Tietoturvaratkaisut etätyöskentelyn turvaamiseksi yrityksen tietokoneilla

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Tietojenkäsittelyn koulutusohjelma, Hämeenlinnan korkeakoulukeskus
kevät, 2021

Lauri Latva-Pietilä

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn koulutus Tiivistelmä

Hämeenlinnan korkeakoulukeskus

Tekijä Lauri Latva-Pietilä Vuosi 2021

Työn nimi Tietoturvaratkaisut etätyöskentelyn turvaamiseksi yrityksen tietokoneilla

Ohjaaja Erkki Laine

TIIVISTELMÄ

Työn tavoitteena oli vertailla tilaajan, Hämeen korkeakoulukeskuksen Tietohallinnon, esittämien kolmen ratkaisun tekniikoita. Tarkasteltavat ratkaisut olivat Check Point Harmony Endpoint (ent. Checkpoint Sandblast Endpoint Agent), Cisco Umbrella DNS Security sekä Microsoft Defender for Endpoint & CloudApp security (ent. Microsoft Defender ATP.)

Työn teoriaosuudessa avattiin tietoturvallisuuden määritelmiä, etätyöskentely-yhteyden yleisimpiä tekniikoita yhteyden luomiseksi etäpisteen ja yrityksen resurssien välille sekä miten kaksi toimipaikkaa yhdistetään toisiinsa. Opinnäytetyö on tutkimuksellinen. Aineistoa kerättiin ratkaisuja tuottavien palveluntarjoajien omilta verkkosivuilta. Käytännön osuus toteutettiin ratkaisuista kerätyn teoria-aineiston vertailuna.

Työn tuloksena havaittiin tutkittavien ratkaisujen olevan toisiaan muistuttavia, mutta jokainen palveluntarjoaja tarjoaa ratkaisussaan omaa erityisosaamistaan. Esimerkiksi Cisco on profiloitunut tietoliikenneyrityksenä valmistaen etupäässä verkkolaitteita, reitittimiä ja kytkimiä. Check Point on alusta asti profiloitunut palomuurien ja verkkoturvallisuuden ohjelmistojen tuottamiseen. Microsoftin vahvuus näkyy sen tuotteiden suuressa tarjonnassa ja suosiossa, joihin arvioitava ratkaisu voidaan integroida sekä käyttää hyödyntäen ohjelmointirajapintoja.

Avainsanat endpoint, EDR, AIR, VPN, VDI, VPN

Sivut 27 sivua ja liitteitä 1 sivu

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Business Information Technology **ABSTRACT**

Hämeenlinna University Centre

Author Lauri Latva-Pietilä Year 2021

Subject Security solutions to secure telecommuting on corporate computers

Supervisor Erkki Laine

ABSTRACT

The aim of this bachelor's thesis was to compare the techniques of the three solutions presented by the client, Information Management of Häme University of Applied Sciences'. The solutions to be studied were Check Point Harmony Endpoint, Cisco Umbrella DNS Security and Microsoft Defender for Endpoint & CloudApp security.

The theoretical part of the thesis explained the definitions of information security, the most common techniques of teleworking when creating a connection between endpoint and a company's resources, and how two sites are connected to each other. The thesis is research-based. The material was collected from service providers' own websites. The practical part was done by comparing the theoretical data collected from the solutions.

As a result of the work, it was found that the solutions under study are similar to each other, but each of the service providers offers its own special expertise in its solution. For example, Cisco has profiled itself as a telecommunications company that primarily manufactures network devices, routers, and switches. From the beginning, Check Point has profiled itself by producing firewalls and network security software. Microsoft's strength is reflected in the wide range and popularity of its products, into which the solution under study can be integrated and used through software interfaces.

