VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Paavali Aho

TRELLIX

Tietoturva tuotannon laitteissa

Tekniikka

2025

VAASAN AMMATTIKORKEAKOULU
Tietotekniikka

TIIVISTELMÄ

Tekijä	Paavali Aho
Opinnäytetyön nimi	Trellix : Tietoturva tuotannon laitteissa
Vuosi	2025
Kieli	suomi
Sivumäärä	34
Ohjaaja	Ghodrat Moghadampour

Tämän työn tarkoituksena oli tutustua Trellix ePolicy Orchestrator -palvelimen jokapäiväiseen käyttöön ja hallintaan. Sillä jaetaan Trellix agentti tuotannon tietokoneille, seurataan niitten suorituskykyä ja mahdollisia ongelmatilanteita. Työssä keskityttiin agentin asennukseen, ylläpitoon ja sen raportointiin.

Trellix Agent on tietoturvakomponentti, joka on asennettava jokaiselle järjestelmän verkossa olevalle laitteelle. Sen keskeisempiä tehtäviä on tarjota turvallinen viestintäkanava paikallisten palveluiden välillä.

Tietoturvatuotteiden ja käytäntöjen luominen ja jakaminen oli toimivaa ja tehokasta. Myös kyselyiden sekä raporttien laatiminen oli vaivatonta ja suoraviivaista. Tämän työn perusteella Trellixin ePolicy Orchestrator -palvelinta voidaan käyttää jatkossakin tuotannon laitteissa turvaamassa tietoturvaa.

Avainsanat tietoturva, tehokkuus, ylläpito, raportointi, tietotekniikka

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Information Technology

ABSTRACT

Author	Paavali Aho
Title	Trellix : Security on production devices
Year	2025
Language	Finnish
Pages	34
Name of Supervisor	Ghodrat Moghadampour

The purpose of this work was to get familiar with the daily use and management of the Trellix ePolicy Orchestrator server. With it, you are able to distribute Trellix agents to production computers, monitor their performance and address potential issues. Our primary focus was on the installation, maintenance, and reporting aspects of the agent.

The Trellix Agent is a crucial security component that must be installed on every device within a system's network. Its main task is to provide a secure communication channel between local services.

We found that creating and distributing security products and policies was both functional and efficient. Furthermore, generating queries and reports was easy and straightforward. Based on the success of this work, we plan to continue using the Trellix ePolicy Orchestrator server to ensure the security of our production devices in the future.

Keywords security, efficiency, maintenance, reporting, information technology.

SISÄLLYS

KUVAT

KUVIOT

1 JOHDANTO

Kyberturva on yhteiskunnallisen vakauden ja luottamuksen kulmakivi. Kyberturva pyrkii varmistamaan digitaalisen tiedon ja infrastruktuurin luottamuksellisuuden, eheyden ja käytettävyyden. Tiedon luottamuksellisuudella tarkoitetaan sitä, että arkaluontoinen tieto pysyy salassa ja tieto on vain oikeutettujen tahojen saatavilla. Eheydellä varmistetaan, että tieto on oikeaa eikä sitä ole muokattu luvattomasti, mikä on tärkeää esimerkiksi talous- tai terveystiedoissa. Käytettävyys puolestaan takaa, että digitaaliset palvelut ja tiedot ovat saatavilla silloin, kun niitä tarvitaan, estäen esimerkiksi palvelunestohyökkäysten aiheuttamia katkoksia (Sisäministeriö, 2022).

Kyberturvallisuuden uhkakuvat ovat jatkuvassa muutoksessa ja kehittyvät samanaikaisesti teknologian kanssa. Ne ulottuvat yksinkertaisista haittaohjelmista ja tietojenkalasteluista aina valtiollisten toimijoiden toteuttamiin monimutkaisiin kyberhyökkäyksiin, jotka voivat lamauttaa kriittistä infrastruktuuria, kuten sähköverkkoja tai sairaalajärjestelmiä. Kyberturvallisuuden merkitys korostuu myös tietovuotojen myötä, jotka voivat vahingoittaa maineita, aiheuttaa taloudellisia menetyksiä ja vaarantaa yksityisyydensuojaa (Hynninen, 2024).

Sähköistymisen ja automaation globaalina edelläkävijänä ABB on toiminut jo yli 140 vuoden ajan suunnannäyttäjänä kohti kestävämpää ja resurssitehokkaampaa tulevaisuutta. Yhtiön ytimessä on syvällinen asiantuntemus suunnittelusta ja digitalisaatiosta, joiden yhdistäminen auttaa teollisuuden eri toimialoja saavuttamaan korkean suorituskyvyn. Maailmanlaajuisesti noin 110 000 työntekijän voimin ABB työskentelee jatkuvasti luodakseen ratkaisuja, jotka vastaavat aikamme suurimpiin haasteisiin: ilmastonmuutokseen, energiatehokkuuteen ja digitalisaatioon. Yhtiön teknologiaa hyödynnetään laajasti teollisuudessa, infrastruktuurissa ja liikenteessä. Se auttaa asiakkaita optimoimaan prosessejaan ja pienentämään hiilijalanjälkeään. ABB:n

toiminta jakautuu neljään globaaliin liiketoiminta-alueeseen: Electrification, Motion, Process Automation ja Robotics & Discrete Automation (ABB, 2024).

Yksi ABB:n Electrification-liiketoiminta-alueen keskeisimmistä osista on Distribution Solutions. Yksikkö kehittää, valmistaa, myy ja markkinoi kriittisiä sähkönjakeluverkon komponentteja, kuten suojareleitä sekä ohjaus-, automaatio- ja valvontalaitteita. Vikatilanteissa, kuten oikosulussa tai maasulussa, suojarele havaitsee poikkeaman nopeasti, viestii siitä eteenpäin ja laukaisee suojatoimenpiteet. Tämä nopea reagointi estää vakavammat vahingot, suojaa arvokkaita laitteita ja ennen kaikkea ihmishenkiä. Samalla suojareleiden toiminta edesauttaa merkittävästi sähkönsaannin luotettavuutta minimoimalla vian aiheuttaman keskeytyksen keston ja laajuuden. Vaasan tehtaalla valmistettavien suojareleiden lisäksi Suomen kärkiosaamista ovat kaukokäytön ohjaus- ja valvontalaitteet. Nämä laitteet ovat laajasti käytössä energiayhtiöissä ja teollisuudessa ympäri Suomea, mahdollistaen sähköverkon etävalvonnan ja -ohjauksen. Niiden avulla operaattorit voivat nopeasti reagoida häiriötilanteisiin, paikantaa vikoja ja ohjata sähkönvirtausta tehokkaasti, mikä lyhentää sähkökatkoja ja parantaa verkon yleistä häiriönsietokykyä (ABB, 2024).

Kyberturvallisuuden jatkuvan kehityksen haasteeseen on syntynyt useita uusia toimijoita, ja yksi niistä on Trellix. Trellix on moderni kyberturvallisuusyritys, joka muodostettiin yhdistämällä kaksi alan merkittävää toimijaa, McAfee Enterprisen ja FireEyen liiketoiminnat. Tämä yhdistyminen loi laaja-alaisen ja kattavan ratkaisutarjoajan, jonka tavoitteena on kehittää ja mullistaa uhkien havaitseminen ja niihin reagoiminen (Trellix, 2021).

Trellix edustaa laajaa kyberturvallisuuden ekosysteemiä, joka yhdistää reaaliaikaisen uhkien tunnistamisen, laitteiden ja pilvipalveluiden suojauksen sekä tietojen vuotamisen estämisen yhteen yhtenäiseen järjestelmään. Sen vahvat ominaisuudet, kuten monitasoinen Endpoint

Security, pilvitietojen suojaus ja uhkien ennakoiva analytiikka, tekevät siitä työkalun, joka tarjoaa kokonaisvaltaista turvaa yritysten ja organisaatioiden tarpeisiin. Yhtenäisen hallintakonsolin ansiosta yritykset voivat hallita ja seurata suojausratkaisuaan yhdestä paikasta, mikä säästää aikaa ja lisää tehokkuutta. Lisäksi järjestelmän kyky integroitua muihin kyberturvallisuusratkaisuihin tekee siitä joustavan ja mukautuvan työkalun eri tarpeisiin (Trellix, 2024).

Trellix tarjoaa innovatiivisia ratkaisuja, jotka eivät ainoastaan suojaa organisaatioita nykyisiltä vaaroilta, vaan valmistavat niitä myös tulevaisuuden haasteisiin. Se tarjoaa monipuolisen ja tehokkaan kyberturvallisuusratkaisun, joka kattaa useita keskeisiä osa-alueita (Trellix, 2024). Yksi sen tärkeimmistä ominaisuuksista on Endpoint Security, joka suojaa päätelaitteita haittaohjelmilta ja kiristysohjelmilta. Se tarjoaa myös reaaliaikaista uhkien torjuntaa, mikä auttaa estämään hyökkäyksiä ennen kuin ne ehtivät aiheuttaa vahinkoa. Toinen keskeinen osa-alue on Extended Detection and Response (XDR). Tämä teknologia mahdollistaa uhkien laaja-alaisen tunnistamisen ja nopean reagoinnin koko organisaation ekosysteemissä. XDR yhdistää eri lähteistä tulevaa tietoa ja tarjoaa kokonaisvaltaisen näkymän turvallisuustilanteeseen. Data Loss Prevention (DLP) -ominaisuus puolestaan estää arkaluonteisten tietojen vuotamisen. Se suojaa yrityksen kriittisiä tietoja valvomalla ja rajoittamalla niiden siirtoa ja käyttöä. Tämä on erityisen tärkeää tietosuojan ja sääntelyn näkökulmasta. Trellix tarjoaa myös vahvaa Cloud Security -suojaa, joka turvaa pilvipalvelut ja niissä säilytettävät tiedot. Tämä on olennaista nykyaikaisessa, pilvipohjaisessa IT-ympäristössä, jossa tietojen suojaaminen hajautetuissa järjestelmissä on haastavaa. AI-Powered Security hyödyntää tekoälyä ja koneoppimista uhkien ennakoivaan tunnistamiseen ja analysointiin. Tämä mahdollistaa nopeamman reagoinnin uusiin ja kehittyviin uhkiin, joita perinteiset menetelmät eivät välttämättä tunnista. Kaikkia näitä ominaisuuksia hallitaan Unified Management Console -keskushallintaliittymän kautta. Se tarjoaa käyttäjille selkeän ja keskitetyn näkymän, josta voidaan hallita kaikkia

suojausratkaisuja tehokkaasti ja helposti. Lopuksi, Trellixin Resilient Architecture on suunniteltu kestämään erilaisia uhkia ja tarjoamaan joustavuutta sekä paikallisissa että pilvipohjaisissa ympäristöissä. Tämä tekee siitä luotettavan ja skaalautuvan ratkaisun nykyaikaisiin kyberturvallisuustarpeisiin.

