HAMK
Hämeen ammatti-
korkeakoulu

Windowsin koventaminen CAT-CAT Lite -palvelulla

Ammattikorkeakoulututkinnon opinnäytetyö

Tietojenkäsittelyn koulutus

Kevät 2024

Riku Nieminen

HAMK
Hämeen ammatti-
korkeakoulu

Tietojenkäsittelyn koulutus Tiivistelmä
Tekijä Riku Nieminen Vuosi 2024
Työn nimi Windowsin koventaminen CIS-CAT Lite palvelulla
Ohjaaja Ismo Turve

Opinnäytetyön tarkoitus oli esitellä ja käyttää CIS-CAT Lite -palvelua sekä arvioida sen käytännöllisyyttä Windows-ympäristön koventamisen tarkoituksessa. Lopputuloksena tavoiteltiin tutkimuksen toimimista eräänlaisena ohjeena arvioidun ohjelmiston käytöstä, erityisesti pienille yrityksille, joissa kyberturvallisuuden ymmärrys tai osaaminen ei ole nykyajan vaatimalla tasolla.

Tutkimuksen teoriaosassa pohjustetaan CIS-CAT Lite -ohjelmiston taustaa ja sitä, mihin ohjelmiston arviot perustuvat. Tätä ennen käytiin läpi myös kyberturvallisuuden perusteita sekä avattiin termejä, kuten koventaminen. Opinnäytetyö oli enimmäkseen toiminnallinen, ja tutkimuksen aineisto luotiin CIS-CAT Lite -ohjelmistoa käyttämällä ja sen tulosten pohjalta.

Työn tuloksista pystyttiin määrittämään, että CIS-CAT Lite -ohjelmisto on hyvä ehdokas ja apuväline peruskyberturvallisuuden konfigurointiin monenlaisille tahoille, joilta saattaa puuttua tarvittava tietotaito. Tutkimuksessa todettiin, että CIS-CAT Lite tuottaa luotettavia ohjeita, joiden pohjalta moni pystyisi tekemään perustason kyberturvallisuuden konfigurointia. Ohjeet itsessään ovat erittäin hyvin rakennettuja, selkeillä ohjeilla, perusteluilla ja muistiinpanoilla. Ohjelmiston tuottaman raportin pohjalta lukija voi oppia paljon kyberturvallisuuden tarpeellisuudesta sekä konkreettisista vaikutuksista. Johtopäätöksenä voidaan todeta, että CIS-CAT Lite on soveltuva ohjelmisto kyberturvallisuuden tason koventamiseen pienissä yrityksissä.

Avainsanat CIS, CIS-CAT Lite, Koventaminen, Windows 11, kyberturvallisuus
Sivut 39 sivua ja liitteitä 1 sivua

HAMK
Hämeen ammatti-
korkeakoulu

Degree Programme in Business Information Technology
Author Riku Nieminen
Subject Hardening Windows using CIS-CAT Lite
Supervisors Ismo Turve

Abstract
Year 2024

The purpose of this thesis is to critically examine CIS-CAT Lite for Windows 11 operating system hardening purposes for smaller companies. The expected result is that we got conclusion on how good CIS-CAT Lite is for hardening Windows 11 environments for target audience consisting of people who aren't that versed in cybersecurity. The thesis would ideally work as an introductory guide for smaller companies who are interested in options to harden their cybersecurity state.

The theory part consists of giving the basic run down of cybersecurity practices and explaining cybersecurity and the core threats we face in the field of cybersecurity. Theory part also includes the introduction of CIS aka Center for internet security, their work models and what products and services they have introduced to the public, both free and paid.

The results concluded that CIS-CAT Lite works well as a cybersecurity configuration tool. It being free, easy to use with credible information and guidelines in the topic of cybersecurity. During the thesis we got to the conclusion that CIS-CAT Lite produces credible, well written and user-friendly reports with accurate specifics and easy to understand guides for users to increase their cybersecurity state to the better.

Keywords CIS, CIS-CAT Lite, Hardening, Windows 11, Cybersecurity
Pages 39 pages and appendices 1 pages

Sanasto

CIS	Center for internet security
CIS-CAT Pro	Maksullinen versio CIS-CAT Lite palvelusta
CIS-CAT Lite	Center for internet securityn kyberturvallisuuden konfigurointi palvelu
CIS Benchmarks	Tietopohja mihin CAT ohjelmistojen arviot perustuvat
Oracle VirtualBox	Virutaalikone ohjelmisto
Koventaminen	Ympäristön kyberturvallisuuden parantamista tarkoittava prosessi
Kyberturvallisuus	Laitteiden, verkkojen ja ohjelmien suojaamista tarkoittava prosessi
Group policy	Microsoft Windowsin sisään rakennettu käyttäjien sekä tietokoneen hallinta järjestelmä

Sisällys

Kuvat, komennot, ohjelmakoodit, taulukot ja kaavat

Liitteet

Liite 1. Aineistonhallintasuunnitelma (pakollinen kaikille)

1 Johdanto

Yritysten kyberturvallisuus on nykyaikana erittäin ajankohtainen ja tärkeä asia, ja siihen liittyvät yleiset puutteet ja laiminlyönnit ovat kasvava ongelma varsinkin pienten yritysten keskuudessa. Suurimmat ongelmat ovat tietoisuuden puute siitä, miten yritysten kyberturvallisuutta voitaisiin parantaa, tai suoraan asian laiminlyönti osaamattomuuden takia tai tarpeettomuuden uskossa. Opinnäytetyön tarkoitus on määritellä käyttöjärjestelmän koventamisen perusperiaatteet ja koventaa natiivi Windows 11 -käyttöjärjestelmällä toimiva virtuaalikone käyttämällä Center for Internet Securityn ilmaista CIS-CAT Lite -palvelua.

Tässä opinnäytetyössä käydään askel askeleelta läpi CIS-CAT Liten asentaminen, käyttö sekä tulokset. Ennen valitun ohjelmiston käyttöä työssä annetaan tarpeellista kontekstia kyberturvallisuuteen, jotta jälkimmäinen osa olisi helpommin ymmärrettävissä lukijalle. Teorian jälkeen työssä pohjustetaan CIS-CAT Liten toiminnallisuutta sekä käydään läpi, mihin palvelun kyberturvallisuusohjeistukset pohjautuvat ja miten kyseisiä ohjeistuksia pystytään käyttämään valitun ympäristön kyberturvallisuuden parantamiseen.

Kyky koventaa työympäristöä on erittäin tärkeää, ja sen merkitys vain kasvaa tulevaisuudessa. Kyberturvallisuuden laiminlyönnin seuraukset voivat olla vakavia, etenkin kun yhä enemmän tietoa ja palveluita siirtyy täysin verkkoon. Kyberturvallisuus ei ole aiheena helppo, ja sen ymmärtäminen vaatii paljon töitä sekä kärsivällisyyttä. Siksi olisi hyödyllistä, jos tiedossa olisi työkaluja, joiden avulla myös vähemmän kyberturvallisuudesta perillä olevat henkilöt osaisivat koventaa yleisesti käytössä olevia Windows 11 -ympäristöjä perusperiaatteiden mukaisesti ja hieman omaan käyttöön sovellettuna.

Tässä tutkimuksessa etsitään vastauksia seuraaviin kysymyksiin:

1. Miksi ympäristön koventaminen on tärkeää?
2. Miten CIS Cat lite auttaa käyttöjärjestelmän koventamisessa?
3. Mihin CIS Cat liten arviot perustuvat?

2 Kyberturvallisuus Windows-ympäristössä

Kestävän kyberturvallisuuspohjan rakentaminen on nykyajan yrityksille elintärkeää, mutta silti sen laiminlyönti on hyvin yleinen ongelma, varsinkin pienten yritysten keskuudessa. On tärkeää, että nykypäivänä lähes kaikilla olisi peruskäsitys kyberturvallisuudesta ja sen tärkeydestä jokapäiväisessä elämässä. Myös ymmärrys siitä, miten tehdä peruskonfiguraatioita tietokoneille, olisi erittäin tärkeää, mutta epätodennäköistä. Tämän kappaleen tarkoitus on käydä läpi Windows-ympäristön kyberturvallisuuden perusteita ja rakentaa pohjatietoa lukijalle, mikä auttaa ymmärtämään tässä opinnäytetyössä käytettävän palvelun toiminnallisuutta ja tarpeellisuutta. (*Mitä kyberturvallisuus on?*, n.d.)

2.1 Kyberturvallisuus

Kyberturvallisuus koostuu prosesseista, ratkaisuista ja käytännöistä, joiden avulla pystytään suojaamaan kriittiset järjestelmät ja verkot digitaalisilta hyökkäyksiltä. Tähän liittyy myös kyky ennakoida kyberuhkia ja sietää mahdolliset kyberhyökkäykset. Yleisesti tietoturvasta ja kyberturvallisuudesta puhutaan saman asiana, mutta näin ei kuitenkaan ole. Tietoturva liittyy tiedon saatavuuteen ja luottamuksellisuuteen, kun taas kyberturvallisuudella suojataan digitaalista ja verkottunutta ympäristöä sekä sen turvallisuutta. (*Kyberturvallisuuden Sanasto*, Sanastokeskus TSK ry, 2018.)

CIA-triad on lähtökohta kyberturvallisuudelle. CIA-triad koostuu kolmesta päärakenteesta: luottamuksellisuudesta, eheydestä ja saatavuudesta. Luottamuksellisuus tarkoittaa karkeasti yksityisyyttä. Sen tarkoitus on rajoittaa salassapidettävää tietoa kohtaan tehtyjen luvattomien käyttöpyyntöjen määrää. Eheys taas varmistaa, että data on tarkkaa sekä luotettavaa. Datan luotettavuus ei saa vaarantua sitä siirrettäessä, joten eheyteen sisältyy datansiirron luotettavuus ja turvatoimet. Saatavuus on ehdoton osa CIA-triad-mallia, jonka tarkoitus on varmistaa, että tarvittava tieto on saatavilla ja käytettävissä luvan omaaville tahoille. CIA-triad-mallin yleiset käsitteet pätevät ja luovat pohjan sille, mitä nykyaikaiselta kyberturvallisuudelta vaaditaan. (*What Is the CIA Triad?*, n.d.)

Kyberturvallisuuden tarkoitus on siis pitää laitteet sekä data luotettavana ja estää luvattomien henkilöiden pääsy niihin käsiksi. Luotettavuus, eheys ja saatavuus ovat hyvä lähtökohta, joiden kautta pystytään aloittamaan kyberturvallisuuden soveltaminen omiin tarkoituksiin ja varmistamaan, että koti- tai työympäristö on kyberturvallisuuden näkökulmasta luotettava.

2.2 Yleiset uhat

Nykyajan pääuhat kyberturvallisuuteen liittyen ovat haitta- ja kiristysohjelmat, tietojen kalastelu, käyttäjän manipulointi, sisäiset uhat ja kehittynyt jatkuva uhka. Kyberturvallisuuteen liittyy paljon muutakin kuin vain tietokoneen sisällä tapahtuvat asiat. (*Mitä kyberturvallisuus on?*, n.d.)

Sosiaalista manipulointia käytetään paljon kriittisten ympäristöjen hallussapitäjiä vastaan, ja nykypäivänä jokaisen pitää osata erottaa kalastelusähköpostit ja käyttäjän manipuloinnin peruspiirteet. Helpoin tapa taistella sosiaalisen manipuloinnin ja tietojenkalastelun uhkia vastaan on käyttää kaksivaiheista todennusta kirjautumisissa kaikille laitteille. Tapoja ja käytäntöjä, joilla kyberturvallisuuden tasoa ja tietoisuutta voi parantaa, on esimerkiksi Zero Trust -suojausmallistrategia, jonka tarve on kasvanut pandemian aikana ja sen jälkeen lisääntyneen etätyön myötä. Zero Trustin mukaan kannattaa olettaa, että esimerkiksi käyttöoikeuspyyntöihin ei voi luottaa, ja antaa kaikille käyttäjille mahdollisimman rajatut käyttöoikeudet sekä varmistaa kirjautuminen esimerkiksi mobiilitodentimen kautta. Tietoisuutta kyberturvallisuusongelmista pystytään parantamaan järjestämällä koulutuksia ja kehottamalla ihmisiä olemaan aktiivisia ja etsimään tietoa itse asiaan liittyen. Tietenkin myös virustorjuntapalvelut sekä monet teknologiaratkaisut, kuten kyberturvallisuuden konfigurointipalvelut, auttavat kyberturvallisuuden tason nostamisessa. Tässä piilee kuitenkin ongelma varsinkin pienten yritysten keskuudessa, koska suurin osa kattavista kyberturvallisuusratkaisuista ovat maksullisia. Juuri tämän takia lähden tässä opinnäytetyössä käsittelemään, arvioimaan ja esittelemään ilmaista palvelua, joka auttaa nostamaan yritysten kyberturvallisuuden tasoa. (*Mitä kyberturvallisuus on?*, microsoft.)

2.3 Uhat Windows-järjestelmiä kohtaan

Yleisimmät tietoturvauhat eivät ole käyttöjärjestelmäkohtaisia, vaan niitä käytetään yleisesti kaikkia käyttöjärjestelmiä vastaan. Windows-käyttöjärjestelmissä on valmiiksi asennettuna useita ohjelmia, joiden tarkoitus on parantaa kyberturvallisuuden tilaa ja estää uhkien pääsy ympäristöön. Microsoft Defender Antivirus on Windows-ympäristön oma antivirusohjelmisto, jonka tarkoitus on valvoa ja estää haittaohjelmien, virusten tai turvallisuusuhkien pääsy tai toteutuminen tietokoneellasi. *(vinaypamnani-msft, 2023)*

Windows-ympäristössä on paljon muitakin sisäänrakennettuja ohjelmistoja ja käytäntöjä, joiden avulla voidaan helposti parantaa ympäristön kyberturvallisuuden tilaa. Windows-päivitykset ovat tärkeitä kyberturvallisuuden tason ylläpitämiseen, koska kaikki haavoittuvuuksien korjaukset ja ohjelmistopäivitykset tulevat niiden kautta. Yritystarkoituksiin

perusteet eivät yleensä kuitenkaan riitä, vaan käyttäjän pitää usein koventaa ympäristöä käyttäen ulkopuolista apua. *(vinaypamnani-msft, 2023)*

2.4 Koventaminen (Hardening)

Koventaminen on prosessi, jonka tarkoitus on eliminoida hyökkäysmahdollisuuksia korjaamalla haavoittuvuuksia ja poistamalla tarpeettomia ohjelmistoja käytöstä. Koventamiseen liittyy myös muita käytäntöjä, joita tässä opinnäytetyössä avataan ja selitetään. NIST:n eli National Institute of Standards and Technology:n julkaisemassa "A Profile for U.S. Federal Cryptographic Key Management System" -julkaisussa käsitellään ja selitetään koventamisen peruspiirteet. Jokainen organisaatio tarvitsee nykymaailmassa luotettavan ja turvallisen käyttöjärjestelmän, jota ei pysty muuttamaan, siirtämään tai tutkimaan ilman asianmukaisia ja hyväksyttyjä käyttöoikeuksia. (Barker et al., 2015)

Jokaisella nykyaikaisella älylaitteella tulisi olla luotettava ja turvallinen käyttöjärjestelmä pohjanaan, sillä ilman tätä luotettavaa perusrakennetta mitään palvelua tai tiedonsiirtoa ei voida taata varmaksi. Vaaditun turvallisuuden ja luotettavuuden ylläpitämiseksi käytetään koventamista. Kuten aiemmin mainittiin, koventaminen on pääpiirteissään prosessi, jonka avulla korjataan ympäristön haavoittuvuuksia ja ennaltaehkäistään mahdollisia ongelmatilanteita. (Barker et al., 2015)

Koventaminen on omalla tavallaan huolellisuutta siitä, että turvallisena pidettävään ympäristöön ei tehdä tai jätetä haavoittuvuuksia laiskuuden tai huomaamattomuuden takia, esimerkiksi vanhentuneiden turhien sovellusten tai palveluiden kautta. Käyttöoikeuksien seuranta on elintärkeää oikein koventamista soveltavassa ympäristössä. On pidettävä huolta, että liian vahvoja käyttöoikeuksia ei anneta mihinkään ympäristöön vaikuttavaan palveluun tai ohjelmaan. (Barker et al., 2015)

Ympäristössä kannattaa siis jakaa aina tiettyyn tehtävään tarvittavat oikeudet eikä yhtään enempää. Liian laajoilla oikeuksilla kuka tahansa voi tehdä tahallaan tai tahattomasti helposti huomaamatonta vahinkoa, mikä vaikuttaa suoraan ympäristön turvallisuuteen ja aiheuttaa haavoittuvuuksia. Käyttäjätilien hallinnassa on myös oltava tarkkana, koska vahingossa poistamatta jäänyt käyttäjä vahvoilla oikeuksilla on valtava turvallisuusaukko. Siksi aina kun ympäristöön luodaan uusia väliaikaisia käyttäjiä tai ympäristön käyttäjä lopettaa työskentelyn ympäristön kanssa, kyseinen käyttäjätili tulee poistaa tai ottaa pois käytöstä, jotta sitä ei voida käyttää mahdollisessa hyökkäystilanteessa ympäristöä vastaan. On myös tärkeää varmistaa, että käyttäjien salasanat ja avaimet eivät ole vakioita ja että uudelleenasennetut arvot ovat tarpeeksi vahvoja. Lyhyesti selitettynä koventaminen on siis jatkuva prosessi,

jonka avulla varmistetaan turvallisen ympäristön pysyminen turvallisena valvomalla käyttöoikeuksia, käyttäjätilejä ja ohjelmien versionhallintaa. (Barker et al., 2015)

3 CIS-CAT Lite -palvelu

CIS-CAT Lite -palvelu on ilmainen versio Center for Internet Securityn eli CIS:n luomasta CIS-CAT Pro -turvallisuuskonfigurointipalvelusta. CIS-CAT Lite -palvelulla pystytään tarkastamaan valitun ympäristön turvallisuuskonfiguraatiot CIS:n ”Benchmarkkeja” eli vertailupisteitä vasten. Palvelu antaa testatusta ympäristöstä arvosanan väliltä 1-100 ja luo raportin, joka sisältää ohjeet testatun ympäristön turvallisuustason parantamiseen. (*About Us - CIS®*, CIS.)