Keywords endpoint, EDR, AIR, VPN, VDI, VPN

Pages 27 pages and appendices 1 page

Sanasto

AMP	Cisco Advanced Malware Protection
API	Application programming interface, ohjelmointirajapinta
IaaS	Infrastructure as a Service, ulkoistettu verkkoinfrastruktuuri
IDS	Intrusion detection system, tunkeilijan havaitsemisjärjestelmä
IPS	Intrusion prevention system, murron estämisjärjestelmä
IPsec	IP security architecture, TCP/IP-perheeseen kuuluvia protokollia
L2F	Layer 2 forwarding, tunneliprotokolla, OSI-mallin tasolla 2
L2TP	Layer 2 tunneling protocol, VPN-tunnelointiprotokolla
OSI	Open Systems Interconnection Reference Model
Palomuuri	Firewall, järjestelmä, joka estää pääsyn verkosta toiseen
Phishing	Tietojenkalastelu, verkkourkinta
PPTP	Point-to-point tunneling protocol, PPP-protokollaan pohjautuva VPN-tunnelointiprotokolla
Rootkit	Piilohallintaohjelma, piiloutuu usein laiteajureihin
SaaS	Software- as a Service, ulkoistettu ohjelmiston hankinta palveluna
SCCM	Microsoft System Center Configuration Manager
SIEM	Security information and event management
SSL	Secure sockets layer, salausprotokolla
TCP/IP	Transmission control protocol / internet protocol
TLS	Transport layer security, salausprotokolla, ennen SSL
URL	Uniform resource locator, tunniste, jolla osoitetaan WWW-sivuja
VDI	Virtual desktop infrastructure, työpöydän virtualisointi
VPN	Virtual private network, virtuaalinen erillisverkko

Sisällys

Liitteet

1 Johdanto

Vuonna 2019 alkanut ja sittemmin maailmanlaajuiseksi pandemiaksi räjähtänyt koronavirus johti yritykset ympäri maailman siirtämään toimintojaan etätyöskentelyyn. Nopea siirtyminen etätyöskentelyyn kotioloihin yrityksen tietokoneella oman internetyhteyden päähän on pakottanut yritykset tarkastelemaan kriittisesti omaa tietoverkkojen infrastruktuuriaan ja tietoturvakäytänteitään. Useat tietoturvaa ja verkkopalveluita tarjoavat yritykset tarjoavat toisistaan eriäviä ratkaisuja datan suojaamiseksi ja turvallisen etäyhteyden luomiseksi yrityksen tietoverkkoihin. Tietosuojariskit eivät kuitenkaan rajoitu vain yrityksen verkkoon, vaan etätyöskentelyn myötä arkaluontoista materiaalia käsitellään herkässä ja häiriöalttiissa kotiympäristössä, mikä vahvistaa uhkia, jotka ovat erilaisia, kuin valvotussa konttoriympäristössä työskennellessä.

Tämän työn tavoitteena oli vertailla ja tutkia yleisellä tasolla tilaajan esittämien kolmen ratkaisun tekniikoita. Tarkastelussa tutkitaan vain etätyöskentely-yhteyden suojausta yrityksen tietokoneilla, ei työntekijöiden omilla laitteilla. Tarkasteltavat ratkaisut olivat Check Point Harmony Endpoint (entinen Checkpoint Sandblast Endpoint Agent), Cisco Umbrella DNS Security sekä Microsoft Defender for Endpoint & CloudApp security (entinen Microsoft Defender ATP.) Tilaajana toimi Hämeen ammattikorkeakoulukeskuksen Tietohallinto. Opinnäytetyössä pyritään selvittämään mitä teknisiä ratkaisuja tilaajan toivomat ratkaisut käyttävät etätyöskentely-yhteyden suojaamiseksi ja miten ne eroavat toisistaan.

Tämän työn teoriaosuudessa avataan tietoturvallisuuden yleisimpiä määritelmiä ja sen keskeisimpiä termejä. Teoriaosuudessa pohjustetaan etätyöyhteyksien yleisimpiä tekniikoita käytännön osuutta silmällä pitäen.