Tässä työssä keskityn Trellix ePolicy Orchestrator (tästä lähtien ePO) ohjelmaan, ylläpitoon sekä raportointiin tuotannon tietokoneilla. Trellix ePO on keskitetty tietoturvan hallinta-alusta, joka tarjoaa organisaatioille tehokkaita työkaluja kyberturvallisuuden hallintaan (Trellix, 2024). Sen keskeinen vahvuus on Centralized Management, eli mahdollisuus hallita kaikkia päätelaitteita ja tietoturvaratkaisuja yhdestä käyttöliittymästä. Tämä vähentää järjestelmän monimutkaisuutta ja parantaa hallinnan tehokkuutta. Policy Management -ominaisuuden avulla voidaan luoda, hallita ja ottaa käyttöön tietoturvakäytäntöjä koko organisaation laajuisesti. Tämä varmistaa, että turvallisuuskäytännöt ovat yhdenmukaisia ja ajantasaisia kaikilla tasoilla. Trellix ePO hyödyntää myös Threat Intelligence Integration -ominaisuutta, kuten Threat Intelligence Exchange (TIE) -integraatiota. Tämä tarjoaa ajankohtaista ja tarkkaa tietoa uhkista sekä auttaa torjumaan niitä tehokkaasti. Automation and Workflows -toiminnot mahdollistavat tietoturvatehtävien, kuten päivitysten ja uhkien torjunnan, automatisoinnin. Tämä säästää merkittävästi aikaa ja resursseja, ja vähentää inhimillisten virheiden riskiä. Alusta tarjoaa myös kattavat Reporting and Analytics -ominaisuudet. Näiden avulla voidaan seurata tietoturvan tilaa, analysoida tapahtumia ja tunnistaa mahdollisia haavoittuvuuksia järjestelmässä. Trellix ePO tukee yli 150 eri kolmannen osapuolen integraatiota, mikä mahdollistaa saumattoman yhteistyön muiden tietoturvatyökalujen kanssa. Lopuksi, ePO on saatavilla sekä pilvipohjaisena että paikallisena versiona, mikä tarjoaa organisaatioille valinnanvapauden ja joustavuutta erilaisten IT-ympäristöjen tarpeisiin.

Käytännössä ePO auttaa organisaatioita hallitsemaan tietoturvaa tehokkaasti, vähentämään riskejä ja reagoimaan vaaroihin nopeasti. Se on erityisen hyödyllinen suurille organisaatioille, jotka tarvitsevat laajan ja kattavan tietoturvaratkaisun. IP-osoitteet, työhön liittymättömien laitteiden nimet ja muut arkaluontoiset tiedot on piilotettu tietoturvasyistä.

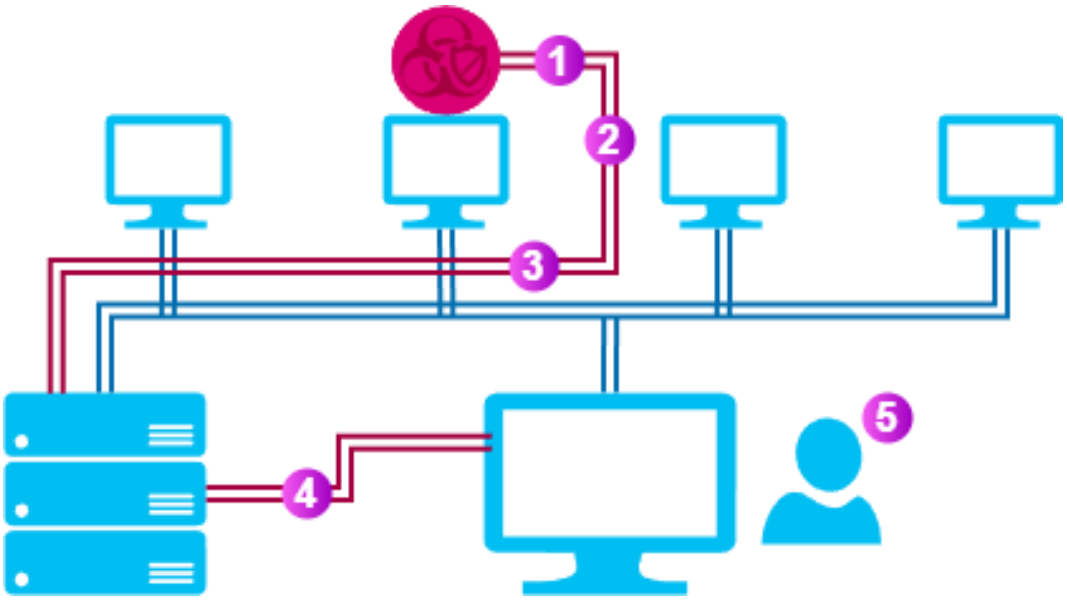
Tässä työssä olen käyttänyt Microsoft Copilotia kielentarkistuksen välineenä. Olen muokannut tekstiä tekoälyn avulla useaan otteeseen, jotta kieli olisi selkeämpää ja helpommin ymmärrettävää, mutta välittäisi asiat yhä alkuperäisen tarkoitukseni mukaisesti. Olen huolehtinut sisällön alkuperäisyydestä ja tekijänoikeuksien kunnioittamisesta. Jos tekoälysovellus on tuottanut tekstiin uusia ideoita, olen aina tarkistanut ne alkuperäisistä lähteistä ja viitannut niihin asianmukaisesti. Kaikki ilmoittamani lähteet ovat itse käyttämiäni, eivät tekoälyn tuottamia. Olen myös käyttänyt Microsoft Copilotia englanninkielisen tiivistelmän kirjoittamisessa sekä kieliasun tarkistamisessa. Olen käyttänyt tekoälysovellusta vastuullisesti ja huolehtinut tietosuojasta.

2 TRELLIX ePO

Trellix ePO on Trellixin tarjoama keskitetty hallintakonsoli organisaation turvallisuuskäytäntöjen ja -ratkaisujen hallinnointiin. Se toimii eräänlaisena komentokeskuksena, jonka avulla yritykset voivat hallita laajoja ja monimutkaisia tietoturvaympäristöjään. ePOn keskeinen etu piilee sen kyvyssä yhdistää useita Trellixin ja sen kumppanien tietoturvatuotteita yhden ja saman hallintaliittymän alle. Tämä mahdollistaa yhtenäisten turvallisuuskäytäntöjen luomisen ja jakamisen organisaation eri osa-alueille – olipa kyseessä sitten päätelaitteiden, palvelimien, verkon tai pilvipalveluiden suojaus. Konsoli tarjoaa kattavan näkymän turvallisuustilanteeseen, esittäen esimerkiksi haittaohjelmahavainnot, haavoittuvuudet ja poikkeamat yhdessä paikassa. Tämä vähentää merkittävästi hallinnollista taakkaa ja parantaa tietoturvatoimien tehokkuutta.

2.1 Toimintaperiaate

Trellixin tietoturvaohjelmisto ja ePO toimivat yhdessä suojatakseen järjestelmää haittaohjelmahyökkäyksiltä ja ilmoittaakseen niiden esiintymisestä. Hyökkäyksen aikana ePOn komponentit ja prosessit pysäyttävät hyökkäyksen, ilmoittavat sen tapahtumisesta ja tallentavat tapahtuman tiedot. Kyberhyökkäyksen aikana järjestelmän suojautuminen tapahtuu monivaiheisesti (Trellix, 2024):



Kuvio 1. Tapahtumakuvio hyökkäyksen aikana tapahtuvista toiminnoista.

1. Haittaohjelman hyökkäys (Kuvio 1, kohta 1): Haittaohjelma aloittaa hyökkäyksen tietokoneeseen, joka sijaitsee ePOn hallinnoimassa verkossa. Tämä voi tapahtua esimerkiksi sähköpostin liitteen, haitallisen verkkosivun tai muiden teknisten haavoittuvuuksien kautta. Kyberuhka tunkeutuu järjestelmään tavoitteenaan aiheuttaa vahinkoa, kerätä tietoja tai häiritä järjestelmän normaalia toimintaa.

2. Haittaohjelman tunnistus ja poisto (Kuvio 1, kohta 2): Trellixin ohjelmisto, kuten Endpoint Security, aktivoituu tunnistaakseen ja neutraloidakseen haittaohjelman. Tämä voi tapahtua automaattisesti ohjelmiston algoritmien avulla tai ylläpitäjän suorittamien tarkistusten kautta. Haittaohjelman poistaminen estää sen leviämisen muihin verkossa oleviin laitteisiin ja minimoi sen aiheuttamat haitat.

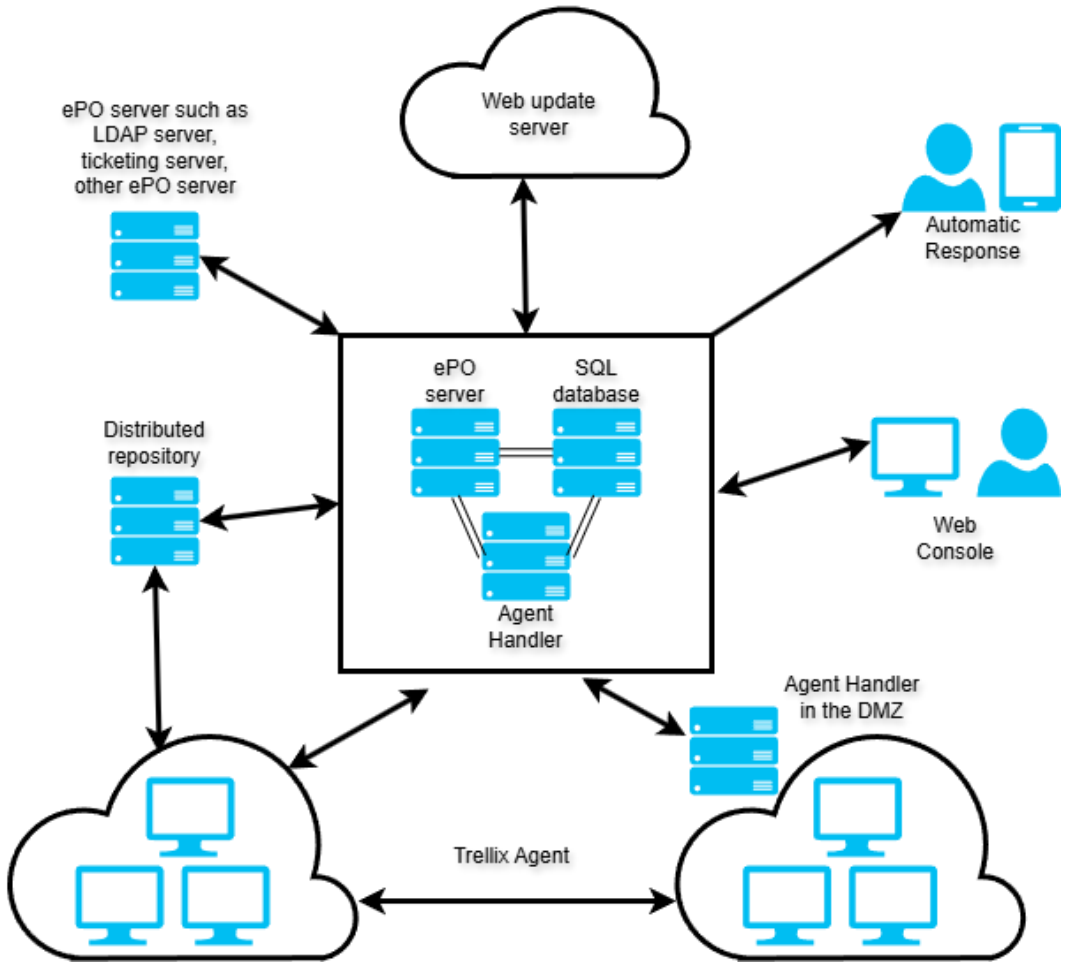
3. Hyökkäyksen ilmoittaminen ePOlle (Kuvio 1, kohta 3): Trellix Agent toimii viestintäkanavana ePOn ja hallittujen järjestelmien

välillä. Kun haittaohjelma on havaittu ja poistettu, Agent lähettää tiedot tapahtuneesta ePOlle. Näin varmistetaan, että ePO saa reaaliaikaisen tiedon hyökkäyksen yksityiskohdista.