3.1 Center for Internet Security

Center for Internet Security eli CIS on voittoa tavoittelematon organisaatio, jonka tarkoituksena on ylläpitää maailmanlaajuisesti tunnettuja ja hyväksyttyjä kyberpuolustusratkaisuja. CIS perustettiin vuonna 2000 pienen ryhmän toimesta, joka koostui useista yritys- ja hallinnollisissa tehtävissä toimivista johtajista. CIS perustettiin vastauksena kasvavien kyberhyökkäysten määrään, ja sen tavoitteena on luoda ja kehittää kyberturvallisuuden tasoa maailmanlaajuisesti. (*About Us - CIS®*, CIS.)

CIS ylläpitää tavaramerkittyjä ja maailmanlaajuisesti tunnettuja sekä arvostettuja CIS Controls- ja CIS Benchmarks -palveluita, joiden tarkoituksena on auttaa käyttäjiään suojaamaan laitteita ja dataa. CIS-CAT Liten toiminta perustuu CIS Benchmark -käytäntöihin. CIS:n organisaatioon sisältyy myös MS-ISAC (Multi-State Information Sharing and Analysis Center), jonka tarkoituksena on suojata, turvata, estää ja palauttaa monia USA:n valtiollisia tahoja kyberuhkia vastaan. CIS rahoittaa toimintaansa myymällä luomiaan kyberturvallisuuspalveluita ja -resursseja. Lisäksi CIS saa rahallista avustusta Yhdysvaltain valtiolta. (*About Us - CIS®*, CIS.)

3.2 CIS Benchmarks

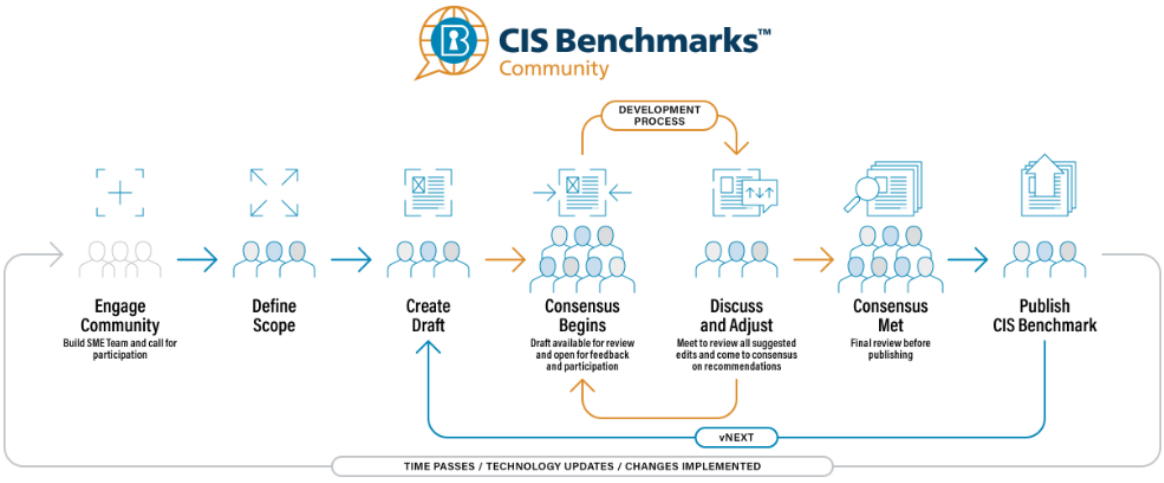
CIS Benchmarks on CIS-yhteisön tuottama suositeltujen turvallisuuden konfiguraatioiden kokoelma organisaatioiden ympäristöjen ja laitteiden kyberturvallisuuden koventamiseen.

Tällä hetkellä CIS tarjoaa yli sata erilaista CIS Benchmarkia 25 eri myyjien tarjoamien laitteistojen tarkistamiseen. (*CIS Benchmarks™ FAQ*, CIS.)

CIS perustelee CIS Benchmarks -palvelun luotettavuutta ja toimivuutta kehitysprosessin kautta. CIS käyttää "Consensus Development Process" -nimistä prosessia CIS Benchmarks -palvelun kehittämiseen. Prosessi tarkoittaa suomeksi yhteisymmärrykseen pohjautuvaa kehitysprosessia. (*CIS Benchmarks™ FAQ*, CIS.)

CIS:n kehitysprosessissa pohjana on "Subject Matter Experts" eli lyhennettynä SME. He ovat asiantuntijoita kaikilta eri sektoreilta, jotka yhdistävät tietotaitonsa uuden CIS Benchmarkin luomiseen tai vanhan päivittämiseen. Kehitysprosessi etenee ryhmän luomisen jälkeen laajuuden määrittämisellä (Kuva 1: Define scope), jonka jälkeen SME-ryhmä luo vedoksen, jonka pohjalta aloitetaan asioiden määritteleminen. Kun yhteisymmärrys saavutetaan, uusi CIS Benchmark julkaistaan. Jonkin ajan kuluttua, kun teknologia päivittyy ja kehittyy, prosessi aloitetaan alusta ja vanhaa Benchmarkkia päivitetään uusien parempien käytäntöjen mukaan. (*CIS Benchmarks™ FAQ*, CIS.)

Kuva 1: Havainnollistava kuva CIS:n kehitysprosessista



CIS Benchmark -palvelu kertoo käyttäjälleen miksi heidän kannattaa käyttää palvelun suosittelemia koventamis keinoja rikkomalla suositukset viiteen eri kategoriaan. Kategoriat ovat kuvaus, perustelu, vaikutus, tarkastus ja korjaus. Kuvaus kohdassa käyttäjälle tiivistetään ja kerrotaan mitä kyseinen suositus tarkoittaa. Perustelussa käyttäjälle perustellaan suosituksen tärkeys ja miksi se kannattaa korjata. Vaikutus kohdassa käyttäjälle selitetään suosituksen hyödyt turvallisuus etujen kautta. Tarkastuksessa kerrotaan, miten käyttäjä pystyy todistamaan tehneensä kyseisen kohdan esimerkiksi auditointia varten.

Viimeisenä korjaus, eli palvelu kertoo käyttäjälle askel askelelta kuinka kyseinen suositus pystytään laittamaan käytäntöön. (*CIS Benchmarks™ FAQ*, CIS.)

3.3 CIS-CAT Lite ja CIS-CAT Pro eroavaisuudet ja ominaisuudet

Kuten luvun alussa mainittiin, CIS-CAT Lite on ilmainen ja rajoitetumpi versio CIS-CAT Pro -palvelusta. Palveluiden eroavaisuuksista suurin on hinta. CIS-CAT Lite on ilmainen, mutta CIS-CAT Pro -palvelun käyttöoikeus maksaa 1470 dollaria eli noin 1354 euroa vuodessa alle 50 henkilön yritykselle "End user" tarkoitukseen. Tämä tarkoittaa CIS:n palveluiden käyttöä omien ympäristöjen ja datan suojaamiseen. (*CIS SecureSuite® Categories and Pricing*, CIS.)

CIS-CAT Pro- ja Lite -palveluiden suurimmat toiminnalliset eroavaisuudet tulevat Prossa mukana olevista lisäominaisuuksista, kuten mahdollisuus verrata muihin kuin CIS:n tekemiin turvallisuusohjeistuksiin, eri tiedostomuotojen käsittelyyn (XML, XCCDF, OVAL), käytetyn benchmarkin muokkausmahdollisuus CIS Workbenchin avulla, tulosten analysoinnin mahdollisuus CIS-CAT Pro Dashboard -palvelun avulla sekä mahdollisuus saada palvelun tuottama raportti teksti-, Excel- tai XML (ARF) -muodossa. (kuva 2). (*CIS-CAT Lite*, CIS.)

Eroavaisuuksista voidaan päätellä, että maksamalla CIS-CAT Pro -palvelusta voi saada suuria hyötyjä, mikäli palvelun hankkiva taho osaa käsitellä ja hyödyntää lisättyjä vertailu-, muokkaus- sekä formaattivaihtoehtoja. Pro-versio palvelusta on tehty selvästi alan ammattilaisille, jotka pystyvät saamaan siitä kaiken irti. Lite-versio on taas hyvin yksinkertainen sekä helppokäyttöinen versio, jonka avulla kyberturvallisuudesta ei niin perillä oleva henkilö pystyy tekemään peruskonfiguraatiota ympäristön kyberturvallisuuden parantamiseksi. Karkeasti Pro-versio on siis tarkoitettu tarkoituksenmukaisille tahoille, jotka osaavat käyttää version tarjoamia palveluita ja mahdollisuuksia hintalapun arvoisella tavalla, ja Lite-versio on tahoille, jotka eivät usko saavansa Pro-versiosta tarpeeksi irti hinnan hyväksymiseksi. Palvelut käyttävät samaa rakennetta, joten Lite-versio on myös hyvä askelkivi Pro-version hankkimiseen tarvittavan osaamisen ja kokemuksen keräämiseen. (*CIS-CAT Lite*, CIS.)

Kuva 2: CIS-CAT Pron ja Liten eroavaisuudet

	Lite	Pro
CIS Benchmarks supported	Select*	80+
Requires a license key		✓
Graphical User and Command Line Interface (GUI and CLI) Options	✓	✓
CIS Controls Assessment Module	✓	✓
Measure assessment results on conformity scale of 0-100	✓	✓
Evidence-based reports in HTML format	✓	✓
Perform unlimited scans	✓	✓
Assess against other SCAP content (i.e. DISA STIGS)		✓
Remotely assess endpoints	✓	✓
Customize CIS Benchmark content via CIS WorkBench		✓
Access to CIS Benchmarks in XML/XCCDF/OVAL		✓
Assess multiple machines at one time via centralized workflows	✓	✓
Analyze assessment results in CIS-CAT Pro Dashboard		✓
Evidence-based reports in Text, Excel, and XML(ARF) formats		✓

*Windows 10, Ubuntu, and Google Chrome

4 Testiympäristön luominen ja CIS-CAT Lite -palvelun käyttäminen

Tämän luvun tarkoitus on esitellä vertailun kohteena olevat palvelut ja käydä pääpiirteissään niiden toiminnallisuus ja asennukset läpi. Luvussa käydään myös läpi testiympäristönä toimivan Windows 11 Pro -käyttöjärjestelmän asennus

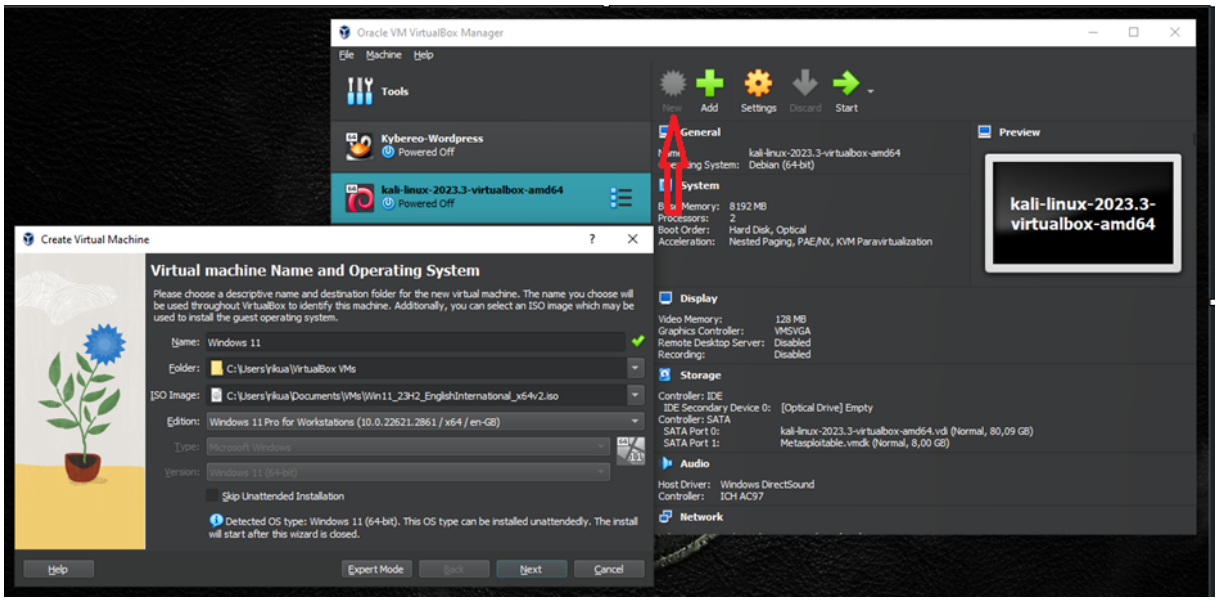
4.1 Testiympäristön luonti

Testiympäristön luominen aloitettiin täysin puhtaalla, juuri ladatulla ja asennetulla Windows 11 Pro -käyttöjärjestelmällä. Puhtaalla käyttöjärjestelmällä aloittaminen mahdollistaa täysin puhtaan testausympäristön testattavan palvelun käyttämiseen. Koskematon käyttöjärjestelmä ei ole vielä valmis turvalliseen käyttöön kyberturvallisuuden näkökulmasta, joten puhtaalla aloittaminen antaa varmasti tarpeeksi tuloksia tarkoituksenmukaisen arvioinnin tekemiseen CIS-CAT Lite -palvelusta.

Testiympäristö luotiin virtuaalikoneelle käyttäen Oracle VirtualBox -sovellusta ja Microsoftin sivuilta ladattua Windows 11 Pro -ISO-tiedostoa. Tämän pohjalta pystytään luomaan testikäyttöön sopiva natiivi Windows-ympäristö.

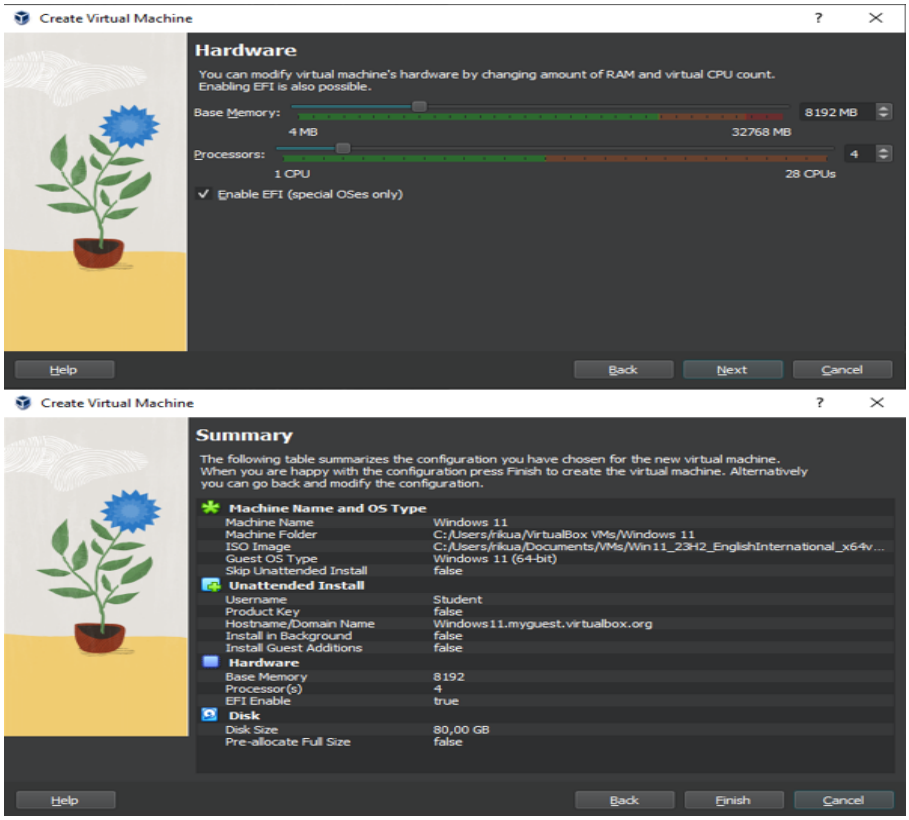
Testiympäristön luonti aloitettiin avaamalla Oracle VirtualBox -sovellus. VirtualBox sovelluksessa painettiin nuolella merkittyä ”New”-painiketta (Kuva 3). Tämä avaa ”Create virtual machine”-ikkunan, missä pystytään nimeämään laite ja valitsemaan aikasemmin ladattu Windows 11 Pro -ISO-tiedosto. Painamalla ”Next” painiketta päästään jatkamaan virtuaalikoneen luomista.

Kuva 3: Virtuaalikoneen luominen



Seuraavassa näkymässä (Kuva 4) pystytään säätämään virtuaalikoneen tehokkuutta. Virtuaalikoneelle asetettiin RAM muistia 8192mb ja neljä prosessoria, jotka riittävät tämän virtuaalikoneen käyttötarkoitukseen.

Kuva 4: Virtuaalikoneen RAM muistin ja prosessoreiden määrän asettaminen sekä laitteen yhteenveto



4.2 CIS-CAT Lite -ohjelmiston käyttöönotto

Virtuaalikone on nyt valmis käyttöön. Se voidaan käynnistää painamalla vihreää nuolta, jonka alla lukee ”Start” (Kuva 3). Käynnistämisen jälkeen virtuaalikoneelle ladataan CIS-CAT Lite -ohjelma. Lataaminen tapahtuu täyttämällä tietosi CIS-CAT Liten lataussivulla olevaan lomakkeeseen (Kuva 5). Tämän jälkeen lomakkeen täyttäjän asettamaan sähköpostiosoitteeseen lähetetään latauslinkki, jonka avulla CIS-CAT Lite pystytään lataamaan virtuaalikoneelle.

