memberchecking Kommentit TMH2	10.2.2024 Pyydetty tarkistamaan sitaattien mukaiset tutkimustulkinnat: "Teemoittelut ovat asianmukaiset ja ns. päätteemä on valittu toimivasti. Kokonaisuuden huomioidaan tukevat johdonmukaista työtä." -Haastateltava 2.		

Teemahaastattelu: TMH3			
Haastattelija: Mies 46 Oulu, Tietoturva-arkkitehti Haastateltava: Mies 53 Helsinki, Työasema-arkkitehti Haastattelun toteutus: kahdenkeskinen, Teams-videoneuvottelu.			
Aineisto	Sitaatti	Tutkimustulkinta	Teema
Litterointi TMH3	"Työasema ympäristöjä on konfiguroitu ja rakennettu niin jossain vaiheessa on microsoftin security compliance toolkit:tiä hyödynnetty siinä, mutta nää viimeiset kerrat niin on enemmänkin perustunut semmoiseen että asiantuntija porukalla on käytty läpi Microsoftin yleisiä teknisiä dokumentteja ja suosituksia ja sitten on käytty esimerkiksi kaikki uudet policy-templatet aina läpi rivi riviltä niihin liittyen aina tarkistettu sitten se mikä se microsoftin suositus on "	Organisaation työasematurvallisuus perustuu manuaaliseen teknisten dokumenttien ja suositusten käsitellyyn asiantuntijatiimillä.	Tietoturvakehysten käytännön hyödynnettävyys
Litterointi TMH3	"Kun me ollaan rakennettu se kokoonpano, jota tullaan ottamaan käyttöön, niin sitten ulkopuolinen auditoija, on sitten saanut siitä sen auditoi tavaksi. Sitten se loppuraportti, jossa on ne nostot on taas käsitelty turvan	Uusi käyttöjärjestelmäkokoonpano auditoidaan ulkopuolisen auditoijan toimesta. Raportin huomiot käsitellään ja implementoidaan sisäisesti asiantuntijatiimin toimesta.	Auditointivaltio ja tilannekuva

	ja tän työasema-asiantuntija porukan kanssa ja sitten päätetty että mitä niistä nostoista voidaan huomioida ja ne on sitten implementoitu.”		
Litterointi TMH3	”Kun töitä tässä päätelaite puolella on valtava määrä ja se vie aika paljon aikaa sitten se läpikäyti. Voi olla, että olisi hyödyllistä käyttää joka kerta, mutta se uusi paketti kun rakennetaan niin se tekninen toimivuus on helppo, mutta sitten just nää turva asetukset ja niiden läpikäyti niin niihin menee todella paljon aikaa sitten.”	Kiire vaikuttaa tietoturva-asetusten tarkasteluväliin. Käytännössä jatkuva tarkastelu vaatii paljon aikaa ja resursseja.	Tietoturvakehysten käytännön hyödynnettävyys
Litterointi TMH3	Tää Windows 11, siinähän nyt sitten tullaan ottamaan isossa määrin sieltä pilvestä esimerkiksi policyt käyttöön ja se on prem puoli jää vähemmälle. Meillä on sitten on MDE:n kautta lisää työ työkaluja mitä voitaisiin hyödyntää siinä niinku esimerkiksi nää security baseline assesmentit. Ja tarkoitus on hyödyntää niitä pilven turva välineitä sitten mahdollisimman paljon. Tässä kumminkin tää 11 Siinä se paino siirtyy enemmän sinne pilven puolelle.	Organisaatio on siirtymässä vahvasti pilven tietoturvatyökalujen käyttöön Windows 11:n myötä.	Työaseman tietoturvan kovennus

Litterointi TMH3	"Varmaan saataisiin nopeasti erittäin turvallisia järjestelmiä hyödyntäen noita kehyksiä paljon, mutta sitten että miten ne sitten toimii tuotannossa sovellusten kanssa. On vakioitu tapa esimerkiksi tää customer testing ryhmä jossa on sitten kattavasti eri toimintoja mukana, niin sieltä kyllä nopeasti saadaan tietysti testituloksia sitten"	Tietoturvamuutokset pitää testata huolellisesti, ennen käyttöönottoa.	Tietoturvakehysten käytännön hyödynnettävyys
Litterointi TMH3	"Niitä joka kierroksella tavallaan, kun tämmöinen alusta, tarkastus tai auditointi on tehty niin sieltä on aina tullut semmoisia suosituksia, jotka me heti pystytään sanomaan, että toi ei oo edes mahdollista ja sitten semmoisia mitä me testataan ja sitten mahdollistetaan jollain tavalla ehkä suppeampana kuin mitä olisi optimaalista, mutta kumminkin."	Vain osa auditoinnin huomioista voidaan ottaa käyttöön sellaisenaan organisaatiossa. Yleensä tarvitaan muutoksia suosituksiin.	Windows-työaseman käytännön tietoturva ja uhkat
Litterointi TMH3	"Meillähän on semmoinen säännöllinen määrämuotoinen rutiini, että joka kuukausi näää Microsoftin turvapäivitykset jaellaan standardilla tavalla. Sitten tietysti aina Microsoftin tietoturva-tiistai,	Tietoturvapäivitysten jakelua ja poikkeamahallintaa tehdään prosessin avulla. Toimittajan tietoturvaviestinnän kautta saadaan lisätietoa havaitusta tietoturvauhkista tai ongelmista.	Työasematurvallisuuden prosessit

	missä käsitellään havaittua tietoturvaongelmaa. Ja sitten jos tämmöinen Tietoturva poikkeama sitten aiheuttaa jotain niin kun käyttäjille näkyvää katkosta niin niistähän tehdään sitten poikkeamaraportti.”		
Litterointi TMH3	"Meillä on tuossa safessa yhtenä korttina uuden releasesen eri ominaisuuksien läpikäynti ja sitten arviodaan, että mitä niistä disabloidaan tai mitä jätetään käyttöön Omana korttina on sitten myös kaikkien uusien turvaominaisuksien läpikäynti ja arvointi ”	Työasematurva tehdään sprintteihin jaetun työn kautta.	Työasematurvallisuuden prosessit
Litterointi TMH3	"Olisi tosi hyvä, että jos olisi käytettäväissä semmoinen. kokenut tietoturva spesialisti jota pystyisi hyödyntämään ja joka pystyisi esimerkiksi näitä kehyksiä käyttämään ja arvioimaan. Me ollaan kumminkin aika paljon niin sanotusti kädet savessa tässä. tässä arkipäivän työssä ja kukaan ei ole niinku erityisesti nyt tietoturvaan niinku erikoistunut.”	Työasematiimiin tarvittaisiin tietoturvaan erikoistunut tekijä. Tällä hetkellä sellaista ei ole.	Työasematurvallisuuden prosessit

Litterointi TMH3	<p>"Tässä työasemapuolella nythän me ollaan ihan tukossa tuosta viime kevästä lähtien. Sitten kun näitä uusia turvakontrolleja on koko ajan otettu käyttöön ja valutettu, että ne on ne on syönyt varmaan leijonanosan meidän työajasta. Mutta jos jos olisi käytettävissä esimerkiksi semmoinen lisäresurssi, jonka voisi. sitten pyytää tarvittaessa vaikka säädöllisesti tekemään jonkin tietyn tsekkauksen ja antaa suosituksia niin se olisi varmaan kaikesta paras.</p> <p>"</p>	Säännöllisin välein tilattava tietoturvakontrollit tarkistava lisäresurssi olisi hyvä keino parantaa toimintaa.	Työasematurvallisuuden prosessit
Memberchecking Kommentit TMH3	1.2.2024 Pyydetty tarkistamaan sitaattien mukaiset tutkimustulkinnat: "Kaikki näyttäisi olevan oikein." -Haastateltava 3		
Teemahaastattelu: TMH4			
Haastattelija: Mies 46, Oulu, Tietoturva-arkkitehti Haastateltava: Mies 47, Helsinki, Työasema-asiantuntija Haastattelun toteutus: kahdenkeskinen, Teams-videoneuvottelu.			
Aineisto	Sitaatti	Tutkimustulkinta	Teema
Litterointi TMH4	<p>"Kertaalleen on aktivoitu tuo baselinerviointi siellä se löytyy meillä tuolta. intunesta, mutta sen kokeilujakso meni umpeen. Jos sitten miettisi näitä yleisiä tietoturvakehyksiä niin varmaan jotain nistiä mitä näitä on niin. varmaan olisi hyvä vähän tarkastella."</p>	Tietoturvakehysten arviontia on testattu, mutta tällä hetkellä ei tehdä.	Tietoturvakehysten käytännön hyödynnettävyys

Litterointi TMH4	"Osan varmaan pystyy suoraankin siiä arviosta kliksurtelemaan päälle tai sitten sitä kautta osoittamaan tiettylle porukalle tehtäväksi ja osa kovennuksesta voi olla sellaisia, että pitää ohjesivuston perusteella lähteä tekemään sitten manuaalisesti. Ja muutoshallinta on siinä taustalla ja tiiminä sovitaan niitä aikataulutuksia Kenelle jaellaan muutos milloinkin, että tuki säilyy toimintakykyisenä.	Vaikka voisikin suoraan kehyksen arviosta jakaa tietoturva-asetuksia päälle, pitää muutoshallinta ja tuen kuormittuvuus ottaa huomioon.	Tietoturvakehysten käytännön hyödynnettävyys
Litterointi TMH4	"Siitä kiireestä johtuu, ettei tule tutustuttua riittävän laajalti sen muutoksen eri puoliin ja kokemuksiin kollegoilla maailmalla. Toisaalta välillä sitten virheet on tullut sen takia että nykyään valitettavan useasti dokumentaatiota joko ei ole ollenkaan tai sitten se on hyvin ylimalkaista tai jopa puutteellista, välillä jopa virheellistä tai vanhentunutta tai monitulkintaista.	Kiire johtaa vajanaisilla tiedoilla tehtäviin muutoksiin. Dokumentaation puutteellisuus ja epävarmat testaushavainnot aiheuttavat ongelmia organisaatioon tehdyissä muutoksissa.	Työasematurvallisuuden prosessit

	Näihin liittyy se, että. kun pyritään testaamaan asioita, niin aina sen asian testaaminen ei ole välttämättä niin mustavalkoista, että voitaisiin joka kerta täydellä varmuudella sanoa, että hei, nyt se muutos meni ja on voimassa tuolla ja nyt kun me testataan niin voimme todeta, että se toimi tällä tavalla, ja että näin se toimii sitten kaikilla muillakin.”		
Litterointi TMH4	”Niitä samanaikaisia muutoksia on todella paljon työn alla, että riittääkö tekijöillä aika. Aina kaikki tehdään viimeisen päälle: perehdytykset, tiedotteet. Mutta siinä on semmoista pientä rapatessa, roiskuu typpistä seurausta sitten.”	Tiedotus tehdystä muutoksista saattaa kiireessä olla puutteellista.	Työasematurvallisuuden prosessit
Litterointi TMH4	”Joo on siellä pilvessä haasteita ollut. Nimenomaan yksi on epämääräisyys. Milloinka asetukset tai asetusmuutokset on kaikille työasemille kohdistunut? Tuolla maassahan se on hyvin selkeetä kun tiedetään että se on tietty kaava. Kyllä tuo pilvessäkin ilmeisesti on, mutta on väillä tuntunut, että siltikään ei välttämättä saman päivän aikana tapahdu yhtään mitään työasemalla, vaikka ehkä pitäisi.”	Pilvessä ei pysty aina sanomaan milloin tehdyt asetusmuutokset ovat kohdistuneet ja menneet työasemille. Maassa helpompaa todentaa.	Työaseman tietoturvan kovennus

Litterointi TMH4	"Maailmanpoliittinen paine 2022 keväällä, siinä tuli jonkun verran kyllä loppukäytäjä vaikutuksia. Kaikista asioista ei tiedetty mitä ne vaikuttavat ja sitten niitä poikkeus sääntöjä ei pystytty etukäteen tekemään, koska ei ollut tiedossa mitä pitäisi poikkeuksena pistää. Joo ja jos vähän toisella tavalla, niin muutos velkaa on aika paljon pitkältä ajalta. Voidaan puhua vaikka kymmenenkin vuoden tai jopa pidemmästä aikajänteestä, mistä on muutosvelkaa ja se näkyy tieteenkin silloin, kun halutaan nopeasti jotakin saada aikaiseksi: sitten tulee törmäyksiä."	Tekninen muutosvelka aiheuttaa kiireellisissä tilanteissa ongelmia, kun kaikkea muutokseen liittyvää ei keretä varmistamaan.	Työasematurvallisuuden prosessit
Litterointi TMH4	"Tietoturvaan liittyen myös erillisvapaudet mitä on annettu aikojen kuluessa tietyille porukoille. Näidenkin purkaminen on melkoisen työlästä. Pitäisi pyrkiä välttämään tilanteita missä ilman selkeetä työnkulullista hyötyä tai teknistä syytä annetaan erillis vapauksia."	Tietoturvan suhteen ei pitäisi tehdä erillispoikkeuksia, koska niiden purkaminen myöhemmin on vaikeaa. Perustelut pojakeksille pitäisi olla sidottu tekniseen tai työnkululliseen haasteeseen.	Työaseman tietoturvan kovennus
Litterointi TMH4	"Meillä on aika hyvin faktoihin perustuva raportti, jossa asetus kohtaisesti näytetty, että tämmöistä on päällä. Ja siitä voi muodostaa kuvan, minkälainen meidän selainturvallisuus esimerkiksi on työasemissa."	Organisaatiolla on olemassa ylätason kuvaus tietoturvakontolleista raportin muodossa.	Auditointivuus ja tilannekuva

Litterointi TMH4	"Aina tai yleensä keksi suunnan, että menenkö maan suuntaan vai pilven suuntaan. Mutta sitten konfiguraation keksiminen niin tota. Ei sitä ihan 10 sekunnissa välttämättä löydää. Osa kontolleista on sitten toisen tiimin ylläpitämä, semmoisessa paikassa, mihin meillä ei ole edes kirjautumisoikeuksia tai edes katselu oikeuksia, joten me ei työasematiimissä pystytä edes muodostamaan kokonaiskuvaa"	Tietoturvakontrollien hallinta on nykytilassa hajautunut eri tuotteisiin ja eri tiimeille. Työasematiimi ei pysty muodostamaan niistä kokonaiskuvaa.	Työasematurvallisuuden prosessit
Litterointi TMH4	"Pilven päässä nähdään paremmin lukuja onnistuneista ja epäonnistuneista konfiguroinnin vaiheista. Maan päässä ei oikeastaan nähdä. muuta kuin tarkastelemalla yksittäisiä työasemia. Mikä ei tietenkään ole mahdollista kuin ehkä satunnaisesti. Puuttuu myösken prosessi säädöllisesti seurata, että konfiguraatiota tai sanotaan että prosessi ei ole ole kaikin puolin kattava. Niin tällä hetkellä käspelillä puututaan oikeastaan jos käyttäjälle joku asia ei toimi."	Tietoturvakovenkuksista saadaan pilvessä paremmin raportteja kuin maassa, mutta säädöllisesti ei seurata yksittäisten laitteiden turvallisuustilannetta. Toiminnallisuusongelmiin puututaan käyttäjän ilmoitusten kautta.	Työasematurvallisuuden prosessit

Litterointi TMH4	että kohdistuuko meihin jotakin ja jos havaitaan että kohdistuu, niin pyritään löytämään sitten ennaltaehkäiseviä keinoja. Väillä vähän liiankin kiireesti, että meilläkin on roiskunut silleen ihan valideja Windows tiedostoja on merkitty, että ne pitää blokata ja toi on aiheuttanut sitten käyttäjillä vähintäänkin ilmoituksia”	Organisaatiossa on reagoitu ulkopuolelta tulleeseen uhka- tai haavoittuvuustietoon nopeastiin, ohittaen muutoshallinta, joka on aiheuttanut myös ongelmia.	Windows-työaseman käytännön tietoturva ja uhkat
Member- checking Kommentit TMH4	2.2.2024 Pyydetty tarkistamaan sitaattien mukaiset tutkimustulkinnat: "Kaikki näyttäisi pitävän paikkaansa, juuri kuten puhuttiinkin." -Haastateltava 4		

Tutkimustuloksissa hyödynnetyt aineistot

Taulukko1. Tutkimusaineistot mukaillen ANTIC-mallia

Tekijä(t)	Otsikko	Sisältö	Avainteemat	Oma arvio	Vastaanotto tai sivuaukutut tutkimuskysymystä tai ongelmaa
Antonucci 2017.	The cyber risk handbook, creating and measuring effective cybersecurity capabilities.	Kuinka riskienhallinnalla voidaan vaikuttaa tietoturvan tilannekuvaan	Tietoturvan tilannekuva	Ainakin teoreettinen viitekehys	Kysymykset 3,4
Atoum, I., Otoom, A., Abu, A. 2014.	Holistic cyber security implementation framework	Tietoturvan hallintamalli, joka ottaa kokonaismallit aistisi huomioon riskit, toteutuksen ym.	Tietoturvakehysten käytännön hyödynnettävyys, vaatimustenmukaisuus	Teoreettinen viitekehys ja tulosten triangulaatiossa.	Kysymykset 3,4
Bongiovanni, I., Renaud, K., Brydon, H., Blignaut, R., Cavallo, A. 2022.	A quantification mechanism for assessing adherence to information security governance guidelines	Tietoturvan tilannekuvantavat asiat. Johdon näkyvyys.	Tietoturvan tilannekuva.	Teoreettinen viitekehys, ehkä triangulaatiossa.	Kysymys 3
Dedeke, A., Masterson, K. 2019.	Contrasting cybersecurity implementation frameworks (CIF) from three countries	Tietoturvakehysten kehitys ja käyttö eri maissa ja organisaatioissa	Tietoturvakehysten käytännön hyödynnettävyys	Teoreettinen viitekehys, hyvä myös tulostriangulaatioissa.	Kysymykset 2,4
Dietrich, C., Krombholz, K., Borgolte, K., Fiebig, T. 2018.	Investigating System Operators' Perspective on Security Misconfigurations	Tietoturvakofiguraatioiden väärinmääritelyiden merkitys käytännön tietoturvassa.	Tietoturvakehysten käytännön hyödynnettävyys.	Teoreettinen viitekehys, ehkä. Vähintään aineistotriangulaatioissa.	Kysymykset 3,4