4. Tietojen dokumentointi (Kuvio 1, kohta 4): ePO tallentaa hyökkäyksen tiedot järjestelmän lokitietoihin. Tämä dokumentointi sisältää hyökkäyksen aikaleiman, sen sijainnin verkossa, käytetyt menetelmät sekä muut olennaiset tiedot. Tapahtuman dokumentointi on kriittistä analysointia ja tulevaisuuden uhkien ennaltaehkäisyä varten.

5. Ilmoitusten näyttäminen (Kuvio 1, kohta 5): Lopuksi ePO näyttää hyökkäysilmoituksen hallintapaneelissa, mikä mahdollistaa ylläpitäjien nopean reagoinnin ja päätöksenteon. Hallintapaneeli tarjoaa selkeän visuaalisen kuvan hyökkäyksestä ja antaa tarvittavat työkalut tilanteen hallintaan.

Kuvion (2) keskellä on ePO-palvelin, joka toimii järjestelmän ytimenä. Siihen on asennettu ePO-ohjelmisto, joka mahdollistaa keskitetyn hallinnan kaikille organisaation hallinnoiduille järjestelmille. Keskitetty hallinta tarkoittaa tässä tapauksessa sitä, että kaikki turvallisuuteen, päivityksiin ja tehtävien suorittamiseen liittyvät toiminnot voidaan hallita yhdestä paikasta.



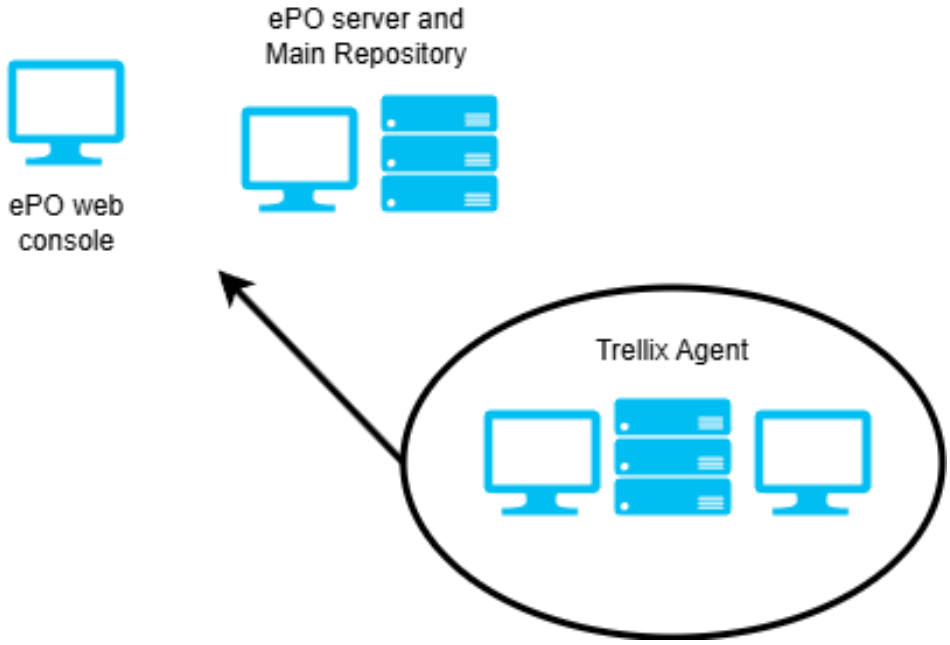
Kuvio 2. Trellix ePOn peruskomponentit ja sekvenssikaavio.

Agent Handlers -komponentit ovat keskeinen osa ePO-arkkitehtuuria, sillä ne jakavat palvelimen työkuormaa tehokkaasti. Ne ottavat vastuulleen Trellix Agent -laitteiden viestinnän ja tapahtumien käsittelyn. Tämä vähentää ePO-palvelimen kuormitusta, mikä parantaa järjestelmän suorituskykyä ja skaalautuvuutta, erityisesti suurissa organisaatioissa. Agent Handlers -osien tehokkuus on suurimmillaan, kun ne sijaitsevat samalla verkkosegmentillä kuin ePOn tietokanta, mikä minimoi verkkoviiveet ja nopeuttaa tietojen käsittelyä.

Microsoft SQL Server -tietokantaa käytetään ePOn luomien ja käyttämien tietojen tallentamiseen. Tämä sisältää esimerkiksi lokitiedot, asetukset, tietoturvakäytännöt ja järjestelmien tilan. Tietokanta toimii vakaana ja luotettavana varastona, joka mahdollistaa tiedon nopean ja tehokkaan saatavuuden analysointia ja raportointia varten. Tietokannan avulla järjestelmä voi säilyttää suuren määrän tietoa ja varmistaa, että tietoturvaprosessit toimivat saumattomasti ja tarkoituksenmukaisesti (Trellix, 2024).

2.2 Trellix Agent

Trellix Agent on ePOn komponentti, joka on asennettava jokaiselle järjestelmän verkossa olevalle laitteelle, jotta ePO pystyisi niitä hallitsemaan. Sen keskeisempiä tehtäviä on tarjota turvallinen viestintäkanava ePOn ja muiden paikallisten palveluiden välillä. Tämän lisäksi se sisältää päivittäjäkomponentin, joka käyttää Sitelist.XML-tiedostoa etsiäkseen ja ladatakseen alku- tai päätelaitetuotteen päivitykset. Se voi hakea tiedostoja HTTP (Hypertext Transfer Protocol) -sivustoilta, FTP (File Transfer Protocol) -sivustoilta, UNC (Universal Naming Convention) -jaoista ja ePO-varastoista. Sivulistan järjestys määrittää, mistä sivustosta lataukset tehdään (Trellix, 2024).



Kuvio 3. Trellix agentin hierarkia.

Trellix Agentin tehtävänä on kerätä tietoa hallituista järjestelmistä, kuten koneiden tilasta, suorituskyvystä ja mahdollisista tietoturvauhkista. Kun Agentti havaitsee tapahtumia, esimerkiksi tietoturvapoikkeamia, se lähettää ne ePO-palvelimelle jatkokäsittelyä ja dokumentointia varten. Lisäksi Agentti vastaa ohjelmistojen ja niiden päivitysten jakamisesta hallituille järjestelmille. Tämä sisältää muun muassa uusien Trellix-turvaohjelmistojen asennuksen sekä olemassa olevien versioiden päivittämisen uusimpiin. Agentti toteuttaa myös ePOssa määritetyt tietoturvakäytännöt. Näihin voi kuulua esimerkiksi haittaohjelmien torjuntaan liittyviä sääntöjä tai verkkosivustojen käyttöön kohdistuvia rajoituksia. Agentti aikatauluttaa ja suorittaa erilaisia tehtäviä hallituissa järjestelmissä, kuten järjestelmäskannauksia tai tietojen varmuuskopiointeja. Lopuksi, Agentti päivittää tietoturvaan liittyvää sisältöä, kuten Endpoint Securityn tai Host Intrusion Preventionin DAT-tiedostoja. Nämä tiedostot sisältävät tietoa tunnetuista haittaohjelmista ja uhista.

3 ePO-PALVELIMEN TYÖKALUT

Kyberturvallisuuden hallinnassa tehokkuus syntyy kokonaisvaltaisuudesta ja systemaattisuudesta. Siksi ePO-palvelimen arkkitehtuuri on rakennettu usean moduulin ympärille. Näistä moduuleista tärkeimmät ovat Järjestelmäpuu, Käytännöt, Laitetehtävät, Ohjelmistoluettelo, Hallintapaneeli ja Raportit & Kyselyt.

3.1 Järjestelmäpuu

Järjestelmäpuun (System Tree) avulla hallitaan organisaation kaikkia hallittuja järjestelmiä yhden yhtenäisen hierarkian kautta. Järjestelmäpuussä järjestelmiä voidaan järjestää, valvoa ja hallita tehokkaasti yhdestä keskitetystä paikasta. Jokaisella ePO-palvelimella on tarkalleen yksi Järjestelmäpuu, joka toimii sen hallinnoinnin perustana (Trellix, 2024).

Järjestelmäpuu sisältää kaikki järjestelmät, joita ePO hallinnoi. Hallittu järjestelmä voi olla esimerkiksi palvelin, tietokone tai muu tietoturvaa vaativa laite. Järjestelmät Järjestelmäpuussä esitetään kahdella eri tavalla:

1. NetBIOS-nimi on järjestelmän verkon tunnistamiseen käytettävä nimi. Se auttaa ylläpitäjiä erottamaan laitteet toisistaan.

2. GUID (Globally Unique Identifier) – ePOn sisäisessä rakenteessa järjestelmät identifioidaan niiden GUID-tunnisteella, joka on yksilöllinen jokaiselle laitteelle.

Järjestelmäpuu alkaa juuritasolta, joka tunnetaan nimellä ”My Organisation”. Tämä juuritason ryhmä muodostaa hierarkian ytimen, jonka ympärille kaikki muut ryhmät ja laitteet järjestetään. Järjestelmänvalvojat voivat luoda hierarkisia ryhmiä ja aliryhmiä, jotka edustavat esimerkiksi osastoja, tiimejä tai maantieteellisiä alueita.

”Lost and Found” on Järjestelmäpuun oletusryhmä, johon uudet laitteet sijoitetaan automaattisesti, mikäli niitä ei ole määritelty mihinkään muuhun ryhmään. Tämä on hyödyllistä tilanteissa, joissa uusia laitteita lisätään nopeasti järjestelmään, ja niiden tarkempi ryhmäjako voidaan tehdä myöhemmin.

Järjestelmäpuun hierarkkinen rakenne auttaa järjestämään laitteet ja ryhmät loogisella ja yksinkertaisella tavalla, mikä tekee kokonaisuuden hallinnasta sujuvampaa. Lisäksi järjestelmän periytyvät asetukset ja käytännöt mahdollistavat automatisoinnin, joka vähentää huomattavasti manuaalisen työn tarvetta ja nopeuttaa ylläpitoprosesseja. Laitteiden ryhmittely ja niiden joustava siirtäminen ryhmien välillä tuovat lisää mukautuvuutta, joka auttaa organisaatiota vastaamaan nopeasti muuttuviin tarpeisiin ja tilanteisiin.

