LAB University of Applied Sciences

# Järjestelmäasiantuntijana kehittyminen yrityksen tietoturvatiimissä

LAB-ammattikorkeakoulu
Insinööri (AMK)
2024
Niko Eriksson

**Tiivistelmä**

| Tekijä(t) | Julkaisun laji | Valmistumisaika |
|---|---|---|
| Niko Eriksson | Opinnäytetyö, AMK | 2024 |
| | Sivumäärä | |
| | 22 | |

Työn nimi

**Järjestelmäasiantuntijana kehittyminen yrityksen tietoturvatiimissä**

Tutkinto ja koulutusala

Insinööri (AMK), Tieto- ja viestintätekniikka

Toimeksiantajaorganisaatio (jos opinnäytetyöllä on toimeksiantaja)

Bauhaus & Co Ky

Tiivistelmä

Opinnäytetyön tavoitteena oli esitellä kahden erilaisen työkalun ominaisuuksia ja kuinka erityisesti niiden yhteistoiminnan avulla voidaan toteuttaa sekä kehittää yrityksen tietoturvaa. Lisäksi seurataan osallistumista projektiin, jossa suunnitellaan ja toteutetaan yritykselle uusi AD (Active Directory) korvaamaan aiempi AD. Päiväkirjamuotoisena toteutetun opinnäytetyön viikkoanalyyseissä seurataan näihin teemoihin liittyviä tehtäviä, toteutuksia, havaintoja sekä kehittymistä.

Ensimmäinen esiteltävistä työkaluista ovat Forcepoint-palomuurit. Näitä hallinnoidaan keskitetyltä hallintakonsolilta, jossa luodaan politiikat sekä seurataan verkkoliikennettä.

Toinen esiteltävistä työkaluista on Lansweeper asset management -työkalu, joka tarjoaa keinon verkon valvontaan verkkoon liitettyjen laitteiden, käyttäjien ja ohjelmistojen osalta. Yhdessä nämä kaksi työkalua tarjoavat keinon valvoa koko verkkoa sekä liikenteen, että laitteiden, käyttäjien ja ohjelmistojen osalta.

Asiasanat

Tieto- ja viestintätekniikka, tietoturva, järjestelmäasiantuntija, verkonvalvonta

**Abstract**


| Author(s) | Type of Publication | Published |
|---|---|---|
| Niko Eriksson | Thesis, UAS | 2024 |
| | Number of Pages | |
| | 22 | |


Title of Publication

**Developing as a system administrator in company's cyber security team**

Degree, Field of Study

Engineer (UAS), Information and communications technology

Organization of the client (if the thesis work is commissioned by another party)

Bauhaus & Co Ky


Abstract

The aim of the thesis was to present the properties of two different tools and how they especially when used together can be used to implement and develop the company's information security. Also participation in a project is monitored where a new AD (Active Directory) is planned and implemented for the company to replace the previous AD. In the weekly analyses of the thesis carried out in the form of a diary, the tasks, realizations, research and development related to these themes are monitored.

The first tool to be introduced is Forcepoint firewalls. These are managed from a centralized management console where policies are created and network traffic is monitored.

Another of the presented tools is the Lansweeper asset management tool which offers a way to monitor the network in terms of devices, users and software connected to the network. Together, these two tools provide a way to monitor the entire network both for traffic and for devices, users, and software.



Keywords

ICT, security, system administrator, network monitoring

Sisällys

**Sanasto**

| | |
|---|---|
| AD | Active Directory. Käyttäjätietokanta |
| AM | Asset Management. Yrityksen verkkoon kytkettyjen laitteiden hallinta |
| API | Application Programming Interface. Ohjelmointirajapinta, jonka avulla eri ohjelmat voivat keskustella keskenään |
| Asset | Yrityksen verkkoon kytketty laite tai yrityksen omistuksessa oleva laite |
| CDR | Credential-free Device Recognition. Lansweeper työkalun konfiguraatio assetien skannaamiseen |
| CISO | Chief Information Security Officer. Yrityksen tietoturvajohtaja |
| CVSS | Common Vulnerability Scoring System. Standardi tietoturva-aukkojen vakavuuden arvioimiseksi |
| DC | Domain Controller. Palvelin, joka vastaa toimialueen tietoturvatodennuspyynnöistä |
| DLP | Data Loss Prevention. Tietojen menetyksen estäminen. Prosessi, jolla pyritään estämään arkaluontoisten tietojen vuotaminen. |
| DoS | Denial of Service. Yhdestä lähteestä tapahtuva hyökkäys, jolla pyritään estämään verkkosivuston tai palvelun käyttö |
| DDoS | Distributed Denial of Service. Useasta lähteestä tapahtuva hyökkäys, jolla pyritään estämään verkkosivuston tai palvelun käyttö |
| FTP | File Transfer Protocol. Tiedonsiirtomenetelmä kahden laitteen välillä |
| GPO | Group Policy Object. Kokoelma sääntöjä, joilla ohjaillaan ryhmien, kone- tai käyttäjätilien toimintaa ja pääsyoikeuksia |
| HA | High Availability. Laitteiden tai järjestelmien keskeytyksetön toiminta |
| HTTPS | Hypertext Transfer Protocol Secure. Protokolla suojattuun tiedonsiirtoon verkkosivuston ja selaimen välillä |
| IDS | Intrusion detection system. Tunkeutumisen tunnistusjärjestelmä |
| IP | Internet Protocol. Protokolla IP-paketeille tietoverkoissa |

| | |
|---|---|
| IP-osoite | Internet Protocol -osoite. Laitteen numeerinen osoite tietoverkossa |
| IPS | Intrusion Prevention System. Tunkeutumisen suojajärjestelmä |
| MDR | Managed Detection and Response. Kyberturvallisuuspalvelu tietoturvauhkien tunnistamiseen ja torjumiseen |
| NGFW | Next generation firewall. Seuraavan sukupolven palomuuri |
| NCSC | National Cyber Security Centre. Kansallinen kyberturvallisuuskeskus |
| On-Prem | On-Premises. Laite sijaitsee fyysisesti yrityksen tiloissa tai järjestelmää ajetaan palvelimelta, joka sijaitsee fyysisesti yrityksen tiloissa |
| M365 | Microsoft 365. Microsoftin pilvipohjainen tuottavuusympäristö |
| RDP | Remote Desktop Protocol. Protokolla toisen laitteen etähallintaan |
| SSO | Single sign-on. Autentikointimenetelmä käyttäjän todentamiseksi |
| TCP | Transmission Control Protocol. Protokolla laitteiden väliseen tiedonsiirtoon |
| VLAn | Virtual Local Area Network. Virtuaalilähiverkko, jossa fyysinen tietoliikenneverkko on jaettu loogisiin osiin |
| WMI | Windows Management Instrumentation. Windowsin infrastruktuuri joka tarjoaa tietoa tietokonejärjestelmän tilasta |

# 1 Johdanto

Nykypäivänä yrityksen tietoturvasta huolehtiminen on tärkeää ja sen toteuttaminen vaatii riittävät resurssit sekä erityisesti oikeanlaiset tarkoituksenmukaiset työkalut. Hyvä tietoturva toki ennaltaehkäisee mutta myös valvoo kaikessa yrityksen verkossa tapahtuvaa. Tämän periaatteen perusteella opinnäytetyön tarkoituksena on selvittää kahden erilaisen työkalun ominaisuuksia, joilla tietoturvasta huolehditaan ennaltaehkäisevästi sekä valvotaan tietoturvan toteutumista.

Tähän opinnäytetyöhön valitut työkalut ovat päivittäisessä käytössäni. Niiden valvonta ja yrityksen tietoturvan kehittäminen näiden avulla ovat keskeinen osa työnkuvaani.

Tietoturva on alana jatkuvan muutoksen kohteena. Uusia tietoturvallisempia protokollia, standardeja, ohjelmistoja ja käytäntöjä tuodaan käyttöön aiempien vanhetessa ja usein jäädessä ilman tukea ja päivityksiä. Alan trendejä ja uutisointia on seurattava tiiviisti, jotta on mahdollista vastata uusimpiin tietoturvauhkiin.

## 2 Lähtötilanteen kuvaus

Olen toiminut nykyisessä työtehtävässäni järjestelmäasiantuntijana kesästä 2022 lähtien. Ensisijainen tehtäväni on ylläpitää ja edistää yrityksen tietoturvaa. Olen tuossa ajassa ehtinyt tutustumaan useisiin erilaisiin ohjelmistoihin, järjestelmiin sekä tietoturvaan yleisesti. Tehtävässä toimiminen edellyttää useiden eri järjestelmien osaamista sekä jatkuvaa alaan liittyvän uutisoinnin seurantaa esimerkiksi meneillään oleviin sekä uusiin tietoturvauhkiin liittyen.

Tieto- ja viestintätekniikan insinööriksi opiskelu on antanut hyvän pohjan alaan liittyvistä peruskäsitteistä mutta itse työ on kuitenkin huomattavasti laaja-alaisempaa kuin koulussa opiskellut asiat. Erilaisten järjestelmien ominaisuuksien ja toiminnallisuuksien opiskelu on ollut vaativaa mutta arvioin, että olen edistynyt kiitettävästi lyhyessä ajassa ja koen olevani jo merkittävä osa yrityksen tietoturvatiimiä. Paljon on vielä opittavaa mutta alun haasteista selviäminen on antanut itseluottamusta työtehtävässä kehittymiseen.