Duncan, B., Whittington, Mark. 2014.	Compliance with standards, assurance and audit: Does this equal security?	Hieno vertailu kehysten käytöstä ja turvallisuuden toteuttamisesta eri näkökulmista	Tietoturvakehykset, auditointi, käytännön tietoturva	Teoreettinen viitekehys ja aineistorian gulaatio	Kysymykset 1,2,3
Dunkerley, M., Tumbarello, M. 2022.	Mastering-windows-security-and-hardening-second-edition	Käsittlee laajasti Windows pohjosten järjestelmien tietoturvavalkoennuksia	Työaseman tietoturvan kovennus	Erittäin hyödyllinen pohjateoria na, sekä teoreettises sa viitekehys essä että kirjallisessa konstruktios sa	Kysymykset 1,2
Goel, R., Kumar, A., Haddow, J. 2020	PRISM: a strategic decision framework for cybersecurity risk assessment.	Kyberturvalli suuden riskien hallintamalli keinona priorisoida tietoturvauhki en käsitellyä.	Tietoturvavalkoennus, tietoturvan tilannekuva	Teoreettise ssa viitekehys essä sekä tutkimustulo ksissa hyödyllinen malli.	Kysymykset 1,2,3,4
Hamdani, S., Abbas, H., Janjua, A., Shahid, W. 2021	Cybersecurity Standards in the Context of Operating System: Practical Aspects, Analysis, and Comparisons	Standardien ja kehysten käyttö suhteessa käyttöjärjestelmän kovennuksiin	Kyberturvallis uuden termistö, tietoturvakehykset, tietoturvavalkoennukset	Käy oikeastaan kaikkiin vaiheisiin tutkimukses sa	Kysymykset 1,2,4
Ibor, A., Obidinnu. J. 2015	System Hardening Architecture for Safer Access to Critical Business Data	Järjestelmäkovenusten määrittely	Tietoturvavalkoennusten määrittelyt	Tutkimustuloksissa, hyvä grafiikka	Kysymys 1,2
Malatji, M., Von, S., Marnewick, A. 2019.	Socio-technical systems cybersecurity framework	Sosio-teknologisen kuilun nostava tietoturvakehysnäkökulma	Tietoturvakehykset, ja käytännön hyödynnettäv yys.	Käy teoreettisen viitekehys sen ja tutkimustria ngulaation vaiheisiin.	Kysymykset 1,4

Mistry, S., Lalwani, P., Potdar, M. 2018.	Endpoint Protection through Windows Operating System Hardening.	Tietoturvako vennusten prosessi-priorisointi- ja tekniikkamall i	Työaseman tietoturvan kovennus ja auditointi	Teoreettinen viitekehys, käsitteiden avaaminen	Ei vastaa, mutta perusmäärittelyynä hyvä.
Nicho, M 2018	A process model for implementing information systems security governance	Tapa hallita vaatimusten mukaisuutta organisaatiossa. Parantaa hallintaa, näkyvyttä ja toimii määrämuotoisen prosessin mukaan (PDCA)	Auditointi, käytännön tietoturva, tietoturvan tilannekuva	Teoreettinen viitekehys ja erittäin hyvä malli tuloksiin verrattavaksi	Kysymykset 2,3,4
Oriyano, S-P. 2017.	Penetration testing essentials	Näkökulma tietoturvakovenusten testaamiseen	Tietoturvakovenus, auditointi, käytännön tietoturva	Teoreettinen viitekehys ja tutkimustulokset	Kysymys 1, 2
Silberschatz, A., Galvin, P., Gagne, G. 2018	Operating system concepts	Windows käyttöjärjestelmän sisältö kattavasti	Windows versiot ja perusteet	Teoreettinen viitekehys, käsitteiden avaaminen	Ei vastaa, mutta perusmäärittelyissä hyvä.
Siponen, M., Willison, R., 2009.	Information security management standards: Problems and solutions	Tietoturvakehysten määritellyitä ja tunnistettuja ongelmia.	Tietoturvakehykset, käytännön hyödynnettävyys	Ainakin teoreettinen viitekehys, voi olla hyvä pointti triangulaatiossa	Kysymykset 1,2
Trustcloud s.a.	Standard vs Framework vs Laws vs Regulations	Vertailua standardien, kehysten ja regulaation eroista	Tietoturvakehykset, käytännön hyödynnettävyys	Tutkimustuloksissa ainakin	Kysymys 1
Weiss, M., Solomon, M. 2015.	Auditing IT infrastructure s for Compliance.	Esiteltävä laajasti windows-pohjaisiin IT-ympäristöihin liittyviä auditointikäsiteitä ja prosesseja.	IT ympäristöjen auditointi	Hyödyllinen sekä teoreettisesä viitekehysessä, että tutkimustulosten synteemiseessä	Kysymykset 3,4
Xu, T., Zhou, Y. 2015.	Systems Approaches to Tackling Configuration Errors: A Survey	Mielenkiintoinen näkökulma järjestelmämuutosten vaikutuksista vikatilanteisiin	Tietoturvakovenukset	Teoreettinen viitekehys, ehdottomas ti triangulaatiossa.	Kysymys 4

Zamora, P., Kwiatek, M., Bippus, V., Elejalde, E. 2019.	Increasing Windows security by hardening PC configuration s	Case- esimerkki n. 8000 Windows laitteen ympäristöss ä tehdystä kovennuspro jektista	Työaseman tietoturvan kovennus	Hyödyllinen teoreettises sa viitekehys essä	Kysymys 4
---	---	--	--------------------------------------	---	-----------

Kirjallinen konstruktio

Tietoturvastandardit -kehykset, -kovennus ja -työkalut

Materiaali työasematurvallisuutta kehittävälle

SISÄLLYS

1. TIETOTURVASTANDARDIT JA -KEHYKSET

- 1.1 Sabsa tietoturvan hallintamalli
- 1.2 NIST Cybersecurity Framework
- 1.3 NIST Security and Privacy Controls
- 1.4 Digitaalisen turvallisuuden arkkitehtuuri (Dtark)
- 1.5 CIS Critical Security Controls
- 1.6 Mitre att&ck ja d3fend
- 1.7 Defense in depth ja kerroksittainen tietoturva

2. KÄYTÄNTÖTASON KEHYKSET JA TIETOTURVAKOVENNUS

- 2.1 Järjestelmäkovenkuksen näkökulmat
- 2.2 CIS Benchmarks
- 2.3 DISA STIG
- 2.4 Windows security ja security baselines
- 2.5 Microsoft SecCon

3. TIETOTURVAKOVENNUKSEN JA AUDITOINNIN TYÖKALUT

- 3.1 Microsoft Purview Compliance manager
- 3.2 Defender for endpoint ja vulnerability management
- 3.3 CIS-CAT ja CIS CSAT
- 3.4 DISA STIG viewer ja SCAP compliance checker

LÄHTEET

KUVALUETTELO

1. TIETOTURVASTANDARDIT JA -KEHYKSET

HIMSS:n (2019) mukaan tietoturvakehykset voivat auttaa organisaatiota hallitsemaan kyberturvallisuuden riskejä, toimimalla organisaation riskienhallinnan tiekarttana. Noudattamalla yhtä tai useampaa tietoturvakeyhystä tai standardia organisaatiot voivat parantaa turvallisuuden tilaansa. Kehykset sisältävät yleisesti määrämuotoisia suosituksia ja tietoturvallisuutta parantavia parhaita käytäntöjä, joiden avulla voidaan pienentää vakavien tietoturvatapahtumien riskiä.

Kehysten tai standardien käyttö myös parantaa mahdollisten hyökkääjien havaitsemista tai hyökkäyksistä toipumista toimivien prosessien avulla. Tietoturvakehykset myös tarjoavat metriikoita tai työkaluja kehyksen käyttöönnoton mittaamiseksi. HIMSS mainitsee, että kehysten käyttö ei ole kuitenkaan organisaation kyberturvallisuuden kypsyyden mittari, eikä täydellinenkään tietoturvakehyksen täyttäminen ole tae organisaation tietoturvan toimivuudesta. HIMSS suositteleekin kaikkien tietoturvaohjelmien mittamista auditoimalla, ja vertaamalla niitä alan tasoon, sekä varmistamalla kaikkien kontrollien toimivuuden kaikilla tasoilla. (HIMSS 2019).

1.1 Sabsa tietoturvan hallintamalli

Tietoturvallisuus voidaan laskea osaksi onnistunutta järjestelmääarkkitehtuuria. Tämän takia kaikki tietoturvallisuuden kovennukset ja auditoitavuus kannattaa sitoa jonkinlaiseen tietoturvallisuuden hallintamalliin tai arkkitehtuuriin. Strategia, prosessit, politiikat, ihmiset ja turvallisuuskulttuuri ovat olennaisia osia onnistuneen mallin hyödyntämisessä. Ilman tietoturvan hallintamallia ei operatiivista tietoturvaa, johon esimerkiksi työasematurvallisuuden kovennukset kuuluvat, voida sitoa miinkään. Tällöin tietoturvan kokonaiskuva jää epäselväksi. (Sabsa s.a).

Sabsan artikkelin (s.a) mukaan heidän mallinsa on itseasiassa metodologia, jonka avulla voidaan rakentaa riskeihin pohjautuva turvallisuusarkkitehtuuri, joka ottaa huomioon liiketoiminnan tarpeet. Sabsa vertaa turvallisuusarkkitehtuurin rakentamista kaupungin tai talon arkkitehtuuriin.

Sabsan mukaan metodologia on kaikille organisaatioille avoin ja ilmainen standardi, joka kattaa useita muita kehyksiä, metodeja sekä prosesseja. Sabsa kertoo standardin olevan helposti skaalautuva, sopivan kaikille toimialoille ja olevan täysin mihinkään IT toimittajaan sitoutumaton neutraali tietoturvakehys (Sabsa s.a.).

Sabsan malli (2009) sisältää kuusi eri kerrosta organisaation tietoturvaarkkitehtuurin rakentamiseen, jotka on jaettu eri näkökulmiin tai rooleihin.

Sabsa myös kertoo operatiivisen (eng. security service management architecture) tietoturvan haasteiden koskettavan kaikkia muita kerroksia.

Kuvassa 1 on kerrottu, kuinka eri näkökulmat tai roolit liittyvät Sabsan mallin mukaisiin arkkitehtuurikerroksiin.

The Business View	Contextual Security Architecture
The Architect's View	Conceptual Security Architecture
The Designer's View	Logical Security Architecture
The Builder's View	Physical Security Architecture
The Tradesman's View	Component Security Architecture
The Service Manager's View	Security Service Management Architecture

Kuva 1. Sabsan tietoturvamallin kerrokset (Sabsa 2009)

Sabsan malli (2009) sisältää myös erittäin yksityiskohtaisia tapoja, dokumenttimalleja ja esimerkkejä kerrosten sisällä, koska Sabsan mukaan he haluavat tarjota jokaiselle organisaatiolle juuri heille sopivan kokonaisuuden. Esimerkki yhdestä dokumenttimallista kuvaaa Sabsan kerroksittaista tietoturvan arkkitehtuurimallia (kuva 2).

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Management Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, Including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identified Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

Kuva 2. Sabsa-Kerroksittainen tietoturva-arkkitehtuurimalli (Sabsa 2009)

Kerroksittaisen tietoturva-arkkitehtuurimallin rakennuksessa on hyvin nähtävillä jokaisen kerroksen läpileikkaavat kysymykset mitä, miksi, kuinka, kuka, missä, milloin. Samat kysymykset pitää viedä läpi koko arkkitehtuurin, riippumatta arkkitehtuurikerroksesta. Noudattamalla mallia saadaan huolehdittua määrämuotoisesti kyseisen koteen koko elinkaaren kattavasta hallinnasta. Sabsan kerroksittainen tietoturva-arkkitehtuurimalli on esimerkki, jonka organisaatio voi muokata itselleen toimivaksi. (Sabsa 2009).

Sabsa –liiketoiminnan näkökulma

Sabsan (2009) mukaan tässä tasossa määritellään konteksti, jossa toimitaan, ja yhdistetään liiketoiminnan vaatimukset tietoturvan vaatimuksiin ja tahtotiloihin. Sabsa painottaa erityisesti tietoturva-arkkitehdin roolia liiketoiminnan ja tietoturvan välisenä tulkkina. Lain vaatimukset ja datan käsitteilyyn liittyvät rajoitteet on syytä käydä tarkkaan dokumentaation tasolla läpi, ja peilata niitä vasten Sabsan mallista löytyviä kysymysmalleja. Tässä kerroksessa esitetään myös malli, jonka avulla liiketoiminnan vaatiman ratkaisun (esim. uusi tietojärjestelmä) arkkitehtuuria lähdetään selvittämään esittämällä mm. seuraavia kysymyksiä: mitä? miksi? kuinka? kuka? missä? milloin? Sabsan mukaan tämän arkkitehtuuritason ohittaminen johtaa usein arkkitehtuuriin, joka ei vastaa käyttäjien (liiketoiminnan) vaatimuksia. (Sabsa 2009).

Sabsa –arkkitehdin näkökulma

Sabsan (2009) mukaan tässä tasossa lähdetään purkamaan liiketoiminnan vaatimuksia konseptuaalisiksi vaatimuksiksi. Sabsa kuvaa tätä tasoa "isoiksi pensselinvedoiksi", jossa maalataan arkkitehdin kokemuksen ja osaamisen pohjalta lähtökohdat tarkemmalle detaljeja sisältävälle työlle. Konseptityössä kerrotaan, mitä tietoturvakyötäntöjä tai konsepteja tullaan käyttämään, esim. kuvien tai kuvausten kautta. Liiketoiminnan vaatimusten apuna voidaan myös käyttää esim. lista, jolla määritellään:

- Mitä halutaan suojata?
- Miksi suojaus on tärkeää?
- Kuinka suojaus toteutetaan?
- Kenen vastuulla on toteuttaa?

Arkkitehdin tulee löytää liiketoimintavaatimuksia vastaava tietoturvastrategia. Esimerkinä konseptitason työstä voidaan käyttää nollaluottamusmallin (eng. zero trust model) hyödyntämistä. (Sabsa 2009).

Sabsa –suunnittelijan näkökulma

Siivä missä arkkitehdin näkemys on isoja linjanvetoja, suunnittelijan rooli on tuottaa selkeä looginen rakenne toteutettavalle tietoturva-arkkitehtuurille. Suunnittelija tunnistaa sidosryhmät ja yhdistää erilaiset vaatimusmäärittelyt ja politiikkadokumentit toteutettavaa tietoturva-arkkitehturia vasten. Lopputuotoksina yleisimmin on loogisia yhteyskaavioita, politiikkalistauksia tai vaatimustenmukaisuuden dokumentteja (liittyen valittuun tietoturvastrategiaan). (Sabsa 2009).

Sabsa –rakentajan näkökulma

Sabsa puhuu artikkelissaan rakentajan näkökulmasta, joka tarkoittaa suunnittelutyötä, jonka tarkoituksesta on purkaa ylempien kerrostenvaukset tarkemmalle tekniselle tasolle. Tällä tasolla tunnistetaan tarvittavia turvallisuusmekanismeja, esim. varmenteet, kryptaus, pääsynhallinta, virustorjunta. (Sabsa 2009).

Sabsa –asiantuntijan näkökulma

Tällä tasolla Sabsa kuvaa käytännön yksityiskohtaisen arkkitehtuurin "rakennuspalkkoiden" kasaamista. Kaikki aiemmillä tasoilla tunnistetut vaatimusmäärittelyt, dokumentaatiot ja kuvat määritetään vasten tarvittavia tietoturvatyökaluja ja tuotteita. Voidaan varmaan sanoa, että tällä kerroksella päästään lopulta konkretiaan käsiksi. Tällä kerroksella keskitytään myös tekijöiden työkaluihin, tarvittavaan osaamiseen ja tiimien rakentamiseen. Ylemmän tason arkkitehtuurin vaatimuksista koostetaan yksityiskohtaiset toteutussuunnitelmat. (Sabsa 2009).

Sabsa –turvallisuusmanagerin näkökulma

Sabsan (2009) mukaan tällä tasolla keskitytään operointiin ja palvelun hallintaan. Arkkitehdit, suunnittelijat ja rakentajat eivät ole yleensä mukana ylläpidossa. Ylemmän tason arkkitehtuurin vaatimuksia pyritään noudattamaan tietoturvaratkaisun ylläpidossa. Erityisesti tällä tasolla pitää pystyä hallitsemaan operationaaliset riskit, raportoimaan ja monitoroimaan ratkaisua sekä takaamaan sen toiminta. Sabsa painottaa, että turvallisuuden hallintopalvelun suunnittelun pitää kuitenkin kuulua yhtenä osana kaikkien muiden kerrosten toteutukseen. Hallintopalvelu on täten läpileikkaava kaikkien muiden kerrosten kanssa. (Sabsa 2009).

Sabsa –auditoijan ja turvallisuuden hallinnan näkökulma

Sabsa kertoo artikkelissaan myös auditoijan ja "laadunhallitsijan" (eng. governor) näkökulmasta. Pääasiana Sabsan mallissa on, että auditointi ja hallinnan rakentaminen kuuluvat sisäänrakennettuna Sabsan arkkitehtuurimallin eri kerroksiin. Koska auditointi on rakennettu valmiiksi sisään arkkitehtuuriin, on mahdollisen auditoinnin tai laadun varmistuksen määrämuotoinen ja systemaattinen toteuttaminen helpompaa osana turvallisuuden hallintopalvelua. (Sabsa 2009).

3.4 NIST Cybersecurity Framework

National Institute of Standards and Technology (NIST) on Yhdysvaltojen valtion virasto, jonka toimialaan kuuluu tieteellinen tutkimus, standardien

kehittäminen sekä teknologisten innovaatioiden ja teollisten kyvykkyyksien edistäminen (NIST 2023). USA:n hallitus antoi Nist:n tehtäväksi vuonna 2014 kehittää kriittisen infrastruktuurin omistajille sopivan kyberturvallisuuden riskipohjaisen kehyksen, jonka avulla infrastruktuurin omistajat voivat paremmin tunnistaa, arvioida ja hallita kyberturvallisuusriskejä. NIST kehitti näistä lähtökohdista nykyään laajasti tunnetun NIST Cybersecurity Frameworkin. NIST:n mukaan kehyksessä on hyödynnetty useita vakiintuneita ja tunnettuja standardeja ja kehyksiä, kuten Cobit, ISO27001, ISA, ja CIS CSC. NIST kertoo kehyksen olevan hyödynnettävissä missä tahansa organisaatiossa ja alalla. Vaikkakin kehys on kehitetty Yhdysvalloissa, eivät parhaat käytänteet ole maasidonnaisia. (NIST 2018; NIST 2022).

NIST kuvaa CSF-mallinsa (versio 1.1) olevan riskipohjaiseen näkökulmaan perustuva tapa hallita kyberturvallisuusriskejä. Mallin mukaan toimien voidaan tunnistaa ja priorisoida kyberturvallisuusriskejä vähentäviä toimia. Malli sisältää poliikan, liiketoiminnan ja teknologisen näkökulman kyberturvallisuusriskien hallintaan. Kehys koostuu kolmesta kerroksesta, joihin viitataan nimillä ydin, käyttöönottokerros ja profiili (eng. core, implementation tiers, profile). NIST mainitsee eri kehysten kerrosten tukavan liiketoiminnan ja kyberturvallisuuden aktiviteettien yhdistämistä. (NIST 2018; NIST 2020).

NIST Core

Ydin koostuu kokonaisuudesta kyberturvallisuuden aktiviteetteja, jotka ovat yleisiä kriittisen infrastruktuurin sektoreilla. Ydin koostuu standardeista, parhaista käytännöistä ja lopputuloksista, joita voidaan hyödyntää organisaatioissa johdosta suorittavaan portaaseen asti. Ydin on jaettu viiteen eri toiminteeseen, 23 kategoriaan, ja 108 alakategorian. (NIST 2018).