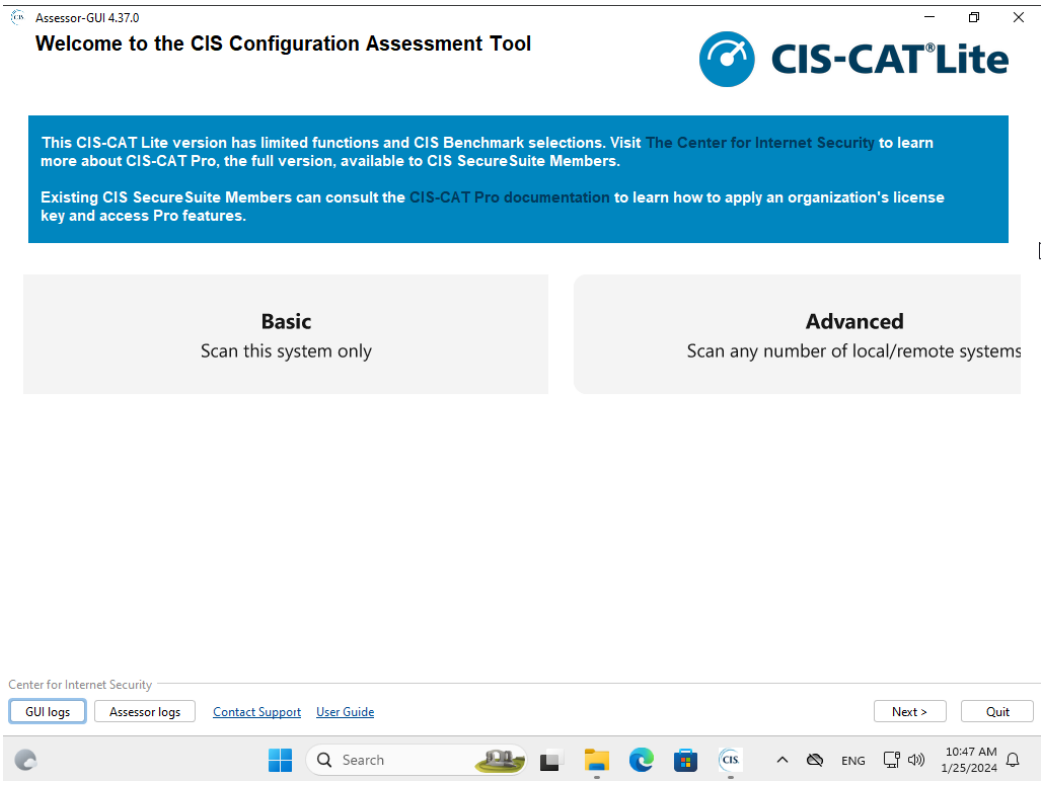
Kuva 5: CIS-CAT Liten latauslomake

CIS-CAT Lite -ohjelman lataaminen tapahtuu Center for Internet Securityn sivuilta täyttämällä lomake ja tilaamalla latauslinkki valitsemaasi sähköpostiosoitteeseen, joka käytiin lyhyesti läpi edellisessä luvussa. Lomake vaatii nimen, organisaation, roolin ja sen tarkoituksen, sähköpostin, työalan ja kotimaan täyttämistä. CIS eli Center for Internet Security haluaa myös tietää organisaatiosi työntekijöiden määrän ja mistä kuulit palvelusta. Puhelinnumeron täyttäminen lomakkeeseen on mahdollista, mutta se ei ole pakollista.

Lomakkeen täytön jälkeen saat sähköpostiisi linkin, jonka kautta pystyt lataamaan CIS-CAT Lite -arviointipalvelun. Lataamisen jälkeen löydät .zip-tiedoston, jonka purkamisen jälkeen

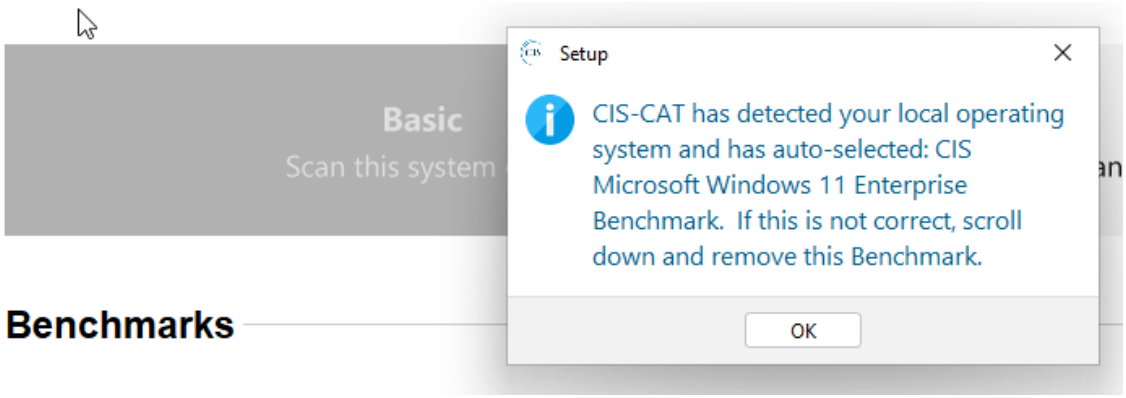
pystyt käyttämään ladattua palvelua avaamalla ohjelmatiedoston. Tämä käynnistää ohjelman ja saat ohjelmiston käyttöösi (kuva 6).

Kuva 6: CIS-CAT Liten etusivu



Pro-versio CIS-CAT -ohjelmistosta tuo lisää muokkausmahdollisuuksia ja analysointityökaluja, mitkä ovat hyödyllisiä laajemmissa tai edistyneemmissä ympäristöissä. Nämä sisältyvät Advanced-vaihtoehtoon. Tässä työssä on tarkoituksena tehdä yhdelle tietokoneelle muutoksia, joten basic CIS-CAT Lite täyttää tarpeelliset vaatimukset. Valitsemalla ”Basic”-vaihtoehdon (Kuva 6) pysytään aloittamaan tämän työn käyttötarkoitukseen riittävä arviointiprosessi. Tämä avaa uuden ikkunan mitä ennen CIS-CAT Lite valitsee virtuaalikoneen käyttöjärjestelmään sopivimman vertailupisteen eli benchmarkin (kuva 7).

Kuva 7: Vertailupiste suositus

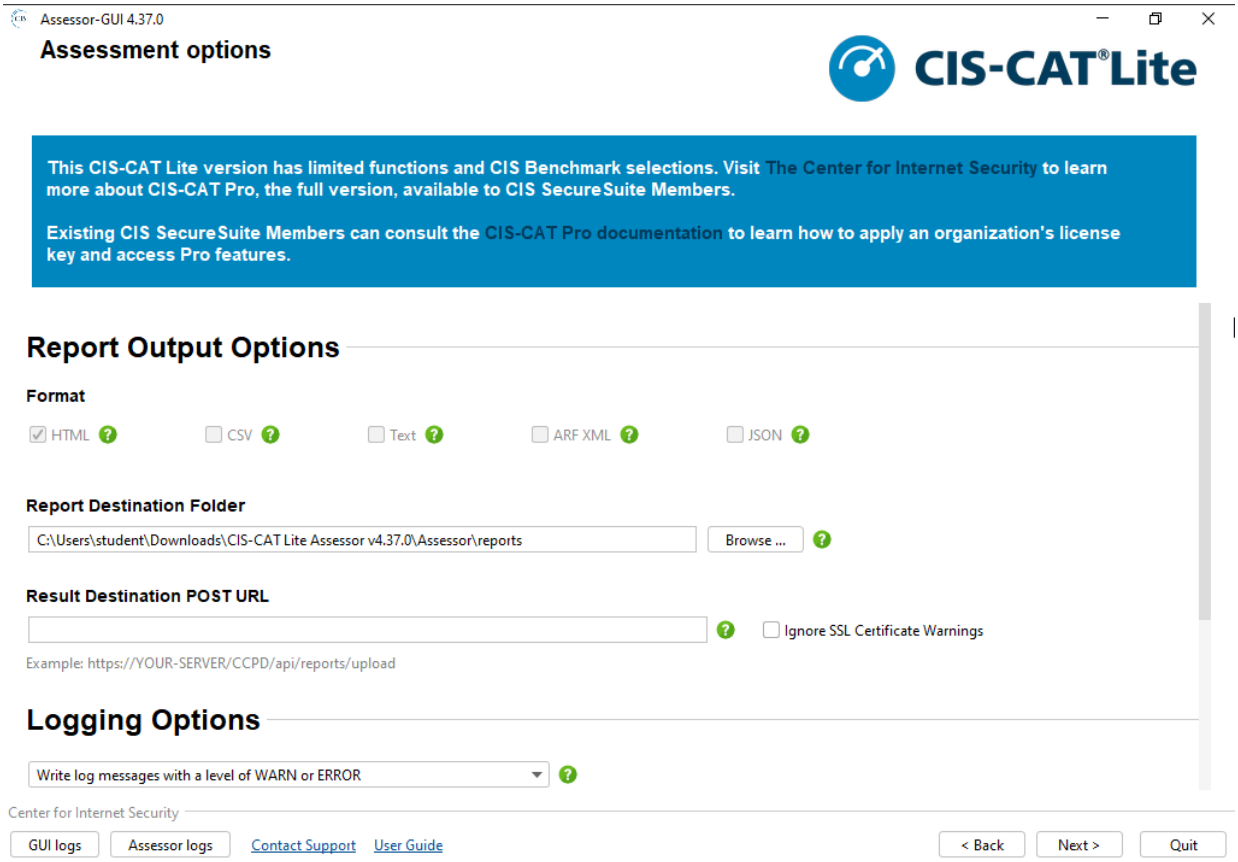


Tarkastamisen jälkeen painamalla ”Next” päästään viimeiseen ruutuun ennen palvelun käyttöä (Kuva 8). Tässä ruudussa pystytään vaikuttamaan minkälaisessa muodossa ohjelman tuottama raportti tulee olemaan ja mihin se tallennetaan.

Kuva 8: Vertailupisteen tarkastaminen

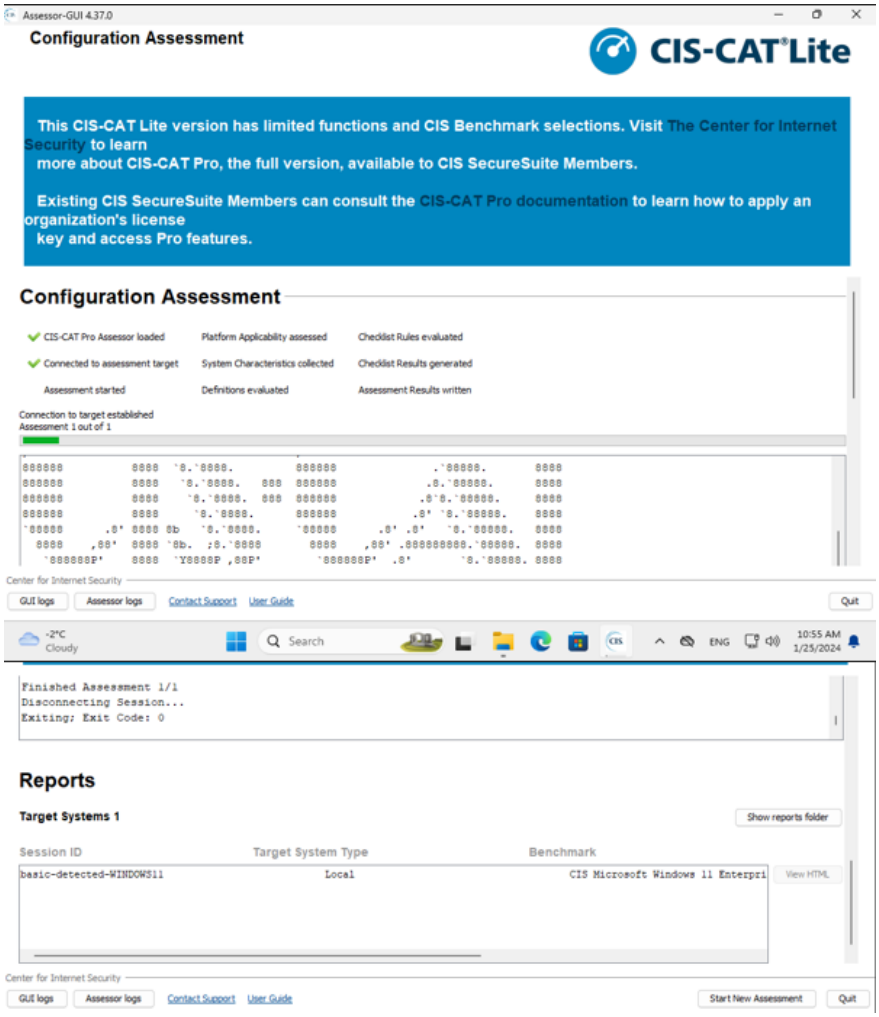
”Assesment options” ruudussa saat vielä valita formatointia ja esimerkiksi mihin lopullinen raportti tallentuu. (Kuva 9)

Kuva 9: Viimeiset valinnat ennen ohjelman ajamista ja tuloksia



Kuvassa 9 tehtyjen päätösten jälkeen ja ”next” näppäintä painamalla CIS-CAT Lite aloittaa varsinaisen toiminnan jonka kulkua pystytään seuraamaan konsoli outputilla mitä CIS-CAT Lite syöttää arvioinnin aikana (kuva 10).

Kuva 10: CIS-CAT Lite käynnissä



Nyt CIS-CAT Lite -palvelun käyttämisen alkuvaiheet on suoritettu, joten ohjelman tuottamien tulosten analysointi voidaan aloittaa.

4.3 CIS Cat liten tulosten läpikäynti

CIS Cat Lite -ohjelman ajaminen tuotti kaksi .log-päätteellä vahvistettua tiedostoa, yhden .txt-tiedoston ja valintojeni mukaan graafisen raportin .html-tiedostona. Graafinen raportti kertoi, missä tietokoneen konfiguroinneissa on puutteita ja mitkä läpäisivät CIS Cat Liten testit. Palvelu myös pisteytti konfiguroinnit ja kertoi maksimipisteet kustakin kategoriasta, jotta lukija pystyy näkemään, mitä vikoja arvioidusta ympäristöstä löytyi ja saamaan alustavan käsityksen siitä, millainen natiivin Windows 11 Pro -käyttöjärjestelmän kyberturvallisuuden taso on. Kokonaisuudessaan virtuaalikone läpäisi 82 testiä ja reputti 297. Täysin natiivi Windows 11 Pro -käyttöjärjestelmä sai CIS Cat Liten arvioinnissa 82/379 pistettä (Kuva 11).

Palvelu ilmoittaa tulokset myös prosentteina, joten kyseinen Windows -käyttöjärjestelmä läpäisi 22% testeistä.

Kuva 11: Yhteenvedon alku ja lopputulokset

Summary

Description	Tests						Scoring		
	Pass	Fail	Error	Unkn.	Man.	Exc.	Score	Max	Percent
1 Account Policies	2	8	0	0	1	0	2.0	10.0	20%
1.1 Password Policy	2	5	0	0	0	0	2.0	7.0	29%
1.2 Account Lockout Policy	0	3	0	0	1	0	0.0	3.0	0%
2 Local Policies	59	38	0	0	1	0	59.0	97.0	61%
2.1 Audit Policy	0	0	0	0	0	0	0.0	0.0	0%
2.2 User Rights Assignment	27	10	0	0	0	0	27.0	37.0	73%
2.3 Security Options	32	28	0	0	1	0	32.0	60.0	53%
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%
2.3.6 Domain member	6	0	0	0	0	0	6.0	6.0	100%
2.3.7 Interactive logon	1	6	0	0	0	0	1.0	7.0	14%
2.3.8 Microsoft network client	2	1	0	0	0	0	2.0	3.0	67%
2.3.9 Microsoft network server	2	3	0	0	0	0	2.0	5.0	40%
2.3.10 Network access	9	3	0	0	0	0	9.0	12.0	75%
2.3.11 Network security	2	7	0	0	1	0	2.0	9.0	22%
2.3.12 Recovery console	0	0	0	0	0	0	0.0	0.0	0%
2.3.13 Shutdown	0	0	0	0	0	0	0.0	0.0	0%
2.3.14 System cryptography	0	0	0	0	0	0	0.0	0.0	0%
2.3.15 System objects	2	0	0	0	0	0	2.0	2.0	100%
2.3.16 System settings	0	0	0	0	0	0	0.0	0.0	0%
2.3.17 User Account Control	5	3	0	0	0	0	5.0	8.0	62%
Total	82	297	0	0	2	0	82.0	379.0	22%

Valittuun vertailupisteeseen sisältyy kymmenen erilaista profiilia eri tarkoituksiin (Kuva 12). Palvelu valitsi profiilin käytön itse tarkastuksen aikana ja valitsi ensimmäisen tason "Corporate/Enterprise environment (general use)" -profiilin. Tämän profiilin tarkoitus on tuottaa aloituspiste organisaatioille, jotka ovat luomassa uutta ympäristöä. Profiilin kuvaus kertoo, että se on tehty käytännölliseksi ja antamaan selviä turvallisuushyötyjä ilman että suljettaisiin teknologian käyttökelpoisuutta hyväksyttävien keinojen ulkopuolella.