# 3 Forcepointin palomuurit

## 3.1 Forcepointin NGFW-palomuureista yleisesti

Forcepointin palomuurit ovat pääasiassa niin kutsuttuja NGFW:tä (Next generation firewall) eli seuraavan sukupolven palomuureja. Siinä missä tavanomainen palomuuri ainoastaan seuraa tilatietoisesti liikennettä molempiin suuntiin, NGFW yleisesti sisältää lisäominaisuuksia kuten application awareness (sovellustietoisuus), IPS (Intrusion Prevention System) ja threat intelligence (uhkatieto). (Cisco)

Forcepointin NGFW-palomuureja on saatavilla useita erilaisia malleja useisiin erilaisiin ympäristöihin. Vaihtoehdoista löytyy soveltuvia malleja esimerkiksi kampusympäristöihin tai pienempiin haarakonttoreihin. (Forcepoint a.)

Forcepointin NGFW-palomuurien teknisistä tiedoista (Kuva 1.) voidaan todeta, että ne ovat soveltuvia alan suurimpien pilvi-infastruktuurien kanssa (Amazon Web Services, Microsoft Azure, Google, Oracle ja IBM). Käyttäjän todennukseen löytyy useita ratkaisuja kuten esimerkiksi AD (Active Directory). (Forcepoint 2023b.)

| PLATFORMS | |
|---|---|
| **Physical Appliance** | Multiple hardware appliance options, ranging from branch office to data center installations |
| **Cloud Infrastructure** | Amazon Web Services, Microsoft Azure, Google, Oracle, IBM |
| **Virtual Appliance** | x86 64-bit based systems; VMware ESXi, VMware NSX, Microsoft Hyper-V, KVM, and Nutanix AHV |
| **Endpoint** | Endpoint Context Agent (ECA), VPN Client |
| **Virtual Contexts** | Up to 250 |
| **Centralized Management** | Enterprise-level centralized management system with log analysis, monitoring, and reporting capabilities. See the Forcepoint Security Management Center datasheet for details. |
| **FIREWALL FEATURES** | |
| **Deep Packet Inspection** | Multi-Layer Traffic Normalization/Full-Stream Deep Inspection, Anti-Evasion Defense, Dynamic Context Detection, Protocol-Specific Traffic Handling/Inspection, Granular Decryption of SSL/TLS Traffic (both TLS 1.2 and 1.3), Vulnerability Exploit Detection, Custom Fingerprinting, Reconnaissance, Anti-Botnet, Correlation, Traffic Recording, DoS/DDoS Protection, Blocking Methods, Automatic Updates |
| **User Identification** | Internal user database, Native LDAP, Microsoft Active Directory, RADIUS, TACACS+, Microsoft Exchange, Client Certificates |
| **High Availability** | › Active-active/active-standby firewall clustering up to 16 nodes<br>› SD-WAN<br>› Stateful failover (including VPN connections)<br>› Server load balancing<br>› Link aggregation (802.3ad)<br>› Link failure detection |
| **IP Address Assignment** | › IPv4 static, DHCP, PPPoA, PPPoE, IPv6 static, SLAAC, DHCPv6<br>› Services: DHCP Server for IPv4 and DHCP relay for IPv4 and IPv6 |
| **Routing** | › Static IPv4 and IPv6 routes, policy-based routing, static multicast routing<br>› Dynamic routing: RIPv2, RIPng, OSPFv2, OSPFv3, BGP, MP-BGP, BFD, PIM-SM, PIM-SSM, IGMP proxy<br>› Application-aware routing |
| **IPv6** | Dual-stack IPv4/IPv6, NAT64, ICMPv6, DNSv6, NAT, Full NGFW features |
| **Proxy Redirection** | HTTP, HTTPS, FTP, SMTP protocols redirection to Forcepoint or third-party Content Inspection Service (CIS) on-premise and cloud |
| **Geo-Protection** | Dynamically updated source/destination country or continent |
| **IP Address List** | Predefined IP categories or using custom or imported IP address lists |
| **URL Filtering (Separate Subscription)** | Custom or imported URL lists; supports QUIC and HTTP/3 |
| **Endpoint Applications** | Application name and version |
| **Network Applications** | 7400+ network and cloud applications |
| **Sidewinder Security Proxies** | TCP, UDP, HTTP, HTTPS, SSH, FTP, TFTP, SFTP, DNS |

Kuva 1. Forcepointin NGFW-palomuurien teknisiä tietoja (Forcepoint 2023b.)

## 3.2 IPS

IPS on yksi Forcepointin NGFW-palomuurien ominaisuuksista. Sen tarkoitus on valvoa pääsyä verkkoon ja suojata sitä mahdollisilta hyökkäyksiltä sekä väärinkäytöksiltä. Toisin kuin IDS (Intrusion Detection System) joka keskittyy vain valvontaan, IPS myös suorittaa

tarvittavia toimenpiteitä, joilla hyökkäys tai väärinkäyttö estetään tai niiden kehittyminen estetään. (Forcepoint b.)

Tällaisia hyökkäyksiä ovat esimerkiksi:

- DoS (Denial of Service)
- DDoS (Distributed Denial of Service)
- Haavoittuvuuksien hyväksikäyttö
- Madot
- Virukset (Forcepoint b).

IPS suorittaa reaaliaikaista pakettien tarkistusta verkossa. Jos haitallisia tai epäilyttäviä paketteja havaitaan, suorittaa IPS jonkin seuraavista toimenpiteistä:

- Katkaistaan hyväksikäytetty TCP-istunto (Transmission Control Protocol) ja estä hyökkäävältä IP-osoitteelta tai käyttäjätililtä pääsy sovelluksiin, kohdepalvelimeen tai muihin verkon resursseihin
- Ohjelmoidaan tai konfiguroidaan palomuuri estämään vastaava hyökkäys tulevaisuudessa
- Poistetaan tai korvataan kaikki haitallinen sisältö, joka jää verkkoon hyökkäyksen jälkeen. Tämä tehdään pakkaamalla hyötykuorma (datalähetys) uudelleen, poistamalla otsikkotiedot ja poistamalla infektoituneet liitteet tiedosto- tai sähköpostipalvelimista. (Forcepoint b.)

## 3.3 Sovellustietoisuus

Sovellustietoisuus (Application Awareness) on Forcepointin palomuurien ominaisuus, jolla voidaan valvoa ja hallita erilaisia sovelluksia. Tämän ominaisuuden avulla voidaan esimerkiksi sallia resurssin (sovelluksen) käyttö vain tietyille käyttäjille tai ryhmille. Tietoturvaa voidaan tiukentaa vaatimalla käyttäjän autentikointia ennen resurssin käytön sallimista. Autentikointi voidaan tehdä esimerkiksi sertifikaatin perusteella, jolloin käyttäjältä ei vaadita manuaalista tunnistautumista. (Forcepoint 2023d.)

Forcepoint pystyy tunnistamaan verkkoliikenteestä useita ennalta määriteltyjä sovelluksia. Tarkastelemalla TCP/IP-protokollan paketteja se kykenee tunnistamaan käytetyn protokollan, vaikka liikennöintiin ei käytettäisikään tavanomaisia portteja (Forcepoint. Getting started with Network Application elements). Oletussovellusten lisäksi on mahdollista lisätä

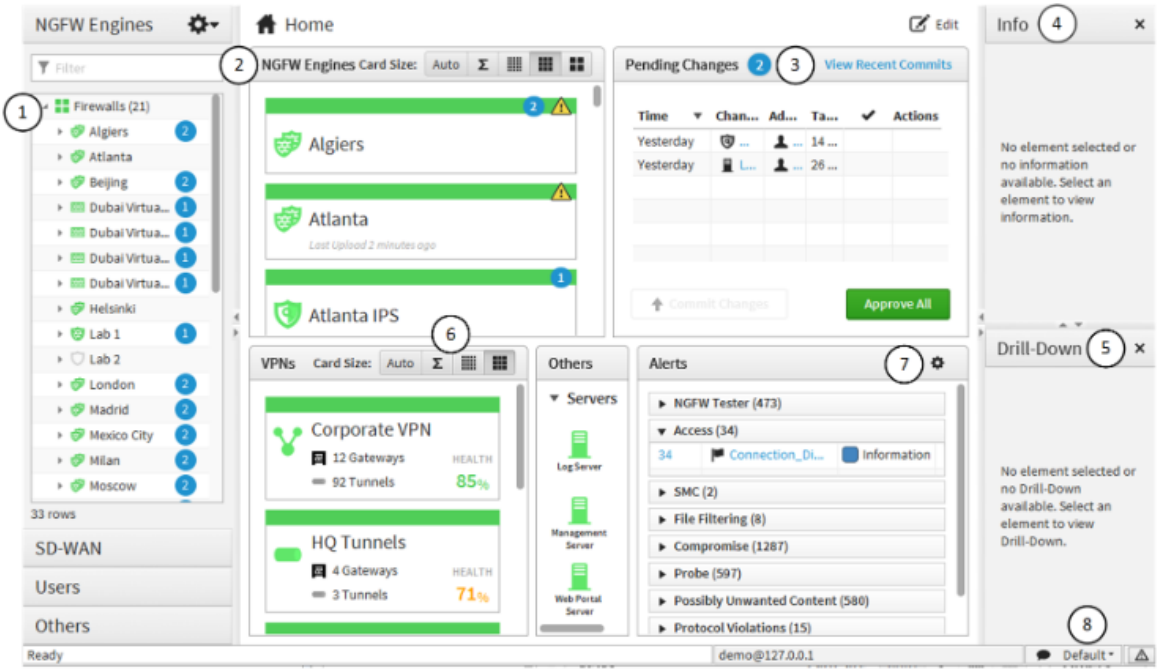
omia sovellustunnisteita, mikäli sovelluksesta tiedetään tarkasti siihen liittyvistä liikennöintimalleista. (Stonesoft 2018b.)