Opinnäytetyö on tutkimuksellinen. Aineistoa kerättiin etätyöskentely-yhteyden suojaamiseen ratkaisuja tuottavien palveluntarjoajien omilta sivuilta, kolmannen osapuolien arvioinneista ja arvosteluartikkeleista. Teoriaosuudessa ja käytännön osuudessa ei oteta kantaa yrityksen verkon muihin suojauksen tekniikoihin, jos ne eivät kuulu ratkaisuun olennaisena osana. Tällaisia tekniikoita voisivat olla esimerkiksi IDS, IPS ja palomuurit.

2 Tietoturvan käsite

Organisaatioiden tietoturvaa ja tietosuojaa säännellään ja ohjeistetaan lakien kautta sekä vaatimuksien ja standardien kautta, joita yrityksen tietoturvapolitiikat noudattavat. Tällaisia ohjeistuksia ovat esimerkiksi ISO/IEC 27001, VAHTI ja JUHTA. (Manninen, 2019) Turvallisuuskomitean Kyberturvallisuuden sanastossa 2018 tietoturva määritellään järjestelyiksi, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus (Turvallisuuskomitea, 2018.) Vastaavasti International Organization for Standardization (ISO) kuvailee tietoturvan olevan toimintaa luottamuksellisuuden, eheyden ja saatavuuden säilyttämiseksi (ISO, 2018.)

Vaikka tämä opinnäytetyö ei käsittele varsinaisesti tietosuojaa tai kyberturvallisuutta, ei voida kuitenkaan välttyä sivuamasta tietosuojan ja kyberturvallisuuden käsitteitä. Alaluvussa 2.1 määritellään lyhyesti tietosuojan ja kyberturvallisuuden käsitteet. Alaluvussa 2.2 tarkastellaan tietoturvatapahtumia Turvallisuuskomitean määritelmin ja alaluvussa 2.3 tutustutaan tietoturvan malleihin.

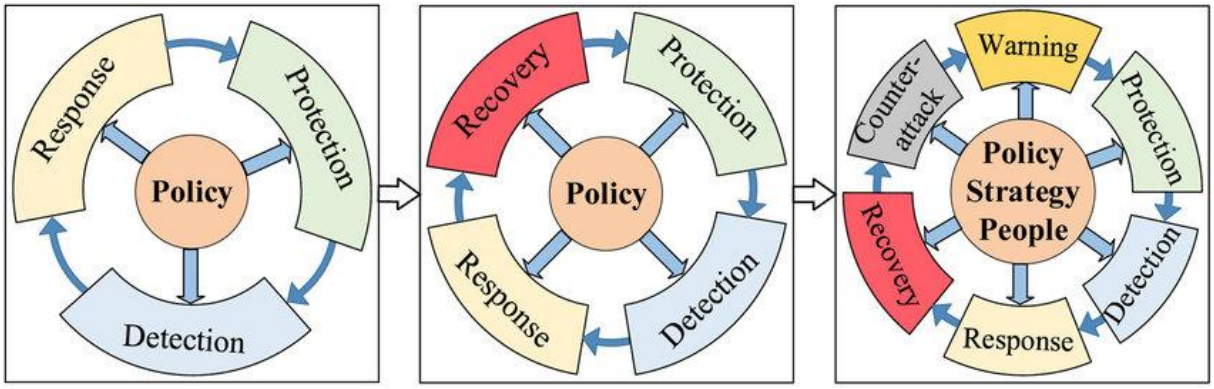
2.1 Tietosuoja ja kyberturva

Tietosuojavaltuutetun toimisto määrittelee tietosuojan jokaisen ihmisen perusoikeudeksi ja henkilötietojen käsittelyn aikana vapauksien toteutumiseksi. Henkilötietoja ovat tiedot, joiden perusteella on mahdollista tunnistaa luonnollinen henkilö suorasti tai epäsuorasti. Tietoturvavaltuutetun toimisto mainitsee tietoturvan osaksi tietosuojaa, työkaluksi, jolla tietosuojaa toteutetaan. (Tietosuojavaltuutetun toimisto, n.d.) Vuonna 2018 sovellettavaksi tullut henkilötietojen käsittelyä sääntelevä EU:n yleinen tietosuoja-asetus 2016/679, General Data Protection Regulation, pyrkii antamaan parempia työkaluja henkilötietojen turvalliseen ja suojattuun käsittelyyn sekä antamaan enemmän tapoja hallita henkilötietojen käsittelyä (Tietosuojavaltuutetun toimisto, n.d.)