Tunnistaminen, suojaaminen, havainnointi, reagointi ja palautumiskyky (eng. identify, protect, detect, respond, recover) ovat viisi eri ylätoimintoa, joiden alle sijoitettuja kategorioita ja alakategorioita on kuvattu kuvassa 3. Näiden lisäksi alakategorian on yhdistetty informatiivinen viite sopiviin standardeihin, käytäntöihin ja kehyksiin. (Pathlock 2022; NIST 2020).

The diagram illustrates the mapping of NIST functions to subcategories and informative references. A large curly brace on the right side groups the subcategory and informative references columns. Another curly brace on the left side groups the function and category columns.

Function	Category	ID	Subcategory	Informative References
Identify	Asset Management	ID.AM	ID.BE-1: The organization's role in the supply chain is identified and communicated	COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05
	Business Environment	ID.BE		ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2
	Governance	ID.GV		NIST SP 800-53 Rev. 4 CP-2, SA-12
	Risk Assessment	ID.RA		COBIT 5 APO02.06, APO03.01
	Risk Management Strategy	ID.RM		ISO/IEC 27001:2013 Clause 4.1
Protect	Supply Chain Risk Management	ID.SC	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	NIST SP 800-53 Rev. 4 PM-8
	Identity Management and Access Control	PR.AC		COBIT 5 APO02.01, APO02.06, APO03.01
	Awareness and Training	PR.AT		ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6
	Data Security	PR.DS		NIST SP 800-53 Rev. 4 PM-11, SA-14
	Information Protection Processes & Procedures	PR.IP		COBIT 5 APO02.01, APO02.06, APO03.01
Detect	Maintenance	PR.MA	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6
	Protective Technology	PR.PT		NIST SP 800-53 Rev. 4 PM-11, SA-14
	Anomalies and Events	DE.AE		COBIT 5 APO10.01, BAI04.02, BAI09.02
	Security Continuous Monitoring	DE.CM		ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3
	Detection Processes	DE.DP		NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
Respond	Response Planning	RS.RP	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	COBIT 5 DSS04.02
	Communications	RS.CO		ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1
	Analysis	RS.AN		NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14
	Mitigation	RS.MI		COBIT 5 APO10.01, BAI04.02, BAI09.02
	Improvements	RS.IM		ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1
Recover	Recovery Planning	RC.RP	ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14
	Improvements	RC.IM		COBIT 5 DSS04.02
	Communications	RC.CO		ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1

Kuva 3. NIST funktiot, kategoriat ja informatiiviset viitteet (Pathlock 2022)

NIST Implementation Tiers

Käyttöönottokerrosten (eng. implementation tiers) malli antaa organisaatiolle tavan katsoa ja mitata organisaation nykyisiä käytäntöjä vasten erilaisia mittareita. Käyttöönottokerros koostuu määritystä, joista saatavan kerrosmallin avulla saadaan tukea päätöksentekoon, kun valitaan organisaatiolle sopiva kyberturvallisuusmalli. Käyttöönottokerros ei ole kuitenkaan mittari organisaation riskienhallinnan kypsyydestä, vaan se on vain tapa kategorioida ja asettaa sopiva strateginen taso organisaation riskinottokykyä vasten. Kuvassa 4 on kuvattu eri käyttöönottokerrosten suhde toisiinsa ja kerrottu, kuinka hallittu ja määrämuotoinen organisaation riskienhallintaprosessi, sisäinen riskienhallinnan ohjelma ja ulkopuolisten toimijoiden osallistaminen liittyvät toisiinsa (eng. risk management process, integrated risk management program ja external participation). (NIST 2018).



Kuva 4. NIST käytöönottokerrokset (Pathlock 2022)

Eri kyvykkystasoja on kuvattu kuvassa 5 termeillä osittainen, riskitietoinen, toistettava, mukautuva (eng. partial, risk informed, repeatable, adaptive) (NIST 2023).

NIST Framework Profile

NIST (2018) kuvailee profilia yleisesti ensimmäisenä askeleena kyberturvallisuuden hallintamallin kehityksessä. Profili voi NIST:n mukaan sisältää nykytilanteen arvion, tai tulevan toivetilanteen. Profiilissa linjataan toiminteiden, kategorioiden ja alakategorioiden vastaavuus liiketoiminnan vaatimuksiin. Profiilin rakentaminen mahdollistaa organisaatioille kyberturvallisuusriskin vähentämiseen tähtäävän tiekartan, jossa pystytään ottamaan huomioon alan, lain ja organisaation vaatimukset sekä käytännöt. Profili on yhteydessä aiemmin kerrottuun käytöönottokerrokseen, ja näitä vertaamalla voidaan löytää esim. resurssi- tai kyvykkyyssuhteita (NIST 2018).

1.3 NIST Security and Privacy Controls

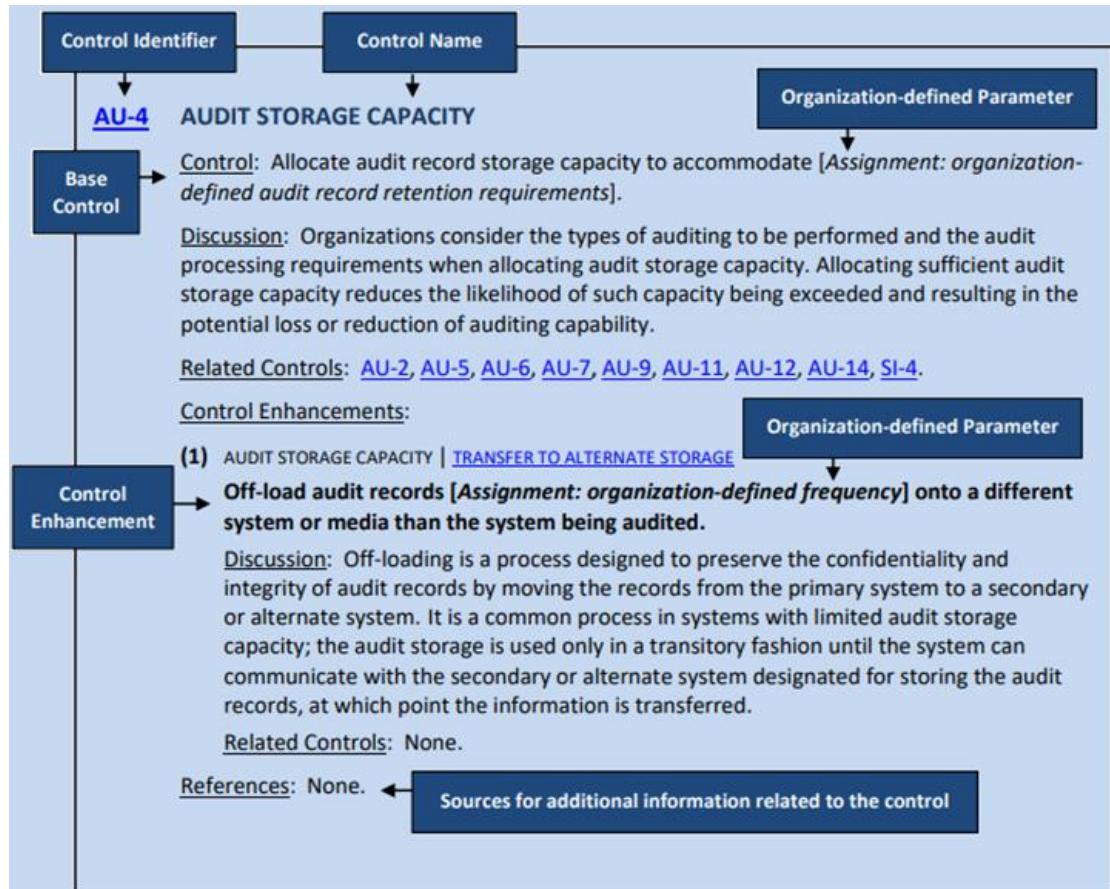
NIST (2020) kuvilee julkaisemansa tietoturvakayheksen (SP 800-53) sisältävän turvallisuuskontrolleja, tai vastakeinoja, joita voidaan asettaa järjestelmiin, jotta mm. tietoturvan, tietosuojan, lain, määräysten, ohjeistusten, vaatimustenmukaisuuden ja eri standardien täyttyminen voidaan varmistaa.

NIST:n mukaan turvallisuuskontrollit varmistavat cia-periaatteen (confidentiality, integrity, availability) toteutumisen tietosuojan sekä tiedon käsittelyn elinkaaren osalta. NIST kertoo myös julkaisussaan turvallisuuskontrollien vastaavan NIST Cybersecurity Framework -tietoturvan hallintamalliin ja siinä esitettyihin toimintoihin. NIST:n mukaan julkaisussa on mukana erilaisia valmiita työkaluja, kuten taulukkomuotoinen kontrollikokonaisuus sekä valmiita ristiin vertailuja (eng. mappings) muihin tietoturvakehyksiin kuten ISO27001:an. Tietoturvakehys on jaettu erilaisiin tietoturvallisuuden ja tietosuojan kontrolliperheisiin. Kuvassa 5 on esitetty nämä 20 erilaista kontrolliperhettä. (NIST 2020).

ID	FAMILY	ID	FAMILY
<u>AC</u>	Access Control	<u>PE</u>	Physical and Environmental Protection
<u>AT</u>	Awareness and Training	<u>PL</u>	Planning
<u>AU</u>	Audit and Accountability	<u>PM</u>	Program Management
<u>CA</u>	Assessment, Authorization, and Monitoring	<u>PS</u>	Personnel Security
<u>CM</u>	Configuration Management	<u>PT</u>	PII Processing and Transparency
<u>CP</u>	Contingency Planning	<u>RA</u>	Risk Assessment
<u>IA</u>	Identification and Authentication	<u>SA</u>	System and Services Acquisition
<u>IR</u>	Incident Response	<u>SC</u>	System and Communications Protection
<u>MA</u>	Maintenance	<u>SI</u>	System and Information Integrity
<u>MP</u>	Media Protection	<u>SR</u>	Supply Chain Risk Management

Kuva 5. NIST SP 800-53 kontrolliperheet (NIST 2020)

Kontrollien kuvaukset ovat strukturoidut, sisältäen aina samat elementit (id, kuvaus, perustason suojaus, laajennettu suojaus, viitteet muihin tietoturvakehyksiin). Esimerkki yhden kontrollin kuvauksesta on esitetty kuvassa 6.



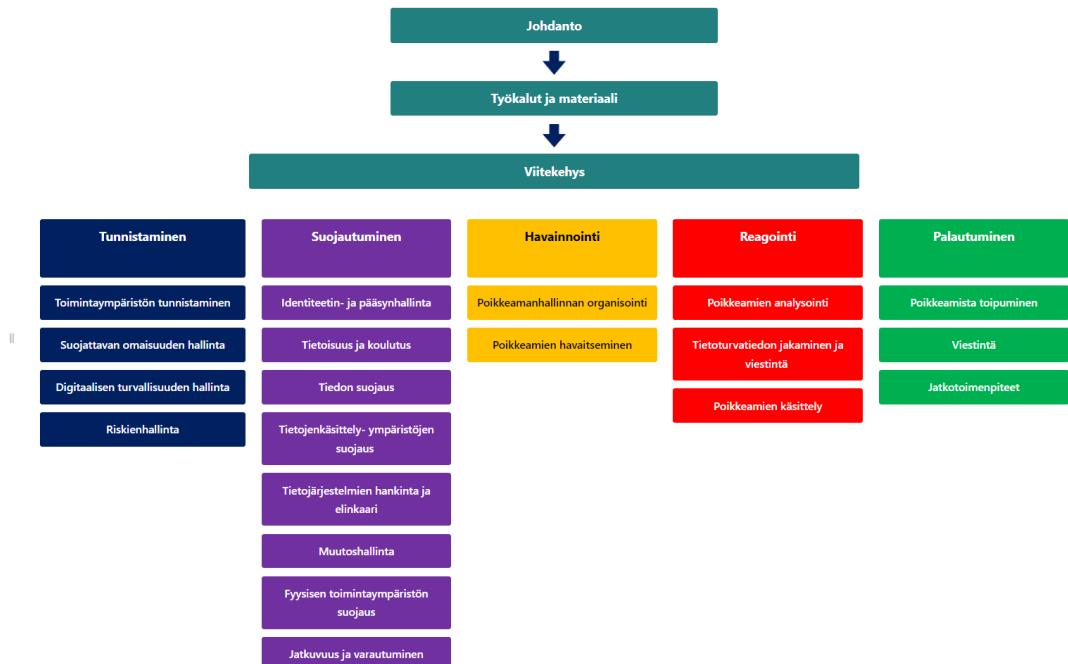
Kuva 6. Esimerkki NIST SP800-53 kontrollien kuvauksista (NIST 2020)

Kontrolliperheet sisältävät peruskontrollit, sekä niitä laajemmat tiukemmat kontrollit. Organisaatio voi valita käyttävänsä tiukempia kontrolleja tietojenkäsittely-ympäristön tai datan sensitiivisyyden niin vaatiessa (NIST 2020).

NIST kertoo dokumentissaan määritysten hallinnan kategoriasta (eng. configuration management). Mikä tahansa muutettavissa oleva asetus esim. tietokoneissa, käyttöjärjestelmissä, protokollissa ja sovelluksissa voi vaikuttaa tietoturvallisuuden tai tietosuojan tilaan. NIST:n mukaan organisaatio määrittää itse sopivan organisaatiotasoinen perustason (baseline), ottaen huomioon järjestelmien laitteisto, ohjelmisto tai laiteohjelmiston (eng. firmware) kyvyt. NIST:n mukaan tietyn teknologian tai tuotteen turvallisuus voidaan varmistaa noudattamalla yleisiä turvallisuuden tarkistuslistoja tai kovennusohjeistuksia. NIST mainitsee STIG ohjeistuksen hyödyntämisen turvallisen määritystason toteuttamiseen. (NIST 2020, 103–104)

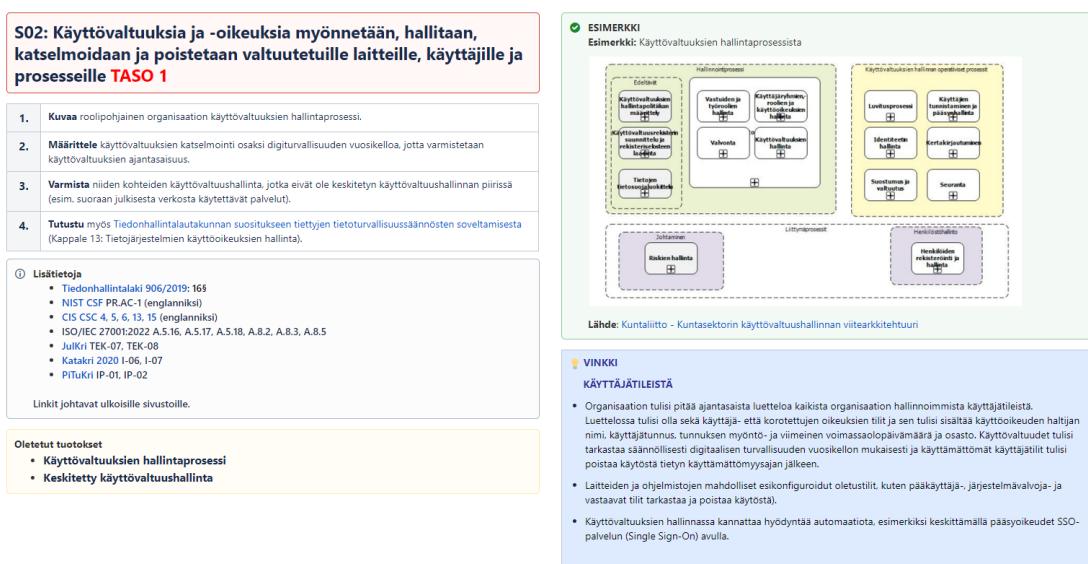
1.4 Digtalaisen turvallisuuden arkkitehtuuri (Dtark)

Digi ja väestötietovirasto (2022) on julkaissut (suomalaisten) julkisten organisaatioiden tarpeisiin muokatun digitaalisen turvallisuuden arkkitehtuurin viitekehyn. Kyseinen malli pohjautuu vahvasti NIST CSF-tietoturvakehykseen, mutta se on täysin suomennettu, jonka lisäksi sitä on rikastettu erityisesti suomalaisen lainsääädännön, viitekehysten ja suomalaisten viranomaisohjeistusten pohjalta. Digi ja väestötietovirasto on myös kasannut viitekehyn käyttöönottoa ja hyödyntämistä varten erilaisia työkaluja, ohjeistuksia sekä erimuotoisia suomenkielisiä koulutusmateriaaleja. Kuvassa 7 Digi ja väestötietovirasto havainnollistaa arkkitehtuurimalliaan, joka selvästi pohjautuu NIST CSF:ään, sisältäen samat pääkategoriat. (Digi ja väestötietovirasto 2022).



Kuva 7. DVV:n Dtark viitekehyn malli (Digi ja väestötietovirasto 2022)

Esimerkki eräästä identiteetin- ja pääsynhallinnan alakategorian kohdasta on kuvassa 8, josta näkee myös hyvin, kuinka NIST:in tietoa on rikastettu mm. suomalaisen tiedonhallintalain, Julkri:n, Katakri:n ja Pitukri:n relevanteilla alakohdilla.



Kuva 8. Dtark lisätietokentän rikastaminen Suomen omilla erityisillä standardeilla (Digi ja väestötietovirasto 2022)

1.5 CIS Critical Security Controls

Center for Internet Security (CIS) kertoo olevansa voittoa tavoittelematon yhteisöpohjainen organisaatio. CIS:n mukaan organisaation päätavoitteena on tarjota IT-alan parhaiden osaajien yhdessä tekemät parhaat käytännöt IT-järjestelmien ja datan turvallisuuden määrittelyyn (CIS s.a.c.).

CIS:n (s.a.h) mukaan critical security controls -tietoturvakehys sisältää kokonaisuuden yksityiskohtaisia ja tehokkaita kyberturvallisuuden puolustustoimia, joiden avulla organisaatio voi puolustautua laajavaikuttelisilta hyökkäyksiltä. CIS:n kontrollit on rakennettu niin, että ne voidaan ottaa käyttöön minimitasosta lähtien, laajentaen sitten tehokkaampiin ja vaativampiin kontolleihin. Kontolleja on yhteensä 18, jotka CIS:n mukaan pysäyttävät suurimman osan nykyään nähtävistä hyökkäyksistä. CIS kertoo kontrollien suunnitteluperiaatteena olevan minimitason priorisoinnin, jotta organisaatioiden on helpompi valita mitä kyberturvallisuutta parantavia toimia pitäisi ensin toteuttaa. Kontrollit eivät ole korvike muille tietoturvakehyksille, vaan CIS:n mukaan ne päinvastoin vertautuvat useimpiin isoihin tietoturvakehyksiin, kuten NIST CSF, PCI DSS ja ISO27000 -sarja. (CIS s.a.b, s.a.h).