## 3.4 Keskitetty hallinta

Forcepoint-palomuurien hallinta on hyvin käyttäjäystävällistä hallintakonsolin avulla, josta ohjataan keskitetysti kaikkia palomuureja. Hallintakonsolista voi asentaa applikaation työasemalle tai hallintakonsoliin voi vaihtoehtoisesti muodostaa yhteyden myös web-käyttöliittymällä.

Alla on kuva (Kuva 2.) Forcepointin palomuurien hallintakonsolin yleisnäkymästä ja numeroidut selitteet hallintakonsolin näkymän moduuleihin.

1. Palomuurien status
2. Valvottujen elementtien tilakortit
3. Odottavat muutokset esim. konfiguraatio- ja politiikkamuutokset
4. Valitun elementin lisätiedot
5. Pikakuvake valitun elementin lisätietoihin
6. Vaihtoehdot tilakorttien näkymien hallintaan
7. Hälytykset. Esimerkissä järjesteltynä tyypin mukaan
8. Järjestelmän valvonnan lokaatio

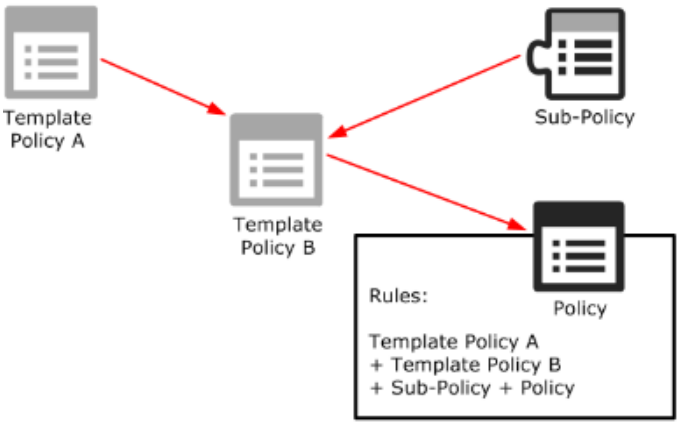



Kuva 2. Esimerkkikuva Forcepointin palomuurien hallintakonsolista (Stonesoft 2018c.)

## 3.5 Politiikat ja säännöt

Politiikoiden konfiguroinnit muodostuvat neljästä politiikkaelementistä (Kuva 3.). Näitä ovat:

- Inspection policy (Tarkastuspolitiikka)– Korkeimman tason elementti. Määrittelee sallitun liikenteen analyysin.
- Template policy (mallipolitiikka) – Toisiksi ylimmän tason elementti. Sapluuna, josta voidaan johtaa uusia mallipolitiikoita tai politiikoita.
- Sub-policy (alapolitiikka) – Elementti, jolla määritellään kriteerit ehtojen mukaisen liikenteen salliminen tai estäminen. Esimerkkinä sallitaan kaikki HTTPS-liikenne verkosta A verkkoon B.
- Policy (politiikka) – Lopputuote. Politiikkaan kerätään yhteen kaikki yllä mainitut (Stonesoft. 2018a.)




Kuva 3. Politiikkahierarkia (Stonesoft, 2018a)

Politiikat on syytä selkeyden vuoksi nimetä loogisesti ja käyttötarkoitustaan kuvaavasti. Esimerkiksi tilanne, jossa yrityksellä on useita toimistoja, joissa useita verkkoja. Tavoitteena luoda kuvaava politiikka, joka koskee toimiston A työasemaverkkoa, voidaan luoda mallipolitiikka (template policy) ”Toimisto_A_policy” johon liitetään alapolitiikka (sub-policy) ”Toimisto_A_työasemaverkko”. Loogisella ja käyttötarkoitustaan kuvaavalla politiikoiden nimeämiskäytännöillä politiikoiden kokonaiskuva pysyy selkeänä, vaikka politiikoita kertyisikin huomattava määrä.

# 4 Lansweeper asset management -työkalu

## 4.1 Lansweeperistä yleisesti

Lansweeper on yrityskäyttöön suunniteltu IT-työkalu, jonka tarkoitus on automatisoida sekä helpottaa verkon assetien (laitteiden) inventointia sekä hallintaa. Lansweeper tarjoaa useita käyttömalleja, joita ovat esimerkiksi:

- Asset discovery – Verkon laitteiden löytäminen
- Asset Inventory – Laitteiden tunnistus ja laitetiedot
- Analytics – Erilaista analytiikka esimerkiksi laitemääristä, raporteista yms.
- Risk Insights – Tunnistaa laitteiden tai verkon haavoittuvuuksia
- Network Topology Diagrams – Generoi automaattisesti visuaalisen verkkotopologian
- Integrations – API-pohjaiset (Application Programming Interface) integraatiot

(Lansweeper. 2023a.)

Lansweeper tarjoaa kolmea erilaista tilaustyyppiä, joita ovat Starter, Pro ja Enterprise. Tilaustyyppi määrittelee, minkälaisia ominaisuuksia on käytettävissä ja hinnoittelu perustuu tilaustyypin lisäksi skannattavissa olevien assetien määrään.

Lansweeper tarjoaa myös ilmaisen tilaustyypin, jossa assetien määrä on rajoitettu 100 assetiin. Tämä malli soveltuu pienille yrityksille tai yksityiseen käyttöön. (Lansweeper, 2023b)

Lansweeperin avulla voi luoda esimerkiksi raportteja verkon uusista laitteista, AD:n uusista käyttäjä- tai konetileistä, tietokoneisiin asennetuista sovelluksista ja niiden versioista. Lansweeper kykenee tunnistamaan verkossa ja laitteissa esiintyviä haavoittuvuuksia erityisesti päivittämättömien ohjelmistoversioiden osalta. Lansweeper siis tarjoaa valikoiman erilaisia työkaluja ja ominaisuuksia verkon valvontaan laitteiden osalta.

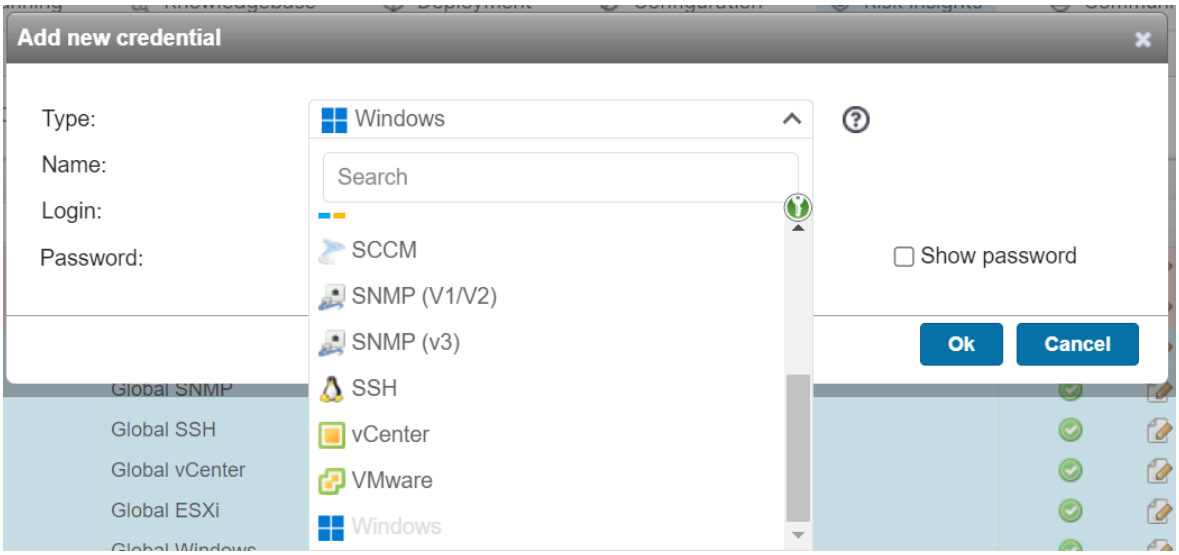
## 4.2 Lansweeperin käyttöönotto

Lansweeperin voi ottaa käyttöön on-prem pohjalta tai hybridinä (on-prem + cloud). On-prem ratkaisu toteutetaan yleensä luomalla palvelin ainoastaan Lansweeperiä varten. Asennus tehdään kyseiselle palvelimelle ja Lansweeperin suorittamat ympäristöjen sekä verkkojen skannaukset suoritetaan tuolta palvelimelta.