Kyberturvallisuus määritellään laajemmin yhteiskunnalliseksi turvallisuuden osa-alueeksi. Tietoturva linkittyy osaksi kybertuvallisuutta, joka pyrkii takaamaan turvallisuutta yhteiskunnallisesti merkittävien järjestelmien häiriöiden tunnistamiseksi, ehkäisemiseksi ja häiriöihin varautumiseksi. (Tietoturvatapahtuma, n.d.)

Kuvassa 1 kuvataan kyberturvallisuuden mallien kehittyminen. Mallien kehitys pätee myös useimpien yritysten tapaan käsitellä tietoturvaa. Varhaisimmassa vaiheessa toimet rajoittuvat havainnointiin, suojaamiseen ja vastatoimiin. Viimeistään ensimmäisen uhkan realisoiduttua, mukaan otetaan uhkasta palautuminen. Viimeisessä kuvassa kyber- tai tieto turvallisuus on otettu osaksi yrityksen strategiaa ja koko henkilöstö toimii sen mukaisesti. Mukaan otettu vastahyökkäys voidaan ajatella toimeksi, jolla pyritään välttämään vastaavan tapahtuman uusiutuminen tulevaisuudessa, esimerkiksi käytänteitä tai ohjeistuksia muuttamalla.

Kuva 1 Kyberturvallisuuden mallien kehittyminen



2.2 Tietoturvan termejä

Tietoturvaan vaikuttavia asioita nimitetään tietoturvatapahtumiksi, tietoturvauhkiksi, tietoturvapoikkeamiksi, tietoturvariskeiksi ja tietoturvahaavoittuvuuksiksi. Puolustusministeriön yhteydessä toimiva Turvallisuuskomitea Kyberturvallisuuden sanastossaan vuodelta 2018 määrittelee termit seuraavasti: Tietoturvahaavoittuvuus on ”alttius tietoturvaan kohdistuville hyökkäyksille.” Huomautuksena tässä yhteydessä mainitaan, että ”Haavoittuvuus voi olla mikä tahansa heikkous… Haavoittuvuuksia voi olla tietojärjestelmissä, prosesseissa ja ihmisen toiminnassa.” Tietoturvatapahtuma on ” tietojärjestelmän tai organisaation toimintojen tapahtuma, jonka seurauksena tietojen tai palvelujen tila on muuttunut ja joka saattaa vaikuttaa tietoturvaan.” Tietoturvahäiriö on ”yksi tai useampi toisiinsa liittyvä odottamaton tai ei-toivottu tietoturvatapahtuma, joka vaarantaa tietojen ja palvelujen tietoturvan sekä vaikuttaa organisaation toimintaan epäsuotuisasti.” Tietoturvaloukkauksen määritelmä on ”oikeudeton puuttuminen tietoon tai tietojärjestelmään.” (Turvallisuuskomitea, 2018)

2.3 Tietoturvamallit

Yleisimmin käytetty tietoturvan malli on niin kutsuttu CIA-triadi, eli CIA-kolmikko tai CIA-malli. CIA-mallia on kritisoitu suppeaksi nykyisessä nopeasti muuttuvassa tietokonemaailmassa, jonka vuoksi sitä usein laajennetaan CIA-AAA-malliksi tai Parkerin hexadiksi. Lyhenne CIA, juontuu käsitteistä confidentiality, integrity ja availability (Kauppi, 2019.) Kuten mainittu, on CIA-malli sittemmin osoittautunut rajoittuneeksi, joten käsitteistöä on laajennettu lisäämällä CIA-malliin authentication, authorization ja accounting (Geek-university, 2019.) Niin kutsutussa Parkerin hexadissa on CIA-mallin lisäksi lisätty käsitteet possession, utility ja authenticity (Staffhost Europe, 2019.)