CIS:n (s.a.i) kertoo dokumentissaan, kuinka uusin kahdeksas versio kontolleista perustuu CIS:n kehittämään yhteisöpohjaisen puolustuksen malliin (eng. community defense model). Tämä malli pohjautuu CIS:n mukaan useisiin lähteisiin, kuten Verizon DBIR-raporttiin ja MS-ISAC:n tietoihin tärkeimmistä hyökkäyksistä. Tämän datan perusteella CIS kuvailee dokumentissa viisi merkittävintä hyökkäystyyppiä vasten Mitre ATT&CK tietoturvakehystä. Mallin avulla voidaan verrata ja mitata CIS:n mukaisten suojauskontrollien tehokkuutta hyökkäysten torjunnassa. (CIS s.a.i).

CIS (s.a.i) kertoo kontrollien jaottelusta eri kontrolliperheisiin, käyttöönottoryhmiin ja suojauskontrolleihin. CIS havainnollistaa kontrolliperheitä, käyttöönottoryhmiä ja niiden suhdetta suojauskeinoihin kuvassa 9.



Kuva 9. CIS kontrolliperheet, käyttöönottoryhmät ja suojauskeinot (CIS s.a.i)

CIS (s.a.i) jatkaa mallinsa kuvausta kertomalla, kuinka kontrollit on jaettu kolmeen eri käyttöönottoryhmään (eng. implementation group):

Ryhmä 1 sisältää 56 kappaletta erillisiä suojauskeinoja (eng. safeguards). CIS nimittää ryhmää yksi perusluonteiseksi kyberhygieniaksi (eng. essential cyber hygiene). Ryhmän kontrollien on ajateltu sopivan pienille tai keskisuurille organisaatioille, joilla on vain rajoitetusti resursseja sekä omaa osaamista IT:n ja kyberturvallisuuden osalta. CIS:n mukaan näiden organisaatioiden datan sensitiviteetti on yleensä aika matala ja suurin huoli on yrityksen toiminnan jatkuvuus. Ryhmän kontolleilla voidaan vastata yleisimpiin hyökkäyksiin. (CIS s.a.i.).

Ryhmä 2 sisältää 74 lisäsojauskeinoa, joilla voidaan varautua sensitiivisen asiakas, tai yritysdatan suojaamiseen. Ryhmän kaksi organisaatioissa on erikseen palkattua henkilöstöä IT infrastruktuurin suojaamiseen, joiden erikoisosaamista vaaditaan tarvittavien kontrollit täyttävien teknologioiden ylläpitoon. CIS:n mukaan näiden organisaatioiden lisähuolena on yleensä merkittävä julkisen mainehaitan estäminen. Tämän tyypisiin organisaatioihin saattaa myös kohdistua regulaatiovaatimuksia (CIS s.a.i.).

Ryhmä 3 sisältää 23 lisäsojauskeinoa, joiden avulla voidaan poistaa kohdistettujen hyökkäysten mahdollisuksia sekä pienentää nollapäivähäavoittuvuuksien vaikutuksia. Näiden suojausten käyttöönotto vaatii organisaatiolta monialaisia tietoturvan asiantuntijoita. CIS:n mukaan tämän ryhmän suojauskeinoilla suojataan sellaista organisaation dataa, joka on varmasti sensitiivistä ja siihen kohdistuu regulatoorisia ja vaatimustenmukaisuuden määritystä. Organisaation, joka hyödyntää ryhmän kolme lisäsojauskeinoja täytyy yleensä varmistaa ja osoittaa CIA-periaatteen toteutuminen. CIS:n mukaan organisaatioon kohdistuneet onnistuneet hyökkäykset voivat aiheuttaa merkittävää haittaa julkiselle hyvinvoinnille. (CIS s.a.i.).

Yksittäinen suojauskontrolli sisältää siis CIS:n (s.a.i) mukaan yhden tai useamman suojauskeinon, riippuen valitusta käyttöönottoryhmästä. Jokaisen suojauskontrollin rakenne noudattelee kautta linjan samaa kaavaa. Kontrolli sisältää yleisesittelyn, perusteet kontrollin kriittisyydelle, toimet ja työkalut, sekä kontrollin sisältämien suojaustoimien esittelyn. Toimet ja työkalut sisältävät viittaukset muihin tietoturvakehyksien tarkempiin asiaan liittyviin

ohjeistuksiin. Suojaustoimet esittelevät teknisempiä kuvausia prosesseista ja teknologioista. Yhden kontrollin sisältöä on havainnollistettu kuvassa 10. (CIS s.a.i.).

CONTROL 01 Inventory and Control of Enterprise Assets

SAFEGUARDS TOTAL 5 **IG1 2/5** **IG2 4/5** **IG3 5/5**

OVERVIEW Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

Why is this Control critical? Enterprises cannot defend what they do not know they have. Managed control of all enterprise assets also plays a critical role in security monitoring, incident response, system backup, and recovery. Enterprises should know what data is critical to them, and proper asset management will help identify those enterprise assets that hold or

Procedures and tools This CIS Control requires both technical and procedural actions, united in a process that accounts for, and manages the inventory of, enterprise assets and all associated data throughout its life cycle. It also links to business governance through establishing data/asset owners who are responsible for each component of a business process. Enterprises can use large-scale, comprehensive enterprise products to maintain IT asset inventories. Smaller enterprises can leverage security tools already installed on enterprise assets or used on the network to collect this data. This includes doing a discovery scan of the network with a vulnerability scanner; reviewing anti-malware logs, logs from endpoint security portals, network logs from switches, or authentication logs; and managing the results in a spreadsheet or database.

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	Devices	Identify	●	●	●
Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.						
1.2	Address Unauthorized Assets	Devices	Respond	●	●	●
Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.						
1.3	Utilize an Active Discovery Tool	Devices	Detect	●	●	●
Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.						

Kuva 10. CIS controls, esimerkki kontrollista (CIS s.a.i)

Kontrollin sisältämien suojauskeinojen esittelyssä selvennetään mitä resurssityyppiä (eng. asset type) ja turvallisuuden osa-alueutta (eng. security function) ne koskevat. Suojauskeinojen käyttöönottoryhmien jaottelu on havainnollistettu myös (CIS s.a.i).

1.6 Mitre att&ck ja d3fend

Mitre on voittoa tavoittelematon julkisrahoittein tutkimusorganisaatio, joka operoi useita tutkimuskeskuksia Yhdysvalloissa. Rahoittajina on mm.

Yhdysvaltojen puolustusministeriö ja aiemmin tässä työssä mainittu NIST. Mitren toimiala on laaja, eikä rajoitu pelkästään kyberturvallisuuden kehittämiseen (Mitre s.a.a).

Mitre att&ck on tietoturvakehys, jonka ideologia on lähestyä tietoturvan hallintaa hyökkääjien käyttämien taktiikkoiden, tekniikkoiden ja proseduurien kautta. Mitren kokoama tietoturvakehys kiinnittää erityisesti huomiota hyökkääjien käyttäytymismalleihin (Mitre s.a.a). Tietoturvakehys on jaettu erilaisiin matriiseihin, joilla voidaan tarkentaa kehyksen kohdistumista esim. Windows-käyttöjärjestelmään. Kuvassa 11 on kuvattu Windows matriisin yhtä yksittäistä hyökkäystekniikkaa, proseduuriesimerkkejä, havaitsemiskeinoja sekä korjauskeinoja (Mitre s.a.b).

Home > Techniques > Enterprise > Drive-by Compromise

Drive-by Compromise

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring Application Access

Token.

Procedure Examples

ID	Name	Description
G0138	Andariel	Andariel has used watering hole attacks, often with zero-day exploits, to gain initial access to victims within a specific IP range. ^{[3][4]}
G0073	APT19	APT19 performed a watering hole attack on forbes.com in 2014 to compromise targets. ^[5]

Mitigations

ID	Mitigation	Description
M1048	Application Isolation and Sandboxing	Browser sandboxes can be used to mitigate some of the impact of exploitation, but sandbox escapes may still exist. ^{[58][59]} Other types of virtualization and application microsegmentation may also mitigate the

Detection

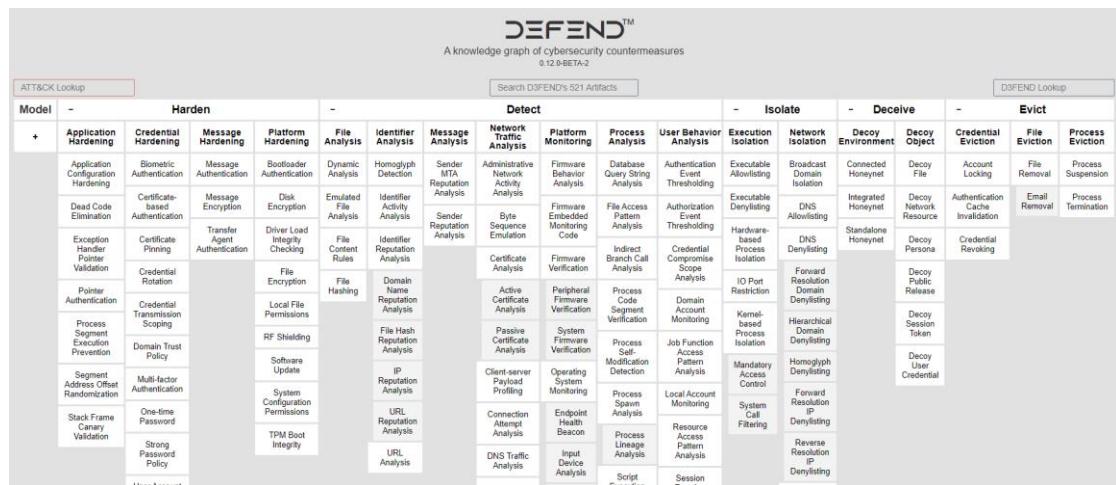
ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Firewalls and proxies can inspect URLs for potentially known-bad domains or parameters. They can also do reputation-based analytics on websites and their requested resources such as how old a domain is, who it's registered to, if it's on a known bad list, or how many other users have connected to it before.
DS0022	File	File Creation	Monitor for newly constructed files written to disk to gain access to a

Kuva 11. Mitre Att&ck kuvaus (MITRE s.a.c)

Jokainen kuvattu taktiikka, teknikka ja proseduuri johtaa lopulta myös hyökkäyksen pienentävään keinoon (eng. mitigation) (Mitre s.a.c).

Mitre d3fend on tietoturvakehys, jonka ideologia on tarjota julkiseen käyttöön tietämystietokanta vastatoimenpiteistä, joilla suojaudutaan hyökkääjien käyttämiltä tekniikoilta. Tietämystietokanta on järjestetty kovenna, tunnista, rajoita, huijaa, ja häädä -kategorioihin (eng. harden, detect, isolate, deceive ja evict).

Kuvassa 12 on esitetty tietämyskannan luokittelumalli ja vastatoimenpidelista (Mitre s.a.d).



Kuva 12. D3fend kehyksen tietämyskannan malli (Mitre s.a.d)

Näissä kategorioissa on puolustustekniikoita, jotka vastaavat aiemmin esitetyihin att&ck-kehyskseen hyökkäystekniikoihin. Jokaisen puolustustekniikan osalta on esitetty referenssi sopivan tietoturvakovenkukseen, ja kuvaus puolustustoiminnosta (Mitre s.a.d).

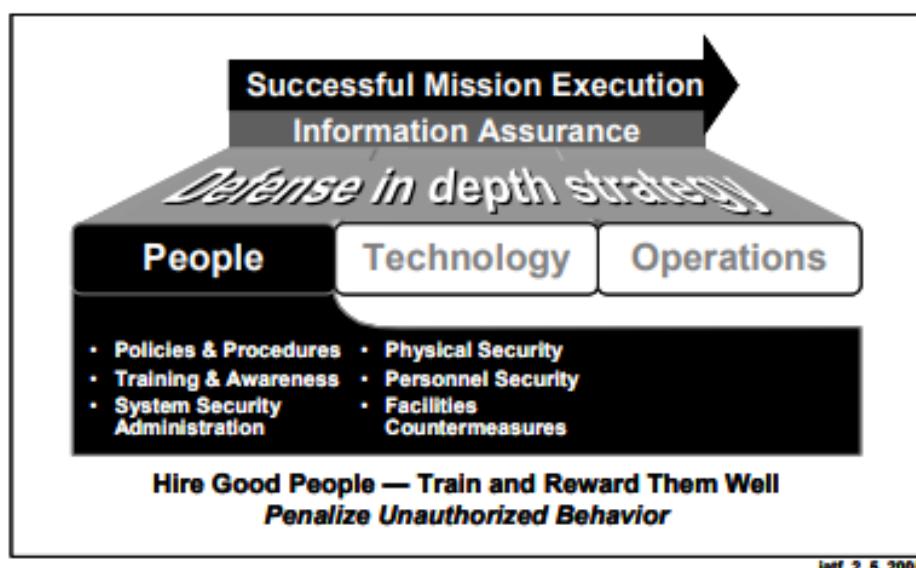
1.7 Defense in depth ja kerroksittainen tietoturva

Yhdysvaltojen NSA-virasto (2002) esitti 2000 luvun taitteessa defense-in-depth-strategian tavaksi hallita tietojärjestelmien tietoturvaa (NSA 2002).

NSA:n mukaan tietoturvallisuus saavutetaan varmistamalla, että tieto ja tietojärjestelmät on suojauduttava kattavasti hyödyntäen hyvin tunnettuja luottamuksellisuuden, eheyden ja saatavuuden (eng. confidentiality, integrity and availability) periaatteita. NIST (1977) mainitsee näiden periaatteiden noudattamisesta jo 1977 luvulla julkaistussa ohjeistuksessaan. NSA esittää näiden cia-periaatteiden päälle pohjautuvan defense-in-depth-strategian vaativan ihmisten, operaatioiden ja teknologian hallinnan kaikilla organisaation infrastruktuurin keroksilla (NSA 2002, luvut ES1, 1, 2).

Defense-in-depth-ihmiset

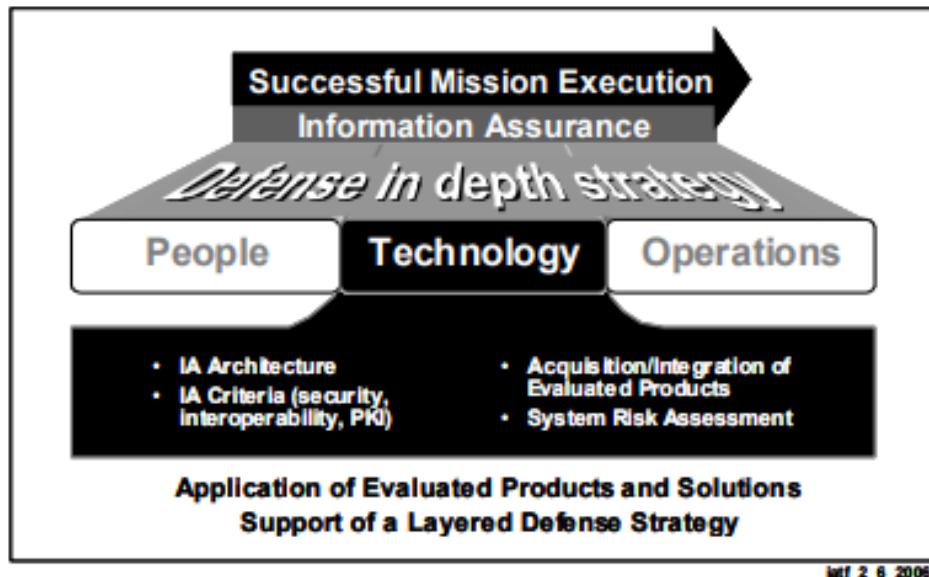
NSA:n mukaan defense-in-depth strategian tietoturvatavoitteiden saavuttamiseksi, täytyy organisaation johdon sitoutua tunnistettujen uhkien torjuntaan. Johto määrittelee poliikit ja käytännöt, joita organisaatio sitoutuu noudattamaan toiminnassaan. Henkilöstö koulutetaan ja henkilökohtaiset vastuut määritellään. Fyysisen- ja henkilöstöturvallisuuden poliikit määritetään ja otetaan käyttöön. Kuvassa 13 listataan muutamia tärkeimpä kategorian mukaisia huomiokohtia. (NSA 2002, luvut ES1, 1, 2).



Kuva 13. Defense-in-Depth, ihmiset (NSA 2002)

Defense-in-depth-teknologia

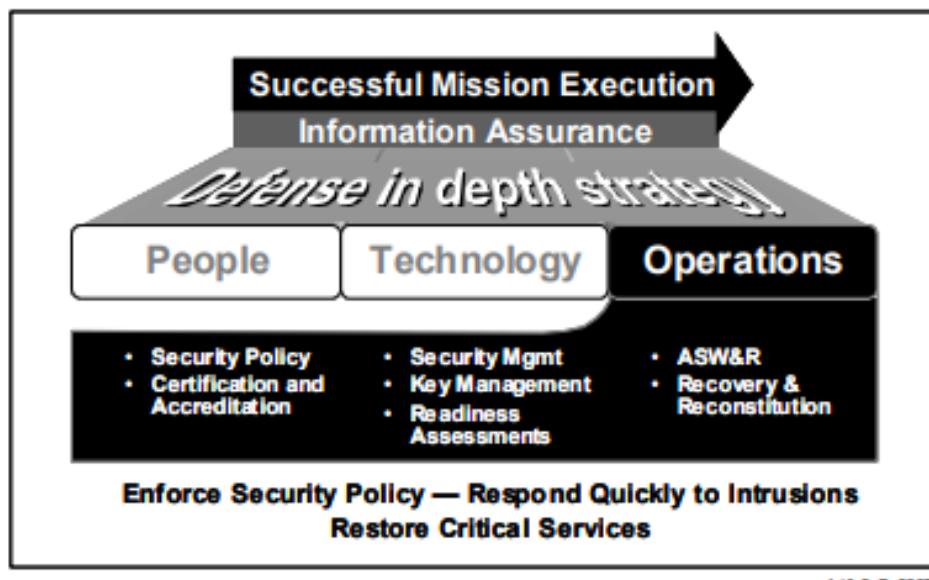
Teknologiakerroksella keskitytään hankittavien teknologoiden varmistamiseen. NSA:n (2002) mukaan organisaation tulee ottaa käyttöön riskipohjainen, poliikkoihin ja prosesseihin pohjautuva tapa hallita teknologian hankintaa ja käyttöönnottoa. Arkkitehtuurivalinnat tulee varmistaa luotettavan kolmannen osapuolen kanssa. Käyttöönnottoprosessit ja järjestelmäintegraatiot pitää arvioida riskipohjaisesti, hyödyntäen standardeja ja tietoturva-arkkitehtuurikuvaauksia. Kuvassa 14 listataan muutamia tärkeimpä kategorian mukaisia huomiokohtia. (NSA 2002, luvut ES1, 1, 2).