Hybridimalli toimii muuten samalla tavalla kuin on-prem ratkaisu, mutta tämän lisäksi on-prem ratkaisu yhdistetään pilvisivustoon. Sen sijaan, että Lansweeperin käyttöliittymään pääsy vaatisi pääsyä palvelimelle kuten on-premissä, lähetetään Lansweeperin keräämä data pilveen, jossa käyttöliittymään on pääsy kaikkialta. Tämän ratkaisun etuina on ainoastaan pilvessä hyödynnettävissä olevat toiminnot kuten esimerkiksi Risk Insights, Network Topology Diagrams ja erilaiset integraatiot, joita on-premillä ei ole tarjota. Varsinkin jos yrityksellä on useita Lansweeper asennuksia, mahdollistaa pilviratkaisu niiden kaikkien datan tarkastelun yhdestä paikasta. Tämä tietysti edellyttää, että kaikki nuo kaikki asennukset ovat yhdistettynä pilveen.

## 4.3 Lansweeperin skannaukset

Lansweeperin voi konfiguroida suorittamaan skannauksia agentittomana tai agentin avulla. Agentitonta skannausta varten Lansweeperin täytyy luoda tunnus/salasana-pari jolla on riittävät oikeudet. Tyyppejä on monenlaisia (Kuva 4.), moneen eri käyttötarkoitukseen ja esimerkiksi Windows-tunnusten käyttö edellyttää, että skannattavan domainin AD:hen on luotu vastaava tunnus. Näitä tunnuksia käytetään Windows-tietokoneiden ja -käyttäjien skannaukseen. Tunnuksilla on oltava järjestelmänvalvojan oikeudet koneille sekä read-only tason pääsy AD:hen. Skannaukset voidaan ajastaa suoritettavaksi tietyin väliajoin. Tässä on syytä huomioida, että mitä useammin skannauksia tehdään, sitä enemmän se vaatii resursseja sekä palvelimelta, että päätelaitteilta. On siis syytä seurata palvelimen resurssienkäyttöä, jotta voidaan varmistua, että palvelimen suorituskyky riittää.




Kuva 4. Lansweeper credentials (Niko Eriksson, 2023)

Agentillinen skannaus edellyttää LsPush tai LsAgent -agentin asennusta kaikkiin skannattaviin koneisiin. Näillä on keskenään muutamia keskeisiä eroavaisuuksia, joihin on syytä tutustua ennen käyttöönottoa (Kuva 5.).

Esimerkiksi LsPush ei kykene skannaamaan Linux-käyttöjärjestelmällä operoivia koneita eikä se kykene päivittämään itseään. LsAgent ei vaadi skannattavien koneiden olevan kytkettyinä verkkoon sillä se voi internetin avulla kerätä tällaisten koneiden datan. (Lansweeper, 2023c.)

| | LsPush | LsAgent |
|---|---|---|
| Introduced in | Lansweeper 4.2 | Lansweeper 7.0 |
| Scan Windows computers | ✓ (Windows 2000 and higher) | ✓ (Windows 7, SP1 and higher) |
| Scan Linux computers | ✗ | ✓ |
| Scan Mac computers | ✗ | ✓ |
| Scan computers where inbound traffic is blocked | ✓ | ✓ |
| Send scanned data directly to your Lansweeper installation | ✓ | ✓ |
| Send scanned data to your Lansweeper installation securely over the Internet (HTTPS and TLS 1.2) | ✗ | ✓ |
| Permanently installed as a software on the computer | ✗ | ✓ |
| Scanning schedule automatically configured | ✗ | ✓ |
| Option for automatic import of scanned data | ✓ | ✓ |
| Option for manual import of scanned data | ✓ | ✗ |
| Integrate in logon scripts or group policies | ✓ | ✗ |
| Automatic agent updates (on Windows computers) | ✗ | ✓ |

Kuva 5. LsPush ja LsAgent (Lansweeper 2023c)

## 4.4 Raportit

Lansweeperin on-prem- sekä pilviasennuksessa on mahdollista luoda vakioraporttien lisäksi räätälöityjä raportteja esimerkiksi laitteista, niiden ominaisuuksista sekä ohjelmistoista. Molemmista löytyy visuaalinen työkalu raporttien luomiseen mutta on-premissä se rakentuu enemmän SQL-osaamisen ympärille, joskin työkalu sisältää myös kevyen visuaalisen työkalun raporttien luomista varten.

Lansweeperin on-prem asennuksen raportointityökalun tietokanta sisältää useita eri taulukoita. Näiden avulla voidaan luoda räätälöity raportti tapauskohtaisesti. Visuaalinen työkalu soveltuu käyttäjälle, jonka SQL osaaminen on perusteiden tasolla ja SQL-editoria voi käyttää taas sellainen käyttäjä, jolla on riittävä tieto SQL-kielellä suoritettavista tietokantakyselyistä.

Pilvisivustolla raporttien luominen on rakennettu kaiken tasoisille käyttäjille, eikä raportin luominen välttämättä edellytä minkäänlaista SQL:n tuntemusta. Pilvessä on lisäksi mahdollisuus luoda raportteja Javascript -koodieditorin avulla. Tämä jälkimmäinen työkalu on tarkoitettu kokeneemmalle ohjelmoijalle.

Raportteja voidaan lähettää sähköpostitse ajastetusti ja tietyille käyttäjille tai ryhmille. Esimerkiksi kerran päivässä lähetettävä raportti AD:n uusista käyttäjä- tai konetileistä mahdollistaa uusien tilien ja niiden asianmukaisuuden kontrolloidun tarkastamisen.

## 4.5 Työkalun tietoturvasta

Kun tehdään inventaariota yrityksen koko laitekannasta, verkkotopologiasta, tietoliikennelaitteista sekä käyttäjistä, on tietoturvaan syytä kiinnittää erityistä huomiota. Vaikka Lansweeperin keräämä data ei suoraan vaaranna yrityksen tietoturvaa, ei tällaista dataa silti ole syytä sallia päätyvän asiattomien tahojen saataville.

On-prem asennuksessa tietoturvaa voidaan kiristää palomuurin avulla esimerkiksi sallimalla pääsy Lansweeperin web-käyttöliittymään ainoastaan tietystä verkosta tai vain tietyistä ip-osoitteista. Web-käyttöliittymän voi konfiguroida niin, että yhteys muodostetaan ainoastaan HTTPS:llä (Hypertext Transfer Protocol Secure). SSO (Single Sign-On) voidaan ottaa käyttöön, jolloin käyttöliittymään pääsy autentikoidaan käyttäjän AD-tunnuksella. Palvelimelta, jonne Lansweeper on asennettuna, voidaan myös web-käyttöliittymä poistaa käytöstä, jolloin käyttöliittymään pääsy edellyttää palvelimelle kirjautumista, jonne on voitu luoda omat sääntönsä valtuutetuista käyttäjistä ja yhteyksistä.

Pilvisivustolla tietoturva on toki viime kädessä palveluntarjoajan vastuulla mutta tähän voi myös käyttäjänä vaikuttaa ottamalla käyttöön sivustolle kirjauduttaessa kaksivaiheinen

tunnistautuminen tai SSO. Jälkimmäinen tosin on mahdollista ainoastaan Pro ja Enterprise tilaustyypeille. Pilvisivusto ei myöskään tallenna skannauksissa käytettyjä tunnuksia (credentials) pilveen vaan ne ovat tallessa ainoastaan on-premissä.

# 5 Active Directory

## 5.1 Active Directorysta yleisesti

AD eli Active Directory on Microsoftin kehittämä palvelu keskitettyyn tietojen tallennukseen ja organisoimiseen. AD tarjoa identiteetin- ja pääsynhallintaratkaisun, jonka avulla voidaan todentaa käyttäjä ja määrittää käyttäjälle sallittuja toimenpiteitä. Tietokantaan voidaan tallentaa käyttäjistä tietoja kuten erilaisia sähköposteja, puhelinnumeroita ja salasanoja. AD:n palveluita ajetaan Windows-palvelimelta, jota kutsutaan domain controlleriksi eli toimialueen ohjaimeksi. LDAP eli Lightweight Directory Access Protocol on protokolla, jonka avulla voidaan suorittaa kyselyitä hakemistopalveluita, kuten AD:ta vasten. (Manage Engine 2024)

## 5.2 Active Directoryn rakenne

AD tallentaa verkon resursseja sekä niihin liittyvää informaatiota objekteina. Tällaisia ovat esimerkiksi käyttäjätilit, tietokonetilit ja ryhmät. Edellä mainittuja objekteja voidaan autentikoida, jolloin niitä kutsutaan turvallisuusperiaatteiksi (security principals). Objekteja, joita ei voida autentikoida kutsutaan resursseiksi. (Manage Engine 2024)

Objektit sisältävät attribuutteja, joista osa kuten esimerkiksi sAMAccountName tai userPrincipalName (UPN) on oltava uniikkeja. Tämä tarkoittaa, että esimerkiksi kahdella eri käyttäjätilillä ei voi olla identtinen UPN. Jokaisella objektilla on domainissa yksilöllinen tunniste (GUID, Globally Unique Identifier) sekä turvallisuustunniste (SID, Security Identifier). (Manage Engine 2024)

Näistä objekteista ja resursseista voidaan muodostaa OU:ita (Organizational unit) tai ryhmiä. Näitä OU:ita tai ryhmiä voidaan hyödyntää esimerkiksi GPO:issa.