2.3.1 CIA-malli ja CIA-AAA-malli

CIA-mallissa mainitut luottamuksellisuus, eheys ja saatavuus määritellään seuraavasti: Luottamuksellisuus (confidentiality) tarkoittaa, että tietoihin pääsevät käsiksi vain henkilöt, joille on annettu siihen oikeus (Visma, 2019.) Eheydellä (integrity) tarkoitetaan, että tietoja pääsevät muuttamaan vain siihen oikeutetut tahot (Kyberturvallisuuskeskus, 2020) ja että tieto on yhdenmukaista alkuperäisen tiedon kanssa (Turvallisuuskomitea, 2018.) Eheys tarkoittaa myös ei haluttujen muutosten tai poistamisten estämistä sekä datan palauttamista tilanteissa, joissa toimenpide on ollut hyväksytty (Leijona Security, 2019.) Saatavuuden (availability) määritelmässä tieto tai palvelu on saatavissa silloin, kun sitä tarvitaan (Turvallisuuskomitea, 2018.)

Koska CIA-mallia on kritisoitu suppeaksi, on sitä täydennetty lisäämällä todennus (authentication), valtuutus (authorization) ja kirjanpito (accounting.) Todennus tarkoittaa, että päästäkseen käsiksi tietoihin tai dataan, on käyttäjän todistettava olevansa oikeutettu pääsyyn. Todennuksena voidaan käyttää esimerkiksi käyttäjätunnuksen ja salasanan yhdistelmää, biometrisiä tunnisteita tai toimikortteja. (Päivärinta, 2020) Valtuutus määritellään oikeuksien antamisena tietyn tehtävän tai toimen suorittamiseksi. Tehdäkseen jonkin toimenpiteen esimerkiksi tietokantapalvelimella, tulee käyttäjän tunnuksella olla oikeus, eli valtuutus toteuttaa toimenpide. (IBM, n.d.) Kirjanpito tarkoittaa käyttäjien suorittamien tapahtumien tallentamista lokitiedostoihin. Kirjanpidolla on siis hyvin suuri rooli IT-forensiikassa. (PM World Journal, 2017) Kirjanpito voidaan tuntea myös termillä kiistämättömyys (non-repudiation). Kiistämättömyys tarkoittaa, että järjestelmään tai

tietoihin tehdyt toimet ovat jälkeenpäin tutkittavissa ja merkinnät on tehty tarkkuudella, joka voidaan katsoa riittävän luotettavaksi. (Järvinen, 2003)

2.3.2 Parkerin hexadi

Toinen tapa täydentää CIA-mallia on lisätä hallinta (possession), aitous (authenticity) sekä hyödyllisyys (utility), jolloin saadaan Parkerin hexadi, jonka keskiössä on tieto tai palvelu. Hallinnalla tarkoitetaan, että tietoturvariskien hallinta on jatkuvaa, hallittua ja suunnitelmallista. Tietoturvariskien vaikutukset ja merkittävyys tunnistamalla ja arvioimalla voidaan tietoturvariskien uhkiin vastata oikein suhteutettuna. (Tietoturvariskien arviointi, n.d.) Aitoudella osoitetaan tiedon, viestin, tapahtuman tai muun tiedonvaihdon olevan lähteestä, josta sen väitetään olevan peräisin. Usein aitouden osoittamiseen käytetään digitaalisia sertifikaatteja, jotka osoittavat sertifikaatin haltijan olevan luotettu osapuoli. (Bright Hub, 2009) Hyödyllisyys tarkoittaa tiedon käyttökelpoisuutta, eli kuinka hyvin hyödynnettävää tieto on (Leijona Security, 2019.) Esimerkiksi kryptattu tiedosto ilman kryptauksen purkavaa salausavainta on hyödytöntä. Jopa tärkein selkomuotoisesta salatuksi kryptattu tieto menettää hyödyllisyytensä salausavaimen kadotessa. (Staff Host, 2019)

Kuva 2 Parkerin hexadi

3 Etätyöyhteyden toteutus

CIA-määritelmän mukaisesti etätyöskentely-yhteyden ja sen suojauksen on kyettävä varmistamaan datan eheys, saatavuus ja luottamuksellisuus. CIA-mallia voidaan tässä yhteydessä käyttää vähimmäisvaatimuksena tekniikoiden sovellutuksille.