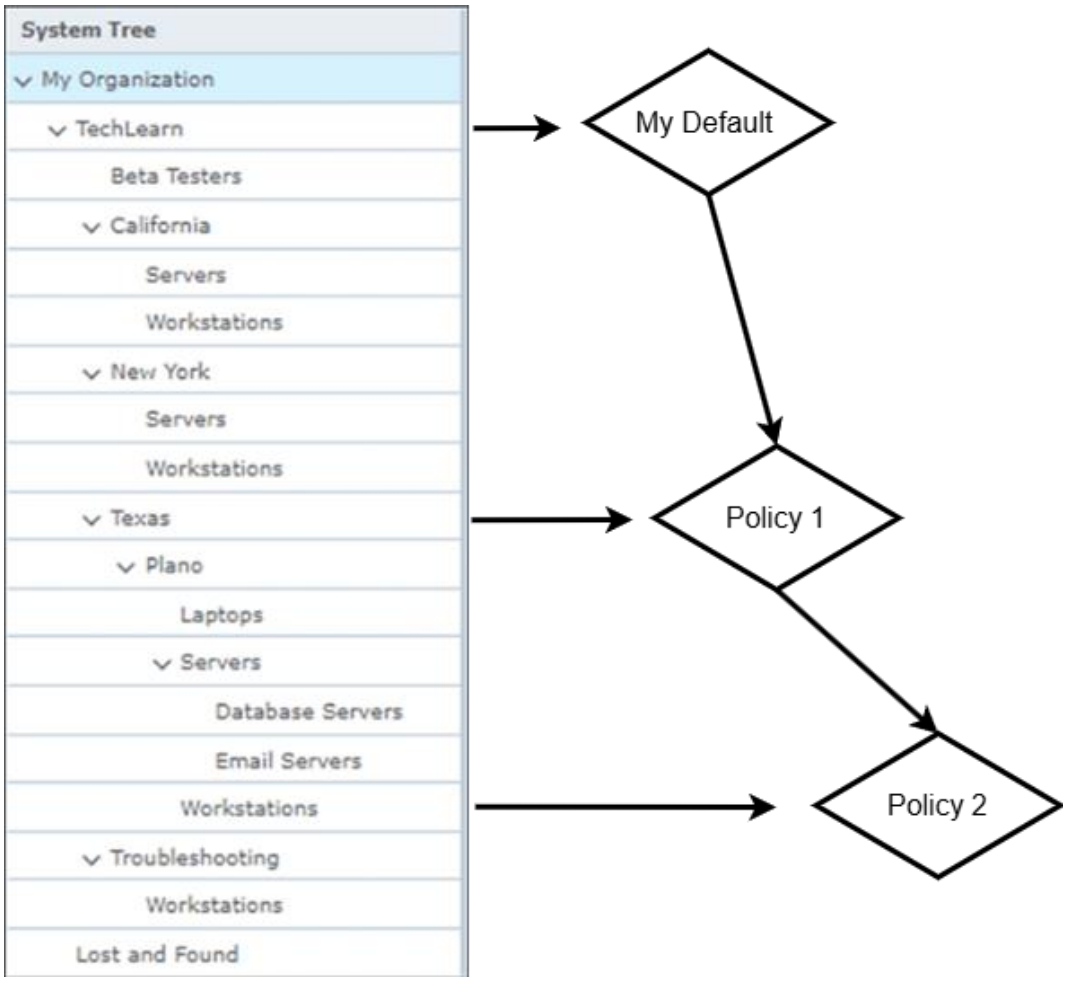
3.2 Käytännöt

Käytännöt (Policies) ovat sääntöjen ja asetusten kokoelma, jotka määrittävät, kuinka hallitut järjestelmät toimivat. Käytännöillä järjestelmät toimivat turvallisesti, tehokkaasti ja organisaation vaatimusten mukaisesti. Trellixin käytäntöjen avulla voidaan hallita tehokkaasti organisaation tietoturvaa, toimintarajoituksia, ohjelmistojen asennuksia ja päivityksiä (Trellix, 2024). Näitä sääntöjä sovelletaan laajasti eri laitteisiin ja järjestelmiin, ja ne muodostavat keskeisen osan keskitettyä hallintaa.

Yksi käytäntöjen tärkeimmistä eduista on hallinnan keventäminen. Suurissa organisaatioissa yksittäisten käyttäjien tai järjestelmien sääntöjen hallinta voi olla työlästä ja altistaa virheille. Käytännöt mahdollistavat yleisesti sovellettavien sääntöjen, kuten peruskäytäntöjen, hyödyntämisen koko Järjestelmäpuu-hierarkiassa. Toinen keskeinen ominaisuus on mukautettavuus. Käytännöt voidaan räätälöidä organisaation yksilöllisten tarpeiden mukaan. Asetuksia voidaan muokata ja kohdistaa tiettyihin järjestelmiin tai ryhmiin, mikä

mahdollistaa joustavan ja tarkasti kohdennetun tietoturvan hallinnan. Lisäksi käytännöt tukevat vertailtavuutta ja versiohallintaa. ePOn käyttöliittymässä voidaan tarkastella ja vertailla eri käytäntöjä keskenään, mikä auttaa ylläpitäjiä tunnistamaan niiden yhtäläisyydet ja erot. Tarvittaessa voidaan myös palata aiempiin versioihin, esimerkiksi virheen korjaamiseksi tai muutosten vaikutusten arvioimiseksi. Yhdessä nämä ominaisuudet tekevät käytännöistä tehokkaan työkalun organisaation tietoturvan hallintaan, erityisesti silloin kun hallittavia kohteita on paljon ja vaatimukset vaihtelevat.

Useimmat järjestelmät organisaatiossa vaativat identtisen tai hyvin samankaltaisen kokoonpanon. Tämä tarkoittaa sitä, että suurimmalle osalle laitteista sovelletaan samoja sääntöjä ja asetuksia. Kuitenkin pieni osa järjestelmistä saattaa edellyttää merkittävästi erilaisia asetuksia, kuten erityisiä tietoturvaratkaisuja tai toimintarajoituksia. Käytäntöjen perinnän avulla voidaan toteuttaa tämä tilanne joustavasti. Käytäntöjen perintä toimii hierarkian avulla. Järjestelmäpuu -hierarkian ylemmällä tasolla määritetyt käytännöt periytyvät alempien tasojen ryhmille ja järjestelmille automaattisesti. Jos tietty ryhmä tai järjestelmä tarvitsee omia sääntöjä, voidaan perintä katkaista ja määrittää yksilölliset käytännöt, jotka korvaavat ylemmän tason käytännöt. Käytäntöjen perinnän toimintaa havainnollistetaan kuviossa 4.



Kuvio 4. Käytäntöjen periytyminen ryhmästä toiseen.

Esimerkissä TechLearn-ryhmä toimii perustason ryhmänä, jolle on määritetty käytäntö X. Tämä käytäntö sisältää perusasetukset esimerkiksi tietoturvaa varten. Texas-ryhmä on TechLearn-ryhmän alaryhmä, ja se perii automaattisesti käytännön X. Tämän lisäksi Texas-ryhmälle on määritetty oma käytäntö Y, joka täydentää tai tarkentaa perittyjä asetuksia. Näin Texas-ryhmällä on käytössä sekä käytäntö X että käytäntö Y. Workstations-ryhmä puolestaan on Texas-ryhmän alaryhmä. Se perii sekä TechLearnin käytännön X että Texasin käytännön Y. Lisäksi Workstations-ryhmälle on määritetty oma käytäntö Z. Tämän seurauksena Workstations-ryhmällä on käytössä käytännöt X, Y ja Z.

3.3 Laitetehtävät

Laitetehtävät (Client Tasks) mahdollistavat erilaisten järjestelmänhallintaan liittyvien tehtävien automatisoinnin. Näitä voivat olla esimerkiksi ohjelmistopäivitysten asennus, uusien ohjelmistotuotteiden jakelu tai olemassa olevien tuotteiden ylläpito. Automatisoinnin ansiosta tehtävät voidaan suorittaa ilman jatkuvaa manuaalista valvontaa, mikä säästää aikaa ja resursseja organisaatiossa.

Laitetehtävien aikataulutus on joustavaa ja monipuolista. Tehtävät voidaan ajoittaa tiettyyn ajankohtaan, jolloin ne suoritetaan esimerkiksi määriteltyinä kellonaikoina tai päivinä. Vaihtoehtoisesti ne voidaan asettaa toistuvaksi, jolloin tehtäviä suoritetaan säännöllisin väliajoin, esimerkiksi päivittäin tai viikoittain. Vaikka laitetehtävät voidaan määrittää ryhmätasolla, tehtäviä voidaan myös kohdentaa yksittäisille laitteille. Tämä mahdollisuus tarjoaa lisää joustavuutta, sillä yksittäisiä laitteita voidaan käsitellä erityistapauksina, jos niiden vaatimukset tai olosuhteet poikkeavat muista. Laitetehtävien hallinnassa toimii sama hierarkinen perintämekanismi kuin käytännöissä. Ryhmille ja järjestelmille määritetyt laitetehtävät periytyvät automaattisesti hierarkiassa alemmille ryhmille (Trellix, 2024).

3.4 Ohjelmistoluettelo

Ohjelmistoluettelo (Software Catalog) tarjoaa organisaatiolle kattavan näkymän sen käyttämien ohjelmistojen hallintaan. Se tiedottaa uusien ja päivitettyjen ohjelmistotuotteiden saatavuudesta, mukaan lukien sekä lisensoidut ohjelmistot että kokeiluversiot (Trelix, 2025). Näin organisaation ylläpitäjät voivat helposti pysyä ajan tasalla ohjelmistovalikoiman muutoksista ja hyödyntää uusimpia päivityksiä tietoturvan ja toimintojen tehostamiseksi.

Ohjelmistoluettelo ei pelkästään tiedota saatavuudesta, vaan mahdollistaa myös hallinnoitujen tuotekomponenttien tarkastamisen, päivittämisen ja tarvittaessa poistamisen suoraan ePO-palvelimelta. Tämä ominaisuus antaa ylläpitäjille keskitetyn hallintapisteen, jossa ohjelmistojen päivitykset ja hallinta voidaan suorittaa tehokkaasti ilman tarvetta käyttää erillisiä työkaluja tai menetelmiä. Ohjelmistojen saatavuus riippuu organisaation lisenssiavaimesta.

3.5 Hallintapaneeli

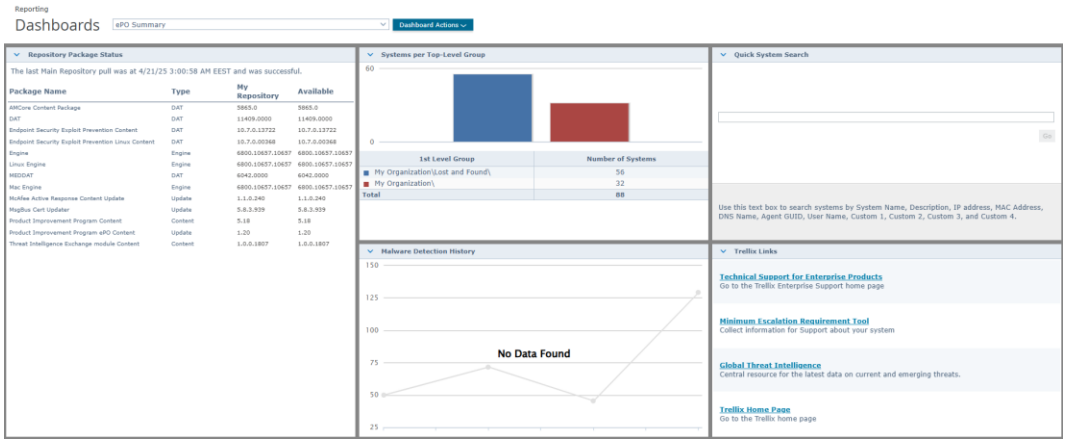
ePO-hallintapaneelisivu (Dashboard) tarjoaa keskitetyn näkymän organisaation hallinnoimiin järjestelmiin. Hallintapaneelin ydin koostuu kokoelmasta monitoreja, jotka on suunniteltu auttamaan järjestelmien hallinnassa, seurannassa ja niihin liittyvien toimenpiteiden toteuttamisessa. Nämä näytöt voivat esittää tietoja hyvin erilaisista lähteistä – esimerkiksi kaavioon perustuvista kyselyistä tai pienistä verkkosovelluksista, jotka tarjoavat reaaliaikaista tietoa ja toiminnallisuutta (Trellix, 2024).