# 6 Tietoturvatyökalut käytännössä

Forcepointin keskitetty hallinta ja intuitiiviset ominaisuudet tekevät siitä helppokäyttöisen työkalun. Forcepointista löytyy lokihistoria, joka tallentaa kaiken liikenteen eri laitteiden ja verkkojen välillä sekä niiden käyttämät protokollat ja portit. Saman voi tehdä myös reaaliajassa. Tämän ominaisuuden avulla on helppo selvittää esimerkiksi, mikäli toimimattoman yhteyden syynä on olemassa oleva tai puuttuva palomuurisääntö (politiikka). Tai jos liikennettä ei näy ollenkaan lähteestä, josta sen olisi tarkoitus tulla voidaan todeta, että vika on lähteen konfiguroinnissa, joka nopeuttaa vianselvitystä ja ratkaisua.

Lansweeper on myös helppokäyttöinen ja monipuolinen työkalu. Sen avulla voidaan rakentaa esimerkiksi raportteja laitekannasta. Jos yrityksen politiikka on uusia käyttäjien tietokoneet esimerkiksi 3 vuoden välein, voidaan Lansweeperillä rakentaa raportti, joka listaa kunkin laitteen, joilla tuo aika lähenee. Vastaavasti voidaan seurata jonkin kriittisen ohjelmisto- tai laitepäivityksen tilannetta luomalla raportti, joka listaa kaikki laitteet, jossa ei vielä viimeisintä päivitystä ole.

Lansweeper ja Forcepointin palomuuri ovat kaksi melko erilaista työkalua, jotka kuitenkin täydentävät toisiaan ja pyrkivät samaan lopputulokseen eli tietoturvan toteutumiseen. Toisen avulla voidaan valvoa verkkoliikennettä ja toisen avulla verkossa toimivaa laitekantaa, jolloin saadaan aikaiseksi kattava valvonta.

# 7 Toteutus

## 7.1 Järjestelmäasiantuntijana Bauhausissa

Opinnäytetyötä aloittaessa olin ehtinyt jo vuoden työskentelemään Bauhausin pääkonttorin IT-osastolla järjestelmäasiantuntijana. Suurin osa tuosta ajasta oli kulunut erilaisiin järjestelmiin, ohjelmistoihin ja toimintamalleihin tutustuessa. Minut palkattiin kesällä 2022 IT-osastolle erityisesti osaksi tietoturvatiimiä, jonka vastuulla on yrityksen Suomen sekä Viron tietoverkkojen ja laitteiden tietoturva.

Opinnäytetyötä varten valittiin seurantajakson pituudeksi 10 viikkoa, jona aikana kirjattiin ylös päivittäiset työtehtävät. Työtehtävät olivat hyvin monipuolisia mutta tuon 10 viikon aikana nousi esiin kolme merkittävää kokonaisuutta, jotka onnistuin omaksumaan nopeasti. Näistä kokonaisuuksista muodostettiin kolme asiateemaa opinnäytetyötä varten.

## 7.2 Palomuurin sääntöjen päivitys

Yksi merkittävistä työtehtävistä oli palomuurin hallinta. Tämä käsitti erilaisten politiikoiden tai sääntöjen päivitystä ja uusien luomista keskitetyn hallintakonsolin avulla. Ennen opinnäytetyön seurantajakson alkua olin kollegaltani saanut pitkän ja kattavan perehdytyksen palomuurin hallintakonsolin käyttöön.

Sain aika ajoin joko kollegoilta tai yhteistyökumppaneilta pyyntöjä tehdä tarvittavia avauksia eli sääntöjä palomuuriin uusia yhteyksiä varten tai vaihtoehtoisesti pyynnön päivittää olemassa olevia sallittuja yhteyksiä.

Sääntöjen päivittäminen oli näistä helpompaa ja vaati yleensä joko yhteyden lähtöosoitteen, kohdeosoitteen tai sallitun protokollan muutosta sääntöön. Toisinaan oli tarve päivittää yksisuuntainen yhteys sallituksi myös toiseen suuntaan. Jos aiemmin oli sallittu yhteys A:sta B:hen https-protokollaa käyttäen niin tuli se tällaisissa tapauksissa sallia myös B:sta A:han.

## 7.3 Palomuurin sääntöjen luominen

Uusien sääntöjen luominen oli hieman työläämpi prosessi ja tätä varten tarvitsi selvittää peruste uuden yhteyden sallimiseksi. Mihin yhteyttä käytettiin ja minkälaista dataa yhteyden avulla siirrettiin? Mistä ja mihin dataa siirrettiin? Oliko pyydetty protokolla tietoturvallisin vaihtoehto mahdollisista? Esimerkiksi http-protokollan sijasta tulisi käyttää mahdollisuuksien mukaan tietoturvallisempaa https-protokollaa. Usein yhteydet vaativat useampia protokollia ja portteja sallituksi yhteyttä varten. Tällaisissa tapauksissa tuli tarkistaa joko

tekniseltä yhteistyökumppanilta tai ohjelmistotoimittajalta tarvittavat protokollat ja portit, jotta yhteydelle oli sallittu kaikki tarvittavat mutta ei kuitenkaan mitään ylimääräisiä protokollia tai portteja. Yrityksen tietoliikenneverkko on hyvin segmentoitu, joten tarvitsi myös selvittää missä verkossa ja minkä palomuurin takana lähtö- ja/tai kohdeosoite sijaitsevat, jotta sääntö saadaan luotua oikeaan säännöstöön. Kun sääntö oli luotu, pyysin osallisia testaamaan yhteyttä. Seurasin samalla palomuurin reaaliaikaisesta lokista, että yhteys onnistuu palomuurin läpi ja kaikki tarvittavat portit ja protokollat on lisättynä sääntöön eikä palomuuri pudota näistä mitään pois sen takia, että jokin portti tai protokolla ei olisi sisällytettynä sääntöön.

## 7.4 Uuden AD:n suunnittelu

Toinen merkittävä ja pitkä projekti on ollut kokonaan uuden AD:n luominen yritykselle. Tämä toteutettiin tiiviissä yhteistyössä teknisen yhteistyökumppanimme kanssa. Iso osa käytännön toteutuksista tehtiin yhteistyökumppanin toimesta. Lukemattomat suunnittelupalaverit auttoivat luomaan selkeän kuvan kokonaisuudesta ja logiikasta. Tässä vaiheessa roolini oli vielä melko pieni ja koostui lähinnä ajoittaisesta omien näkemyksien esittämisestä tuleviin toimintamalleihin tai tarvittavien sääntöjen luomisesta palomuurin tulevaa uutta AD:ta varten.

Olin päässyt tutustumaan edeltävän AD:n GPO:ihin melko syvällisesti ja olin yrityksemme puolelta ehkä asiantuntevin henkilö tarjoamaan mielipiteitä ja näkemyksiä esimerkiksi, mitä GPO:ita tulisi tuoda uuteen AD:hen tai mitkä olisi syytä jättää tuomatta. Parin palaverin aikana kävimme läpi kaikki edeltävän AD.n GPO:t ja keräsimme listan siirettävistä GPO:ista,

## 7.5 Uuden AD:n käyttöönotto

Siirryin ensimmäisenä käyttämään uutta AD:ta osana hyvin pientä pilottiryhmää. Tarkoituksena oli tehdä havaintoja, joiden pohjalta mahdollisesti toimimattomat asiat voidaan vielä korjata ennen kuin käyttäjiä aletaan laajemmin siirtää uuteen domainiin.

Oma aikansa meni oppia ymmärtämään uuden AD:n logiikka käytännössä verrattuna vanhaan AD:hen. Esimerkiksi GPO:t toimivat uudessa AD:ssa tiukan hierarkisesti. Vaikka kesti hetken sisäistää tämä uusi hierarkia niin oli se ehdottomasti askel eteenpäin.

Tämän myötä sain vastuulleni suurelta osin esimerkiksi uusien sovellusten tai selainlaajennusten hyväksymisen GPO:iden avulla. Oletuksena kaikki sovellukset ja selainlaajennukset ovat estettyjä ja jokainen niistä vaatii erillisen hyväksynnän. Tietoturvatiimin kanssa loimme prosessin, jolla käyttäjät voivat pyytää sovelluksen tai selainlaajennuksen hy-

väksymistä työkäyttöön. Jokainen pyyntö käsitellään tapauskohtaisesti ja mikäli pyyntö hyväksytään, lisätään se AD:n AppLocker -työkalussa sallittujen listalle ja sille määritellään käyttöoikeus ryhmä- tai käyttäjäkohtaisesti.