Yksinkertaisimmillaan etätyöskentelyä tehdään käyttäen apuvälineinä sähköpostia ja puhelinta. Yleensä yhtälössä on kuitenkin muitakin työkaluja, joilla työstetään tai otetaan yhteyttä yrityksen palvelimen resursseihin. Jo sähköpostin käyttäminen ilman suojaavia toimenpiteitä voi olla riskialtista. Viimeistään yhteyden ottaminen yrityksen palvelimelle vaatii yhteyden ja työaseman suojaamista etätyöskentelyn suojaukseen tarkoitetulla ratkaisulla. (Nextiva, 2020)

Etätyöyhteys järjestetään luomalla verkkoyhteys yrityksen verkon palvelimen ja työntekijän käyttämän tietokoneen tai laitteen välille. Työntekijä on usein yhtälön heikoin lenkki ottaessaan yhteyttä esimerkiksi kotinsa lähiverkosta. Pelkkä työaseman suojaus ja kovennus ei riitä, jos kodin lähiverkko voidaan murtaa ja yhteyttä seurata. Työntekijän omalla tietoturvakäyttäytymisellä on osansa turvallisessa etätyöskentelyssä. Riskejä voivat aiheuttaa esimerkiksi vierailleminen varmentamattomilla sivustoilla, lataamalla tarkistamattomia tiedostoja tai avaamalla huijaussähköposteja tai linkkejä. Nykyiset pitkälle kehittyneet endpoint security -ratkaisut tarjoavat apua ja työkaluja riskien havaitsemiseksi, riskien toteutumisen pienentämiseksi ja vaikutuksien minimoimiseksi. (Forcepoint, n.d.)

Mitä tahansa työntekijän verkkoon liitettyä laitetta, työasemat, kannettavat tietokoneet, mobiililaitteet, maksupäätteet ja palvelimet, nimitetään termillä endpoint device. Työntekijää kutsutaan termillä end-user. Puhuttaessa etätyöskentelyn tietoturvasta käytetään laajasti endpoint security -termiä. Endpoint security määritellään lyhyesti etäpisteiden tai loppukäyttäjän laitteen sisääntulopisteen suojeluna haitallisilta osapuolilta. (McAfee, n.d.)

Etäpisteiden suojaus auttaa suojaamaan ja hallitsemaan yrityksen tärkeitä järjestelmiä, henkistä omaisuutta ja asiakastietoja haittaohjelmilta ja varjo-IT:n haitoilta. Esimerkkejä tietoturvauhkista ovat kiristysohjelmat, kalasteluviestit ja kyberhyökkäykset. (Webroot, n.d.) Etäpisteiden suojaamiseksi vaaditaan etäpisteiden keskitettyä hallintaa. Hallintaa voidaan kutsua myös palvelun

koventamiseksi. Hallinta pitää sisällään etäpisteiden havainnoinnin, jakelun, käyttöönoton, päivittämisen ja ongelmanratkonnan. (AT&T Business, 2020)

Varjo-IT tai harmaa-IT tarkoittaa palvelua tai sovellusta, joka on otettu organisaatiossa käyttöön vastoin ohjeistuksia tai ilman lupaa. Harmaata-IT:tä voivat olla myös erilaiset hyväksymättömät laitteet (rogue device) ja pilvipalvelut. Varjo-IT johtaa ennemmin tai myöhemmin tiedot pirstaloitumiseen, tietoturvauhkien ja -haavoittuvuuksien kasvuun, koska organisaation oma tietohallinto ei tiedä tiedon sijaintia ja kaikkia yhteyksiä sovellusten tai järjestelmien välillä. (Tivi, 2016)