Oletuksena ePOssa on useita valmiiksi määritettyjä näyttökokoelmia, joista ”ePO Summary” ja ”Threat Events” ovat erityisen hyödyllisiä. Näistä ”ePO Summary” -näyttökokoelmassa (Kuva 1) on oletuksena viisi monitoria:

1. Repository Package Status seuraa ePOn arkistossa olevien ohjelmistopakettien tilaa. Tämä sisältää tiedot siitä, mitkä paketit ovat saatavilla, onko niitä päivitetty äskettäin ja ovatko ne valmiita jaettavaksi hallituille järjestelmille.
2. Systems per Top-Level Group esittää hallittujen järjestelmien jakautumisen ylimmän tason ryhmiin Järjestelmäpuu -hierarkiassa. Tämä antaa ylläpitäjille visuaalisen kuvan siitä, kuinka laitteet ja järjestelmät ovat organisoitu hierarkian eri tasoilla.

3. Malware Detection History tallentaa ja näyttää tietoja havaituista haittaohjelmista. Se tarjoaa näkymän siihen, milloin ja missä haittaohjelmat havaittiin, sekä antaa tietoja niiden käsittelystä.
4. Quick System Search mahdollistaa hallittujen järjestelmien nopean ja helpon haun. Tällä ylläpitäjä voi löytää nopeasti tiettyjä järjestelmiä ePOn hallintapaneelista, esimerkiksi niiden NetBIOS-nimen perusteella.
5. Trellix Links tarjoaa linkkejä Trellixin tärkeisiin resursseihin ja palveluihin.

Näiden valmiiksi määritettyjen näyttökokoelmien lisäksi ePO tarjoaa mahdollisuuden rakentaa räätälöityjä näyttökokoelmia organisaation yksilöllisten tarpeiden mukaan.



Kuva 1. Esimerkkikuva ePO Summary -näyttökokoelmasta.

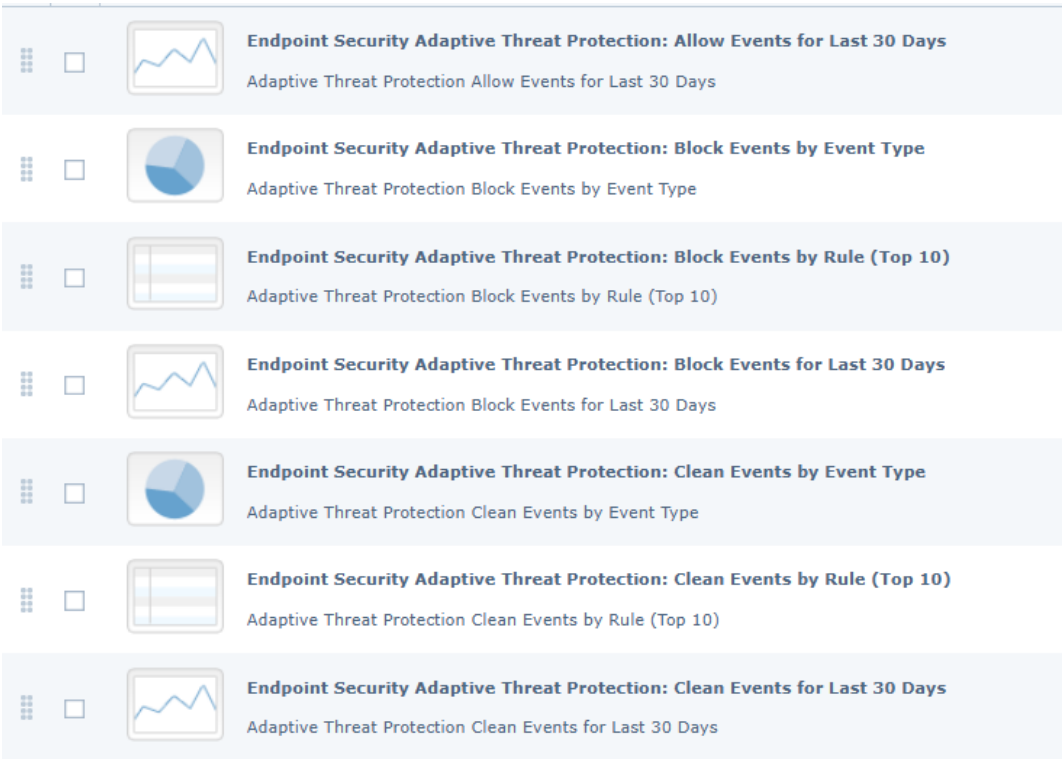
3.6 Raportit ja kyselyt

ePO tarjoaa tehokkaat ja joustavat raportointi- ja kyselyominaisuudet (Reports and Querys), jotka tukevat järjestelmänhallinnan tarpeita. Näiden työkalujen avulla järjestelmänvalvojat voivat kerätä, tarkastella ja analysoida tietoja, jotka koskevat ePO-palvelimen ja hallittujen järjestelmien tapahtumia (Trellix, 2024).

Palvelimelle on ennalta määritetty yli 50 erilaista kyselyä (Kuva 2), jotka voivat auttaa käyttäjiä analysoimaan mm. järjestelmän suorituskykyä sekä haittaohjelmien havaitsemista. Kyselyt voivat olla erilaisia kaavioon perustuvia visualisointeja tai taulukkomuotoisia esityksiä, jotka tuovat esiin tärkeää tietoa selkeässä ja helposti ymmärrettävässä muodossa.

Palvelintehtävä (Server task) on työkalu, jonka avulla kyselyitä voidaan suorittaa säännöllisesti. Järjestelmänvalvojat voivat asettaa automaattisen aikataulun kyselyiden ajamiselle, jolloin dataa kerätään ja analysoidaan jatkuvasti. Kyselyille voidaan asettaa lisätehtäviä, kuten tulosten lähettäminen sähköpostitse tai käytäntöjen tai merkintöjen lisääminen niiden perusteella.

Raportit tarjoavat dokumentoituja ja visuaalisesti jäsenneltyjä yhteenvetoja kerätystä datasta. Raportit ovat muokattavia asiakirjoja, jotka voivat sisältää tietoa yhdestä tai useammasta kyselystä. Raporttien joustavuus mahdollistaa niiden yhdistämisen tietoon, joka on peräisin useammasta tietokannasta.



Kuva 2. Muutama esimerkki ePOn ennalta määritetystä kyselystä.

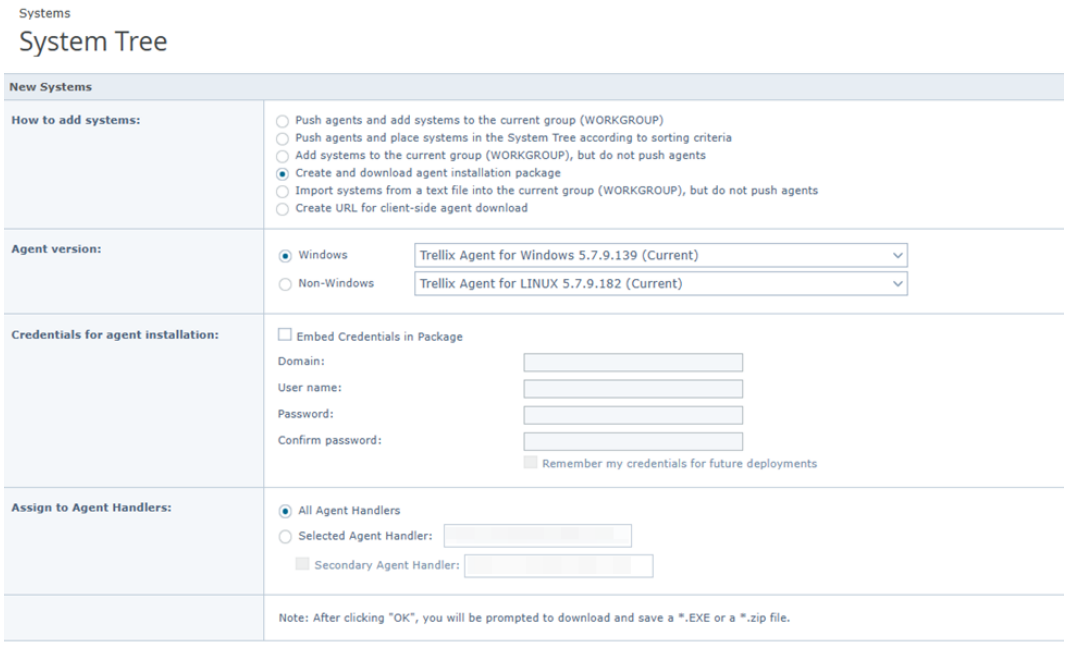
Lisäksi lokitiedot ovat tärkeä osa ePOn tiedonhallintaa. Ne dokumentoivat kaikki ePO-palvelimella ja verkossa tapahtuvat toimet, mikä tarjoaa järjestelmänvalvojille arvokasta taustatietoa järjestelmän toiminnasta. Lokitiedot auttavat ymmärtämään järjestelmän historiadataa ja muodostavat pohjan tarkempiin analyyseihin ja tietojen seurantaan.

4 TESTILAITTEEN ASENNUS

Aloitin tämän työn ottamalla käyttöön uuden Dell XE4 -pöytätietokoneen, mikä on myös tuotannossa laajasti käytössä. Asensin tietokoneeseen Windows 10 -käyttöjärjestelmän. Valitsin tämän käyttöjärjestelmän siitä syystä, että suurin osa tuotantolinjan testilaitteista ei vielä tue laajamittaisesti Windows 11 -versiota. Tuotannossa ollaan tekemässä siirtymistä uudempaan käyttöjärjestelmään, mutta valitsemalla vakiintuneen ja yhteensopivan Windows 10 -järjestelmän varmistin saumattoman integroinnin ja yhteensopivuuden muiden järjestelmien kanssa. Asennuksen jälkeen muutin tietokoneen nimeksi "PATest" ja loin laitteelle uuden käyttäjän nimellä "test".

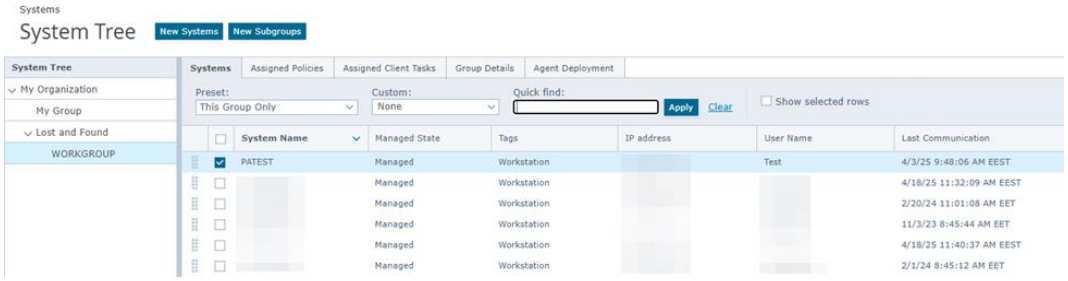
4.1 Testitietokone ja Trellix-agentti

Trellix ePO-palvelimella siirryin luomaan tietokoneelle agenttipaketin (Kuva 3). Valitsin agentin viimeisimmän version ja siirsin paketin Remote Desktop -ohjelmalla testitietokoneeseen.