Tärkeää oli myös kerätä käyttäjiltä tietoa heidän käyttämistään ja heidän työtehtäviensä kannalta välttämättömistä ohjelmista, jotta käyttäjien siirryttäessä uuteen AD:hen ei heidän työnsä esty edes hetkellisesti sen takia, että jokin välttämättömistä ohjelmista ei toimi.

## 7.6 Lansweeperin asennus

Yrityksen käytössä on Lansweeper asset management -työkalu, jonka pääasiallisena käyttäjä olen toiminut melkeinpä työsuhteen ensimmäisestä päivästä lähtien. Tänä aikana olen ehtinyt tutustumaan tuotteeseen perusteellisesti ja muuttamaan konfiguraatioita esimerkiksi vastaamaan paremmin ohjelmistotoimittajan omia suosituksia parhaista käytännöistä.

Lansweeperiin liittyen projektina on luoda täysin uusi asennus uudelle palvelimelle ja uuden AD:n uuteen domainiin. Tämä projekti on tässä opinnäytetyön toteutuksessa kuvatuista teemoista haastavin ja mielenkiintoisin koska tässä vaaditaan merkittävää osaamista kaikista kolmesta teemasta eli palomuurien hallinnasta, Active Directorysta sekä Lansweeperistä.

Aloitin projektin luomalla toteutussuunnitelman, jonka pohjalta tulisin etenemään. Ensimmäisenä tarvitsin uuden virtuaalipalvelimen johon Lansweeperin asennus tultaisiin tekemään. Virtualisointialustana yrityksemme käyttää VMwarea. Aikataulun optimoimiseksi pyysin teknistä yhteistyökumppaniamme luomaan uuden virtuaalipalvelimen tätä varten aliverkkoon, joka on tarkoitettu erilaisille hallintapalvelimille. Palvelimen käyttöjärjestelmänä on Windows Server 2022.

Kun uusi virtuaalipalvelin oli saatu luotua, seuraavana vuorossa oli luoda palomuuriin sääntö, jolla tietyltä hyppypalvelimelta oli sallittua ottaa RDP-yhteys tähän palvelimelle. Loin myös säännön palomuuriin, joka salli tältä uudelta palvelimelta internet-yhteyden Lansweeperin sivustolle asennusohjelman lataamista varten.

## 7.7 Konfigurointi

Asennus sujui ongelmitta ja asennuksen jälkeen loin Lansweeperiin paikallisen hallintatilin, jolla pääsin luomaan tarvittavia konfiguraatioita ohjelmaan. Ensimmäiseksi enabloin SSO-kirjautumisen ja konfiguroin tietyille domainin käyttäjätileille eritasoiset käyttöoikeudet Lansweeperiin. IT-osaston henkilöstön käyttäjätason käyttäjätileille sallin viewer-tason

oikeuden Lansweeperiin. Tämä tarkoittaa, että käyttäjätason käyttäjätilillä on oikeus tarkastella asseteista kerättyjä tietoja ja dataa. Myös eri raportteihin on näillä tileillä lukuoikeus. Minkäänlaisia konfiguraatioita näillä tileillä ei kuitenkaan pääse muokkaamaan tai edes tarkastelemaan. Domainin IT-osaston henkilöstön järjestelmänvalvoja-tason tileille annoin oikeuden tarkastella ja muokata konfiguraatioita.

Jotta Lansweeperin käyttö ei vaadi aina erillistä kirjautumista palvelimelle, otin käyttöön Lansweeperin web-portaalin. Käyttäjä voi näin omalta työasemaltaan muodostaa https-yhteyden Lansweeperin hallintakonsoliin. Tätä varten palomuuriin luotiin sääntö, joka sallii pääsyn ainoastaan tietyistä työasemaverkoista. Https-yhteyttä varten pyysin teknistä yhteistyökumppaniamme luomaan sertifikaattipalvelimella sertifikaatin, joka otettiin käyttöön tällä uudella palvelimella.

Toin vanhasta Lansweeperistä skannattavat aliverkot uuteen Lansweeperiin, jotta niitä ei tarvitse jokaista syöttää uudestaan yksitellen.

## 7.8 LsAgent

Aiemman Lansweeperin skannaukset perustuivat pääasiassa vanhaan AD:hen Lansweeperiä varten luotuihin tunnuksiin, joilla järjestelmänvalvojan oikeuksin se pystyi skannaamaan verkon laitteita ja näihin liittyvää informaatiota.

Uuden Lansweeperin myötä kaikille työasemille ja palvelimille asennettavaa agenttia hyödynnetään huomattavasti enemmän. LsAgent suorittaa skannauksia työasemilla sekä palvelimilla ja lähettää ne Lansweeperin palvelimelle. Mikäli työasema tai palvelin ei olisi verkossa eikä näin ollen LsAgentilla olisi yhteyttä Lansweeperin palvelimeen, käyttää se julkiverkossa välityspalvelinta datan lähettämiseen Lansweeperin palvelimelle. Tämän etuna on se, että työasemista ja palvelimista saadaan ajankohtaista tietoa, vaikka skannattava kohde ei olisikaan yhteydessä yrityksen verkkoon esimerkiksi etätöissä.

Testasin LsAgentin uudet konfiguraatiot asentamalla sen omalle työasemalleni ja suorittamalla skannauksen. Data siirtyi ongelmitta uudelle palvelimelle, joten sovin teknisen yhteistyökumppanimme kanssa uusien konfiguraatioiden sisältävän LsAgentin jakelusta isommalle testiryhmälle, joiden työasemat liikennöivät eri aliverkosta kuin oma työasemani. Kun testiryhmän työasemille oli asennettu LsAgent huomasin, että näiden eri aliverkoista liikennöivien työasemien LsAgent ei saanut suoraan yhteyttä Lansweeperin skannauspalvelimelle. Näiltä työasemilta data kulki ainoastaan välityspalvelimen kautta skannauspalvelimelle. Syy tähän löytyi palomuurista, joka esti kyseisestä aliverkosta liikennöinnin skannauspalvelimelle. Loin kyseistä aliverkkoa koskevan säännön, joka salli liikennöinnin kyseisestä aliverkosta tiettyä TCP-porttia käyttäen skannauspalvelimelle. Tä-

män tehtyäni data alkoi siirtymään työasemilta suoraan skannauspalvelimelle. Tein vastaavat säännöt palomuuriin myös kaikille muille aliverkoille, joista olisi tarpeen saada data kulkemaan LsAgentin avulla suoraan skannauspalvelimelle. Tämän jälkeen LsAgent jaeltiin yhteistyökumppanin avulla kaikille työasemille ja palvelimille.

# 8 Pohdinta

Tämän päiväkirjamuotoisen opinnäytetyön tavoitteena oli seurata työtehtävässä kehittymistä 10 viikon seurantajaksolla viikkoanalyysien muodossa. Työtehtävät ovat hyvin monimuotoisia mutta opinnäytetyöhön on valittu pääteemoiksi Lansweeper -työkalu, Forcepoint -palomuuri sekä uusi AD-projekti. Viikkoanalyysit nostavat esiin näihin teemoihin liittyviä tehtäviä sekä näihin liittyvää oppimista ja kehittymistä.

Päiväkirjamuotoisena toteutettu opinnäytetyö haastoi suunniteltua enemmän erityisesti ajankäytön osalta. Työtehtävien ylös kirjaaminen kiireisten työpäivien aikana nousi suurimmaksi haasteeksi. Näiden muistiinpanojen pohjalta täytyi vielä työpäivän jälkeen kirjoittaa selkeämpi kuvaus kuluneen päivän työtehtävistä. Jos muistiinpanot kuluneelta päivältä olivat yhtään epäselvät tai suuripiirteiset niin sitä joutui käyttämään ylimääräistä aikaa palaamalla esimerkiksi sähköpostiviesteihin muistin virkistämiseksi. Harrastus- ja henkilökohtaiset kiireet lisäsivät haastetta ylläpitää kurinalaista kirjoitusrytmiä joka työpäivän päätteeksi.

Opinnäytetyö tarjosi kuitenkin mahdollisuuden yhdistää jo opittua sekä syventää osaamista tutustumalla yksityiskohtaisesti ohjelmistotuottajien parhaisiin käytäntöihin, tuotekuvauksiin ja teknisiin ohjekirjoihin. Varsinkin nämä kolme viimeisintä ovat olleet keskeisessä roolissa uusien toimintamallien kehityksessä ja ideoinnissa. Ideani ovat saaneet hyvän vastaanoton tietoturvatiimin palavereissa ja ideoista on luotu konkreettisia tulevaisuuden suunnitelmia ja projekteja.

Vaikka päiväkirjamuotoisena toteutettu opinnäytetyö tarjosi omat haasteensa, oli siinä myös etunsa. Näistä suurin oli tarve pysähtyä miettimään menneitä työpäiviä ja -tehtäviä. Useasti se auttoi ymmärtämään syvemmin tehtyä ja pohtimaan olisiko jotain voinut tehdä vielä paremmin tai toisin. Opinnäytetyö kasvatti erityisesti itseluottamusta ja uskoa siihen, että vaikka ala on haastava ja se vaatii ison määrän uusien asioiden oppimista niin kaikki nämä on todellakin mahdollista oppia.