Kuva 14. Defense-in-depth, teknologia (NSA 2002)

Defense-in-depth-operaatiot

NSA (2002) kuvaa operaatioiden liittyvän päivittäisen tietoturvan tilan hallintaan. Toisaalta valmiussuunnittelu, palautuminen, turvallisuuspolitiikkojen pakottaminen, havainnointikyky ja reagointi kuuluvat operaatiokerrokselle. Kuvassa 15 listataan muutamia tärkeimpiä kategorian mukaisia huomiokohtia (NSA 2002, luvut ES1, 1, 2).



Kuva 15. Defense-in-depth, operaatiot (NSA 2002)

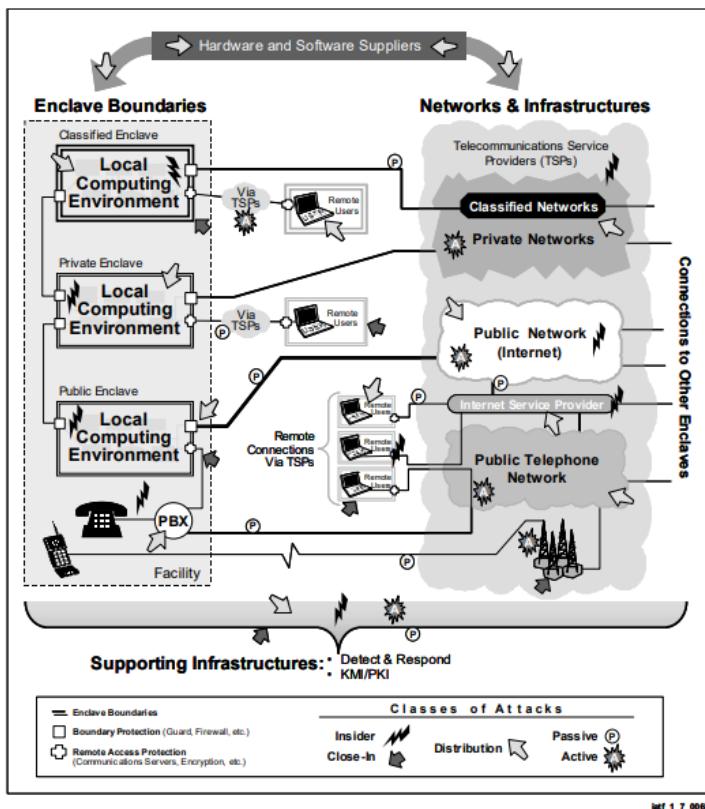
Defense-in-depth-strategia ei keskity NSA:n (2002) mukaan pelkästään suojausmekanismien käyttöönnottoon, vaan myös hyökkäysten ennakoinnin,

havainnointikykyjen ja palautumiskykyjen kuuluvat olennaisesti kokonaisuuteen. Dokumentissaan NSA kuvaa myös kerroksittaisen tietoturvan käsitteen, jonka ideana on, että täydellistä tietoturvaa on mahdotonta rakentaa. Tämän takia tietojärjestelmien tietoturva tulee rakentaa sisältämään sarja toisiaan tukevia tietoturvateknologioita ja kontolleja (NSA 2002, luvut ES1, 1, 2).

Näillä peräkkäisillä kyvykkyyksillä voidaan yhden suojauskuoren pettäessä hidastaa mahdollisen hyökkääjän etenemistä tietojärjestelmissä. Samalla hyökkääjälle asetettujen uniikkien peräkkäisten puolustusmekanismien murtaminen nostaa myös hyökkääjän riskiä paljastua. Hyökkääjää pakotetaan käyttämään aikaa, resursseja sekä rahaa, joka mahdollisesti johtaa hyökkääjän luovuttamiseen. (NSA 2002, luvut ES1, 1, 2).

Information assurance technical framework

Strategian kehittyessä, NSA (2002, luvut ES1, 1, 2) on julkaissut useita versioita tekniseen tietoturvaan keskittynytä information assurance technical framework (IATF) -dokumentistaan. NSA esittelee dokumentissaan tietoturvallisuuden rakennusprosessin (eng. information system security engineering). NSA havainnollistaa rakennusprosessiin kuuluvia neljää teknistä pääosa-alueita ja niiden riippuvuuksia toisiinsa kuvassa 16.



Kuva 16. Defense-in-depth -teknologianäkökulmat (NSA 2002)

NSA:n (2002) mukaan teknologian eri näkökulmat liittyvät osaksi defense-in-depth-strategian muodostumista. NSA:n jaottelu näistä näkökulmista on seuraava:

- **Local Computing Environment**
 - Paikallisen tietojenkäsittely-ympäristön sisäinen suojaaminen. Esimerkiksi palvelimet, työasemat, tulostimet.
- **Enclave Boundaries**
 - Yhdistelmä paikallista tietojenkäsittely-ympäristöä suojaavia loogisia ja fyysisiä ohjelmisto- ja rautapohjaisia suojauskeinoja. Esimerkiksi palomuurit, pääsylistat, fyysiset suojauskeinot.
- **Networks and Infrastructures**
 - Verkot, verkkoteknologiat ja niitä tukevat teknologiat, jotka yhdistävät paikalliset tietojenkäsittely-ympäristöt toisiinsa. Esimerkiksi lan/wan teknologiat, Internet, langattomat verkot, radioverkot sekä verkonhallinta.
- **Supporting Infrastructures**
 - Tietojenkäsittelyä tukevat teknologiat, kuten nimipalvelut, julkisen avaimen infra sekä tietoturvalvonnan järjestelmät.

NSA kuvaaa dokumentissaan hyvin laaja-alaisesti tekniset turvallisuuden vastakeinot, joilla voidaan vähentää tai poistaa hyökkääjien keinoja päästä paikalliseen tietojenkäsittely-ympäristöön käsiksi. Potentiaaliset riskit, eri

hyökkäyskeinot ja kerroksellisen tietoturvan rakentaminen vasten pääosa-alueita on myös kerrottu, viitaten sopiviin teknologioihin. (NSA 2002, luvut 6–8).

Paikallisen tietojenkäsittely-ympäristön suojaamisen NSA jakaa kolmeen osaan: sovellusten turvaaminen, käyttöjärjestelmän turvaaminen ja isäntäpohjaisten havainto- ja suojaustyökalujen käyttö. Käyttöjärjestelmän suojaamisen osalta dokumentissa mainitaan aie keskitetyn, turvallisesti rakennetun käyttöjärjestelmäpohjan osalta. NSA ohjeistaa järjestelmälläpitäjiä käyttämään työkaluja, joilla ensimmäinen määrittely on turvallinen, huolehtimaan että vain tarvittavat palvelut ovat aktiivisena ja käyttöjärjestelmätoimittajan päivitykset ovat ajantasaisia. Lisäksi käyttöjärjestelmämäärittelyiden ja muutosten täytyy vähintään ylläpitää tai mieluummin parantaa tietoturvallista määrityskokoonpanoa. Osana hyvää turvallisuutta suositellaan säännöllisiä määrittelyiden tietoturvatarkastuksia. (NSA 2002, luku 7).

2. KÄYTÄNTÖTASON KEHYKSET JA TIETOTURVAKOVENNUS

NSA:n esittelemän defense-in-depth periaatteen pohjalta on myöhemmin kehitetty useita käytäntötason tietoturvakehyksiä ja standardeja. Nämä käytäntötason kehykset ja standardit menevät vaihelevalla tarkkuudella syvemmälle teknisiin yksityiskohtiin. NIST (2008; 2018; 2020) lähestyy dokumenteissaan käytäntötason tietoturvaan erilaisten suositusten kautta, erityisesti SP 800-123 standardin (2008) kautta, jossa esitellään mm. käyttöjärjestelmäkovennuksen periaatteita. Järjestelmäkovennuksen NIST määrittelee yleisesti järjestelmän hyökkäysrajapinnan pienentämiseksi, paikkaamalla haavoittuvuudet ja sammuttamalla tarpeettomat palvelut (NIST 2015, 82).

Useat muut yksityisen sektorin toimijat mm. redswitches (2023), cimcor (s.a), Cyphere (2021), Intel (s.a) ja beyondtrust (2023) kertovat samoista järjestelmäkovennuksen periaatteista omissa artikkeleissaan, laajentaen niitä omilla näkökulmillaan. Yksityisten toimijoiden artikkeleissa referoidaan useita käytäntötason järjestelmäkovennukseen keskittyviä standardeja, kuten CIS benchmarks, NIST SP 800-53 ja DISA STIGS.

2.1 Järjestelmäkovennuksen näkökulmat

NIST Guide to General Server Security (SP 800-123)

NIST kertoo yleisesti saatavilla olevien käyttöjärjestelmien, kuten Windowsin olevan luonteeltaan yleiskäyttöisiä ja suosittelee käyttöjärjestelmän tietoturvan ja asetusten määrittelyä organisaation vaatimuksia ja tarpeita vastaaviksi. Määrittelyiden toteuttamisen tueksi NIST mainitsee yleisesti saatavilla olevat tietoturvallisuuden kovennuslistat, kuten DISA STIG:n. Käyttöjärjestelmän perustasoinen tietoturvan saavuttamiseksi NIST suosittelee päivitysten ja korjausten asennuksia, käyttöjärjestelmän kovennusta, tietoturvaan tukevien ohjelmistojen asennusta ja käyttöjärjestelmän kovennusten ja määritysten

testaamista. Erityisenä huomiona NIST mainitsee vasta asennettujen järjestelmien suojaamisen päivitysten ja korjausten asennusten aikana. Asennuksen aikaisen suojaukseen NIST suosittelee toteuttamaan esim. tiukasti rajoitetun erillisen asennusverkkoalueen avulla. (NIST 2008, luku 4).

NIST (2008) määrittelee käyttöjärjestelmän kovennuksen tarkemmin kolmeen pääosaan:

1. Poista tarpeettomat palvelut, sovellukset ja protokollat.

NIST korostaa palveluiden, sovellusten ja protokollien poistoa niiden päältä laiton sijasta. NIST:n mukaan jokainen käyttöjärjestelmän osa lisää hyökkäysrajapintaa sekä mahdollistaa ihmillisistä tai teknisten virheiden kautta tapahtuvat haavoittuvuudet. Käyttöjärjestelmän kovennuksen tulisi tähdätä mahdollisimman tarkkaan rajatun tarpeen mukaan määritellyn konfiguraation rakentamiseen. Jos mahdollista, käyttöjärjestelmä tulisi asentaa minimimääriyksillä, jonka jälkeen siihen asennetaan vain tarvittavat palvelut ja sovellukset. NIST suosittelee esim. tulostus- ja tiedostonjakopalveluiden, etäkäyttöominaisuuksien, etähallinnan, järjestelmän kehitystyökalujen ja hakemistopalveluiden poistoa, jollei niille ole tarvetta. Poistamalla tarpeettomia osia vähennetään myös käyttöjärjestelmän tietoturvalkitapahtumia, joka helpottaa tietoturvavalvonnan toteuttamista. (NIST 2008, luku 4.2.1).

2. Määrittele käyttäjääutentikointi

NIST:n mukaan yleisesti tunnetut oletustunnukset ja ei-interaktiiviset tunnuksit tulee joko poistaa tai laittaa pois päältä. Vain oleelliset paikalliset tunnukset luodaan ja kohdejärjestelmän käyttö sallitaan niille. Järjestelmän ylläpitäjien pääsyä ja määrää rajataan pienelle joukolle. Organisaation salasana politiikka tulisi olla määritelty ja kaikki kirjautumistapahtumat pitää lokittaa. NIST suosittelee tunnus/salasanaparien käyttöä vain suojaatujen tiedonsiirtomekanismien, kuten SSL tai IPsec kautta, jotta hyökkääjän on vaikeampi saada tunnuksia ja salasanoja haltuunsa (NIST 2008, luku 4.2.2).

3. Määrittele resurssikontrollit

NIST:n mukaan käyttöoikeuksien avulla voidaan rajoittaa tiedostojen, hakemistojen, laitteiden ja muiden laiteresurssien käyttöä. NIST suosittelee minimaalisten oikeuksien käyttöä sekä käyttäjien että ylläpitäjien oikeuksien osalta. Käyttäjien oikeudet suorittaa järjestelmäkäskyjä tai työkaluja tulee estää mahdollisuksien mukaan. Käyttöjärjestelmän omilla työkaluilla voidaan joskus myös luoda ns. kupla (eng. sandbox) joka sisältää virtualisoidun ympäristön, josta käsin ei ole oikeusia käsitellä suoraan käyttöjärjestelmää tai sen tiedostojärjestelmää (NIST 2008, luku 4.2.3).

Redswitches:n näkökulma

Redswitches:n (2023) mukaan järjestelmäkovennus tarkoittaa kyberuhkien minimointia tai poistoa, hyödyntäen standardeihin pohjautuvia proaktiivisia keinoja. Järjestelmäkovennus vahvistaa ja täydentää muita kyberturvallisuuden toimintoja ja johtaa kerroksittaisen tietoturvaan. Samalla kovennus on oleellinen osa hallittavaa kyberturvallisuuden puolustusta. Redswitches esittää järjestelmäkovennuksen jaon *palvelin, ohjelmisto, käyttöjärjestelmä, tietokanta ja verkko*-kategorioihin ja painottaa sen olevan jatkuva, koko infrastruktuuriin kohdistuva prosessi. Redswitches esittelee artikkelissaan tyyppillisen infrastruktuurin turvaamisen prosessin, jossa on kuusi vaihetta:

1. Arviointi ja riskianalyysi

Haavoittuvuus-skannauksia, penetraatiotestausta ja tietoturva-auditointia hyödynnetään ymmärtämään nykyinen tietoturvan tila, ja potentiaaliset uhkat infrastruktuurille.

2. Suunnittelu ja poliikan kehittämисvaihe

IT-tiimit kehittävät standardeihin pohjautuvan suunnitelman ja kehyksen turvallisuusparannuksien asettamiseksi

3. Konfiguraation ja päivitystenhallinta

Tässä vaiheessa implementoidaan suunnitelman mukaan parannukset ja siirrytään ylläpitovaiheeseen

4. Pääsynhallinnan vaihe

Vähimmän käyttöoikeuden periaatteen (eng. least privilege) ylläpito ja vahvan autentikoinnin varmistaminen

5. Verkon turvallisuus

Verkkotasoisten kontrollien asettaminen sekä lähtökohtaisesti vain tarvittavien pääsyjen salliminen

6. Monitorointi ja jatkuva parannus

Lokienhallintajärjestelmän hyödyntäminen monitorointiin, ja turvallisuuspoikkeamien tunnistaminen ja nopean reagointikyvyn mahdollistaminen. Järjestelmäkovenkuksen politiikkaa ylläpidetään ja uusien uhkien muodostamia muutostarpeita otetaan huomioon sekä monitoroinnin että ylläpidon toimesta. (Redswitches 2023).

CIMCOR:n näkökulma

Cimcor (2023) kertoo järjestelmien olevan oletuksena turvattomia, ja käytöönnotettaessa päivittämättömiä. Järjestelmäkovenkus pienentää järjestelmän haavoittuvuutta kyberuhkille, kun se toteutetaan parhaita käytäntöjä noudattaen. Cimcor mainitsee kaikkien isojoen vaatimustenmukaisuuden kehysten, kuten PCI-DSS, HIPAA ja FedRAMP vaativan erikseen järjestelmien koventamista, hyödyntäen tunnettuja järjestelmäkovenkuksen standardeja. Cimcorin mukaan useimpien organisaatioiden kannattaa ohittaa NIST:n system hardening checklist (SP 800-70), koska se on tyypiltään enemmän suosituksellinen standardi.

Cimcor suosittaakin tekemään valinnan CIS benchmarksin ja DISA STIG:n välillä. Erityisenä huomiona CIS:n ja STIG:n eroista Cimcor kertoo CIS:n olevan laajasti hyväksytty ja kehitetty julkisen sektorin, teollisuuden, akateemisten instituutioiden sekä yksityisen sektorin käyttöön. Cimcor:n mukaan CIS benchmarks on myös kehitetty vastaamaan useiden yleisten tietoturvakehysten kuten ISO 27001 ja NIST CSF vaatimuksia. DISA STIG on kehitetty vastaamaan erityisesti Yhdysvaltojen virastojen tarpeita ja pohjautuvan vain NIST:n tietoturvakehyksiin. (Cimcor 2023).

Cimcor suosittelee järjestelmäkovenkuksen toteuttamiseen perustason selvittämistä (eng. baseline) joko manuaalisesti tai automaatiota hyödyntäen,

jonka jälkeen ko. perustasoa auditoidaan poikkeuksien tunnistamiseksi. Cimcor tuo omassa artikkelissaan esille erityisesti muutoshallinnan roolin järjestelmäkovenkuksessa. Organisaatiolla tulee olla tapa tunnistaa mitä infrastruktuurissa on muuttunut, tarkistaa onko muutos ollut hallittu/sallittu organisaation valitsemassa tietoturvan perustasossa, sallia/estää/peruuttaa muutos ja ylläpitää perustasoa tehdyllä muutoksilla (Cimcor 2023).

Cyphere:n näkökulma

Cyphere (s.a) kertoo järjestelmäkovennuksen vaativan kriittistä analysointia ja määrämuotoista lähestymistä, jotta kaikki tietyn järjestelmän haavoittuvuudet ja väärät määrittelyt voidaan tunnistaa ja poistaa. Myös Cyphere suosittelee järjestelmäkovenkuksen standardin noudattamista. Artikkelissa mainitaan järjestelmäkovenkuksen yhtenä etuna järjestelmän paremman suorituskyvyn ja vähäisemmän ylläpidon tarpeen. Esimerkinä artikkelissa kerrotaan palvelinkovenkuksen eri osa-alueista, joissa erityishuomiona on fyysisen turvallisuuden huomiointi kovenkuksissa. Cyphere korostaa erityisesti tarkistuslistojen lisäksi tehtäviä kovenkuksia, kuten antivirus- ja tunkeutumisenestoohjelmistojen (eng. antimalware and intrusion detection) asennuksia. (Cyphere s.a).

Intel:n näkökulma

Järjestelmäkovenne (eng. system hardening) on laaja metodologia, joka Intelin (s.a) mukaan on suositeltavaa ottaa käyttöön kerroksittaisen, koko it-ympäristön kattavan strategian avulla. Hyvä kovennestrategia ottaa huomioon sekä ohjelmistot, käyttöjärjestelmät että laitteistot. Muutamia järjestelmäkovenkuksen perusasioita, joista on helppo lähteä liikkeelle, ovat:

- it-järjestelmien inventointi (näkyvyys)
- käyttöoikeuksien auditointi (sekä käyttäjien että laitteiden)
- käyttöjärjestelmän ja laitteiston tietoturvan kovenustavan valinta
- haavoittuvuuskorjausten ja ohjelmistopäivitysten automatisointi
- käyttäjien tietoturvakoulutus
- tietoturvakovenkuksen tarkistuslistat.

Järjestelmäkovenkuksen avulla tunnistetaan ja kohdistetaan tietoturvan kehittämistoimia (esim. hyökkäysrajapinnan pienentäminen). Järjestelmäkovenkuksen pääasiallinen tavoite on estää mahdollista

hyökkääjää saamaan järjestelmää haltuunsa, varastamaan järjestelmästä dataa, tai estää hyökkääjää etenemästä muihin yrityksen järjestelmiin. (Intel s.a.).