3.1 Etätyöyhteyden muodostus

Etätyöyhteys muodostetaan lähes poikkeuksetta käyttäen TLS-salausprotokollaa. RDP eli Microsoft Remote Desktop Protocol mahdollistaa etäyhteyden ottamisen palvelimella toimivaan etätyöpöytään. Useat muut käyttöjärjestelmät tukevat RDP-ominaisuutta. RDP salataan RC4-jonosalaimella. (Microsoft, 2018) Muita suosittuja esimerkkejä muodostaa yhteys ovat seuraavaksi esiteltävät VDI ja VPN. VDI, eli virtuaalinen työpöytä (Virtual Desktop Infrastructure) on noussut lähes standardiksi tuottaa etätyöskentelypalveluita (Hirvonen, 2011). Toinen mainittu tapa käyttää yrityksen jakamia resursseja on VPN, eli virtuaalinen erillisverkko (Virtual Private Network) (Oksanen, 2019.)

Työasemavirtualisoinnissa käyttäjän työasemalle latautuu verkkoyhteyden ylitse vain graafinen näkymä palvelimella ajettavasta virtualisoidusta käyttöjärjestelmästä, ja palvelimelle siirtyvät vain käyttäjän syötteet, hiiren liikuttelu ja näppäimistösyöte sekä mahdolliset audiovisuaaliset elementit. Työasemavirtualisoinnissa tietoa ei tallenneta paikalliselle työasemalle, vaan yrityksen omalle verkkolevylle, jolloin käyttäjän ei tarvitse huolehtia tiedon katoamisesta oman paikallisen tietokoneen hajotessa. Palvelinvirtualisoinnissa varmuuskopioiden tekeminen on nopeaa ja fyysisen työaseman rajoitukset eivät juurikaan vaikuta työskentelyyn virtualisoidulla tietokoneella. (Hirvonen, 2011) Virtualisoidut käyttöjärjestelmät ja sillä ajettavat ohjelmistot on helppoa muokata ja päivittää uusiin. Virtualisoitujen tietokoneiden suorituskyky saattaa usein olla jopa parempi, kuin vastaava lokalisoitu versio, sillä palvelinkoneiden resursseja voidaan skaalata ja lisätä tarpeen mukaan. Virtualisointi alentaa myöskin ylläpitokustannuksia poistamalla tarpeen

olla päivittämässä työntekijöiden tietokoneita paremmiksi ja tehokkaammiksi. (Ace Cloud Hosting, 2018)

VPN mahdollistaa salatun yhteyden kahden pisteen välillä hyödyntäen tunneliprotokollia. Tieto kryptataan salausavaimilla ja laite yhdistetään VPN-palvelimeen. (VPNyhteys, n.d.) VPN-tyypeistä yleisimmät ovat etäyhteys (Remote Access VPN) ja sivusto sivuun -yhteys (Site-to-Site VPN.) Yhteystavoista etäyhteys tulee kysymykseen tilanteessa, jossa työntekijä ottaa yhteyttä yrityksen verkkoon ja resursseihin. (Techradar, 2020.)

Etäyhteystavassa yrityksellä on ennalta luotu ja määritelty VPN-palvelin, johon työntekijä ottaa yhteyden henkilökohtaisilla tunnuksillaan. Yhteyden muodostamista varten käyttäjän tulee käyttää erillistä ohjelmaa VPN-yhteyden muodostamiseksi. (Techradar, 2020) Etäyhteystapaa tukevat PPTP, L2TP, L2F ja IPsec -tunneliprotokollat. (Sharma & Yadav, 2015)

Site-to-site VPN yhdistää kaksi VPN-palvelinta pysyvästi toisiinsa. Yleisimmin käytetään IPsec-protokollaa yhdistämään toimipisteet tai konttorit eli ”sites” toisiinsa. Organisaatiot ovat alkaneet 2010-luvulla kasvavissa määrin siirtämään toimintojaan pilvipalveluihin, mikä osaltaan on vähentänyt tarvetta site-to-site VPN-yhteyksille. Pilvessä voidaan käyttää esimerkiksi yksityisiä pilvitallennustiloja ja palvelumalleja, kuten SaaS ja IaaS. (Palo Alto Networks, 2021)