CIS-CAT Lite raportoi arvioidun ympäristön virheet selvästi ja käyttäjäystävällisesti. Palvelun tuottamassa raportissa kerrotaan selkeästi käsiteltävä vertailupiste ja oliko se konfiguroitu oikein vai ei. Raportti kertoo lyhyesti kunkin vertailupisteen tarkoituksen ja perustelee, miksi juuri tämä asia on tarkastettu. Jokaisessa kohteessa on yleensä muutama huomio, jotka auttavat asian korjaamisessa tai antavat lisätietoa siitä ja miksi sen korjaaminen on tärkeää.

Kaikissa virheellisissä kohdissa kerrotaan myös, miten kyseinen ongelma korjataan, ja raportissa käsitellään jokaisen vertailupisteen vaikutuksia turvallisuuteen.

Kuva 12: CIS Cat liten tarjoamat profiilit valittuun vertailupisteeseen

Profiles

This benchmark contains 10 profiles.The **Level 1 (L1) - Corporate/Enterprise Environment (general use)** profile was used for this assessment.

Title	Description
Level 1 (L1) - Corporate/Enterprise Environment (general use)	Items in this profile intend to: • be the starting baseline for most organizations; • be practical and prudent; • provide a clear security benefit; and • not inhibit the utility of the technology beyond acceptable means. Show Profile XML
Level 1 (L1) + BitLocker (BL)	This profile extends the "Level 1 (L1)" profile and includes BitLocker-related recommendations. Show Profile XML
Level 1 (L1) + Next Generation Windows Security (NG)	This profile extends the "Level 1 (L1)" profile and includes Next Generation Windows Security-related recommendations. Show Profile XML
Level 1 (L1) + BitLocker (BL) + Next Generation Windows Security (NG)	This profile extends the "Level 1 (L1)" profile and includes BitLocker and Next Generation Windows Security-related recommendations. Show Profile XML
Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)	This profile extends the "Level 1 (L1)" profile. Items in this profile exhibit one or more of the following characteristics: • are intended for environments or use cases where security is more critical than manageability and usability; • may negatively inhibit the utility or performance of the technology; and • limit the ability of remote management/access. **Note:** Implementation of Level 2 requires that **both** Level 1 and Level 2 settings are applied. Show Profile XML
Level 2 (L2) + BitLocker (BL)	This profile extends the "Level 2 (L2)" profile and includes BitLocker-related recommendations. Show Profile XML
Level 2 (L2) + Next Generation Windows Security (NG)	This profile extends the "Level 2 (L2)" profile and includes Next Generation Windows Security-related recommendations. Show Profile XML
Level 2 (L2) + BitLocker (BL) + Next Generation Windows Security (NG)	This profile extends the "Level 2 (L2)" profile and includes BitLocker and Next Generation Windows Security-related recommendations. Show Profile XML
BitLocker (BL) - optional add-on for when BitLocker is deployed	This profile contains BitLocker-related recommendations, if your organization chooses to use it. It is intended be an optional "add-on" to the Level 1 (L1) or Level 2 (L2) profiles. Show Profile XML
Next Generation Windows Security (NG) - optional add-on for use in the newest hardware and configuration environments	This profile contains advanced Windows security features that have specific configuration dependencies, and may not be compatible with all systems. It therefore requires special attention to detail and testing before implementation. If your environment supports these features, they are highly recommended as they have tangible security benefits. This profile is intended to be an optional "add-on" to the Level 1 (L1) or Level 2 (L2) profiles. Show Profile XML

Heti raportin alussa mainitaan, mitä profiilia CIS-CAT Lite käytti. Profiilien erot määrittyvät testatun ympäristön turvallisuustason perusteella, ja palvelu valitsi käytettäväksi tason 1 profiilin, mikä on tarkoitettu luomaan hyvän, mutta turvallisen pohjan organisaatioiden käyttöön. Taso 1 tarjoaa selkeän turvallisuushyödyn ja pyrkii olemaan rajoittamatta teknologian käyttöä sulkemalla turvallisuusasetukset pois. Ensimmäisen tason suojauksen päätarkoitus on pienentää ympäristön hyökkäyspinta-alaa samalla pitäen laitteistot käyttökelpoisina. (*CIS Benchmarks™ FAQ*, CIS.)

Tason 2 suojaus on tarkoitettu ympäristöille, joissa turvallisuus on prioriteetti. Tason 2 suositellut konfiguraatiot voivat vaikuttaa organisaation ympäristöön merkittävästi, jos niitä ei toteuteta huolellisesti ja ammattimaisesti. (*CIS Benchmarks™ FAQ*, .)

Raportin pituus on yllättävä ja se kuinka laajasti ja yksityiskohtaisesti raportissa selitetään jokainen kohta on erittäin positiivista. Syiden ja lyhyiden kuvausten antaminen palvelun käyttäjälle on erittäin fiksua ja todennäköisesti lisää arvioinnin tekijän ymmärrystä aiheeseen liittyen ja halua korjata esiin tuodut ongelmat.

5 CIS-CAT Lite palvelun analyysi ja arviointi

On selvää, että kaikkien raportissa esiintuotujen ongelmien korjaaminen tämän työn puitteissa ei ole tarkoituksenmukaista. Raportissa on 19 lukua, jotka jakavat kohteet järkeviin kokonaisuuksiin. Työssä korjataan 10 kohtaa raportin antamien ohjeiden mukaisesti, jonka jälkeen CIS-CAT Lite ajetaan uudestaan ja tarkastetaan, löytääkö CIS-CAT Lite aiemmin tehdyt korjaukset ja näkyvätkö ne uudessa raportissa.

5.1 Korjattavien ongelmien valinta, esittely ja korjaaminen

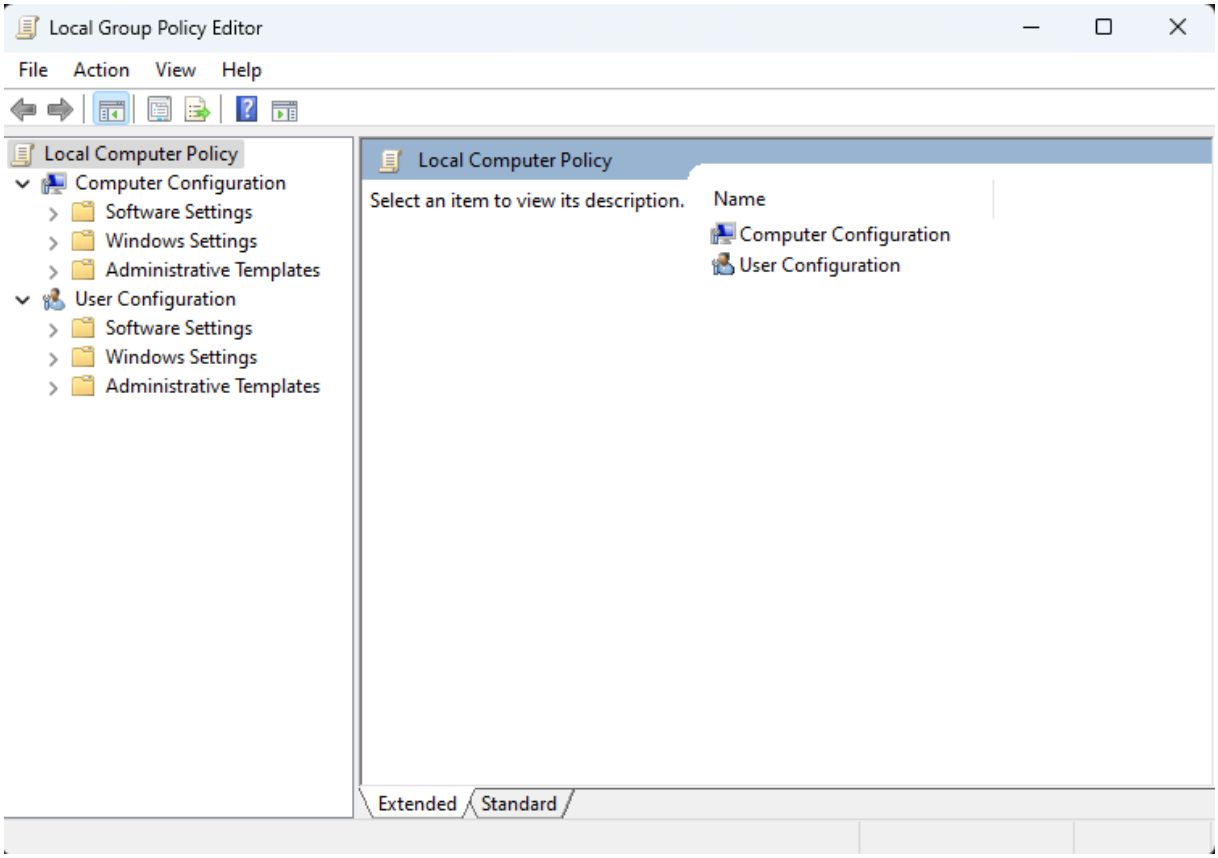
Korjattavien kohtien valinta tapahtuu suhteellisen satunnaisesti, jotta korjattavat kohdat kattavat mahdollisimman laajan ja monipuolisen kirjon. Raportti on jaettu useaan lukuun ja alaotsikkoon, mutta kaikissa luvuissa ei ole raportin mukaan korjattavia ongelmia. Valinnat pyritään tekemään mahdollisimman tärkeistä kohdista.

Korjattavat kohdat valittiin suhteellisen satunnaisesti, jotta niiden sisältö ja vaikutus ovat mahdollisimman monipuolisia, ja lukija saa yleiskäsityksen siitä, millaisia kyberturvallisuusheikkouksia uuteen Windows-ympäristöön kohdistuu. Kohdat käydään läpi kertomalla kohteen perusasiat raportista otetun kuvan avulla. Tämän jälkeen selvitetään, miten kyseinen kohta voidaan korjata ja mitä korjaamiseen vaaditaan.

5.2 Microsoft Group Policy

Kaikki korjaukset tehdään Microsoft Group Policy -työkalun avulla, joka on Windowsiin sisäänrakennettu käyttöliittymä käyttäjä- ja tietokoneasetusten hallitsemiseen. Group Policyä voidaan käyttää myös tietokoneen asetusten hallitsemiseen. Tämän avulla pystytään tekemään graafista käyttöliittymää käyttämällä korjauksia laitteen sekä käyttäjien konfigurointeihin. Seuraavan luvun korjaukset turvallisuuskonfigurointeihin tehdään navigoimalla Group Policyn graafisen käyttöliittymän avulla jokaisen korjattavan kohdan omien ohjeistusten mukaan. Yleensä ohjeistukset ovat niin sanottu ”path” eli reitti, jonka pitkin navigoidaan ja etsitään korjauksien kohteet Group Policyn rakenteesta. (Archiveddocs, 2016) (Kuva 13)

Kuva 13: Group policy käyttöliittymä



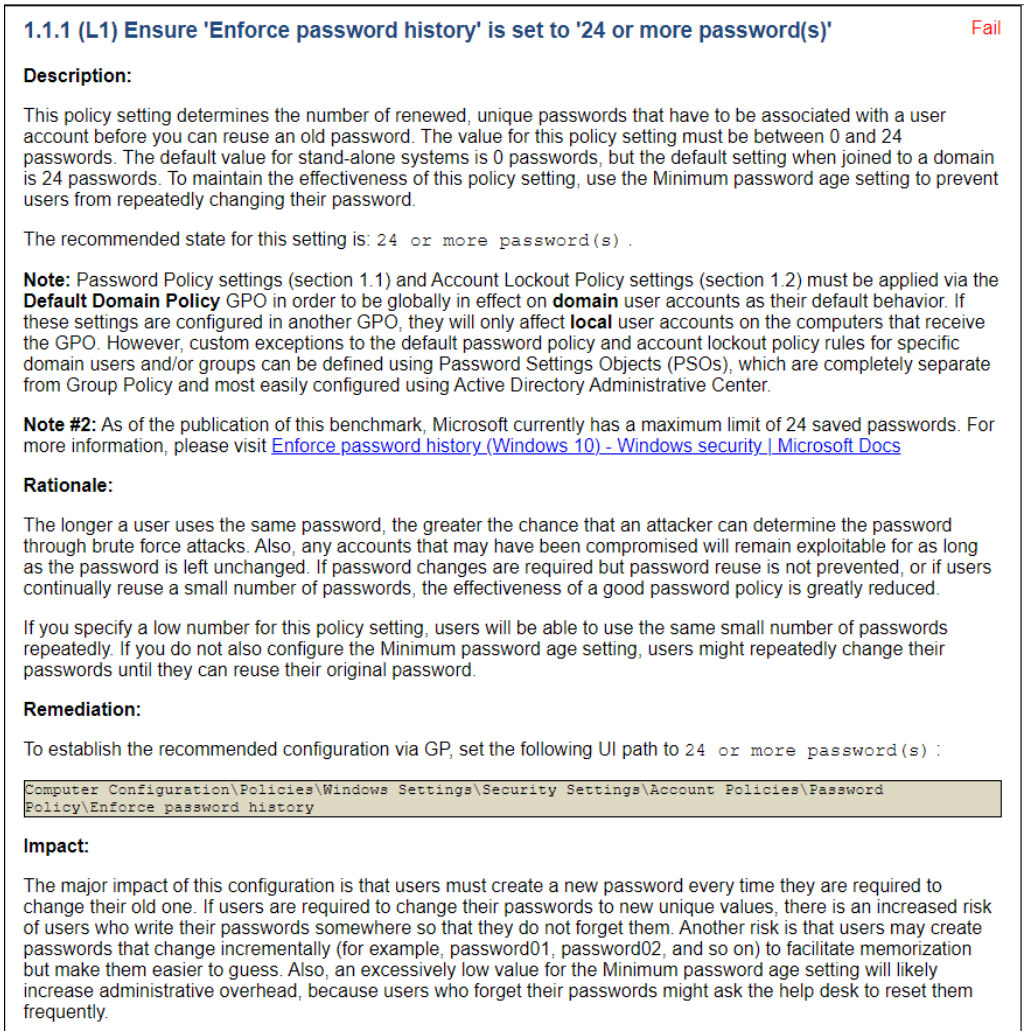
5.3 Korjauksien tekeminen

Korjaukset tehdään täysin CIS-CAT Liten suosittelemalla tavalla. Korjattavat kohdat jaetaan yksittäin alalukuihin tämän luvun alle. Jokaisessa kohdassa pohditaan ja käydään kohta läpi yksityiskohtaisesti sekä tehdään tarvittavat muutokset raportin ohjeiden mukaisesti.

5.3.1 ’Ensure password history’ is set to ’24 or more password(s)’

Ensimmäinen korjattava kohta (Kuva 14) käsittelee käyttäjän salasanojen luotettavuutta määrittämällä, kuinka monta uniikkia ja uudistettua salasanaa pitää olla asetettuna ennen kuin käyttäjä voi käyttää samanlaista salasanaa uudelleen. Perusasetus tälle on 0, mutta raportissa suositellaan tämän asetuksen asettamista luvulle 24 tai suuremmalle. Tämä tarkoittaa, että kun asetuksen arvo on vaihdettu, käyttäjät eivät voi käyttää samaa salasanaa 24 uudistetun salasanan välein.

Kuva 14: Salasana historia



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)` :

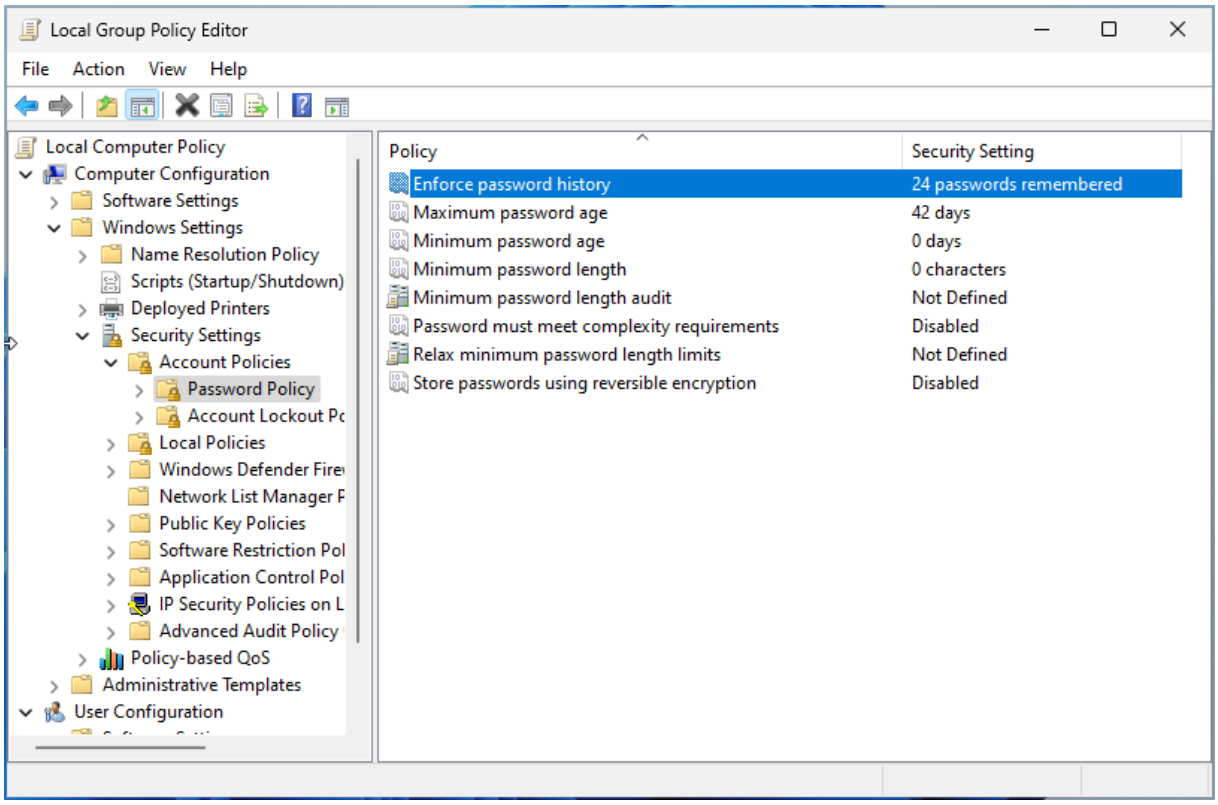
```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password
Policy\Enforce password history
```

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, and so on) to facilitate memorization but make them easier to guess. Also, an excessively low value for the Minimum password age setting will likely increase administrative overhead, because users who forget their passwords might ask the help desk to reset them frequently.