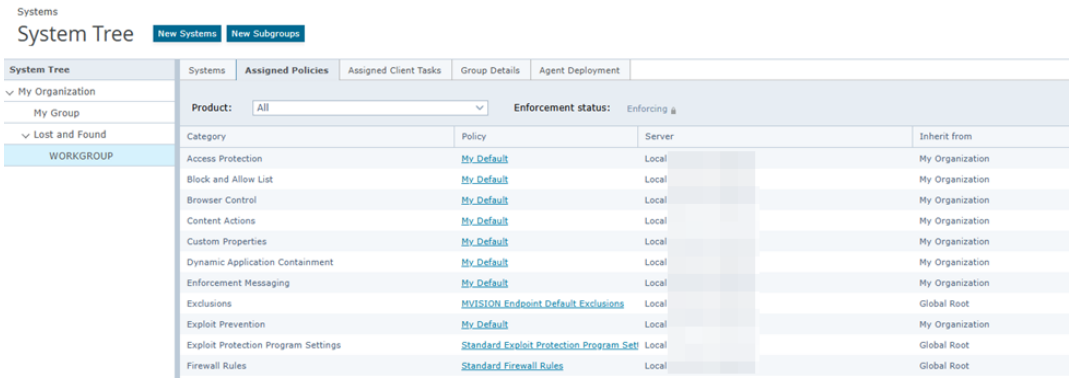
Kuva 3. Agenttipaketin luominen ePO-palvelimella.

Agentin asennuksen jälkeen tietokone on nähtävissä ePO-järjestelmässä (Kuva 4). Agentin luontihetkellä olin ”Lost and Found” ryhmän aliryhmässä nimeltä ”WORKGROUP”, minkä takia testitietokone ohjautui tähän ryhmään. Ryhmässä on nähtävissä muitakin tuotannon testikoneita. Laitteiden lisäksi tällä sivulla nähdään, onko laite käyttöhetkellä hallinnoitu, mikä merkintä, IP-osoite ja hallinoiva käyttäjä laitteella on sekä laitteen viimeisin kommunikointipäivämäärä.



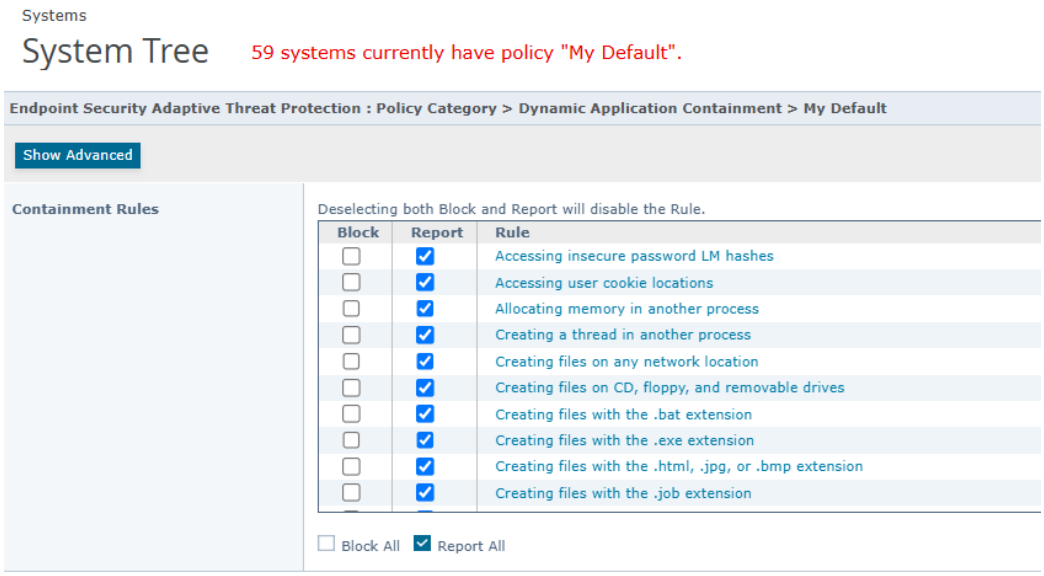
Kuva 4. Uusi järjestelmä ePO-kirjastossa.

Järjestelmäpuussa ”WORKGROUP” -ryhmään kuuluvien laitteiden lisäksi voidaan nähdä, mitkä käytännöt ja säännöt ryhmän laitteisiin vaikuttavat ”Assigned Policies” välilehdellä (Kuva 5). Välilehdellä nähdään käytännön kategoriat, mikä käytäntö on asetettu, miltä palvelimelta ja ryhmältä käytäntö periytyy.



Kuva 5. WORKGROUP-ryhmään vaikuttavat käytännöt.

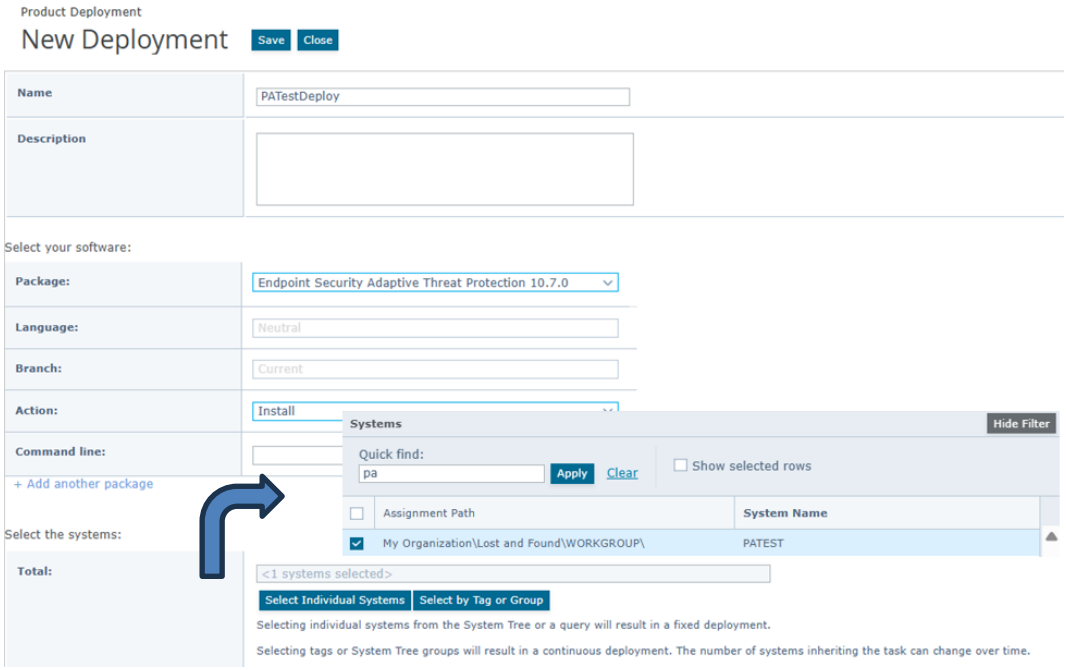
Esimerkiksi ”Dynamic Application Containment” -kategorian ”My Default” -käytännössä on säädetty tapahtumien raportointi sääntöjen rikkoutumisen tapahtuessa. Raportoinnin lisäksi säännön voi asettaa estetyksi, niin käyttäjä ei pysty kyseistä toimintoa suorittamaan.



Kuva 6. Osa My Default -käytäntöön asetetuista säännöksistä.

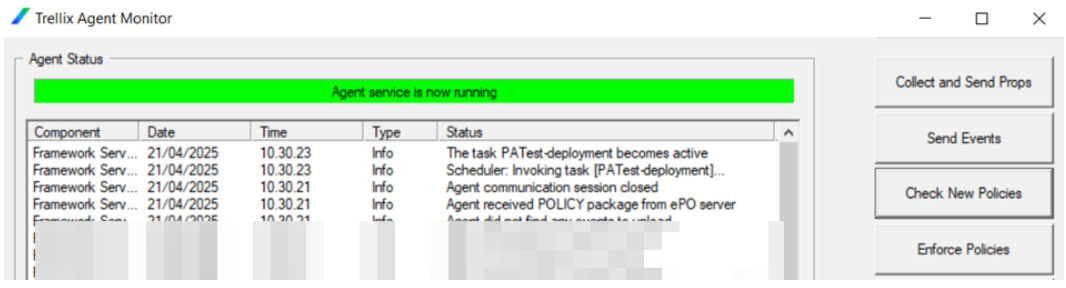
4.2 Trellix-tuotteiden lisääminen

Seuraavaksi lisäsin testikoneelle Trellixin Endpoint Security Adaptive Threat Protection-tuotteen sekä muita Trellixin tuotteita organisaation käytäntöjen mukaisesti. Siirryin ePOssa Product Deployment välilehdelle ja loin uuden tuotelähetyksen. Nimesin sen ”PATestDeploy”, valitsin halutun paketin ja testilaitteen mihin paketin asentaa (Kuva 7).



Kuva 7. Uusi tuotelähetys testilaitteelle.

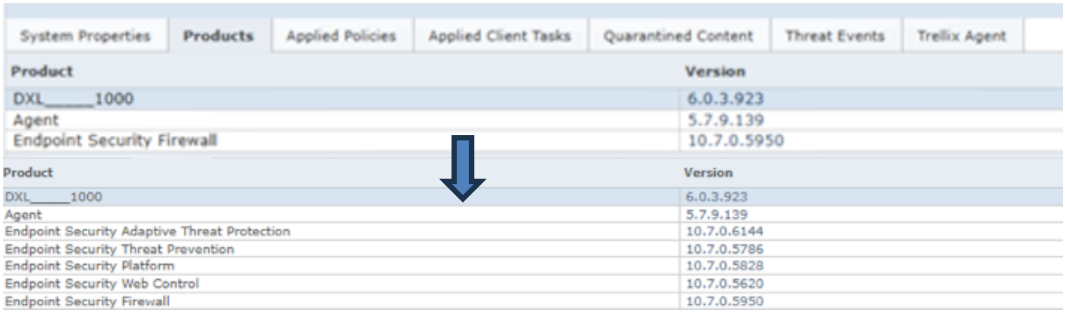
Hyväksymällä tehdyt asetukset, palvelin lähetti paketin eteenpäin testilaitteelle. Agentti aktivoitui vastaanottamaan uutta pakettia testilaitteessa (Kuva 8).



Kuva 8. Agentti vastaanottaa käytäntöpaketin ja aloittaa tehtävän ajamisen.

Hetken kuluttua valitut tuotteet olivat asentuneet testilaitteelle (Kuva 9). ”Adaptive Threat Protection” -paketin lisäksi asensin testilaitteelle

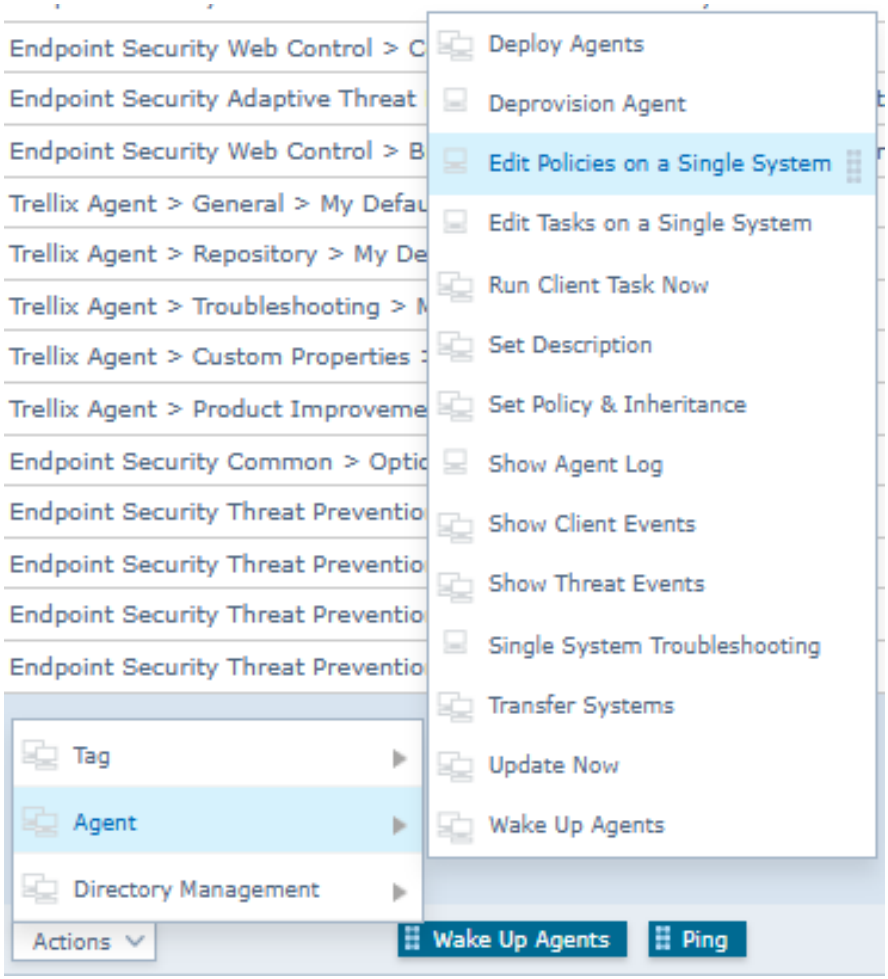
organisaation käytäntöjen mukaisesti ”Threat Prevention”, ”Platform”, ”Web Control” sekä ”Firewall” -paketit.