Beyondtrust:n näkökulma

Beyondtrust (s.a) jakaa järjestelmäkovenusten hyötyjä artikkelissaan järjestelmien parempaan toimivuuteen, parempaan tietoturvaan sekä vaatimuksenmukaisuuden ja auditoitavuuden helpompaan toteuttamiseen. Järjestelmällisen lähestymisen tapaa suositellaan sekä auditoinnin, tunnistamisen sekä tietoturvakkontrollien asettamisen kanssa (Beyondtrust s.a.).

Beyondtrustin mukaan erityinen painoarvo tulee olla järjestelmäkovenusten toteuttamisessa koko teknologian elinkaaren ajan. Teknologian elinkaari voidaan jakaa seuraaviin vaiheisiin:

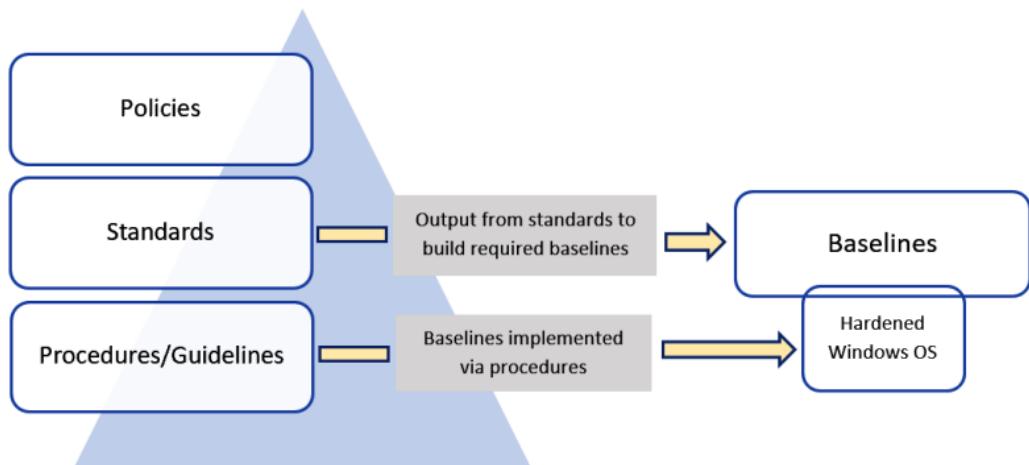
- Asennus ja määrittelyt
- Ylläpito ja tuki
- Elinkaaren päättyminen (eng. end of life)

Beyondtrust mainitsee myös tietoturvakehysten käytön ja vaatimustenmukaisuuden täyttämisen yleistyneen yhtenä ehtona kyberturvavakuutuksissa. (Beyondtrust s.a).

Ammattikirjallisuuden näkökulma

Dunkerley ja Tumbarello (2022) lähestyvät Windows-työaseman kovenusta nykyaikaisen zero-trust ideologian kautta. Kirjailijat lähestyvät työasemakovenusta hyökkääjien käyttämien keinojen kautta, tavoitteena löytää tapa suojata työasemaa. Kirjailijat suosittelevat vertailemaan käyttöjärjestelmän oletusarvoihin tehtyjen muutosten vaikutuksia kokonaistietoturvaan. Huomionarvoista on, että kirjailijat suosittelevat tietoturvakovenusten rakentamista vasta siinä vaiheessa, kun organisaatio on ensin rakentanut prosessinsa kuntoon. Yleensä työasemakovenusten teko aloitetaan joka tapauksessa jonkinlaisen peruspohjan (eng. baseline) rakentamisella. (Dunkerley & Tumbarello 2022, 23–26, 33–35).

Kuvassa 17 on esitetty malli, missä vaiheessa ja miten Windowsin tietoturvan kovennus aloitetaan. Organisaatiota suositellaan rakentamaan hallintamalli sekä valitsemaan oikeat standardit, ja tietoturvakehykset, joita vasten lähtää rakentamaan tietoturvan perusmalleja (Dunkerley & Tumbarello 2022).



Kuva 17. Politiikka, standardit, proseduurit (Dunkerley & Tumbarello 2022)

Muutoshallinnan osuus mainitaan oleellisena osana tietoturvakovennusten rakentamista. Kyseessä on kirjailijoiden mukaan jatkuva prosessi, joka vaatii hallittavan rakenteen, muutoin yksittäiset muutokset jäävät huomaamatta, ja perusta hapannee (Dunkerley & Tumbarello 2022).

2.2 CIS Benchmarks

CIS:n (s.a.h) mukaan kontrollien ja määrityskokoonpanojen (eng. Controls, benchmarks) ero on siinä, että kontrollit ovat yleisiä suositteltuja käytäntöjä järjestelmien ja laitteistojen suojaamiseen, kun taas määrityskokoonpanot ovat tarkempia ohjeistuksia esim. tiettyjen käyttöjärjestelmien ja ohjelmistojen koventamiseen. CIS painottaa kontrollien suosituksia turvallisten määritysten toteuttamisesta. CIS:n mukaan esimerkiksi Windows kokoonpanodokumentin suositukset vastaavat CIS controls safeguards ja implementation group luokitteluun (s.a.f).

CIS (s.a.d) kertoo sivuillaan määrityskokoonpanojensa (eng. benchmarks) kattavan 25 eri toimittajan tuoteperheet. Tuoteperheet on sivuilla jaettu kahdeksaan eri kategoriaan, esim. verkkolaitteet, käyttöjärjestelmät ja mobiililaitteet. CIS on jakanut esimerkiksi Windowsin kokoonpanot

käyttöjärjestelmäversioittain, mutta Windows10 versiosta lähtien valittavissa on kaksi eri versiota kokoonpanosta: organisaatiotaso ja yksittäinen laite (eng. enterprise ja stand-alone). CIS kertoo jokaisen kokoonpanodokumentin prosessiin kuuluvan yhteisön vertaisarvion. Tämä prosessi on jaettu kahteen osaan: kehitysvaiheeseen ja palautevaiheeseen. Kehitysvaiheessa kokoonpanoa kokoontuu tekemään monenlaisista eri taustoista koostuva ryhmä, joka koostaa, testaa ja keskustelee tekeillä olevasta kokoonpanosta. Tätä vaihetta jatketaan niin kauan, kunnes ryhmä saavuttaa yhteisen konsensuksen kokoonpanosta ja se julkaistaan. Toisessa vaiheessa internet-yhteisöltä saadun palautteen perusteella konsensuksen saavuttanut ryhmä arvioi muutospyynnöt ja ottaa ne mahdollisesti huomioon suosituksissa. (CIS s.a.d.).

Enterprise kokoonpanodokumentissa CIS (s.a.d) kertoo dokumentin kattavan vain Active Directoryn liitetyt laitteet, ja käyttöönnoton vaativan ryhmäkäytäntöjen hyödyntämistä. CIS myös suosittelee määritysten lisäksi käyttöönottamaan toimivan käyttöjärjestelmän tietoturvapäivitysprosessin, sekä sovellusten ja kirjastojen haavoittuvuushallinnan. **Stand-Alone**-kokoonpanodokumentin mukaiset suositukset vaativat CIS:n mukaan paikallisen ryhmäkäytäntötyökalun tai Microsoft local group policy object toolin käyttöä (CIS s.a.d.).

CIS:n kokoonpanodokumentti (s.a.d) kuvailee myös profiileja, jotka on jaettu kahteen eri tasoon sekä niitä tukeviin alakategorioihin. Alakategoriat tuovat lisää tietoturvaa koventavia Windowsin ominaisuuksia, kuten Bitlocker-levynkryptaus. **Enterprise/Corporate** -profiili on tarkoitettu yleiskäyttöiseksi yritysympäristön profiiliksi, jossa on riittävä perustasoiset suojauskset, jotka eivät kuitenkaan estä teknologian hyödyntämistä liian tiukkojen tietoturvamääritysten myötä. **High security/sensitive data** on tiukemmin rajattu profiili, jossa esim. etäkäyttö ja sovellusten hyödyntämistä on selvästi rajoitettu niin, että tietoturvakovenukset voivat vaikuttaa sovellusten käytettävyyteen (CIS s.a.d.).

Jokainen yksittäinen suositus noudattaa samaa CIS:n kehittämää standardia tapaa kuvata sen taustat ja merkityksellisyys. Yksittäisten suosituksien

kuvaukseen on liitetty myös aiemmin määritetty profiili, jolla voidaan paremmin kohdistaa suojauskset tiettyä profiilia vasten. Kuvassa 18 on esitetty esimerkki yhdestä suojauskontrollista, joka kattaa profiilin, kuvauksen, taustoituksen, merkityksellisyyden, auditointiohjeistuksen, määrittelyohjeen, oletusasetuksen ja viittauksen sopiviin artikkeleihin sekä aiemmin mainittuihin CIS kontolleihin ja käyttöönottotasoihin (CIS s.a.d).

1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value for stand-alone systems is 0 passwords, but the default setting when joined to a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password.

Rationale:

The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced.

Impact:

The major impact of this configuration is that users must create a new password every time they are required to change their old one. If users are required to change their passwords to new unique values, there is an increased risk of users who write their passwords somewhere so that they do not forget them. Another risk is that users may create passwords that change incrementally (for example, password01, password02,

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to 24 or more password(s):