Korjaaminen tapahtuu Group Policyn muuttamalla "Remediation" -kohdassa mainittua GP-reittiä kohtaan "Enforce password history" arvoon 24 (Kuva 15). Vasemmalla puolella pystytään seuraamaan reittiä, miten korjattava kohta löydettiin, ja tässä kuvassa korjattu kohta on korostettu sinisellä värillä.

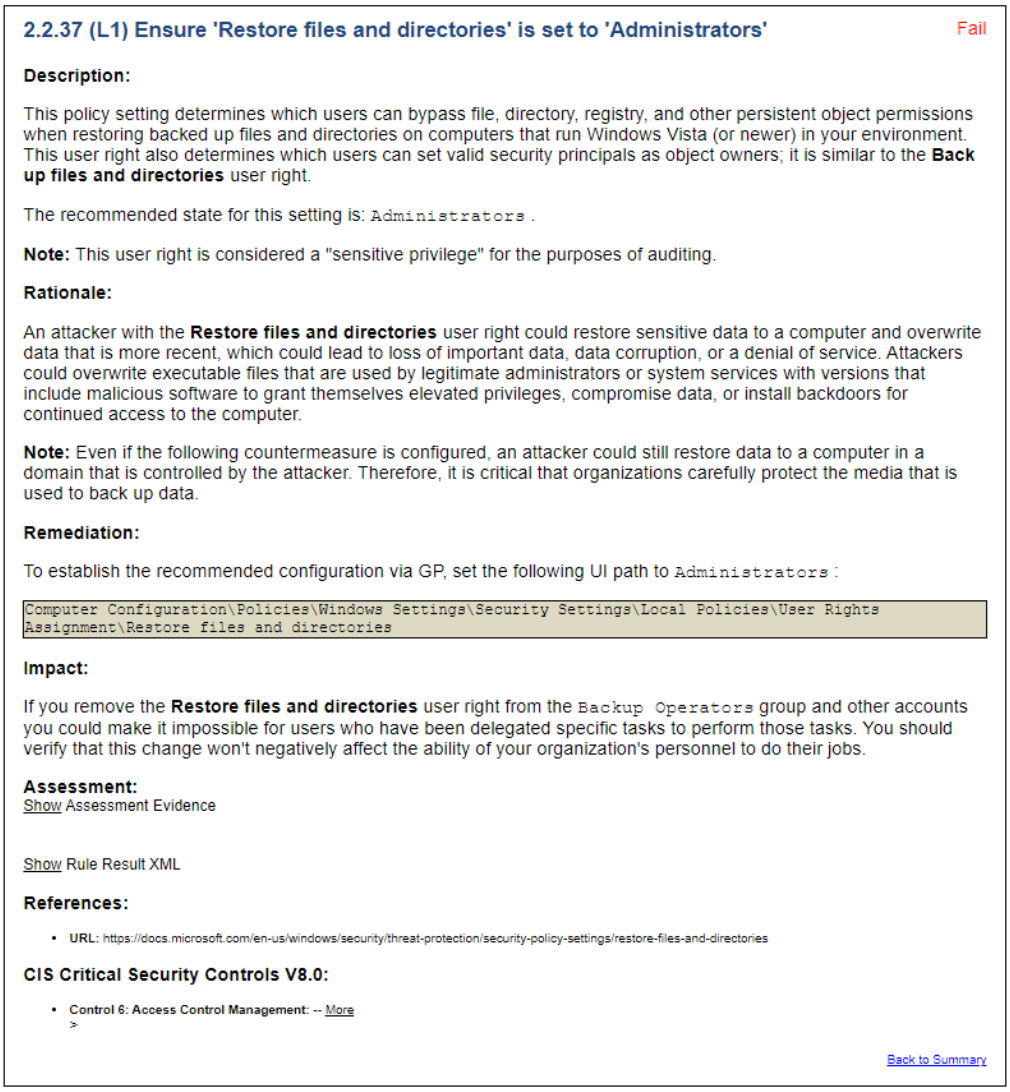
Kuva 15: Salasana historian korjaus



5.3.2 Ensure ’Restore files and directories’ is set to ‘Administrators’

Toinen korjattava kohta (kuva 16) käsittelee tiedostojen ja hakemistojen palauttamista ja tämän asetuksen rajoittamista pelkästään admin-käyttäjille. Tämä kohta määrittää, mitkä käyttäjät voivat ohittaa tiedostojen, hakemistojen, rekisterin ja muiden pysyvien objektien käyttöoikeudet tiedostojen tai hakemistojen palauttamisprosessissa kyseiselle tietokoneelle. Tämän asetuksen tarkoitus on estää mahdollisia hyökkääjiä palauttamasta vanhempia tiedostoja, joilla he voivat korvata uudemmat ja paremmat tiedostot. Tämän avulla hyökkääjät voisivat laajentaa hallintaansa koneessa. Tämän muutoksen haittapuolena on, että se saattaa joissakin ympäristöissä vaikeuttaa käyttäjien työtä, ja raportissa kehotetaan varmistamaan, että tämä ei vaikuta kehenkään ennen kuin muutokset tehdään.

Kuva 16: Tiedostojen ja hakemistojen palauttaminen



2.2.37 (L1) Ensure 'Restore files and directories' is set to 'Administrators' Fail

Description:

This policy setting determines which users can bypass file, directory, registry, and other persistent object permissions when restoring backed up files and directories on computers that run Windows Vista (or newer) in your environment. This user right also determines which users can set valid security principals as object owners; it is similar to the **Back up files and directories** user right.

The recommended state for this setting is: `Administrators` .

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

An attacker with the **Restore files and directories** user right could restore sensitive data to a computer and overwrite data that is more recent, which could lead to loss of important data, data corruption, or a denial of service. Attackers could overwrite executable files that are used by legitimate administrators or system services with versions that include malicious software to grant themselves elevated privileges, compromise data, or install backdoors for continued access to the computer.

Note: Even if the following countermeasure is configured, an attacker could still restore data to a computer in a domain that is controlled by the attacker. Therefore, it is critical that organizations carefully protect the media that is used to back up data.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators` :