Kuva 9. Ennen ja jälkeen Trellix-tuotteiden asennuksen.

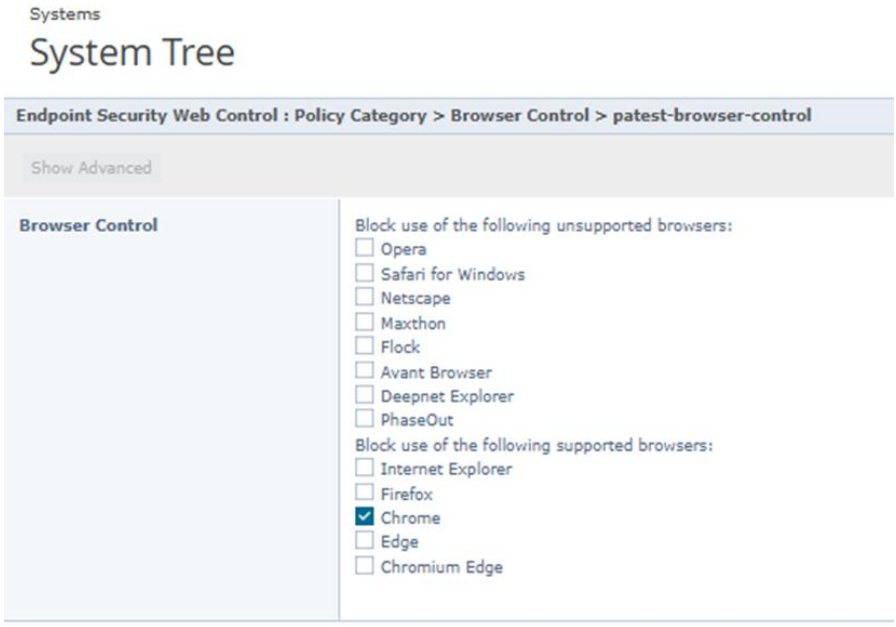
4.3 Testilaitteen uusi käytäntö

Testasin käytäntöjen rajaamista ePOlla tekemällä testilaitteelle uuden käyttörajoituksen. Järjestelmäpuu-ikkunassa valitsin PATest-laitteen ja siirryin mukauttamaan yhden laitteen käytäntöjä (Kuva 10.). Testin kohteeksi valitsin Google Chrome -selaimen.



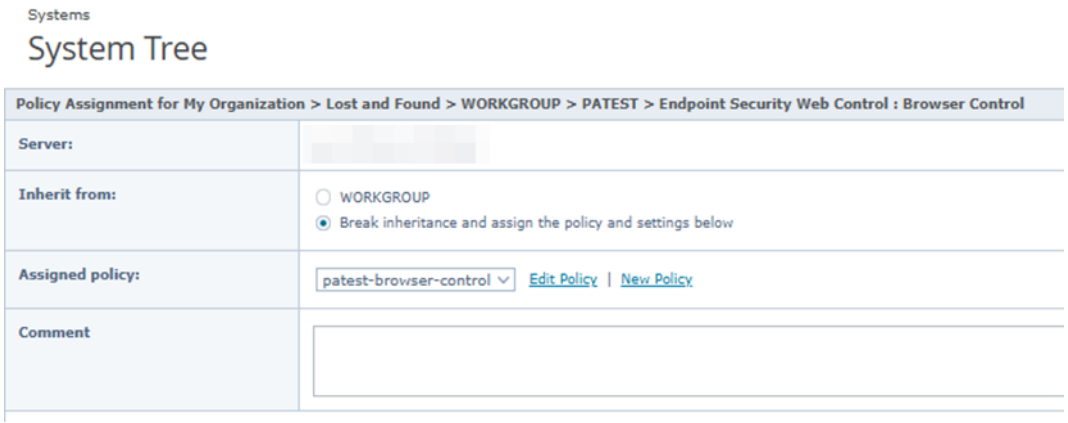
Kuva 10. Yhden laitteen käytäntöjen muokkaaminen ePOssa.

Voidakseni hallita, mitä selainta testikäyttäjä voi käyttää, valitsin käytännön pohjaksi ”Browser Control” ja lisäsin Chromen estolistalle (Kuva 11). Annoin käytännölle nimen ”PATest-browser-control” ja sen jälkeen erotin tämän käytännön ryhmäperiytymisestä (Kuva 12).



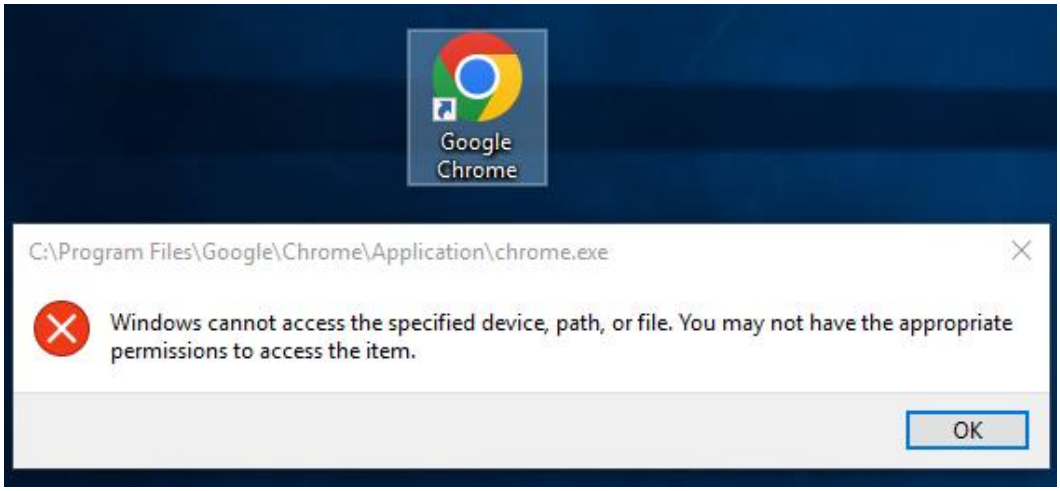
Kuva 11. Chrome-selaimen poisrajaaminen.

Käytännön tallentamisen ja seuraavan agenttikommunikaation jälkeen siirryin testilaitteelle ja kirjauduin testikäyttäjällä sisään. Kun käyttäjä yritti käynnistää Chrome-selaimen, se ei käynnistynyt ja sain kuvan mukaisen virheilmoituksen (Kuva 13.).



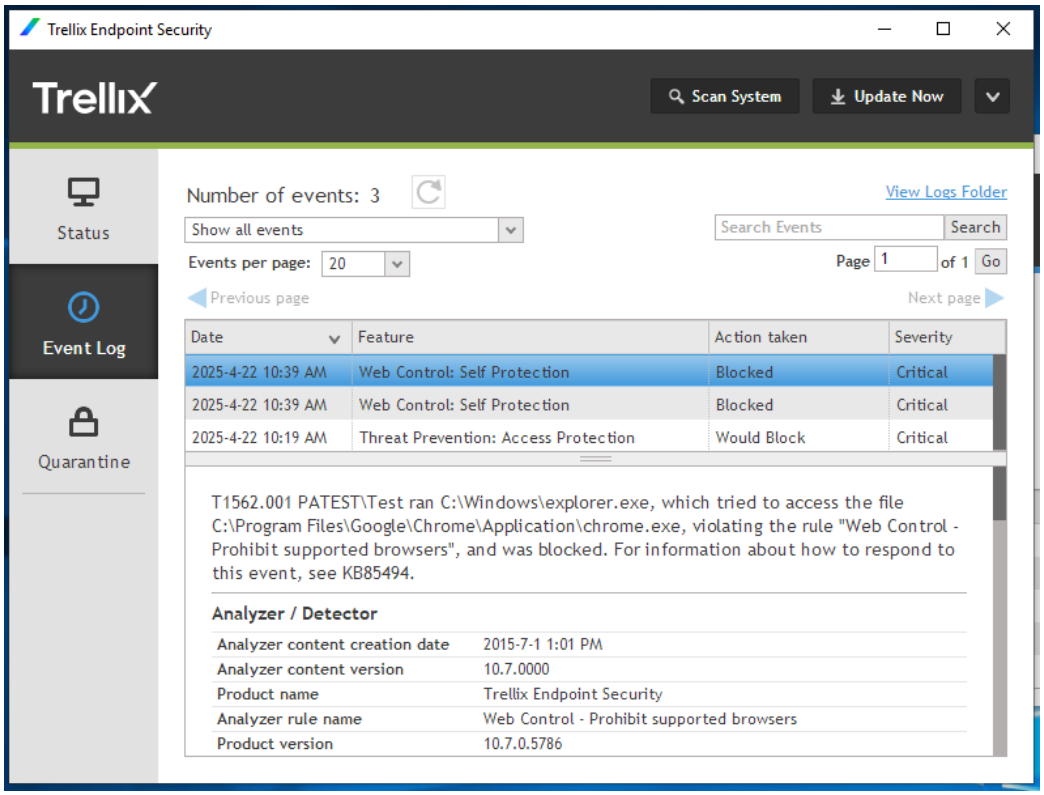
Kuva 12. Uuden käytännön poissulkeminen ryhmästä omaksi käytännöksi.

Virheilmoituksessa sanotaan, että ”Windows ei voi käyttää määritettyä laitetta, polkua tai tiedostoa. Sinulla ei ehkä ole asianmukaisia käyttöoikeuksia kohteen käyttämiseen.” Olin onnistuneesti rajannut testikäyttäjän oikeuksia käyttää käytäntöjenvastaista selainta.



Kuva 13. Testikäyttäjän yritys käyttää Chromea uuden käytännön aikana.