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history
```

Default Value:

24 passwords remembered on domain members. 0 passwords remembered on stand-alone workstations.

References:

1. <https://www.cisecurity.org/white-papers/cis-password-policy-guide/>
2. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

Kuva 18. Mukailleen CIS benchmarks. Esimerkki Windows10 Enterprise kovennuksista (CIS s.a.d)

2.3 DISA STIG

Titanian (s.a) mukaan DISA (eng. defense information systems agency) on osa Yhdysvaltojen puolustusvirastoa (eng. department of defense). DISA on virasto, jonka vastuulla on ylläpitää ja suojata puolustusviraston alaisia IT palveluja sekä verkkoa. **STIG** (eng. security technical information guide) on DISAN kehittämä tietoturvaan keskittyvä teknisen käytöönnoton standardi, jonka noudattaminen on osa puolustusviraston alaisten virastojen vaatimustenmukaisuutta (Titania s.a).

Titanian mukaan DISA on kehittänyt satoja erilaisia mallipohjia (eng. benchmark), joiden avulla voidaan merkittävästi koventaa tuotteiden perustasoisia tietoturvamääritelyksiä. Mallipohjat kattavat IT-alan toimittajien laitteistoja, käyttöjärjestelmiä, sovelluksia ja jopa pilvipalveluita. Titania kertoo, että minkään tuotteen käyttöä ei hyväksytä puolustusviraston alaisissa tietoverkoissa, ilman että sille on olemassa valmis STIG (Titania s.a).

Titanian mukaan useita erityyppisiä STIG mallipohjia yhdistämällä voidaan kattaa koko systeemin arkkitehtuuri, ml. verkkoelementit. Yhdistely saattaa vaatia mallipohjien päällekkäisyyttä, jotta kaikki elementit tukevat toisiaan. Mallipohjat suunnitellaan DISA:n toimesta aina tiettyä laite-, ohjelmisto- tai käyttöjärjestelmäversiota varten. Titania huomauttaakin tämän vaativan tarkkuutta versioiden välisen muutosten käytöönnotoissa (Titania s.a).

DISA julkaisee uudet ja päivitettyt STIG mallipohjat neljännesvuosittain. Joskus myös nopeammin, jos uudet tunnistetut uhkat tai ongelmat edellyttävät sitä. Titania kertoo mallipohjien julkaisuun liittyvän myös elinkaarenhallinta, jossa vanhemmat tuotteiden mallipohjat siirretään ns. auringonlaskun tilaan. Tämä tarkoittaa sitä, että tuotteesta on tullut uudempi versio ja vanhaa mallipohjaa ei enää ylläpidetä. Mallipohja jää kuitenkin edelleen saataville yhteensopivuuden varmistamiseksi. Yleensä DISA kehittää mallipohjat itse, mutta usein myös ohjelmisto tai laitevalmistajien kanssa yhteistyössä. Pohjen kehityksen lähtökohtana on puolustusviraston kyberturvallisuuden vaatimukset, jonka takia mallipohjat keskittyvät olemaan korkealla tietoturvan tasolla. Titanian mukaan tällä voi olla vaikutuksia sovellusten toiminnallisuuksiin ja siksi

toimittajan osallistaminen pohjen kehitykseen johtaakin parempaan turvallisuuden ja toiminnallisuksien tasapainoon. (Titania s.a).

DISA on jakanut mallipohjat kolmeen kategoriaan tai vaatimusluokkaan (eng. compliance levels). Vakavimmat tietoturvariskit tai

konfiguraatiohaavoittuvuudet määritellään kuuluvan **kategoriaan 1** ja Titanian mukaan niiden korjaamattomuus voi aiheuttaa välittömän ja suoran cia-periaatteen rikkoutumisen, luvattoman pääsyn dataan tai pääsyneston.

Kategoria 2 on hieman lievämpi kategoria, jonka sisältämät konfiguraatiohaavoittuvuudet voivat johtaa kategoria 1:sen tasolle ja vaarantaa sen hetkisen operatiivisen tehtävän sekä cia-periaatteen.

Kategoria 3 on matalin taso, jonka sisältämien kontrollien puuttuminen vaikeuttaa cia-periaatetta, ja voi johtaa kategoria 2:sen tasoiseen konfiguraatiohaavoittuvuuteen. Tällä tasolla tapahtuvat haavoittuvuudet voivat hidastaa katkoksista toipumista ja vaikuttaa datan ja informaation ajantasaisuuteen. (Titania s.a).

Jokaisen kategorian sisällä on lisäjaottelu DoD:n (department of defense) määrittelemiin luottamustasoihin: salainen, arkuunteinen ja julkinen (eng. confidentiality levels, classified, sensitive, public). DoD:n mukaan luottamustasoilla määritellään järjestelmän vaatima yleinen henkilöstöturvallisuuden taso, sekä pääsyluvat. Tarkemmin kuvattuna on kerrottu myös järjestelmän tiedonkäsittelyn hyväksyttävät käytötavat, kuten pääsy järjestelmään langattoman verkon kautta (Department of Defense 2004).

DISA (2023) kertoo STIG:ien seuraavan Microsoftin nykyistä WaaS-mallia (Windows as a service). Käytännössä STIG:ejä päivitetään ja niihin saattaa tulla muutoksia samaan tahtiin, kuin Microsoft tuo uusia ominaisuuuspäivityksiä Windowsin päivityspakettien avulla. DISA:n mukaan tämä muuttaa myös STIG:ejä käyttävien organisaatioiden tapaa toimia: käyttöjärjestelmäversioiden pitää olla uusimmilla tasolla, jos STIG:eistä haluaa täyden hyödyn. Jokainen STIG sisältää määritysten lisäksi laitteisto- ja käyttöjärjestelmävaatimukset. STIG:ejä hyödyntävien organisaatioiden on tämän takia oltava käyttöönottojen

kanssa valmiita tarkastamaan nämä mahdollisesti muuttuvat määritykset. Jokainen Windows STIG-paketti sisältää mukautetut ryhmäkäytäntöpohjat, joiden avulla käyttöönotto voidaan toteuttaa. (DISA 2023).

DISA tekee myös yhteistyötä NIST:n kanssa, ja on mukauttanut osan omista STIG:eistään (pääasiassa yleisimmät käyttöjärjestelmät) vastaamaan NIST:n kehittämää security content automation protocol (SCAP) standardia (DISA 2023; NIST 2023). SCAP on NIST:n (2023) mukaan yhteisöpohjalta kehitetty turvallisuuskontrollien automaatiostandardi. Standardi sisältää kuvauskielen, jota NIST toivoo eri toimittajien noudattavan tietoturvatuotteissaan. Tämä tavoite on yhteisöpohjainen ja pyrkii erilaisten työkalujen ja kehysten tietoturvakovenusten pohjadatan standardiin hyödyntämiseen tuotteiden välillä (NIST 2023).

2.4 Windows security ja security baselines

Microsoft (2023a) kertoo Windows-tietoturvan perusteita esittelevässä artikkelissaan organisaatioiden ympäri maailmaa siirtyvän nollaluottamusmallin (eng. zero trust) käyttöön. Nollaluottamusmallin hyödyntäminen Windows-tietoturvassa vähentää Microsoftin mukaan riskejä, koska käyttäjät ja laitteet varmennetaan jokaisen pääsyypisteen osalta erikseen ilman poikkeuksia. Näin toimien voidaan pääsy antaa vain tarvittaviin resursseihin, sopivaksi ajaksi. Microsoftin mukaan nollaluottamusmalli on oleellinen osa Windows 11 laitteiden tietoturvaa. Microsoftin mukaan he toteuttavat nollaluottamusmallia jo laitteistotasolta lähtien suunnittelemassa tietoturvan yhteistyössä piirivalmistajien kanssa. (Microsoft 2023a).

Microsoft (2023a) jakaa Windows-tietoturvan eri kerroksiin kuten turvallinen ohjelmistokehitys, laitteistotaso, käyttöjärjestelmätila, sovellustaso, identiteettitaso ja pilvitason tietoturva (eng. security foundations, hardware security, operating system security, application security, identity protection, cloud protection). Microsoft nimittää näitä osa-alueita ja niiden sisällä olevia ominaisuuksia kuten palomuuria, virustorjuntaa, selaintason suojaus ja hyökkäysrajapinnan suojausmekanismia "Windows security" -kokonaisuudeksi (Microsoft 2023a).

Microsoftin (2023b) mukaan Windows on turvallinen suoraan käyttöönnotettaessa, mutta koska monet organisaatiot haluavat tarkempaa kontrollia käyttöjärjestelmän turvallisuusomaisuuksiin, he tarjoavat asiakkaidensa käytöön valmiita turvallisuuspohjia (eng. security baselines). Microsoftin mukaan Windows 10 sisältää yli 3000 ryhmäkäytäntöasetusta, joista vain osa on tietoturvaan liittyviä. Turvallisuuspohjat ovatkin hyödyllisiä organisaatioille, jotka panostavat tietoturvan hallintaan vähentäen asiakkaiden työtaakkaa asetusten läpikäynnissä. Microsoft kertoo koostavansa pohjet itse, asiakkailta ja kumppaneilta tulleen palautteen avulla. Pohjet sisältävät Microsoftin suosittelemia määrittyksiä, joissa myös selitetään niiden käyttöönnoton vaikutukset. (Microsoft 2023b).

Microsoft (2023b) mainitsee turvallisuuspohjien käyttöönottotavaksi ryhmäkäytännöt (eng. group policy), Microsoft Configuration Managerin tai Microsoft Intunen. Microsoftin julkaisema **Security compliance toolkit** sisältää turvallisuuspohjien lisäksi useita työkaluja, joiden avulla ylläpitäjät voivat ladata, analysoida, testata ja hyödyntää Microsoftin turvallisuuspohjia. **Policy Analyzer** -työkalun avulla ylläpito voi verrata nykyisiä ryhmäkäytäntöjä turvallisuuspohjiin ja löytää esim. päällekkäisyyksiä tai puutteita. **Local Group Policy Object** työkalua voi hyödyntää silloin, kun halutaan mallintaa, varmistaa ja tuoda paikallisia ryhmäkäytäntöpohjia koneille. (Microsoft 2023b, 2023c).

Security baselines Intunen avulla

Microsoft (2023d) kertoo että intune-hallintaan liitettyihin Windows 10/11 laitteisiin ja käyttäjiin voidaan kohdistaa turvallisuuspohjia (eng. security baselines). Nämä turvallisuuspohjat ovat samoja kuin ryhmäkäytännöillä jaellut turvallisuuspohjat, lukuunottamatta paikallisiin toimialueen ohjauskoneisiin liittyviä asetuksia. Microsoftin mukaan Intunen avulla tehtävä turvallisuusmääritysten jakelu ja hallinta mahdollistaa määritysten tilan ja tietoturvaturvaryhdin (eng. security posture) seurannan, hallinnan ja raportoinnin. Intune mahdollistaa myös yksittäisten tietoturva-asetusten seurantaa laitekohtaisesti, joka helpottaa esim. vianselvitystä (Microsoft 2023d, 2023e).

2.5 Microsoft SecCon

Microsoft (2019a) kertoo artikkelissaan julkaisevansa jokaisen uuden Windows version ohessa tietoturvan kovennukseen sopivan peruspohjan (eng. Windows security baseline). Microsoftin mukaan tämä tietoturvan peruspohja on kuitenkin tunnistettu ongelmalliseksi monissa organisaatioissa, koska tietoturvapolitiikkojen asettaminen toiminnallisuuksien kanssa yhteen on vaikeaa ja peruspohjan vaatimukset ovat joissain tapauksissa liian vaativia. Microsoft on lähtenyt kehittämään uutta tietoturvakehystä helpottamaan yksittäisten päätelaitekovennustehävien priorisoinnin (Microsoft 2019a).

Microsoftin (2019a) mukaan tämän takia kehyksessä ei ole yksityiskohtaista listaaa tietoturvakontrolleja, vaan ne on ryhmitelty erityyppisiin ja -tasoihin tietoturvakooponpanoihin. Mitä suurempi kokoonpanon luku, sitä tiukempi tietoturvakonfiguraatio laitteella on. Microsoft mainitsee tärkeäksi myös näkyvyyden ja vertailukyvyn muiden organisaatioiden vastaaviin konfiguraatioihin. Tähän vertailukykyyn mainitaan secure score toiminnallisuden (osa Microsoft Defender ATP-tuotetta) kyky tuottaa kvantitatiivisesti mitattavia raportteja ja näkymiä organisaation päätelaitetietoturvan tasosta, verrattuna suosituksiin (Microsoft 2019b).

SecConin turvatasoja on viisi kappaletta, joista kolme alinta on ryhmitelty "tuottavuuslaitteiden" (eng. productivity devices) kategorian alle. Kaksi ylimpää tasoa on ryhmitelty "korkean käyttöoikeuden työasemiksi" (eng. privileged access workstations). Kuvassa 19 havainnollistetaan näitä ryhmittelyjä ja tasuja.



Kuva 19. SecCon ryhmät ja päätelaitteiden ryhmittely (Microsoft 2019b)

Tasoa 1, nimeltään yrystason perus tietoturva (eng. enterprise basic security), Microsoft suosittelee minimitasoksi kaikille yrystason laitteille. Tavoitteena tämän tason käyttöönnotolle on 30 päivää.

Tasoa 2, nimeltään yrystason parannettu tietoturva (eng. enterprise enhanced security), Microsoft suosittelee luottamuksellisen tai sensitiivisen tiedon käsittelyyn. Tavoitteena tämän tason käyttöönnotolle on 90 päivää.

Tasoa 3, nimeltään yrystason korkea tietoturva (eng. enterprise high security), Microsoft suosittelee organisaatioille, joilla on riittävästi resursoitu ja osaava tietoturvatiimi. Tämän typpistä tasoa voidaan käyttää esim. pörssiyrityksissä tai organisaatioissa, joissa datan varkaudella olisi merkittäviä vaikutuksia joko mainehaittana tai jopa organisaation rikosvastuuun osalta. Tämän tason saavuttaminen vie Microsoftin mukaan vähintään 90 päivää, ja yleensä enemmän.

Tasoa 4, nimeltään erikoistyöasema (eng. specialized workstation), Microsoft suosittelee kehittäjille tai testaajille, esim. DevOps-käytössä. Erityisesti pääsy liiketoimintakriittiin järjestelmiin ja dataan määritää erityissuojattavan työaseman tason.

Tasoa 5, nimeltään ylläpitäjän työasema (eng. administrator workstation), on selkeästi korkeimmilla pääsyoikeuksilla varustetun ylläpitäjän erityinen työasema. Tällä tasolla on kaikkein isoin riski datan ja palveluiden tietoturvan suhteen. (Microsoft 2019b).

Microsoftin (2019b) kokoamat tasot on jaoteltu neljään eri määritykseen: laitteisto, politiikat, kontrollit ja käyttäytyminen (eng. hardware, policies, controls, behaviours). Alemman tason määritykset sisältyvät ylempien tasoihin.

- Laitteistotasolla otetaan kantaa tason vaatimiin laitteiston tietoturvatoiminnallisuksiin, kuten TPM moduuliin tai UEFI secure boot toimintoon.
- Politiikkatasolla suositellaan yksittäisiä käyttöjärjestelmän tietoturvakovennuksia, kuten salasanojen monimutkaisuus, tai käyttöjärjestelmän käyttämät autentikointiprotokollat.

- Kontrollitaso keskittyy käyttöjärjestelmään kuuluiin, tai sen päällä oleviin turvakyvykkyyksiin ja niiden käyttöönnottoon. Esimerkiksi Windows defender credential guard ominaisuus suositellaan ottamaan käyttöön.
- Käytäytymistolasolla ohjeistus keskittyy organisaation tapaan toimia, ja kehittää työasematurvallisuutta. Esimerkiksi paikallisten järjestelmänvalvojaoikeuksien poisto tai ylläpidon pysyvien oikeuksien tarkennukset.

Microsoft suosittelee tasojen mukaisten kontrollien käyttöönnottoa vaiheistetusti, jotta esim. mahdolliset yhteensopivusongelmat saadaan selville.

Microsoftin mukaan tämä tietoturvakehys on vielä kehityksen alla ja tavoitteena on parantaa ja tarkentaa kehystä asiakkailta, toimittajilta sekä kumppaneilta saadun palautteen pohjalta. (Microsoft 2019b).

3. TIETOTURVAKOVENNUKSEN JA AUDITOINNIN TYÖKALUT

Aiemmin tässä työssä esitelty Windows-työasematurvallisuuden koventaminen on yksinkertaisimmillaan tarkistuslistojen mukaan tehtävää yksittäisten asetusten määrittelyä. Tietoturvakovennuksien toteuttamiseen, auditointiin ja hallintaan jatkokehityksenä voi olla keskitetty hallinta, tai automaatiot. Työkaluja tarjoavat sekä toimittaja itse että lukuisat tietoturvaan keskittyneet organisaatiot. Näiden työkalujen joukosta oikeiden valinta on alan ammattilaisillekin vaikeaa.

3.1 Microsoft Purview Compliance manager

Microsoftin (2023f) mukaan Purview Compliance Manager on tuote jonka avulla organisaatiot voivat hallita ja arvioida vaatimustenmukaisuutta yhden työkalun kautta. Microsoft kertoo tuotteen soveltuwan useisiin vaatimuksenmukaisuuden tehtäviin, kuten suojaavan tiedon riskien inventointiin, tarvittavien kontrollien hallintaan, regulaation ja sertifointien ajan tasalla pitämiseen sekä raportointiin auditoijille. Microsoft kertoo tuotteen

sisältävän jopa 360 erilaista yleistä ja paikallista tietoturvastandardia tai regulaatiota kuten NIST, CIS, Katakri ja PiTuKri (Microsoft 2023f).

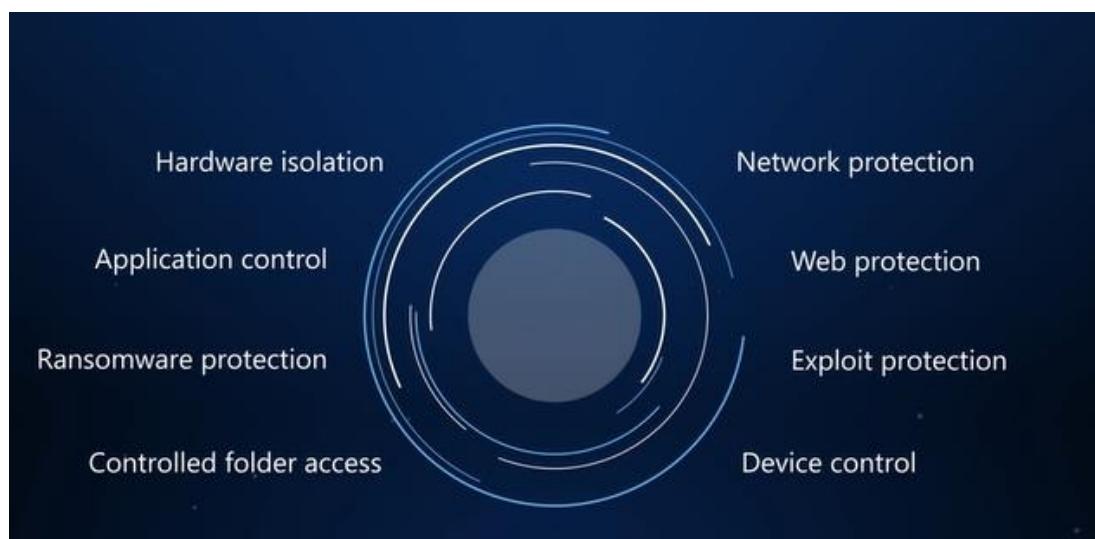
Tuotteen avulla voidaan ajaa valittuja standardeja tai tietoturvakehyksiä vasten tarkastuksia (eng. assessment). Tarkastustehtävät voidaan asettaa jatkuvamuotoisiksi, jolloin saadaan käyttöön jatkuvasti kehittyvä tietoturvan kokonaiskuva. Tarkastustehtävät muodostavat automaattisesti priorisoidun listan organisaatiota koskevista tietoturvan parannusehdotuksista (eng. improvement actions). Microsoftin mukaan parannusehdotusten suorittaminen muodostaa organisaatiolle riskitason numeraalisen mittarin, jota Microsoft nimittää Compliance Scoreksi. Parannusehdotuksia voidaan myös hallita ja vastuuttaa organisaation sisällä tehtäväksi. Samaan työkaluun voidaan Microsoftin mukaan tallentaa todistelu, muistiinpanot ja muutoshistoria tehdystä parannustoimista. (Microsoft 2023f).

3.2 Defender for endpoint ja vulnerability management

Defender for endpoint on Microsoftin pilvipohjainen työaseman tietoturvatuote. Tuote vaatii erillisen lisensoinnin. Tuotteen toiminta nojaa vahvasti Microsoftin pilvipalvelun asiakasdatalla rikastamaan koneälyyn. Nämä koneäly ominaisuudet laajentavat Microsoftin (2023g) mukaan normaalialla Windows päätelaitetietoturvan suojaa paremalla näkyvyydellä, älykkäällä korrelaatioilla ja nopeammalla dynaamisella tietoturvaominaisuksien hyödyntämisellä. Hallintaan Microsoft suosittaa Defender for endpoint ja Intune tuotteita, tosin ainakin osa ominaisuuksista on vähintään käytöönnoton osalta mahdollista toteuttaa ryhmäkäytännöillä, configuration manager tuotteella, tai jopa powershellillä (Microsoft 2023g).

Microsoft luokittelee tuotteensa nk. Endpoint detection and response kategoriaan (EDR). Microsoftin (2023g) mukaan tuote sisältää tietoturvan kovennukseen luettavia ominaisuuksia, kuten hyökkäysrajapinnan pienentämiseen tarkoitettun attack surface reduction (ASR) kokonaisuuden. ASR-ominaisuudet sisältävät useita alatoimintoja, kuten Application control kategorian alla oleva Windows defender Application control, jolla voidaan

hallita sovellusten suoritusoikeuksia työasemissa. Näitä ominaisuuksia on havainnollistettu kuvassa 20 (Microsoft 2023g).



Kuva 20. Defender attack surface reduction ominaisuudet (Microsoft 2023g)

Microsoft on tuonut M365 defender tuoteperheeseen mukaan lisätuotteen nimeltä **Defender vulnerability management**. Tämä tuote tarjoaa Microsoftin mukaan kyvyn havaita, monitoroida ja arvioida havaittuja turvallisuusriskejä automaattisesti. Tuote pystyy havaitsemaan haavoittuvia ohjelmistoja, laitteistoajureita, rautatason ohjelmistohaavoittuvuuksia, varmenteita ja selainlaajennuksia. Tuote sisältää myös assessment-arvointiosuuden, jolla organisaatio voi tehdä omista työasemistaan arvointiraportin vasten tietoturvakehyksiä (Microsoft 2023h).