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Restore files and directories
```

Impact:

If you remove the **Restore files and directories** user right from the `Backup Operators` group and other accounts you could make it impossible for users who have been delegated specific tasks to perform those tasks. You should verify that this change won't negatively affect the ability of your organization's personnel to do their jobs.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/restore-files-and-directories

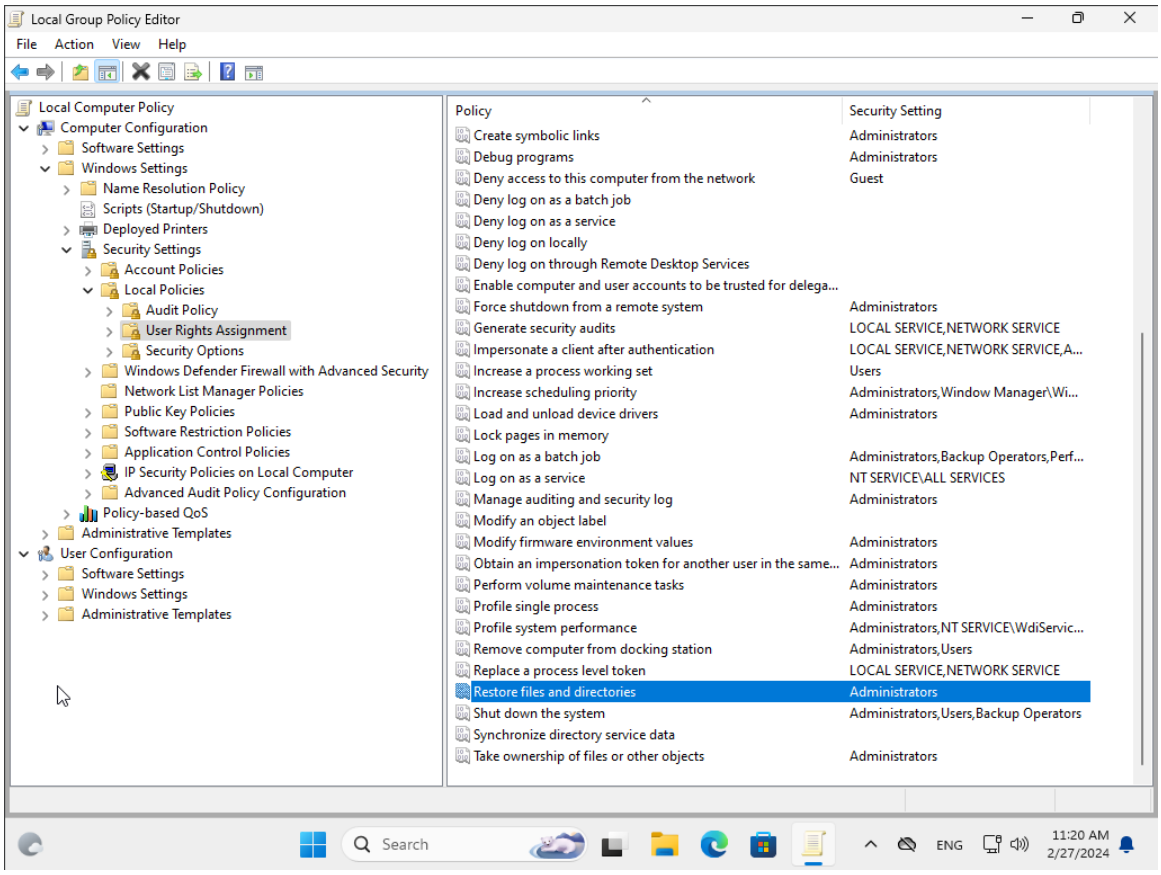
CIS Critical Security Controls V8.0:

- **Control 6: Access Control Management:** -- More >

Back to Summary

Kuvassa 17 nähdään kuinka tämä kohta korjattiin. Oikean kohdan löytäminen tapahtui jälleen korjaus kohdassa annetun GP reitin avulla. Kuvassa 17 nähdään vasemassa sarakkeessa kuljettu reitti sekä korostettuna korjattu kohta uudella parannetulla arvolla.

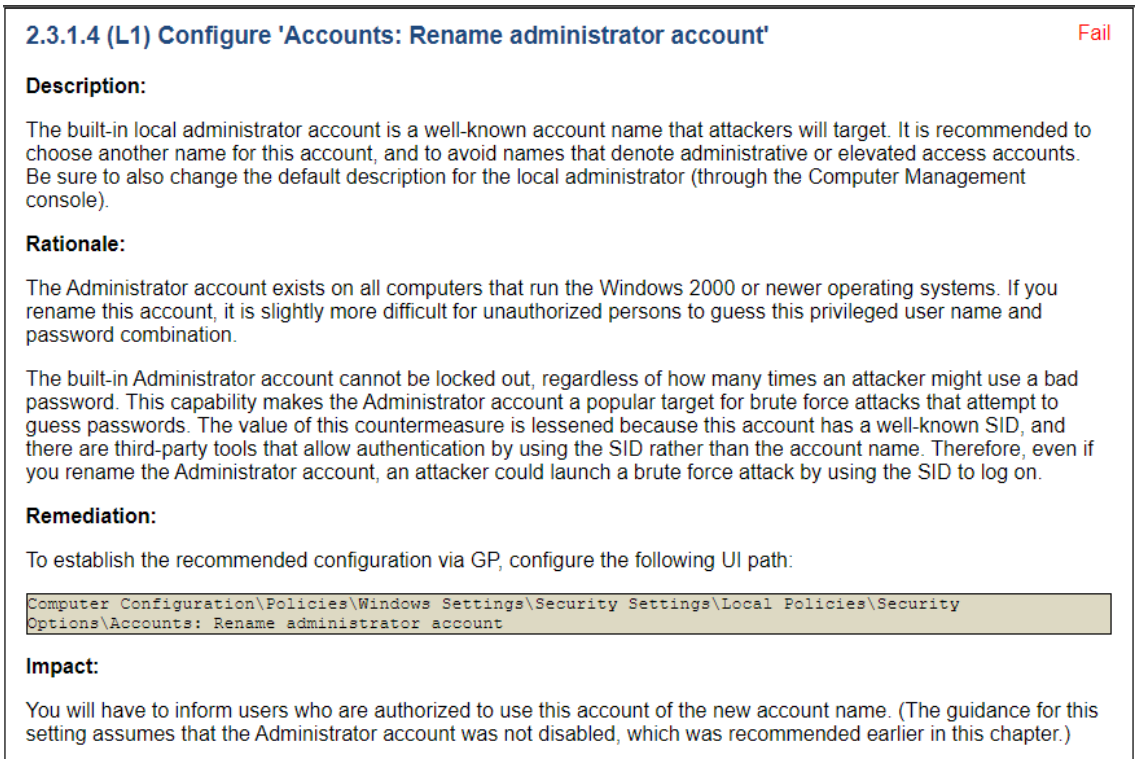
Kuva 17: Tiedostojen ja hakemistojen palauttamisen korjaaminen



5.3.3 Configure ’Accounts: Rename administrator account’

Kolmannessa kohdassa (kuva 18) kehotetaan vaihtamaan ”Administrator” käyttäjän oletus käyttäjänimi. Yleisesti tunnettua käyttäjänimeä pystytään käyttämään hyväkseen hyökkäystarkoituksessa.

Kuva 18: Admin käyttäjän uudelleen nimeäminen



2.3.1.4 (L1) Configure 'Accounts: Rename administrator account' Fail

Description:

The built-in local administrator account is a well-known account name that attackers will target. It is recommended to choose another name for this account, and to avoid names that denote administrative or elevated access accounts. Be sure to also change the default description for the local administrator (through the Computer Management console).

Rationale:

The Administrator account exists on all computers that run the Windows 2000 or newer operating systems. If you rename this account, it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination.

The built-in Administrator account cannot be locked out, regardless of how many times an attacker might use a bad password. This capability makes the Administrator account a popular target for brute force attacks that attempt to guess passwords. The value of this countermeasure is lessened because this account has a well-known SID, and there are third-party tools that allow authentication by using the SID rather than the account name. Therefore, even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

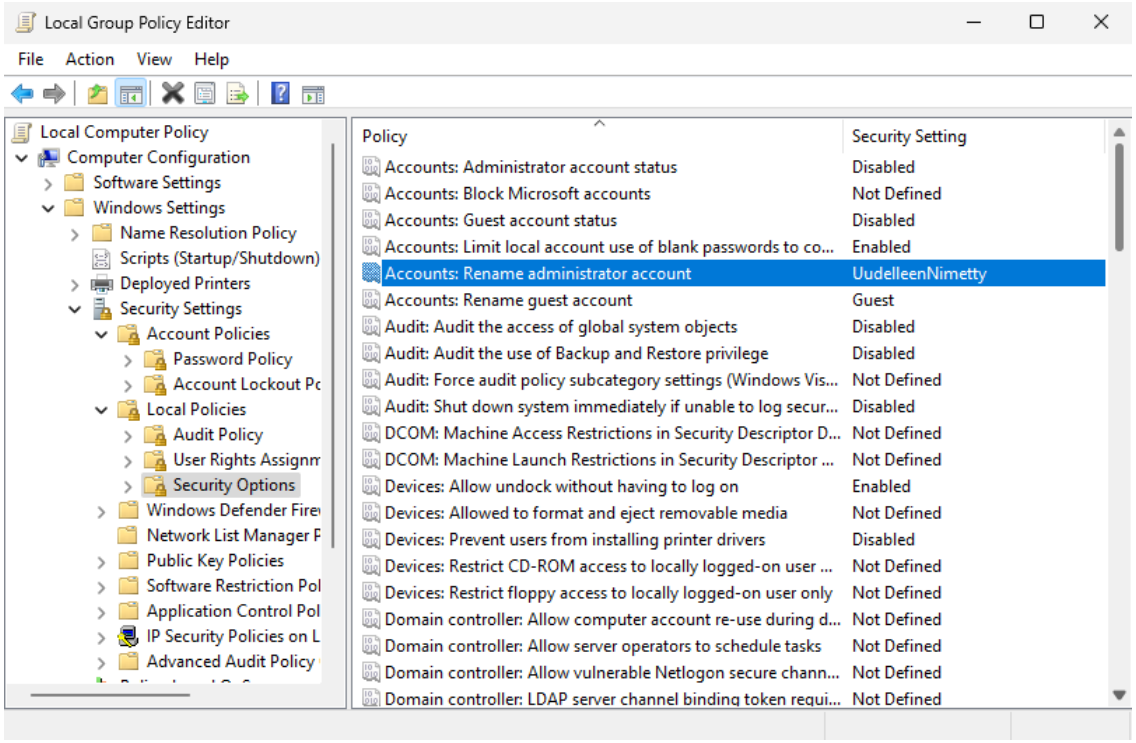
```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Accounts: Rename administrator account
```

Impact:

You will have to inform users who are authorized to use this account of the new account name. (The guidance for this setting assumes that the Administrator account was not disabled, which was recommended earlier in this chapter.)

Käyttäjänimen vaihtaminen suojaa ympäristöä hyökkäyksiä kohtaan. Kuvassa 19 nähdään kolmannen kohdan korjaustoimenpide käyttäen kuvan 18 korjaus kohdassa annettua GP reittiä. Käyttäjän uusinimi kannattaa asettaa omakohtaiseksi ja mahdollisimman uniikiksi, koska se heikentää hyökkääjien mahdollisuuksia löytää ympäristön admin käyttäjä mahdollisen järjestelmään murtautumisen yhteydessä.

Kuva 19: Admin käyttäjän uudelleen nimeäminen ja sen korjaus



5.3.4 Ensure ’Interactive logon: Machine inactivity limit’ is set to ‘900 or fewer second(s), but no 0’

Neljännessä kohdassa käsitellään laitteen näytönsäästäjän ajastinta (kuva 20). Näytönsäästäjän ajastin kannattaa asettaa 900 sekunnin ja yhden sekunnin välille. Jos tämän asetuksen asettaa nollaan sekunttiin se poistaa näytönsäästäjän päältä. Näytönsäästäjä kannattaa olla päällä, koska jos käyttäjä unohtaa lukita koneen poistuttuaan siltä, näytönsäästäjä lukitsee koneen ja estää muiden ihmisten pääsyn tietokoneelle.

Kuva 20: Näytönsäästäjän ajastimen säätö

2.3.7.4 (L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' — Fail

Description:

Windows notices inactivity of a logon session, and if the amount of inactive time exceeds the inactivity limit, then the screen saver will run, locking the session.

The recommended state for this setting is: `900 or fewer second(s), but not 0`.

Note: A value of `0` does not conform to the benchmark as it disables the machine inactivity limit.

Rationale:

If a user forgets to lock their computer when they walk away it's possible that a passerby will hijack it.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `900 or fewer seconds, but not 0`:

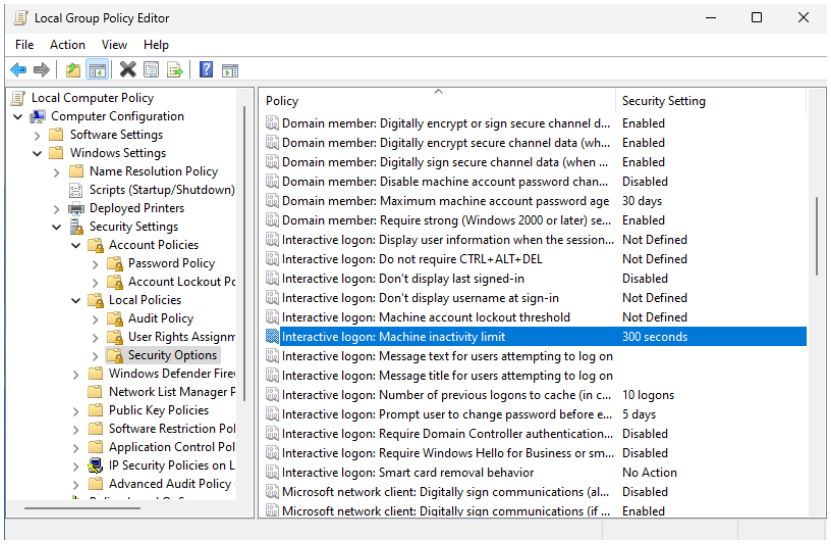
```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine inactivity limit
```

Impact:

The screen saver will automatically activate when the computer has been unattended for the amount of time specified. The impact should be minimal since the screen saver is enabled by default.

Kuvassa 21 nähdään korjauskohdan GP-reitin tulos (kuva 20) sekä korjattu arvo. Tässä kohdassa päätettiin asettaa ajastimeksi 300 sekunttia eli 5 minuuttia

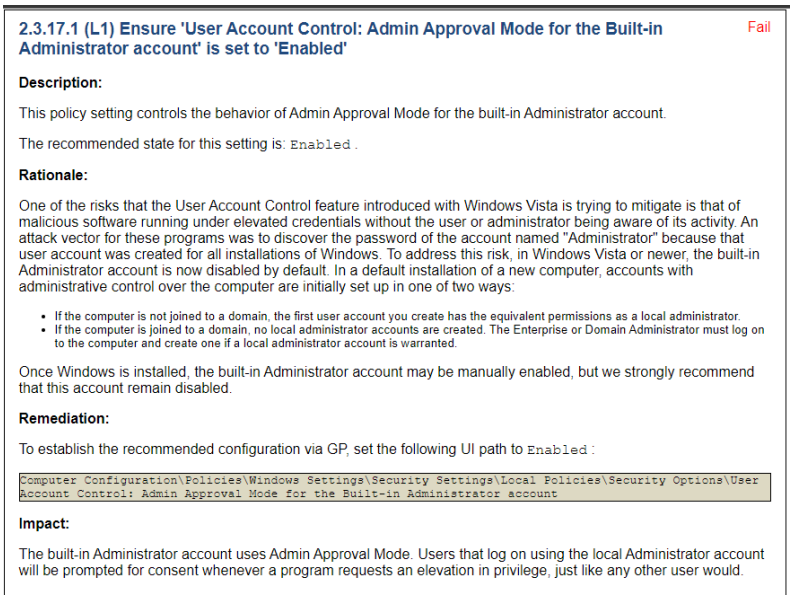
Kuva 21: Näytönsäästäjän ajastimen korjaus



5.3.5 Ensure ’User Account Control: Admin Approval Mode for the Built-in Administrator account is set to ‘Enabled’

Viides kohta (Kuva 22) käsittelee sisäänrakennetun admin-käyttäjän muutosten tekokykyä lisäämällä vahvistusnäkymän ennen jokaista tehtyä muutosta varmistamaan, että käyttäjä haluaa tehdä kyseisen muutoksen järjestelmään. Asetuksen tarkoitus on estää mahdollisten salattujen haittaohjelmien toimintaa salaa korotetuilla oikeuksilla. Yleensä Windowsin normaali administraattorikäyttäjä on oletusarvoisesti poissa käytöstä, mutta kaikki varotoimenpiteet kannattaa ottaa käyttöön.

Kuva 22: Admin hyväksyntä tila



2.3.17.1 (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' Fail

Description:

This policy setting controls the behavior of Admin Approval Mode for the built-in Administrator account.

The recommended state for this setting is: `Enabled`.

Rationale:

One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. An attack vector for these programs was to discover the password of the account named "Administrator" because that user account was created for all installations of Windows. To address this risk, in Windows Vista or newer, the built-in Administrator account is now disabled by default. In a default installation of a new computer, accounts with administrative control over the computer are initially set up in one of two ways:

- If the computer is not joined to a domain, the first user account you create has the equivalent permissions as a local administrator.
- If the computer is joined to a domain, no local administrator accounts are created. The Enterprise or Domain Administrator must log on to the computer and create one if a local administrator account is warranted.

Once Windows is installed, the built-in Administrator account may be manually enabled, but we strongly recommend that this account remain disabled.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

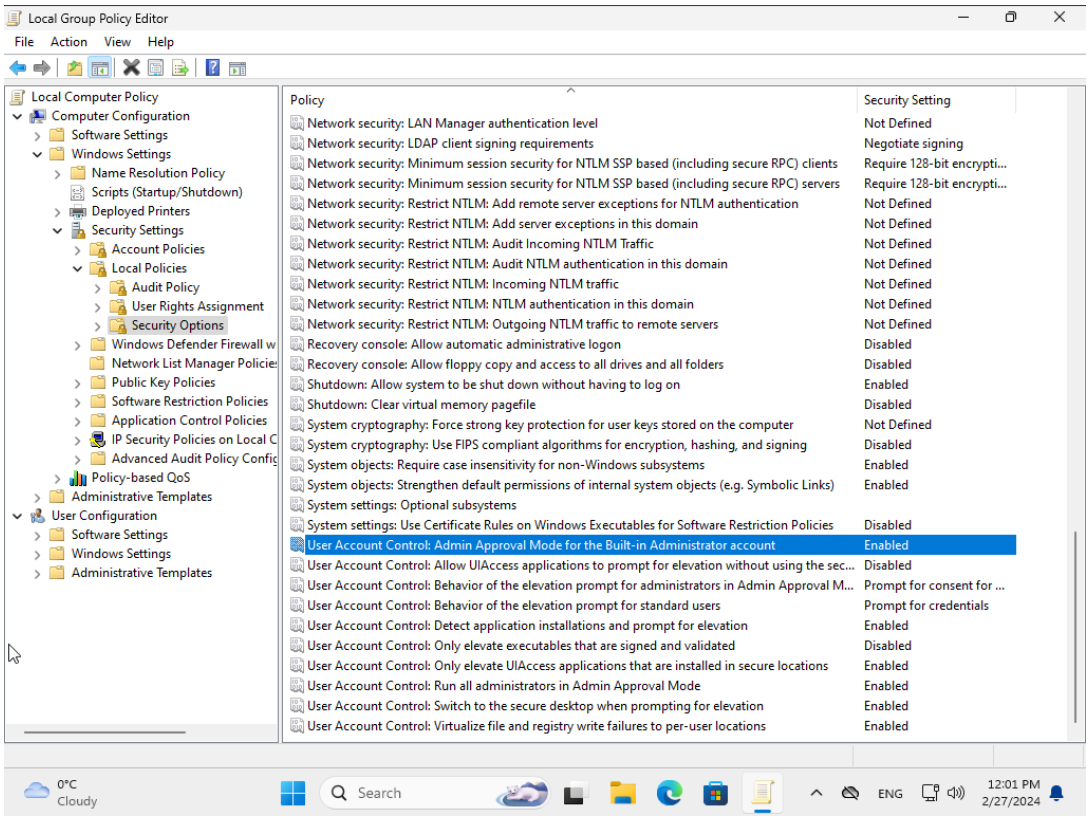
```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Admin Approval Mode for the Built-in Administrator account
```

Impact:

The built-in Administrator account uses Admin Approval Mode. Users that log on using the local Administrator account will be prompted for consent whenever a program requests an elevation in privilege, just like any other user would.

Kuvassa 23 nähdään jälleen GP-reitin (kuva 22) avulla löydetty asetus ja sen korjaaminen raportin suosittelemaan tilaan.

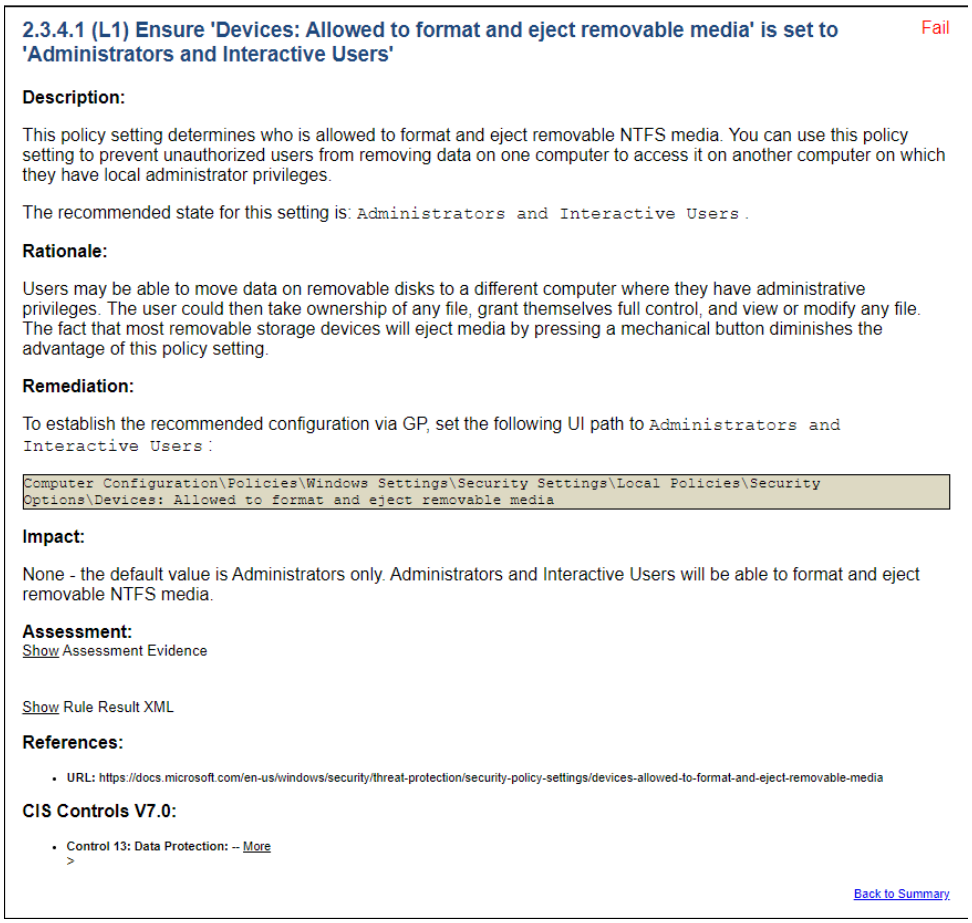
Kuva 23: Admin hyväksyntä tilan korjaus



5.3.6 Ensure ’Devices: Allowed to format and eject removable media’ is set to ‘Administrators and Interactive Users’

Kuudennessa kohdassa (Kuva 24) käsitellään poistettavan median formatointia ja siirtämistä sekä tämän prosessin käyttöoikeuksia. Tämä asetus estää käyttäjiä siirtämästä kyseisiä tiedostoja ympäristöön, missä heillä ei ole ylläpitäjän oikeuksia, ja sitten siirtämästä niitä ympäristöön, missä heillä on ylläpitäjän oikeudet, esimerkiksi käyttämällä muistitikkua. Siirron jälkeen käyttäjä voi tutkia ja lukea mahdollisen datan ylläpitäjän oikeuksilla. Tämän käytännön heikkous on raportin mukaan se, että suurin osa ulkoisista tallennuslaitteista lataa tiedot mekaanisen näppäimen kautta.

Kuva 24: Siirrettävän median käyttöoikeudet



2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators and Interactive Users' Fail

Description:

This policy setting determines who is allowed to format and eject removable NTFS media. You can use this policy setting to prevent unauthorized users from removing data on one computer to access it on another computer on which they have local administrator privileges.

The recommended state for this setting is: `Administrators and Interactive Users`.

Rationale:

Users may be able to move data on removable disks to a different computer where they have administrative privileges. The user could then take ownership of any file, grant themselves full control, and view or modify any file. The fact that most removable storage devices will eject media by pressing a mechanical button diminishes the advantage of this policy setting.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators and Interactive Users`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Allowed to format and eject removable media
```

Impact:

None - the default value is Administrators only. Administrators and Interactive Users will be able to format and eject removable NTFS media.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/devices-allowed-to-format-and-eject-removable-media

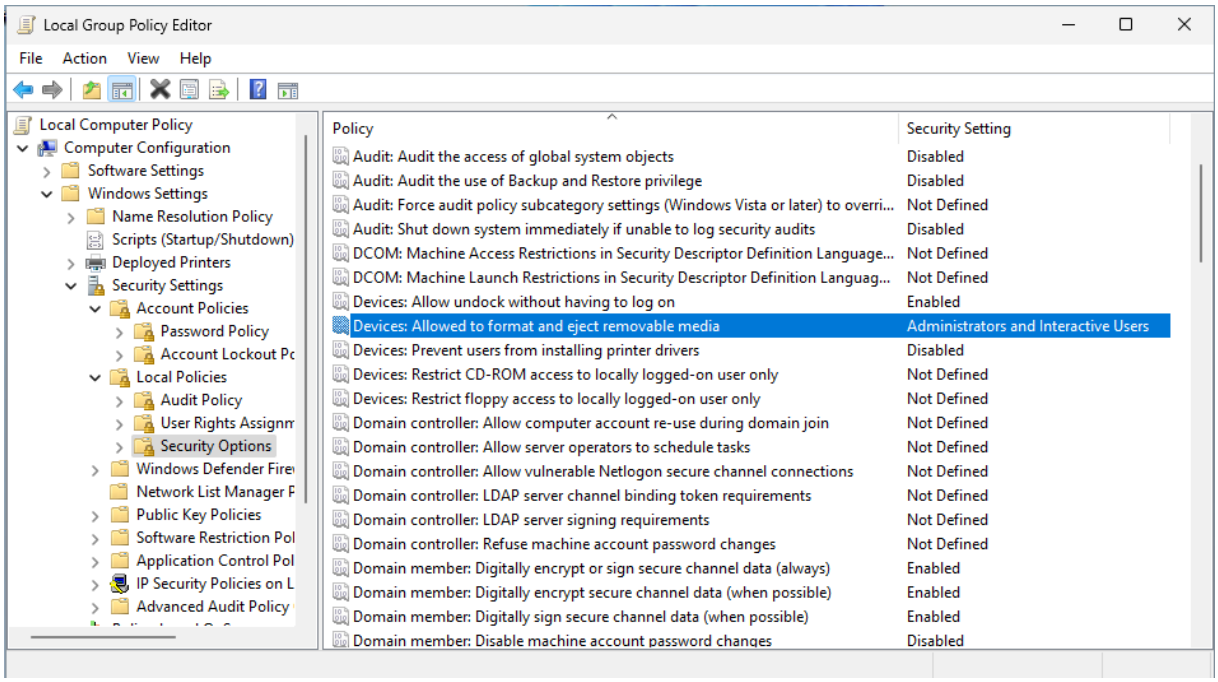
CIS Controls V7.0:

- **Control 13: Data Protection: --** More >

Back to Summary

Kuvassa 25 nähdään GP-reitin avulla (Kuva 24) löydetty asetus ja sen säätäminen raportin ehdotuksen mukaiseksi.