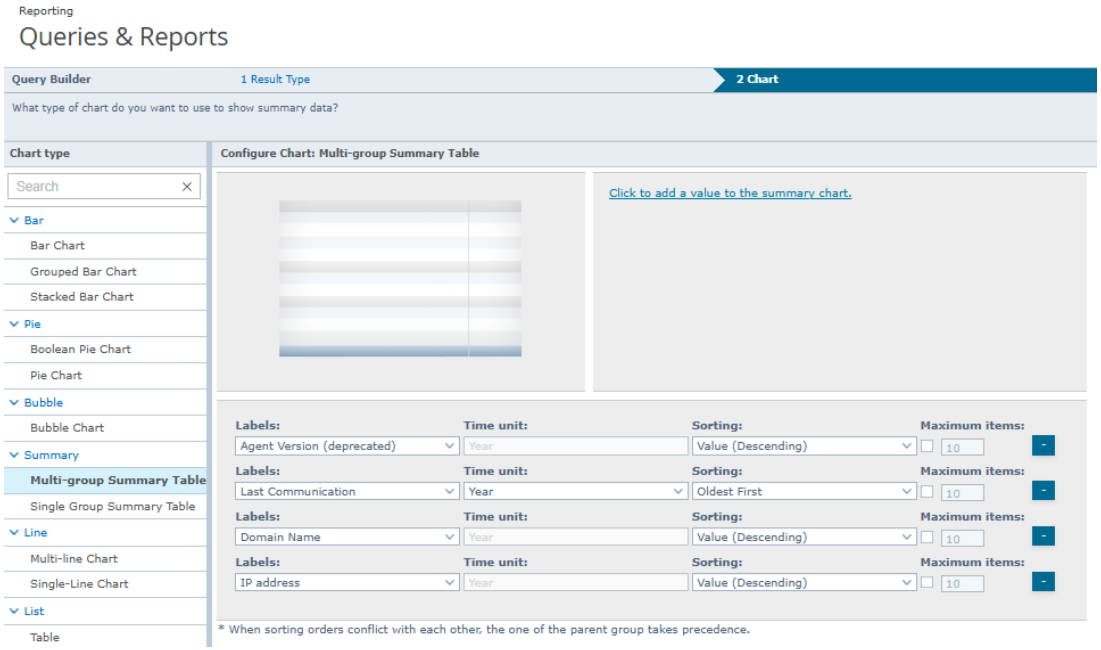
Trellix Endpoint Security-ohjelmassa sain Agentin tallentaman raportin tapahtumasta (Kuva 14.). Raportista näin, mitä ohjelmaa yritetään ajaa ja mistä polusta. Lisäksi raportti näytti, mitä käytäntöä oli rikottu ja mitä toimenpiteitä suoritettiin.



Kuva 14. Trellix Endpoint Securityn ilmoitus käytännönvastaisesta käytöstä.

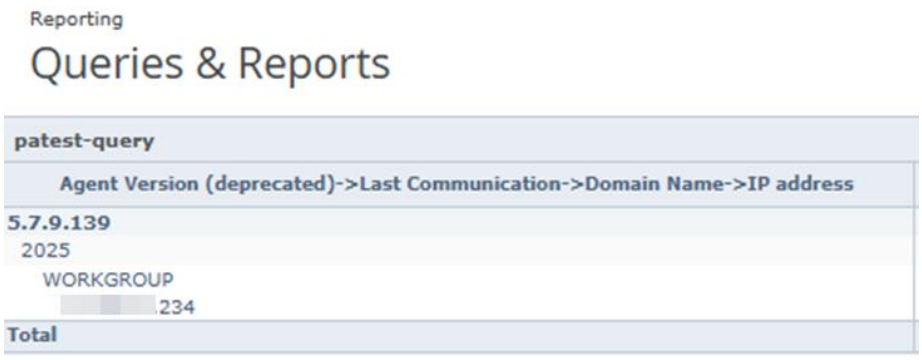
4.4 Uuden kyselyn testaaminen

Tulevien kyselyjen tarpeen vuoksi kokeilin uuden kyselyn luomista. ePO-palvelimella siirryin Queries & Reports-välilehdelle ja valitsin kyselyn pohjaksi Laitehallinnan. Tahdoin, että kysely palauttaa testilaitteesta seuraavat tiedot: Agentin versio, viimeinen kommunikointiajankohta, verkkotunnus sekä IP-osoite (Kuva 15). Seuraavaksi rajasin kyselyn kohteeksi PATest-testilaitteen.



Kuva 15. Uuden kyselyn luominen.

Uuden kyselyn tallentamisen jälkeen ajoin sen ja sain haluamani tiedot testilaitteelta (Kuva 16). Tuloksista nähtiin, että Agentin versio on 5.7.9.139, laite on viimeksi kommunikoinut vuonna 2025, sen verkkotunnus on WORKGROUP ja IP-osoite on xxx.xxx.xxx.234.



Kuva 16. Uuden kyselyn saama vastaus.

5 LOPPUPÄÄTELMÄ

Projektin tavoitteena oli tutustua syvemmin Trellix ePOn toimintaan ja sen tuomiin ylläpitomahdollisuuksiin organisaation tuotannon laitteissa. Työllä pyrittiin ymmärtämään järjestelmän potentiaalia IT-ympäristön hallinnassa ja suojaamisessa. Työ keskittyi ePOn päivittäiseen käyttöön, joka sisältää kolme keskeistä osaa, kuten uuden laitteen lisäämiseen järjestelmään, tietoturvatuotteiden ja käytäntöjen jakamiseen sekä kyselyihin ja raportointiin.

5.1 Haasteet

Uuden laitteen lisäämisessä kohtasin ongelman Agentin asentamisessa verkon kautta. Työn aikana ongelmaan ei löytynyt ratkaisua, mutta todennäköistä on, että ongelmalla oli jotain tekemistä AD-tunnusten (Active Directory) kanssa eikä oikeuksia ollut tarpeeksi laitteen lisäämiseen verkon kautta organisaatiossa. Tämä ongelma saatiin kierrettyä käyttämällä ePOn muita uuden laitteen lisäämisvaihtoehtoja, mikä tässä työssä oli Agentti-paketin luominen ja sen siirtäminen etäyhteydellä Remote Desktopilla testilaitteeseen.

Työstä teki haastavan myös se, ettei selkeitä tai kattavia ohjeita ollut, joihin olisi voinut tukeutua työtä tehdessä. Tämä vaikeutti työskentelyä erityisesti alussa, kun ohjelman perustoiminnotkin olivat vielä vieraita. Edellisen käyttäjän kokemus olisi ollut myös arvokasta ja säästänyt aikaa. Jos ohjelman käyttöä halusi oppia kunnolla, ainoa vaihtoehto oli rekisteröityä erilliselle kurssille, jossa ohjelmaa opetettiin.

5.2 Saavutukset

Agentin asentaminen verkon kautta ei onnistunut, mutta Agentin luominen ja sen asentaminen onnistui moitteetta. Sen lisäksi myös tietoturvatuotteiden, -käytäntöjen, kyselyiden sekä raporttien luominen

ja jakaminen oli helppoa ja tehokasta. Kymmenien eri tietoturvatuotteiden sekä -käytäntöjen automatisoiminen yhdeltä palvelimelta satoihin eri laitteisiin helpottaa huomattavasti järjestelmävalvojan taakkaa sekä nopeuttaa merkittävästi tietoturvauhkien havaitsemista.

Kurssille ilmoittautuminen osoittautui erinomaiseksi ratkaisuksi ohjelman oppimisen kannalta. Erityisen hyödylliseksi kurssi osoittautui siksi, että opittua tietoa pystyi soveltamaan käytännössä heti. Kurssilla saadut taidot eivät jääneet pelkästään teoreettisiksi, vaan niitä voitiin hyödyntää suoraan työtehtävissä.

5.3 Jatkotoimenpiteet

Trellix ePO on osoittautunut arvokkaaksi työkaluksi modernissa IT-ympäristössä, jossa tehokkuus ja tietoturva ovat keskeisiä tavoitteita. Tämän projektin aikana keskityttiin ePOn ylläpitokyvyn perusteisiin ja päivittäisiin toimintoihin, mutta ePOn täysi potentiaali on vielä tutkimatta, ja sen kattavampi hyödyntäminen voisi tuoda merkittäviä etuja organisaation tietoturvan parantamisessa sekä operatiivisen tehokkuuden lisäämisessä. Järjestelmän mahdollisuuksien syvällisempi arviointi voi avata uusia näkökulmia ja ratkaisuja tietoturvan hallintaan ja prosessien optimointiin.

LÄHTEET

ABB. 2024. *ABB lyhyesti*. Noudettu 31.5.2025 osoitteesta https://new.abb.com/fi/abb-lyhyesti

ABB. 2024. *ABB Oy - Distribution Solutions*. Noudettu 31.5.2025 osoitteesta https://new.abb.com/fi/abb-lyhyesti/suomessa/liiketoiminnat/distribution-solutions

Hynninen Ensio. 2024. *Kyberturvallisuuden tulevaisuus*. Noudettu 31.5.2025 osoitteesta https://mindspace.fi/kyberturvallisuuden-tulevaisuus-haasteet-ja-mahdollisuudet/

Sisäministeriö. 2022. *Kyberturvallisuus*. Noudettu 31.5.2025 osoitteesta https://intermin.fi/kansallinen-turvallisuus/kyberturvallisuus

Trellix. 2021. *Combination of McAfee Enterprise and FireEye Complete*. Noudettu 31.5.2025 osoitteesta https://www.trellix.com/news/press-releases/combination-of-mcafee-enterprise-and-fireeye-complete/

Trellix. 2024. *Dashboards, Queries, and Reports – Dashboards Overview*. Noudettu 26.4.2025 osoitteesta https://training-catalog.trellix.com/Course/135678/elearning-epolicy-orchestrator-on-prem-essentials

Trellix. 2024. *Dashboards, Queries, and Reports – Queries and Reports Overview*. Noudettu 26.4.2025 osoitteesta https://training-catalog.trellix.com/Course/135678/elearning-epolicy-orchestrator-on-prem-essentials

Trellix. 2024. *Endpoint Security*. Noudettu 26.4.2025 osoitteesta https://www.trellix.com/products/endpoint-security/

Trellix. 2024. *ePO Overview – How it Works*. Noudettu 26.4.2025 osoitteesta https://training-catalog.trellix.com/Course/135678/elearning-epolicy-orchestrator-on-prem-essentials

Trellix. 2024. *ePO Overview – Basic Product Components*. Noudettu 26.4.2025 osoitteesta https://training-

catalog.trellix.com/Course/135678/elearning-epolicy-orchestrator-on-prem-essentials

Trellix. 2024. *Policy Management – Policy Management*. Noudettu 26.4.2025 osoitteesta https://training-catalog.trellix.com/Course/135678/elearning-epolicy-orchestrator-on-prem-essentials

Trellix. 2024. *Product Management – Client Task Management*. Noudettu 26.4.2025 osoitteesta https://training-catalog.trellix.com/Course/135678/elearning-epolicy-orchestrator-on-prem-essentials

Trellix. 2024. *Product Management – Software Catalog*. Noudettu 26.4.2025 osoitteesta https://training-catalog.trellix.com/Course/135678/elearning-epolicy-orchestrator-on-prem-essentials

Trellix. 2024. *Server Configuration – System Tree overview*. Noudettu 26.4.2025 osoitteesta https://training-catalog.trellix.com/Course/135678/elearning-epolicy-orchestrator-on-prem-essentials

Trellix. 2024. *Trellix – Datasheet*. Noudettu 26.4.2025 osoitteesta https://www.trellix.com/assets/docs/data-sheets/trellix-epo-datasheet.pdf

Trellix. 2024. *Trellix Agent Overview - Product Overview*. Noudettu 26.4.2025 osoitteesta https://training-catalog.trellix.com/Course/135678/elearning-epolicy-orchestrator-on-prem-essentials