Assessment-ominaisuuden hyödyntäminen vaatii Intune-hallintaa, jotta arvioinnit voidaan kohdistaa sen keräämään dataan, tässä tapauksessa työasemien inventaarioon. Työkalulla ei voi suoraan jaella korjauksia arvointien pohjalta, tähän Microsoft mainitsee keinona ryhmäkäytännöt. Tässä työssä aiemmin esitellyt CIS benchmarks ja DISA Stig formaatit ja niiden sisältämät tasot on tuottu Microsoftin oman kehyksen lisäksi arvointipohjiksi. Arvointi näyttää ryhmä- ja laitetasolla vaatimustenmukaisuuden täyttymisen ja mahdollistaa myös poikkeuksien hallinnan (Microsoft 2023h).

3.3 CIS-CAT ja CIS CSAT

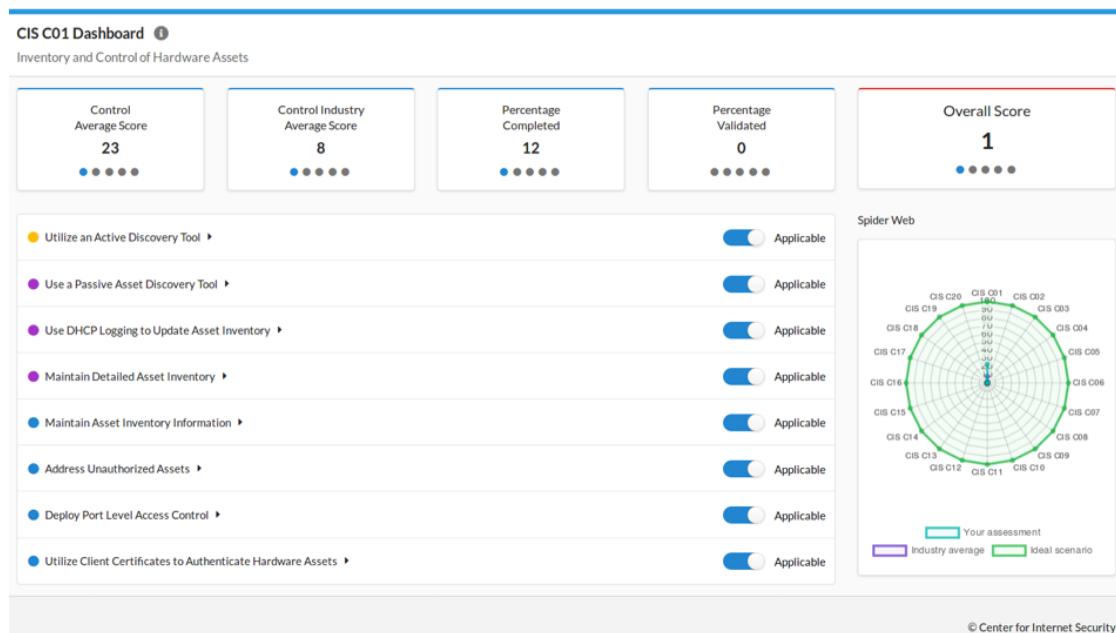
CIS:n (s.a.f) mukaan **CIS-CAT** (CIS Configuration Assesment Tool) on työkalu, jonka avulla voidaan tehdä automatisoitu arvio CIS määrityskokoonpanojen (eng. benchmarks) tietoturvakovenkuksista vasten kohdejärjestelmää. Arvio on raportti, joka sisältää havaintojen ja korjaustoimenpiteiden lisäksi numeraalisen arvion asteikolla 0–100, joka kertoo kuinka hyvin kohdejärjestelmä vastaa kyseistä CIS määrityskokoonpanoa. Työkalulla voi arvioida lisäksi CIS käyttöönottoryhmän 1 turvallisuuskontrollien määrityksiä Windows 10 tai Windows Server ympäristöissä. (CIS s.a.f).

CIS:n (s.a.f) mukaan työkalusta on olemassa sekä maksullinen Pro- että Lite-versio, joista jälkimmäinen on rajoittunut raporttimuotojen ja käytettävän CIS määrityskokoonpano -valikoiman suhteen. Työkalu tukee security content automation protocol (SCAP) -spesifikaatioon pohjautuvia arvointikriteeristöjä. Pro versio tai CIS:n pilvipalvelu (CIS securesuite) sisältää "build-kit" - ominaisuuden, jonka avulla raportin sisältämät Windows-tietoturvakovenukset voidaan muodostaa valmiiksi ryhmäkäytännöiksi (eng. group policy). Nämä ryhmäkäytännöt voidaan ladata ja ottaa käyttöön organisaation omassa ympäristössä normaalilin ryhmäkäytäntöjakelun kautta. CIS:n pilvipalvelu mahdollistaa myös määrityskokoonpanojen muokkaamisen organisaation tarpeiden mukaisiksi. Mukanut kokoonpanot voidaan tuoda arvointityökaluun ja tehdä arvio niitä vasten. (CIS s.a.f).

CIS:n (s.a.g) mukaan **CIS CSAT** (CIS Controls Self Assesment Tool) on tuote, jonka avulla organisaatiot voivat tehdä arvion organisaationsa CIS controls:n tilasta. Työkalussa on mahdollista valita mitä suojauskeinoja arviodaan, ladata todisteita ja seurata arvointien mukaisten parannuskeinojen tilaa. CIS kertoo työkalun sisältävän vertailumahdolisuuden muihin tietoturvakehyksiin, kuten NIST CSF:n ja NIST SP 800-53:n. Lisäksi työkalu mahdollistaa vertailun muihin organisaatioihin. CIS tarjoaa työkalusta ilmaisen selainpohjaisen version ei-kaupalliseen käyttöön. Maksullinen Pro versio kuuluu osaksi CIS securesuitea, mahdollistaen mm. paikallisen käytön, paremman

organisaatiotasoinen jaottelun arvioinneissa ja tiedon jaon rajoitukseen organisaatiovertailuissa. (CIS s.a.g).

CIS (s.a.h) kertoo selainpohjaisen version olevan kehitetty alunperin excel-muotoisesta taulukosta, yhteistyössä EthicalHat -yrityksen kanssa. Kuvassa 21 on näkyvissä CSAT työkalun selainpohjainen hallintanäkymä, jossa näkyy mm. yhden kontrollin sisältämät suojauskeinot ja kyseisen kontrollin arvioinnin taso (CIS s.a.h).



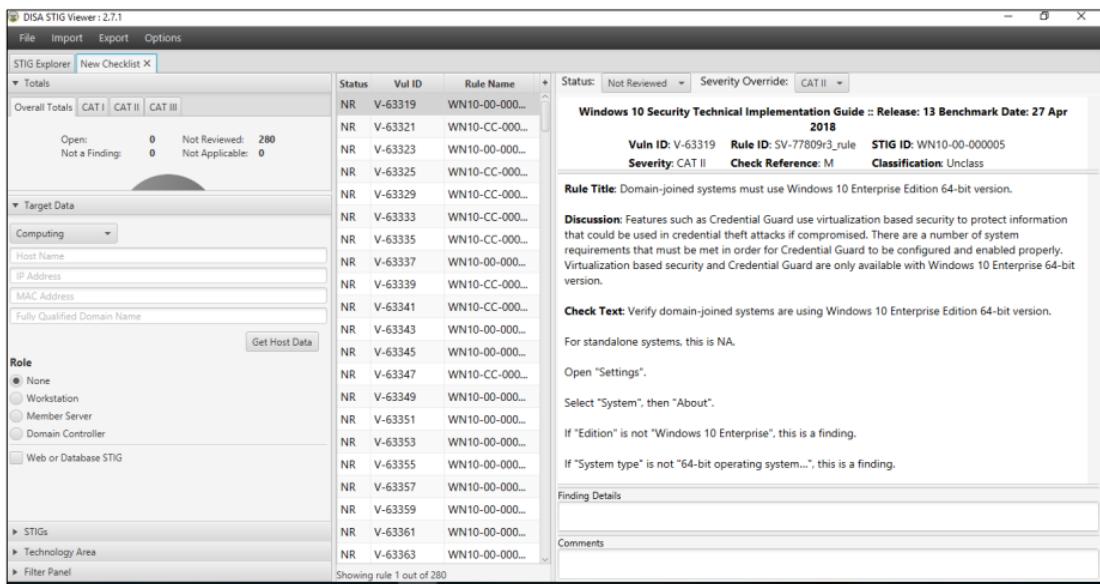
Kuva 21. CIS CSAT selainhallinnan käyttöliittymä (CIS s.a.h)

CIS:n (s.a.h) mukaan csat työkalulla voidaan seurata kontrollien dokumentaatiota, käytöönottoa, automaatiota ja toteuttaa raportointia. Työkalun sisällä voidaan jakaa käytöönottotoimia organisaation sisällä. CIS kertoo automaattisesta raportointimahdollisuudesta, kuten myös mahdollisuudesta viedä arvioden sisältämä data, taulukot ja tulokset suoraan powerpoint, excel tai pdf -muotoon (CIS s.a.h).

3.4 DISA STIG viewer ja SCAP compliance checker

DISA:n (2024) mukaan heidän rakentamansa **STIG viewer** työkalu mahdollistaa XCCDF-pohjaisten STIG-mallipohjien katselun helposti luettavassa muodossa. Työkaluun voidaan tuoda mallipohjia sekä hakea ja

suodattaa niiden sisältöjä esim. haavoittuvuuksien prioriteettien tai kategorioiden avulla. Työkalu mahdollistaa myös valitun datan viennin html, rtf ja csv -formaateissa jatkokäsittelyyn esim. tekstinkäsittelyohjelmaan. DISA:n mukaan työkaluun tuoduista mallipohjista voidaan koostaa manuaalisia tarkistuslistoja (eng. checklist). Yksi tarkistuslista voi sisältää useita eri mallipohjia, tai osia valituista mallipohjista. Tarkistuslistaan voidaan tuoda myös SCAP compliance checker työkalulla saadut tulokset, joita voidaan täydentää manuaalisesti tehdyllä arvioinnilla. Kuvassa 22 on esitetty STIG viewer työkalun käyttöliittymässä auki oleva tarkistuslista. (DISA 2024).



Kuva 22. STIG viewer checklist näkymä (DISA 2024)

NIWC Atlantic on yhdysvaltojen merivoimien ja puolustusviraston alainen virasto, jonka tehtävänä on tehdä tutkimustyötä ja kehitystä tukeakseen informaationsodankäyntiä (NIWC Atlantic s.a). **SCAP compliance checker** on useiden yhdysvaltojen virastojen (mm. DISA ja NSA) rahoittama ja NIWC Atlantic organisaation rakentama, automaattinen SCAP-pohjaisten määritysten tarkistustyökalu. NIWC Atlantic:n mukaan työkalua voidaan ajaa komentorivi, käyttöliittymä tai palveluasennuksena (eng. command line, Gui, service). NIWC Atlantic kertoo tarkemmin SCAP kokoonpanojen koostuvan zip-pakatuista tiedostoista, jotka sisältävät tarvittavat XCCDF ja OVAL (xml-pohjaiset) määritystiedostot. Näissä tiedostoissa kerrotaan mitä tarkistuksia kyseinen kokoonpano sisältää ja miten tarkistustyökalun tulee ne suorittaa. (NIWC Atlantic 2021).

SCAP compliance checker pystyy käyttämään hyväkseen vain SCAP kokoonpanoja, eikä esim. DISA STIG määrityskokoonpanoja. DISA:n sivulta on saatavilla valmiina yleisimmille käyttöjärjestelmille ja selaimille sopivat SCAP kokoonpanot. NIWC Atlantic kertoo lisäksi tarjoavansa laajennettuja STIG SCAP määrityskokoonpanoja, joissa automaattisten tarkistusten lisäksi on olemassa manuaalisia tarkistuksia ja kysymyksiä. NIWC Atlantic:n mukaan työkalu tukee DoD:n mukaisia kategorioita ja luottamustasoja valittavien profiilien kautta, mutta niiden käyttö on täysin SCAP kokoonpanon luojan päätettävissä. NIWC Atlantic:n mukaan esim. DISA:n STIG pohjaiset SCAP:it sisältävät kaikki kolme kategoriaa ja luottamustasoa valittavina profiileina. Työkalulla voi myös muokata siihen tuotuja määrityskokoonpanoja, jotta tarkistukset saadaan vastaamaan organisaation vaatimuksia. Työkalulla ei voi kuitenkaan NIWC Atlantic:in mukaan tehdä mitään havaintoja korjaavia toimia, vaan sitä voi hyödyntää vain tarkistuksiin ja raportointiin. (NIWC Atlantic 2021).

LÄHTEET

Beyondtrust. s.a. Systems hardening. WWW-dokumentti. Saatavissa: <https://www.beyondtrust.com/resources/glossary/systems-hardening> [viitattu 23.08.2023].

Cimcor s.a. What is System Hardening? WWW-dokumentti. Saatavissa: <https://www.cimcor.com/system-hardening#system-hardening-is> [viitattu 15.10.2023].

CIS. 2022. CIS Community Defense Model 2.0. WWW-dokumentti. Saatavissa: <https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0> [viitattu 18.01.2024].

CIS. s.a.a. CIS Critical Security Controls Navigator. WWW-dokumentti. Saatavissa: <https://www.cisecurity.org/controls/cis-controls-navigator> [viitattu 23.08.2023].

CIS. s.a.b. The CIS Critical Security Controls. WWW-dokumentti. Saatavissa: <https://www.cisecurity.org/controls/cis-controls-list> [viitattu 23.08.2023].

CIS. s.a.c. About us. WWW-dokumentti. Saatavissa: <https://www.cisecurity.org/about-us> [viitattu 23.08.2023].

CIS. s.a.d. CIS Windows 10 Enterprise Benchmark. WWW-dokumentti. Saatavissa: <https://www.cisecurity.org/cis-benchmarks> [viitattu 23.08.2023].

CIS. s.a.e. CIS Windows 10 Stand-Alone Benchmark. WWW-dokumentti. Saatavissa: <https://www.cisecurity.org/cis-benchmarks> [viitattu 23.08.2023].

CIS. s.a.f. What is CIS-CAT. WWW-dokumentti. Saatavissa: <https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/cis-cat-faq> [viitattu 23.08.2023].

CIS. s.a.g. CIS Controls Self Assessment Tool (CIS CSAT). WWW-dokumentti. Saatavissa: https://www.cisecurity.org/controls/cis-controls-self-assessment-tool-cis-csat_pre [viitattu 03.12.2023].

CIS. s.a.h. CIS CSAT: A Free Tool for Assessing Implementation of CIS Critical Security Controls. WWW-dokumentti. Saatavissa: <https://www.cisecurity.org/insights/blog/cis-csat-free-tool-assessing-implementation-of-cis-controls> [viitattu 03.12.2023].

CIS. s.a.i. CIS mapping and compliance. WWW-dokumentti. Saatavissa: <https://www.cisecurity.org/cybersecurity-tools/mapping-compliance> [viitattu 17.11.2023].

Cyphere. s.a. How to reduce your attack surface with system hardening in 2021. WWW-dokumentti. Saatavissa: <https://thecyphere.com/blog/system-hardening/> [viitattu 26.10.2023].

Department of Defense. 2004. INSTRUCTION. PDF-dokumentti. Saatavissa: <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/858001p.pdf> [viitattu 06.12.2023].

DISA. 2024. STIG Viewer 3.x User Guide. PDF-dokumentti. Saatavissa: https://dl.dod.cyber.mil/wp-content/uploads/stigs/pdf/U_STIG_Ver_3-x_User_Guide_V1R3.pdf [viitattu 28.03.2024].

DISA. 2023. Microsoft Windows 10 Security Technical Implementation Guide (STIG) Overview. PDF-dokumentti. Saatavissa: https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_10_V2R8_STIG.zip [viitattu 23.08.2023].

Digi ja väestötietovirasto. 2022. Digitaalisen turvallisuuden arkkitehtuuri. WWW-dokumentti. Saatavissa: <https://wiki.dvv.fi/display/DTARK/> [viitattu 23.08.2023].

Dunkerley, M., Tumbarello, M. 2022. Mastering-windows-security-and-hardening-second-edition. Packt publishing. PDF-dokumentti. Saatavissa: <https://www.packtpub.com/product/mastering-windows-security-and-hardening-second-edition/9781803236544> [viitattu 23.08.2023].

HIMSS. 2019. Cybersecurity frameworks explained. WWW-dokumentti. Saatavissa: <https://www.himss.org/resources/cybersecurity-frameworks-explained> [viitattu 13.10.2023].

Intel. s.a. System hardening. WWW-dokumentti. Saatavissa: <https://www.intel.com/content/www/us/en/business/enterprise-computers/resources/system-hardening.html> [viitattu 23.08.2023].

Microsoft. 2019a. Introducing the security configuration framework: A prioritized guide to hardening Windows 10. WWW-dokumentti. Saatavissa: <https://www.microsoft.com/en-us/security/blog/2019/04/11/introducing-the-security-configuration-framework-a-prioritized-guide-to-hardening-windows-10/> [viitattu 23.08.2023].

Microsoft. 2019b. Introducing the security configuration framework. WWW-dokumentti. Saatavissa: <https://github.com/microsoft/SecCon-Framework/blob/master/windows-security-configuration-framework.md> [viitattu 23.08.2023].

Microsoft. 2023a. Introduction to Windows security. WWW-dokumentti. Saatavissa: <https://learn.microsoft.com/en-us/windows/security/introduction> [viitattu 23.08.2023].

Microsoft. 2023b. Security baselines. WWW-dokumentti. Saatavissa: <https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines> [viitattu 23.08.2023].

Microsoft. 2023c. Microsoft Security Compliance Toolkit – How to use. WWW-dokumentti. Saatavissa: <https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10> [viitattu 23.08.2023].

Microsoft. 2023d. Use security baselines to configure Windows devices in Intune. WWW-dokumentti. Saatavissa: <https://learn.microsoft.com/en-us/mem/intune/protect/security-baselines> [viitattu 23.08.2023].

Microsoft. 2023e. Monitor security baselines and profiles in Microsoft Intune. WWW-dokumentti. Saatavissa: <https://learn.microsoft.com/en-us/mem/intune/protect/security-baselines-monitor> [viitattu 01.12.2023].

Microsoft. 2023f. Microsoft Purview Compliance Manager. WWW-dokumentti. Saatavissa: <https://learn.microsoft.com/en-us/purview/compliance-manager#what-is-compliance-manager> [viitattu 23.08.2023].

Microsoft. 2023g. Microsoft defender for endpoint. WWW-dokumentti. Saatavissa: [https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerability-management?view=o365-worldwide](https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide) [viitattu 23.08.2023].

Microsoft. 2023h. What is Microsoft Defender Vulnerability Management. WWW-dokumentti. Saatavissa: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerability-management?view=o365-worldwide> [viitattu 23.08.2023].

Mitre. s.a.a. FAQ. WWW-dokumentti. Saatavissa: <https://attack.mitre.org/resources/faq/#faq-0-0-header> [viitattu 23.08.2023].

Mitre. s.a.b. CYBERSECURITY. WWW-dokumentti. Saatavissa: <https://www.mitre.org/focus-areas/cybersecurity> [viitattu 23.08.2023].

Mitre. s.a.c. Drive-by Compromise. WWW-dokumentti. Saatavissa: <https://attack.mitre.org/techniques/T1189/> [viitattu 23.08.2023].

Mitre. s.a.d. About the D3FEND Knowledge Graph Project. WWW-dokumentti. Saatavissa: <https://d3fend.mitre.org/about/> [viitattu 23.08.2023].

NIST. 2008. Guide to General Server Security. WWW-dokumentti. Saatavissa: <https://doi.org/10.6028/NIST.SP.800-123> [viitattu 15.10.2023].

NIST. 2015. A Profile for U.S. Federal Cryptographic Key Management Systems. PDF-dokumentti. Saatavissa: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-152.pdf> [viitattu 28.10.2023].

NIST. 2018. Framework for Improving Critical Infrastructure Cybersecurity. WWW-dokumentti. Saatavissa: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> [viitattu 23.08.2023].

NIST. 2020. Security and Privacy Controls for Information Systems and Organizations. WWW-dokumentti. Saatavissa: <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final> [viitattu 23.08.2023].

NIST. 2022. About NIST. WWW-dokumentti. Saatavissa: <https://www.nist.gov/about-nist> [viitattu 23.08.2023].

NIST. 2023. Security Content Automation Protocol. WWW-dokumentti. Saatavissa: <https://csrc.nist.gov/projects/security-content-automation-protocol/SCAP-Content> [viitattu 23.08.2023].

NIWC Atlantic. 2021. SCAP Compliance Checker Version 5.8 User Manual for Microsoft Windows. WWW-dokumentti. Saatavissa: https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/scc-5.8_Windows_bundle.zip [viitattu 06.12.2023].

NIWC Atlantic. s.a. About. WWW-dokumentti. Saatavissa: [About – NIWC Atlantic \(navy.mil\)](#) [viitattu 01.12.2023].

Pathlock. 2022. NIST Cybersecurity Framework Executive Summary And Overview. WWW-dokumentti. Saatavissa: <https://pathlock.com/learn/nist-cybersecurity-framework-executive-summary-and-overview/> [viitattu 23.08.2023].

Redswitches. 2023. What's System Hardening and How It Works: A 5-Phase Process. WWW-dokumentti. Saatavissa: <https://www.redswitches.com/blog/system-hardening/> [viitattu 15.10.2023].

Rsisecurity. 2022. What are system hardening standards? WWW-dokumentti. Saatavissa: <https://blog.rsisecurity.com/what-are-system-hardening-standards/> [viitattu 15.10.2023].

SABSA. s.a. Sabsa executive summary. WWW-dokumentti. Saatavissa: <https://sabsa.org/sabsa-executive-summary/#:~:text=SABSA%20ensures%20that%20the%20needs,methodology%2C%20not%20a%20commercial%20product>. [viitattu 23.08.2023].

SABSA. 2009. Enterprise Security Architecture. WWW-dokumentti. Saatavissa: <https://sabsacourses.com/wp-content/uploads/2021/02/TSI-W100-SABSA-White-Paper.pdf> [viitattu 23.8.2023].

Titania. s.a. DISA STIG Compliance Explained. WWW-dokumentti. Saatavissa: <https://www.titania.com/resources/guides/disa-stig-compliance-explained> [viitattu 03.11.2023].

KUVALUETTELO

- Kuva 1. Sabsan tietoturvamallin kerrokset (Sabsa. 2017)
- Kuva 2. Sabsa-Kerroksittainen tietoturva-arkkitehtuurimalli (Sabsa. 2017)
- Kuva 3. NIST funktiot, kategoriat ja informatiiviset viitteet (Pathlock. 2022)
- Kuva 4. NIST käyttöönottokerrokset (Pathlock. 2023)
- Kuva 5. NIST kontrolliperheet (NIST 2020)
- Kuva 6. Esimerkki NIST SP800-53 kontrollikuvauksesta (NIST 2020)
- Kuva 7. DVV:n Dtark viitekehysen malli (Digi ja väestötietovirasto. 2022)
- Kuva 8. Dtark lisätietokentän rikastaminen Suomen omilla erityisillä standardeilla (Digi ja väestötietovirasto. 2022)
- Kuva 9. CIS kontrolliperheet, käyttöönottoryhmät ja suojauskeinot (CIS s.a.i)
- Kuva 10. CIS controls, esimerkki kontrollista (CIS s.a.i)
- Kuva 11. Mitre Att&ck kuvaus (MITRE. s.a.c)
- Kuva 12. D3fend kehysen tietämiskannan malli (Mitre. s.a.d)
- Kuva 13. Defense-in-Depth, ihmiset (NSA 2002)
- Kuva 14. Defense-in-depth, teknologia (NSA 2002)
- Kuva 15. Defense-in-depth, operaatiot (NSA 2002)
- Kuva 16. Defense-in-depth -teknologianäkökulmat (NSA 2002)
- Kuva 17. Politiikka, standardit, proseduurit (Dunkerley & Tumbarello 2022)
- Kuva 18. Mukailleen CIS benchmarks. Esimerkki Windows10 Enterprise kovennuksista (CIS s.a.d)
- Kuva 19. SecCon ryhmät ja päätelaitteiden ryhmittely (Microsoft. 2019b)
- Kuva 20. Defender attack surface reduction ominaisuudet (Microsoft 2023g)
- Kuva 21. CIS CSAT selainhallinnan käyttöliittymä (CIS s.a.h)
- Kuva 22. STIG viewer checklist näkymä (DISA 2024)

Työasematurvallisuuden käyttöönottomalli.

Saatavilla:

[https://github.com/KarlSynsed/Masters/blob/main/TyoasemaTurvanKayttoonot
toMalli.xlsx](https://github.com/KarlSynsed/Masters/blob/main/TyoasemaTurvanKayttoonotToMalli.xlsx)

Julkisuuslain mukaan salattu havainnointiaineisto (Laki viranomaisten toiminnan julkisuudesta 21.5.1999, 6. luku 24.§ kohta 21).