Kuva 25: Siirrettävän median käyttöoikeuksien korjaus



5.3.7 Ensure ’Turn off picture password sign-in’ is set to ‘Enabled’

Seitsemäs kohta (kuva 26) käsittelee kuvana toimivan salasanan käyttämistä kirjautumiseen. Kuvina toimivat salasanat eivät vastaa tietoturvallisuudessa normaalien salasanojen suojaustasoa, joten tämä asetus kannattaa asettaa pois päältä. Kuvina toimivia salasanoja on helppo muistaa tai jopa havaita vahingossa esimerkiksi toimistolla, jolloin sivullinen voi nähdä hiiren liikkeet ja kirjautua ympäristöön kuvina toimivan salasanan käyttäjänä.

Kuva 26: Kuva salasanalla kirjautumisen poistaminen

18.9.27.6 (L1) Ensure 'Turn off picture password sign-in' is set to 'Enabled' Fail

Description:

This policy setting allows you to control whether a domain user can sign in using a picture password.

The recommended state for this setting is: `Enabled` .

Note: If the picture password feature is permitted, the user's domain password is cached in the system vault when using it.

Rationale:

Picture passwords bypass the requirement for a typed complex password. In a shared work environment, a simple shoulder surf where someone observed the on-screen gestures would allow that person to gain access to the system without the need to know the complex password. Vertical monitor screens with an image are much more visible at a distance than horizontal key strokes, increasing the likelihood of a successful observation of the mouse gestures.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled` :

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Turn off picture password sign-in
```

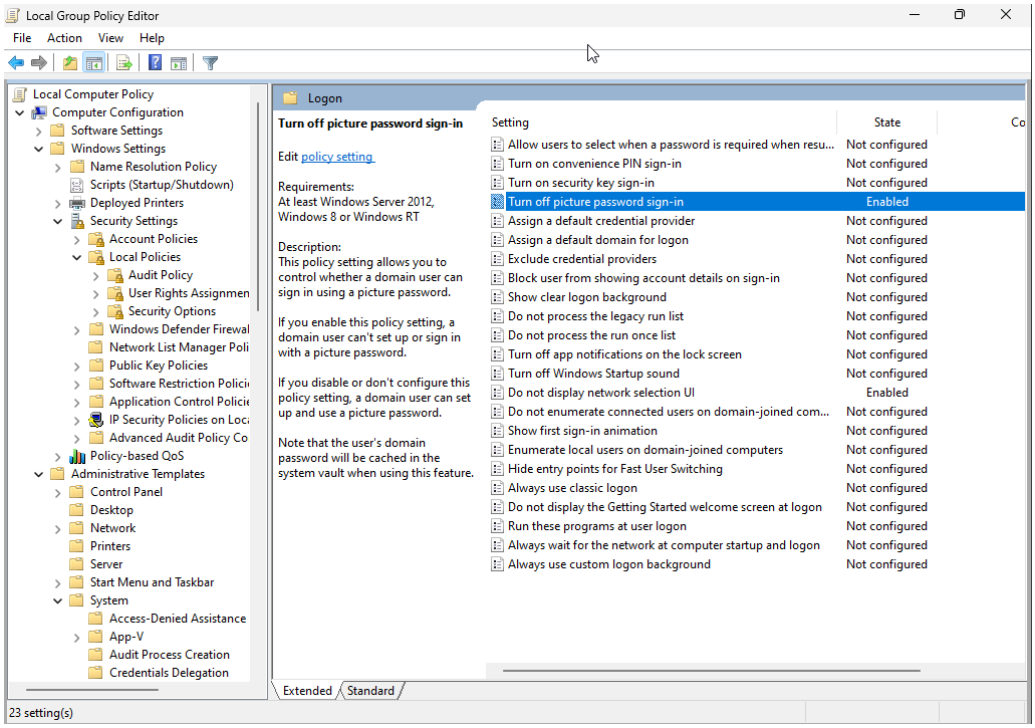
Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CredentialProviders.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

Users will not be able to set up or sign in with a picture password.

Kuvassa 27 nähdään GP-reitin avulla tehty raportin suosittelema muutos tähän kohtaan.

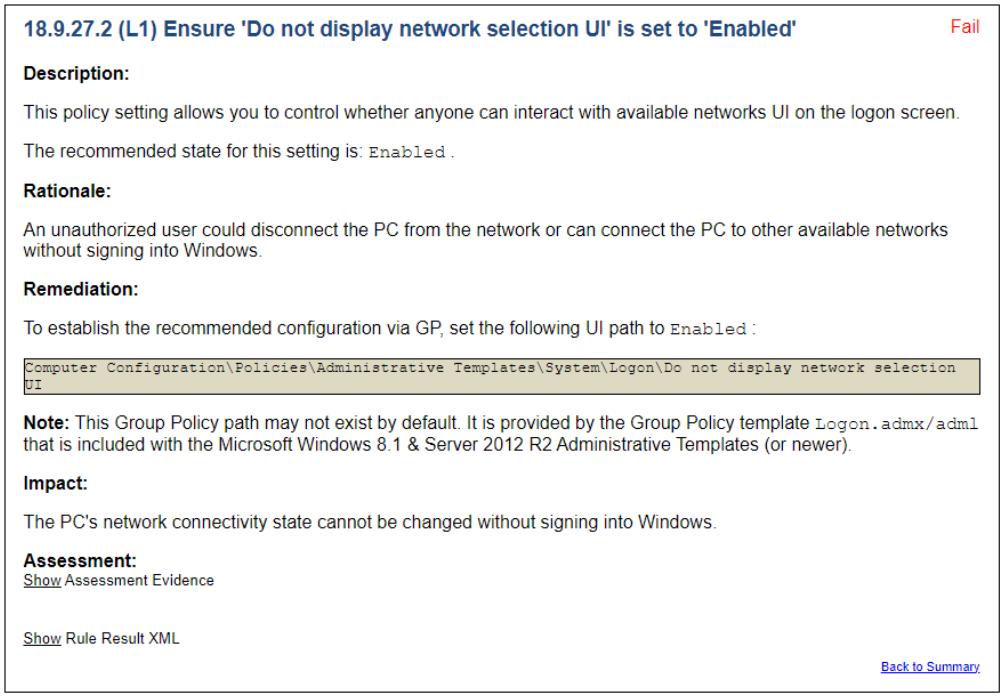
Kuva 27: Kuva salasanalla kirjautumisen korjaus



5.3.8 Ensure ’Do not display network selection UI’ is set to ‘Enabled’

Kahdeksannessa kohdassa (kuva 28) käsitellään verkonvalinnan näkyvyyttä käyttäjille. Kun verkonvalinta on näkyvissä kirjautumissivulla, kuka tahansa pystyy vaihtamaan, missä verkossa laite on kiinni, ilman että käyttäjä on kirjautunut sisään. Tämän kohdan raportin mukaisen asetuksen asettaminen nähdään kuvassa 29 käyttäen kuvan 28 ohjeistusta ja GP-reittiä.

Kuva 28: Älä näytä verkonvalinta näkymää kirjautumisnäkymässä



18.9.27.2 (L1) Ensure 'Do not display network selection UI' is set to 'Enabled' Fail

Description:

This policy setting allows you to control whether anyone can interact with available networks UI on the logon screen.

The recommended state for this setting is: `Enabled` .

Rationale:

An unauthorized user could disconnect the PC from the network or can connect the PC to other available networks without signing into Windows.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled` :

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Do not display network selection UI
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Logon.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Impact:

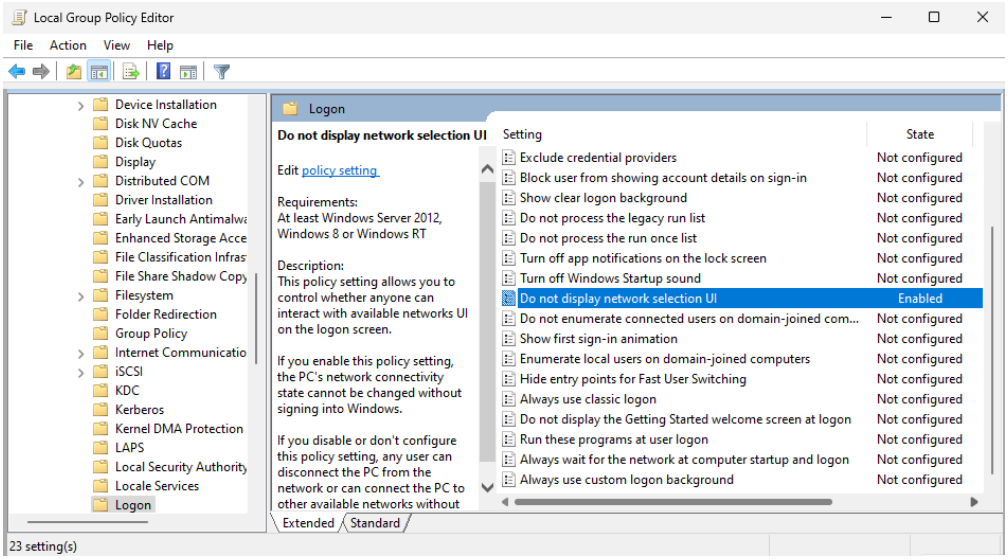
The PC's network connectivity state cannot be changed without signing into Windows.

Assessment:
Show Assessment Evidence

Show Rule Result XML

Back to Summary

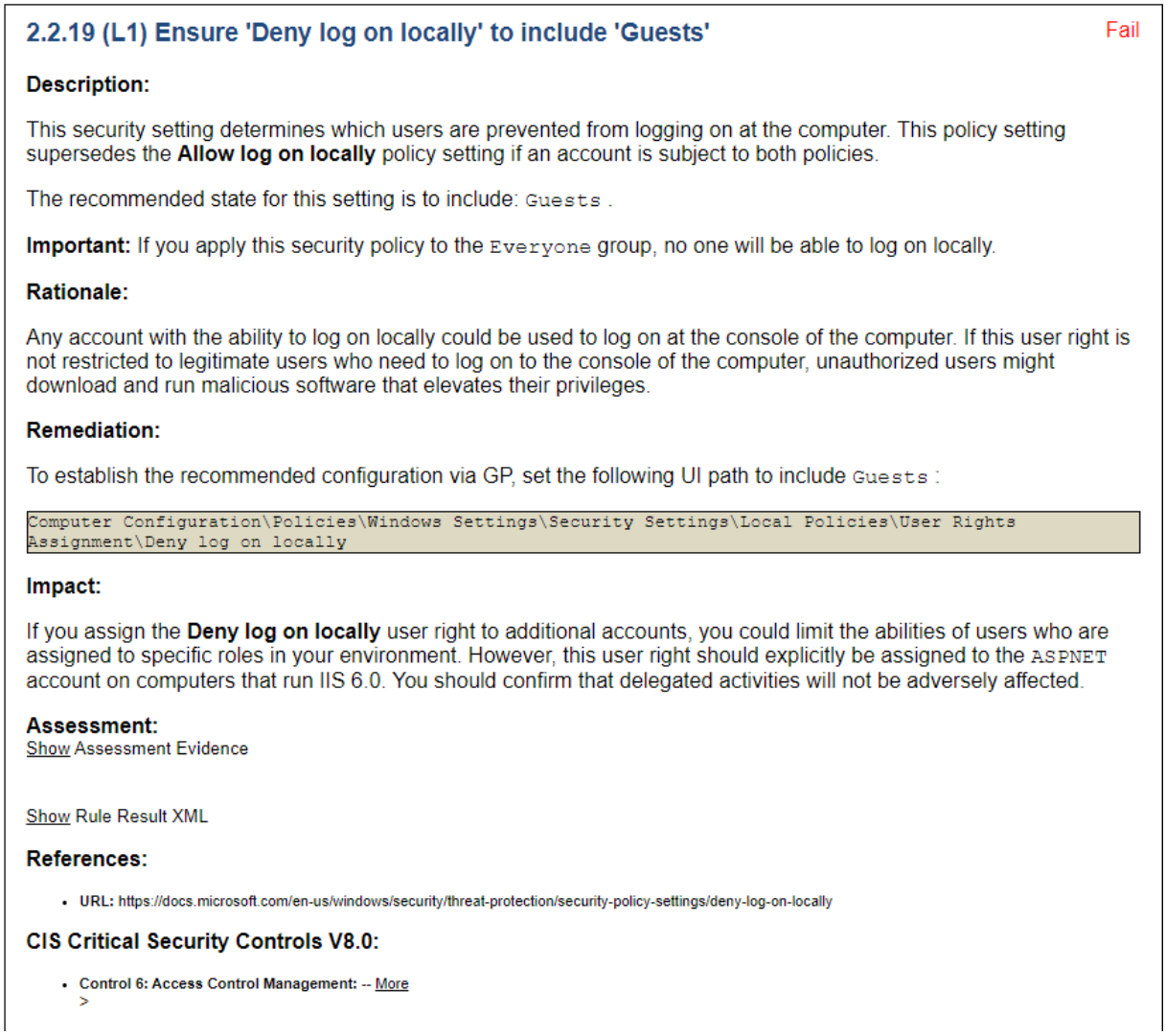
Kuva 29: Verkonvalinta näkymän näkyvyyden korjaus



5.3.9 Ensure ’Deny log on locally’ to include ‘Guests’

Yhdeksännessä kohdassa käsitellään vieraskäyttäjien paikallista kirjautumista ja sen estämistä (kuva 30). Vieraskäyttäjiä ei kannata jättää avoimeksi eli heidän kirjautumismahdollisuutensa on hyvä poistaa. Kaikki käyttäjät, jotka voivat kirjautua koneelle paikallisesti, voivat käyttää konetta konsolin avulla kirjautumalla vieraskäyttäjänä, mikä avaa mahdollisille hyökkääjille mahdollisuuden päästä koneeseen ja ympäristöön kiinni.

Kuva 30: Paikallisen kirjautumisen estäminen vieras käyttäjiltä



2.2.19 (L1) Ensure 'Deny log on locally' to include 'Guests'

Fail

Description:

This security setting determines which users are prevented from logging on at the computer. This policy setting supersedes the **Allow log on locally** policy setting if an account is subject to both policies.

The recommended state for this setting is to include: `Guests` .

Important: If you apply this security policy to the `Everyone` group, no one will be able to log on locally.

Rationale:

Any account with the ability to log on locally could be used to log on at the console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, unauthorized users might download and run malicious software that elevates their privileges.

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Guests` :

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on locally
```

Impact:

If you assign the **Deny log on locally** user right to additional accounts, you could limit the abilities of users who are assigned to specific roles in your environment. However, this user right should explicitly be assigned to the `ASPNET` account on computers that run IIS 6.0. You should confirm that delegated activities will not be adversely affected.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

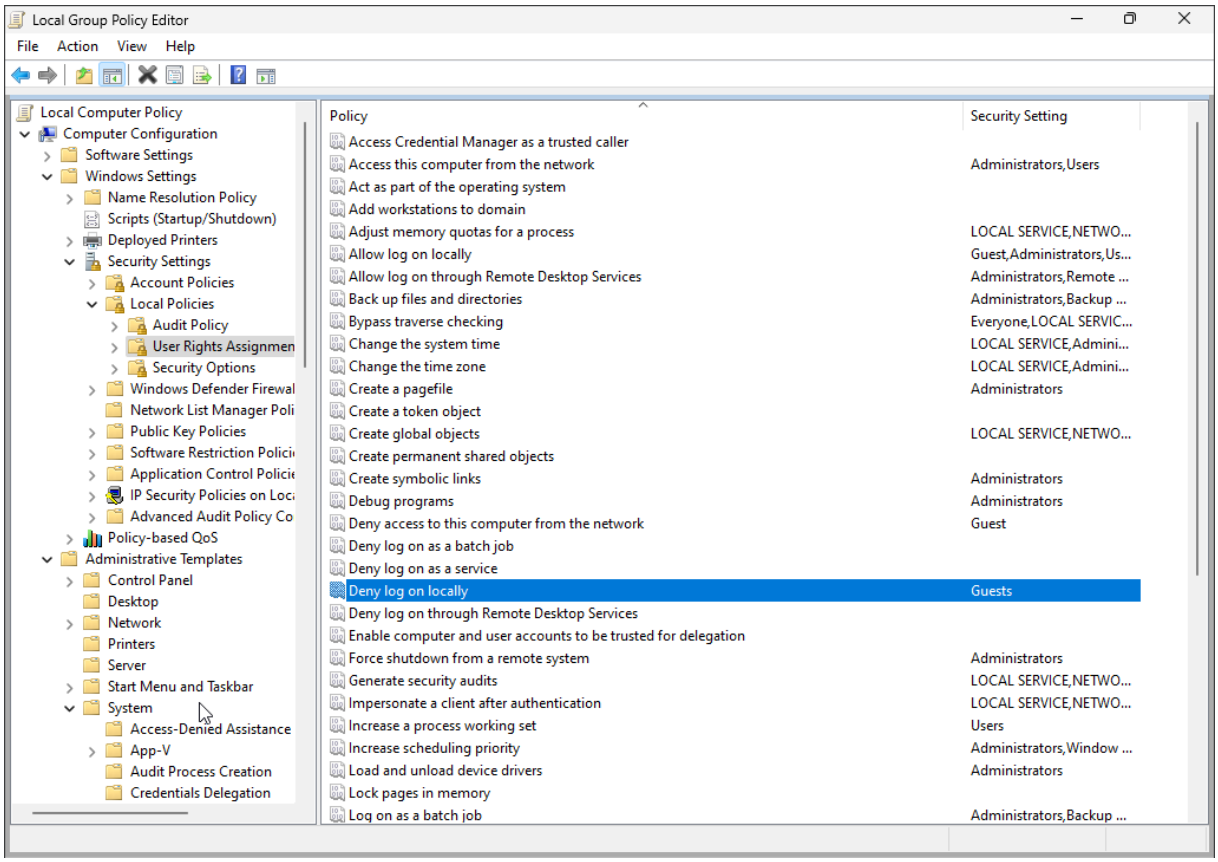
- **URL:** https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-log-on-locally

CIS Critical Security Controls V8.0:

- **Control 6: Access Control Management:** -- More >

GP-reittiä käyttäen pystytään löytämään oikea kohta ja muuttamaan sen arvo siten, että vieraskäyttäjät eivät pysty kirjautumaan ympäristöön paikallisesti (kuva 31).