# 9 Yhteenveto

Opinnäytetyössä oli keskeisinä teemoina Active Directory, Lansweeper asset management -työkalu sekä Forcepointin palomuurit. Tavoitteena oli tutustua näihin teemoihin syvällisemmin ja pyrkiä ylläpitämään sekä kehittämään yrityksen tietoturvaa näiden työkalujen avulla. Lisäksi tavoitteena oli tuoda esille näiden kolmen teeman suhdetta toisiinsa, josta muodostuu yksi kokonaisuus, joka edistää ja ylläpitää yrityksen tietoturvaa.

Uuden Lansweeperin asennus ja käyttöönotto onnistui suunnitellusti. Pystyin tarkasti seuraamaan ennen projektia tekemääni suunnitelmaa projektin eri vaiheista ja toteutusjärjestyksestä. Huolellinen tutustuminen ohjelmistotoimittajan parhaisiin käytäntöihin sekä aiempi kokemus työkalun käytöstä minimoivat mahdolliset konfiguraatiovirheet. LsAgentin ja palomuurin aiempaa parempi konfigurointi tarjoaa jatkossa mahdollisuuden reaaliaikaiseen tietojen keräämiseen työasemilta. Tämä myös poistaa tarpeen konfiguroida työasemien Windows-palomuureja sallimaan Lansweeperin kerätä dataa WMI:ltä (Windows Management Instrumentation).

Forcepoint -palomuurien osalta onnistuin myös tavoitteessa ylläpitää yrityksen tietoturvaa. Tietoturvan ylläpidon osalta tavoite täyttyi noudattamalla yrityksen toimintamallia eli yhteyksiä sallitaan ainoastaan tarpeeseen perustuen ja tämä tarve tulee perustella riittävän huolellisesti. Yhteys tuli myös toteuttaa turvallisinta mahdollista protokolla käyttäen, jonka tarkistin aina suoraan ohjelmistotoimittajalta tai ohjelmistotoimittajan teknisistä dokumentaatioista. Tietoturvan kehityksen osalta suunnittelimme kollegani kanssa toimenpiteet, jolla keräämme käytöstä poistuneet säännöt, joille ei ole enää tarvetta ja poistamme nämä säännöt.

Opinnäytetyön tavoite toteutui ja onnistuin osoittamaan, että jokainen näistä osa-alueista on tärkeä osa kokonaisuutta ja pystyy yksittäisenäkin osana parantamaan yrityksen tietoturvaa mutta erityisesti näiden yhteistoiminnalla voidaan saavuttaa huomattavaa hyötyä. Onnistuin myös yksittäisten teemojen osalta kehittämään omaa osaamistani huomattavasti suhteessa lähtökohtaan.

Erilaiset tietoturvaa ylläpitävät ja kehittävät työkalut ovat tärkeä osa jokaisen yrityksen kokonaisuutta tai ainakin niiden tulisi olla. Tietoturva on kohde josta ei ole syytä tinkiä. Lansweeperin kaltaisella asset management -työkalulla voi tuoda konkreettisia säästöjä yritykselle jo pelkästään säästettyinä työtunteina jos vertaa aikaa joka kuluisi tehdä kaikki ne toiminnot tai edes osa toiminnoista manuaalisesti joihin Lansweeper kykenee. Lisäksi tällaiset työkalujen sekä palomuurien avulla yrityksen on helpompi noudattaa mahdollisia sääntelyvaatimuksia ja standardeja. Tai vaikka tällaisten noudattamista ei yritykseltä vaa-

dittaisikaan niin voi niitä noudattamalla luoda omalle yritykselleen hyvän myyntiargumentin jolla nousta kilpailijoiden ohi. Uskon, että tulevaisuudessa yhä useampi yritys tämänkaltaisia työkaluja tulee hyödyntämään jo pelkästään tietoturvasyistä mutta myös niiden tarjoamien kustannussäästöjen ja tehokkuuden osalta.

## Lähteet

Cisco. What is a Next-Generation Firewall. Viitattu 27.10.2023. Saatavissa https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html

Forcepoint. 2023a. Default elements for user authentication. Viitattu 12.11.2023. Saatavissa https://help.forcepoint.com/ngfw/en-us/6.11.0/GUID-EA3DE30E-443C-4A67-A4AD-1D4CC0FBAB61.html

Forcepoint. 2023b. Forcepoint FlexEdge Secure SD-WAN. Viitattu 3.3.2024. Saatavissa https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet-flexedge-sdwan-en_0_0.pdf

Forcepoint 2023c. Getting started with user authentication. Viitattu 3.3.2024. Saatavissa https://help.forcepoint.com/ngfw/en-us/6.11.0/GUID-AFD838BF-C8EC-49BB-BA28-84029965CEA4.html

Forcepoint 2023d. Default elements for user authentication. Viitattu 3.3.2024 Saatavissa https://help.forcepoint.com/ngfw/en-us/6.11.0/GUID-EA3DE30E-443C-4A67-A4AD-1D4CC0FBAB61.html

Forcepoint. 2023e. Define access rules for authentication. Viitattu 3.3.2024. Saatavissa https://help.forcepoint.com/ngfw/en-us/6.11.0/GUID-988DFDC6-D7B7-4F81-A8DE-D8A7A3FD2C2A.html#GUID-988DFDC6-D7B7-4F81-A8DE-D8A7A3FD2C2A

Forcepoint a. Next Generation Firewall. Viitattu 3.3.2024. Saatavissa https://www.forcepoint.com/product/ngfw-next-generation-firewall

Forcepoint b. What is an intrusion prevention system (IPS). Viitattu 27.10.2023. Saatavissa https://www.forcepoint.com/cyber-edu/intrusion-prevention-system-ips

Fortinet. What is cyber threat intelligence. Viitattu 27.10.2023. Saatavissa https://www.fortinet.com/resources/cyberglossary/cyber-threat-intelligence

Lansweeper. 2023a. Verkkosivu. Viitattu 27.10.2023. Saatavissa https://www.lansweeper.com/lp/branded/?utm_source=google&utm_medium=cpc&utm_campaign=[eu]-brand&utm_term=lansweeper&gad_source=1&gclid=CjwKCAjwv-2pBhB-EiwAtsQZFEcE3lAJEJyM--NAExQz56wbOEp4z5uzJI9GC1V2IDs8qBdQ3YJ6exoCjSQQAvD_BwE

Lansweeper. 2023b. Plans & Pricing. Viitattu 28.10.2023. Saatavissa https://www.lansweeper.com/pricing/?gad_source=1#discover?utm_source=google&utm_medium=cpc&utm_campaign=sitelink_extension&utm_term=pricing

Lansweeper. 2023c. LsPush vs. LsAgent scanning agent. Viitattu 28.10.2023. Saatavissa https://community.lansweeper.com/t5/scanning-your-network/lspush-vs-lsagent-scanning-agent/ta-p/64478

Manage Engine. 2024. What is Active Directory. Viitattu 23.3.2024. Saatavissa https://www.manageengine.com/products/ad-manager/what-is-active-directory-and-how-does-it-work.html

Paloalto Networks. What is an intrusion prevention system. Viitattu 27.10.2023. Saatavissa https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

Stonesoft. 2018a. Default policy elements. Viitattu 29.10.2023. Saatavissa https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.5.0/GUID-CA0203CD-5F2447A8-AF4E-1D99C94B15E2.html

Stonesoft. 2018b. Getting started with Network Application elements. Viitattu 12.11.2023. Saatavissa https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.9.0/GUID-BE114C51-27A3-474E-A987-658F66D6258B.html

Stonesoft. 2018c. How the home view is arranged. Viitattu 27.10.2023. Saatavissa https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.5.0/GUID-7038E4EA-ED89-45C3-9C8D-57F6B1E3C89A.html

Liite 1. Päiväkirja

**Viikko 1 analyysi**

Ensimmäisellä viikolla pidettiin aloituspalaveri uuteen AD:hen liittyen. Palaverissa käytiin läpi suunnitelmaa uuden AD:n toteuttamisesta sekä tarvittavista laitehankinnoista. Työ toteutetaan yhdessä teknisen yhteistyökumppanin kanssa.

Ymmärsin jo ennestään mikä AD:n tarkoitus on mutta palavereista sai vielä yksityiskohtaisemman käsityksen AD:n tarkoituksesta. Uudessa AD:ssa korostuu entistä enemmän tietoturva, joka tulee näkymään konkreettisina muutoksina verrattuna nykyiseen AD:hen ja vaikuttaa jokaisen yrityksen työntekijän toimintamalleihin.

Ensimmäisellä viikolla esittelin myös idean asset management työkalumme Lansweeperin yhdistämisestä pilveen. Etuina tässä ratkaisussa ovat useat erilaiset lisäohjelmat sekä -toiminnallisuudet, joita ei on-prem-Lansweeperistä löydy. Sain tähän esihenkilöltäni luvan ja aloitin työn tutustumalla Lansweeperin dokumentaatioon pilveen yhdistämiseen liittyen ja varmistin, että nykyinen on-prem asennus täyttää vaaditut ehdot.