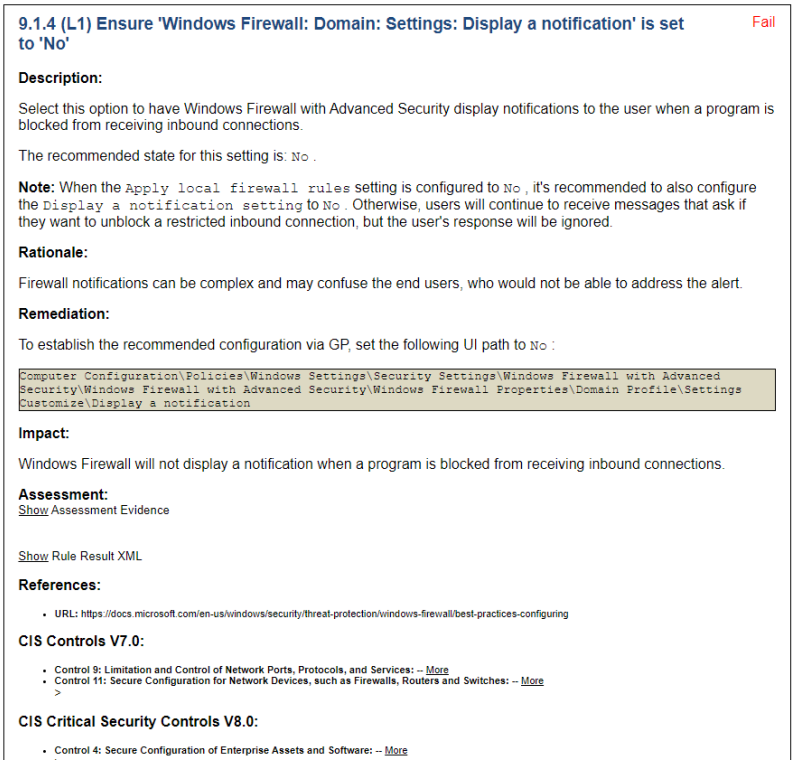
Kuva 31: Vieras käyttäjien lokaalin kirjautumisen estäminen



5.3.10 Ensure ’Windows Firewall: Domain: Settings: Display a notification’ is set to ‘No’

Kymmenes kohta käsittelee tiettyjen palomuurin ilmoitusten poistamista (kuva 32). Ylimääräiset ilmoitukset saattavat vain hämmentää normaaleja käyttäjiä. Muutoksen tekemisen jälkeen palomuuri ei enää anna ilmoituksia estetyistä saapuvista signaaleista.

Kuva 32: Palomuurin ilmoitusten poistaminen käyttäjiltä



9.1.4 (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' Fail

Description:

Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections.

The recommended state for this setting is: `No` .

Note: When the `Apply local firewall rules` setting is configured to `No` , it's recommended to also configure the `Display a notification setting` to `No` . Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored.

Rationale:

Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `No` :

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Settings Customize\Display a notification
```

Impact:

Windows Firewall will not display a notification when a program is blocked from receiving inbound connections.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- URL: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring

CIS Controls V7.0:

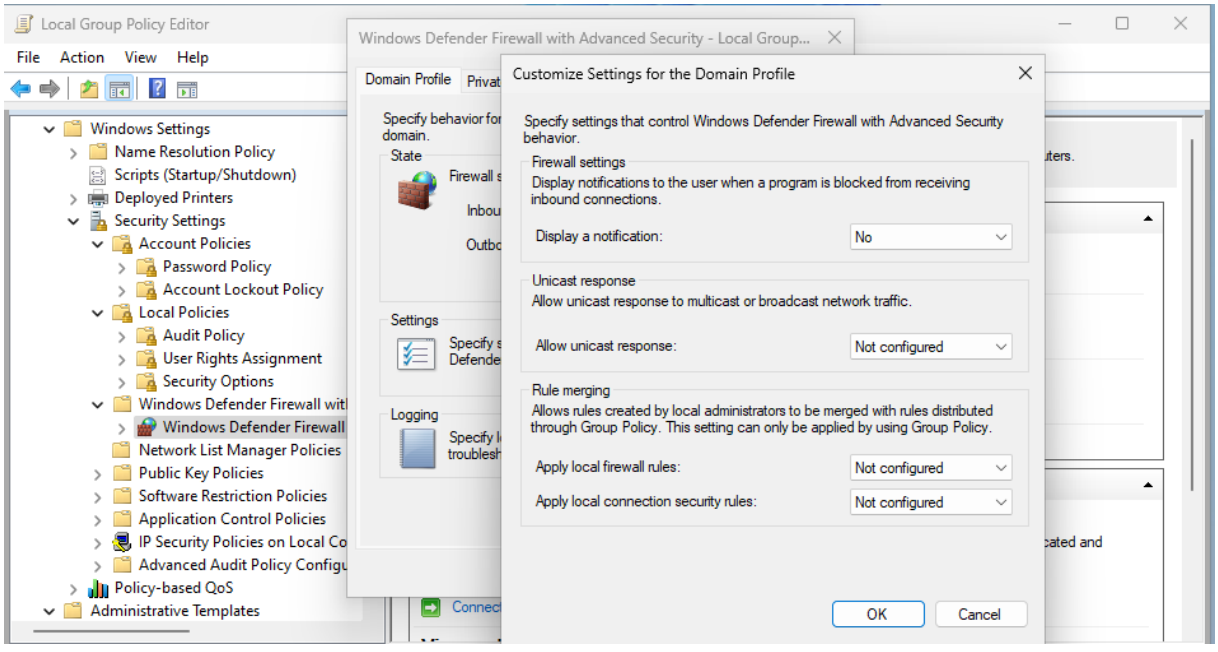
- Control 9: Limitation and Control of Network Ports, Protocols, and Services: -- More
- Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches: -- More
  >

CIS Critical Security Controls V8.0:

- Control 4: Secure Configuration of Enterprise Assets and Software: -- More

Kuvassa 33 nähdään tämän asetuksen asettaminen raportin suosittelemaan arvoon eli ”No”.

Kuva 33: Palomuurin ilmoitusten korjaaminen



6 Tulokset ja johtopäätökset

Tässä luvussa käsitellään ja vertaillaan käytännön vaiheen alussa tehtyä CIS-CAT Lite -raporttia uuteen käyttöön otetun raportin kanssa. Kappaleessa pohditaan myös käytännön osan toimenpiteiden tuottaman konkreettisen käytön kautta sekä teoriaosassa opitun teorian kautta CIS-CAT Lite -palvelun käyttötarkoituksia ja soveltuvuutta Windows-ympäristön koventamisessa.

6.1 Raporttien tulosten vertaaminen

Tässä luvussa vertaillaan CIS-CAT Lite -palvelun tuottamia raportteja (Kuva 11) ja uutta raporttia (Kuva 34). Kuvia vertaamalla voidaan nähdä, että CIS-CAT Lite löysi kaikki kymmenen käytännön osassa tehtyä korjausta. Tämän perusteella sekä luvussa 3.2 käsitellyn teorian pohjalta voidaan todeta, että CIS-CAT Lite toimii hyvin Windows-ympäristön koventamistarkoituksessa ja että sen arviointi perustuu luotettavaan tietopohjaan.

Kuva 34: Raportin tulokset korjauksien jälkeen

Summary

Description	Tests						Scoring		
	Pass	Fail	Error	Unkn	Man.	Exc.	Score	Max	Percent
1 Account Policies	3	7	0	0	1	0	3.0	10.0	30%
1.1 Password Policy	3	4	0	0	0	0	3.0	7.0	43%
1.2 Account Lockout Policy	0	3	0	0	1	0	0.0	3.0	0%
2 Local Policies	65	32	0	0	1	0	65.0	97.0	67%
2.1 Audit Policy	0	0	0	0	0	0	0.0	0.0	0%
2.2 User Rights Assignment	29	8	0	0	0	0	29.0	37.0	78%
2.3 Security Options	36	24	0	0	1	0	36.0	60.0	60%
2.3.1 Accounts	3	2	0	0	0	0	3.0	5.0	60%
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	1	0	0	0	0	0	1.0	1.0	100%
2.3.5 Domain controller	0	0	0	0	0	0	0.0	0.0	0%
2.3.6 Domain member	6	0	0	0	0	0	6.0	6.0	100%
2.3.7 Interactive logon	2	5	0	0	0	0	2.0	7.0	29%
2.3.8 Microsoft network client	2	1	0	0	0	0	2.0	3.0	67%
2.3.9 Microsoft network server	2	3	0	0	0	0	2.0	5.0	40%
2.3.10 Network access	9	3	0	0	0	0	9.0	12.0	75%
2.3.11 Network security	2	7	0	0	1	0	2.0	9.0	22%
2.3.12 Recovery console	0	0	0	0	0	0	0.0	0.0	0%
2.3.13 Shutdown	0	0	0	0	0	0	0.0	0.0	0%
2.3.14 System cryptography	0	0	0	0	0	0	0.0	0.0	0%
2.3.15 System objects	2	0	0	0	0	0	2.0	2.0	100%
2.3.16 System settings	0	0	0	0	0	0	0.0	0.0	0%
2.3.17 User Account Control	6	2	0	0	0	0	6.0	8.0	75%
3 Event Log	0	0	0	0	0	0	0.0	0.0	0%
4 Restricted Groups	0	0	0	0	0	0	0.0	0.0	0%
5 System Services	11	10	0	0	0	0	11.0	21.0	52%
6 Registry	0	0	0	0	0	0	0.0	0.0	0%
7 File System	0	0	0	0	0	0	0.0	0.0	0%
8 Wired Network (IEEE 802.3) Policies	0	0	0	0	0	0	0.0	0.0	0%
9 Windows Defender Firewall with Advanced Security (formerly Windows Firewall with Advanced Security)	1	25	0	0	0	0	1.0	26.0	4%
Total	92	287	0	0	2	0	92.0	379.0	24%

6.2 CIS-CAT Lite -palvelun käytön yhteenveto

Työn aikana CIS-CAT Lite -palvelua käytettiin peruskäyttöön verrattavalla tavalla. Palvelun hieman laajempia käyttötarkoituksia ei lähdetty tutkimaan, vaan työn ideana oli kokeilla CIS-CAT Liten soveltuvuutta ja toimivuutta Windows-ympäristön koventamistarkoituksessa, erityisesti pienten yritysten näkökulmasta. Tarkoituksena oli selvittää, kuinka hyvin pienempi yritys, jolla ei ole kyberturvallisuuteen erikoistunutta henkilöstöä, pystyisi käyttämään CIS-CAT Liteä apuna työympäristön kyberturvallisuuden standardien parantamisessa.

Palvelun käytön yhteydessä tuli selväksi, että CIS-CAT Lite on suunniteltu erittäin käyttäjäystävälliseksi ja luotettavaksi. Palvelun lataaminen ja käyttöönotto ovat helppoja ja helposti opittavissa. Palvelu tarjoaa käyttäjälle selkeitä ohjeita ja selittää sekä avaa mahdolliset vaihtoehdot ennen palvelun käyttöä ja ympäristön arviointia. Itse raportti, jota tässä työssä käsitellään yhteenvedon sekä kymmenen korjattavan kohdan kautta, on helppolukuinen ja selittää korjausta vaativat sekä oikein olevat kohdat ymmärrettävästi. Raportin pohjalta perustaidot IT-asioista omaava henkilö pystyy koventamaan Windows-ympäristön perustason kriteereiden mukaiseksi, mikä parantaa kyseisen ympäristön turvallisuutta merkittävästi kyberturvallisuuden näkökulmasta.

7 Yhteenveto

Tutkimuskysymyksiin vastaaminen on ehdottomasti olennainen osa opinnäytetyötä. Tässä työssä on selkeästi ja perustellusti vastattu valittuihin tutkimuskysymyksiin. Ympäristön koventaminen on keskeistä, koska se muodostaa toimivan ja turvallisen kyberturvallisuuden perustan ja auttaa ehkäisemään joutumista hyökkäyksen kohteeksi korjaamalla monia yleisiä ongelmakohtia Windows-ympäristössä. Windows-käyttöjärjestelmä on luonteeltaan melko avoin, ja rajoitusten asettaminen alusta alkaen voisi tehdä siitä vähemmän käyttäjäystävällisen, mikä korostaa koventamisen tarpeellisuutta entisestään.

CIS-CAT Lite -arvioinnit perustuvat CIS Benchmarks -palvelun tarjoamiin lähtökohtiin. CIS-CAT Lite vertaa skannattuja tuloksia CIS Benchmarks -palvelun lähtökohtiin ja laatii sen perusteella käyttäjälle laajan ja yksityiskohtaisen raportin siitä, miten käyttäjä voi parantaa ympäristönsä kyberturvallisuutta.

CIS-CAT Lite auttaa merkittävästi ympäristön koventamisessa tarjoamalla laajan ja yksityiskohtaisen raportin. Sen avulla lähes kuka tahansa IT-alan työntekijä pystyy seuraamaan ohjeita ja koventamaan peruskäyttöön tarkoitetun Windows-ympäristön.

Työssä opin koventamisen tärkeyden peruspiirteiltään CIS-CAT Lite -palvelun käytön. Koen, että pystyisin koventamaan peruskäyttöön tarkoitetun Windows-ympäristön käyttämällä CIS-CAT Lite -ohjelmistoa. Ymmärrän nyt myös enemmän kyberturvallisuuden perusteista sekä siitä mitä hyvä kyberturvallisuuden taso edellyttää.

Työtä pystytään lähtemään kehittämään muutamalla eri tavalla. Joko lähtee vertailemaan CIS-CAT Lite -ohjelmistoa johonkin muuhun samantyyppiseen palveluun tai lähteä tekemään kokonaisvaltaista koventamista ja analysoimaan tämän tuloksia ja vaikutuksia kovennettuun ympäristöön. Mahdollisesti soveltamalla penetraatiotestausta kovennettuun ja ei-kovennettuun ympäristöön ja vertaamalla tuloksia. Työn kehittämisen mahdollisuuksia on siis paljon ja monipuolisesti.

Lähteet

Mitä on kyberturvallisuus? (p. 1). (n.d.). Microsoft. https://www.microsoft.com/fi-fi/security/business/security-101/what-is-cybersecurity

Kyberturvallisuuden sanasto. 2018. Sanastokeskus TSK ry. https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf?file=pdf/Kyberturvallisuuden_sanasto.pdf

About us—CIS®. (n.d.). CIS. Retrieved 1 April 2024, from https://www.cisecurity.org/about-us/

Benchmarks Overview—CIS®. (n.d.). CIS. Retrieved 1 April 2024, from https://www.cisecurity.org/cis-benchmarks-overview/

CIS Benchmarks™ FAQ. (n.d.). CIS. Retrieved 1 April 2024, from https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/

CIS SecureSuite® Categories and Pricing. (n.d.). CIS. Retrieved 1 April 2024, from https://www.cisecurity.org/cis-securesuite/pricing-and-categories/

Mitä kyberturvallisuus on? | *Microsoft Security*. (n.d.). Retrieved 1 April 2024, from https://www.microsoft.com/fi-fi/security/business/security-101/what-is-cybersecurity

What is the CIA Triad? | *Definition from TechTarget*. (n.d.). WhatIs. Retrieved 1 April 2024, from https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

vinaypamnani-msft. (2023, August 2). *Windows operating system security—Windows Security*. https://learn.microsoft.com/en-us/windows/security/operating-system-security/

Archiveddocs. (2016, August 31). *Group Policy Overview*. https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831791(v=ws.11)

CIS-CAT Lite. (n.d.). Retrieved 1 April 2024, from https://learn.cisecurity.org/cis-cat-lite?_gl=1*1kwsfie*_ga*MjQwNDA4MjU4LjE3MDQzODM2MTA.*_ga_3FW1B1JC98*MTcwOTM3NTU2MC4xNi4xLjE3MDkzNzY4MTMuMC4wLjA.*_ga_N70Z2MKMD7*MTcwOTM3NTU2MC4xNi4xLjE3MDkzNzY4MTMuNTguMC4w)

Liite 1: Aineistonhallintasuunnitelma

Kehitysprojekti:

Kehitysprojektin aikana pidetään päiväkirjaa (aineisto), johon kerätään teknistä tietoa projektista. Tämä tieto analysoidaan opinnäytetyötä varten. Päiväkirjaa säilytetään tekijän tietokoneen C-asemalla, ja siitä tehdään säännöllisesti varmuuskopioita <minne>. Päiväkirjaa säilytetään C-asemalla ainakin vuoden verran opinnäytetyön valmistumisesta.

Kehitysprojektin aikana puhutuista asioista ei pidetty kirjaa sen enempään vaan kaikki on dokumentoitu joko wihiin opiskelijan ja opettajan välisiin viesteihin tai väliaikaisiin muistioihin.

Valmiin projektin onnistumisesta kerätään tietoa wihiin.

Tutkimuksellinen työ:

Opinnäytetyön omistan minä itse.

Työssä käytetty materiaali on luvan kanssa käytettyä ja suurin osa on joko suoraan applikaatiosta tai esittely artikkeleista.

Opinnäytetyöaineiston jatkokäyttö työn valmistumisen jälkeen

1. Et halua hyödyntää tai antaa tutkimusaineistoasi jatkokäyttöön

Tutkimusaineistoa ei jatkokäytetä. Opinnäytetyön tekijä säilyttää aineiston tietoturvallisesti vuoden ajan opinnäytetyön hyväksymispäivästä, jotta opinnäytetyön tulokset voidaan tarvittaessa varmistaa ja hävittää tämän jälkeen aineiston tietoturvallisesti.