**Viikko 2 analyysi**

Toisella viikolla sain kollegalta pyynnön tehdä palomuuriin sääntö, joka sallii ftp-yhteyden palvelimelta toiselle. Varmistin kollegalta, mitkä palvelimet ovat kyseessä ja mitä protokollia niiden välinen liikenne tulee sisältämään. Palvelinten välillä tehdään tiedonsiirtoa FTP:llä (File Transfer Protocol) joten määritin ainoastaan FTP:n sallituksi protokollaksi sääntöön näiden kahden palvelimen välille. Tämä ei vaadi edestakaista liikennettä palvelinten välillä, joten FTP on sallittu ainoastaan palvelimelta A palvelimelle B.

Kollegani oli tehnyt verkkomuutoksia, jotka tuli päivittää myös Lansweeperiin verkkoavaruuksien skannauksia varten. Verkkotopologiamme on dokumentoitu Microsoft Vision -työkalun avulla. Tarkastin dokumentaatiosta viimeisimmät verkkomuutokset ja tein niiden pohjalta muutokset myös Lansweeperiin. Muutoksen käsittivät muutaman uuden aliverkon, jotka konfiguroin Lansweeperiin skannattaviksi aliverkoiksi.

Samalla tutustuin myös Lansweeperin pilviversiossa saatavilla oleviin työkaluihin ja lisäominaisuuksiin ja pohdin, olisiko niissä käyttökelpoista työkalua, joka sopisi yrityksemme käyttötarkoituksiin.

**Viikko 3 analyysi**

Yrityksemme kaikkien maiden tietoturvatiimit kokoontuivat alkusyksystä Suomessa seminaariin, jonka tarkoituksena oli luoda yhteisiä parhaita käytänteitä sekä organisaatiotason ohjeistuksia tietoturvaan liittyen. Yksi yhteinen päämäärä oli kehittää AD:n tilien monito-

rointia joko uusien tai jo olemassa olevien työkalujen avulla. Tämän ohjeistuksen pohjalta loin Lansweeperiin muutaman raportin, jotka seuraavat uusia käyttäjä- ja konetilejä AD:ssa. Raportit lähetetään joka aamu tietoturvatiimimme jäsenille sähköpostitse. Ne listaavat kaikki AD:hen viimeisen 24 tunnin aikana perustetut tilit. Raporttien avulla voidaan manuaalisesti valvoa, että kaikki uudet käyttäjä- sekä konetilit ovat asianmukaisia ja tarpeellisia. Tarkistan raporttien listaamat tilit päivittäin ja teen tarvittaessa lisäselvityksiä, mikäli en heti tiedä, mitä tarkoitusta varten listalta löytyvä tili on perustettu. Loin myös raportin, joka vastaavasti seuraa Administrator-ryhmän jäseniä, mikäli kyseiseen ryhmään lisätään uusia tilejä.

**Viikko 4 analyysi**

Viikkopalaverissa yhteistyökumppanimme kanssa kävimme taas läpi suunnitelmaa uuteen AD:hen liittyen. Pääsyä palvelimille ja erityisesti Active Directory sekä Group Policy Management palveluihin tiukennetaan entisestään.

Hyppypalvelimet tulevat olemaan iso osa tätä tulevaa muutosta. Listasimme hyppypalvelimet sekä palvelimet ja verkot, joihin kultakin hyppypalvelimelta sallitaan pääsy. Tämän listauksen perusteella teimme kollegani kanssa tarvittavat säännöt palomuurien politiikoihin, jotta suunnitellut yhteydet hyppypalvelimilta ovat mahdollisia.

Huolellisesti tehty suunnitelma helpotti hahmottamaan tarvittavia palomuurisääntöjä ja tarjosi selkeän kokonaiskuvan halutusta lopputuloksesta. Suunnitelman sekä kollegan tuen avulla oli suhteellisen helppoa toteuttaa palomuuriin säännöt, joilla hyppypalvelimilta on mahdollista liikennöidä tietyillä protokollilla ja tiettyihin verkkoihin sekä palvelimiin.

**Viikko 5 analyysi**

Tämä oli teemojen osalta hieman hiljaisempi viikko. Saldovapaan takia sen pituus jäi myös ainoastaan neljän työpäivän mittaiseksi.

Loin Lansweeperiin raportin, joka listaa kaikki verkon palvelimet ja sekä jokaisen näiden palvelimen asemien levytilat. Raportti osasi hakea palvelinkohtaisesti levyasemien koot sekä käytetyn ja jäljellä olevan levytilan. Lisäksi päivitin Lansweeperin uusimpaan versioon. Latasin Lansweeperin uusimman version, tarkastin SHA256-sormenjäljen ja otin virtuaalipalvelimesta kaiken varalta snapshotin ennen versiopäivitystä.

Erityisesti tuota luomaani raporttia varten jouduin tutustumaan useisiin lähteisiin ja yhteisökeskusteluihin, jotta sain luotua juuri oikeanlaisen raportin luotua. Versiopäivitys oli melko yksinkertainen prosessi mutta tämä oli hyvä harjoitus, jotta siihen saa luotua tietynlaisen rutiinin, jotta tärkeimmät asiat kuten tuon SHA256-sormenjäljen tarkistus sekä

snapshotin ottaminen virtuaalipalvelimesta ovat jatkossakin versiopäivityksiä tehtäessä toimenpidelistalla.

**Viikko 6 analyysi**

Pidimme palaverin yhteistyökumppanin kanssa vanhan AD:n GPO:iden siirrosta uuteen AD:hen. Palaverissa kävimme läpi vanhan AD:n GPO:ita ja listasimme ne GPO:t jotka tultaisiin siirtämään uuteen AD:hen. Ennen kuin GPO valittiin siirrettävien listalle, tuli sen käytölle olla peruste sekä tarve myös uudessa AD:ssa. Esimerkiksi virtuaalityöasemista tullaan luopumaan kokonaan, joten näihin liittyville GPO:ille ei ole enää käyttöä. GPO:ita on pitkä lista, joten ihan kaikkia ei ehditty yhdessä palaverissa käymään läpi ja tätä päätettiin jatkaa ensi viikolla uuden palaverin merkeissä.

Työntekijöiden työasemat on suojattu Windowsin BitLocker tietoturvaominaisuudella. Kävin kollegalleni läpi kuinka tämä on toteutettu GPO:n avulla ja mistä esimerkiksi saa tarvittaessa tietoon työaseman BitLocker-palautusavaimen.

GPO:iden läpikäynti oli erittäin hyödyllistä jo pelkästään toki, jotta saadaan siirrettyä ne uuteen AD:hen mutta erityisesti sen takia, että niiden tarkoitukseen ja toimintamekanismeihin oli tutustuttava tarkemmin. Tämä kasvatti huomattavasti tietämystä ja ymmärrystä yksittäisistä GPO:ista sekä niiden muodostamasta kokonaisuudesta.

**Viikko 7 analyysi**

Opinnäytetyöhön liittyvien teemojen osalta tämä oli hieman hiljaisempi viikko. Osallistuin kollegani kanssa Helsingin Messukeskuksessa järjestetyille Cyber Security Nordic -messuille. Kaksipäiväinen tapahtuma koostui useista eriaiheisista esityksistä, joita kaikkia yhdisti tietoturva. Esiintyjinä toimi alan johtavia asiantuntijoita sekä yritysten edustajia. Tapahtumassa pääsi kuulemaan erittäin mielenkiintoisia puheenvuoroja ja verkostoitumaan saman alan parissa työskentelevien ihmisten kanssa.

**Viikko 8 analyysi**

Jatkoimme edellisellä viikolla kesken jäänyttä palaveria GPO:iden siirrosta uuteen AD:hen. Kävimme läpi loput GPO:t joita ei viime kerralla ehditty ja saimme viimeisteltyä listan siirrettävistä GPO:ista.

Kuluneella viikolla teimme myös kollegani kanssa palomuuriin sääntöjä uusia aliverkkoja varten. Jotta aliverkoissa olevia palvelimia saadaan päivitettyä säännöllisesti, tuli niihin sallia liikennöinti Microsoftin suuntaan HTTP- ja HTTPS-yhteyksillä. Lisäksi tietyille kytkimille tuli konfiguroida uusia VLANeja joita tarvitaan uudessa AD:ssa. Kollegani suoritti

nämä konfiguraatiot ja ohjeisti samalla yksityiskohtaisesti mitä kaikkea tulee ottaa huomioon näitä VLANeja luodessa.

Erityisesti VLANien konfigurointi kytkimille ole melko lailla uusi asia. Toki näitä on koulussa käyty läpi ja työstetty esimerkiksi Ciscon NetAcad -kursseilla mutta huomattavasti pienemmässä mittakaavassa kuin nyt tehty. Otin kollegani opastuksesta muistiinpanoja ja uskoisin, että tarvittaessa pystyisin vastaavasta tehtävästä suoriutumaan jatkossa myös täysin omatoimisesti.