4 Etätyöyhteyksiä suojaavat järjestelmät

Tarkasteltaviksi ratkaisuiksi valikoituivat tilaajan toimesta Check Point Sandblast Agent, Cisco Umbrella DNS Security sekä Microsoft Defender ATP & CloudApp Security. Check Point Sandblast Agentin ratkaisut siirtyivät 24.2.2021 alkaen pääosin muuttumattomina uuden Harmony Endpoint -nimisen ratkaisun alle. Muutoksen myötä tuki eri Linux-pohjaisille käyttöjärjestelmille parani ja pieniä toivottuja muutoksia saatiin pakettien tarjontaan. Työssä muutokset on otettu huomioon, eikä vanhoja tekniikoita, toiminnallisuuksia tai ominaisuuksia ole otettu työhön mukaan. Myös Microsoftin ratkaisujen nimeämisissä on tapahtunut vuosien 2019–2021 välisenä aikana muutoksia, jotka luovat edelleen hämmennystä ja ristiriitoja ratkaisuita tarkastellessa.

Tekniikoita tarkastellessa tutkitaan pääsääntöisesti palveluntarjoajan sivuilla ilmoitettuja toimintoja ja tekniikoita. Tarvittaessa selvennetään muita lähteitä käyttäen ilmoitetun toiminnon tai tekniikan tarkoitus.

4.1 Checkpoint Harmonyn päätepisteen suojauspalvelut

Check Point Harmony toimii Check Point Infinity -alustan päällä ja tarjoaa neljä eri tasoista endpoint -suojausta, jotka on esitetty sisällöittäin taulukossa 1. Kevyin ratkaisu on Data Protection, joka kuuluu jokaiseen tarjottuun suojausratkaisuun, mutta on myös saatavissa sellaisenaan. Muita ratkaisuja ovat Harmony Basic, Advanced ja Complete. Harmony -paketit toimivat työasemilla Windows 7, ja palvelimilla Windows Server 2008 R2 käyttöjärjestelmistä lähtien. Toimivuus luvataan myös MacOS Sierra 10.12.6, MacOS High Sierra 10.13.4 ja useille Linux-pohjaisille käyttöjärjestelmille. Harmonyn SmartConsolesta, jolla hallinta tapahtuu, on saatavilla paikallisversio (on-premise) sekä selaimessa toimiva pilviversio. Työntekijän tietokoneelle pakotetaan client-ohjelman asennus. (Check Point, 2021)

Taulukko 1 Check Point Harmony -paketit

Harmony Endpoint package	**Basic**	**Advanced**	**Complete**

Access Control and Port Protection	sisältää	sisältää	sisältää
Anti-Malware	sisältää	sisältää	sisältää
Anti-Ransomware	sisältää	sisältää	sisältää
Zero-Day Phishing	sisältää	sisältää	sisältää
Advanced Threat Prevention	sisältää	sisältää	sisältää
Endpoint Detection and Response	sisältää	sisältää	sisältää
Threat Emulation and Threat Extraction	ei sisällä	sisältää	sisältää
Data Security	ei sisällä	ei sisällä	sisältää

Pääsynhallinta ja porttien suojaus kuuluu kaikkiin Harmony-paketteihin ja Data Protection-pakettiin (Check Point, 2021.) Pääsynhallinta ja porttien suojaus tapahtuu halliten laitteen saapuvaa ja lähtevää verkkoliikennettä. Vaatimustenmukaisuuden tarkistuksia tehdään, kun pyritään päästä käsiksi yrityksen resursseihin. Etäyhteyden (VPN) muodostaminen yrityksen resursseihin kuuluu osana pääsynhallintaa ja porttien suojausta. Pääsynhallintaa voidaan ohjata myös Infinity Portalin kautta. (Check Point, 2017)

Haittaohjelmien torjunta kuuluu Harmony Basic-paketeista ylöspäin. (Check Point, 2021.) Haittaohjelmien torjunta (anti-malware) mielletään perinteiseksi virustorjunnaksi. Sen tehtävä on kuitenkin laajemmin suojata käyttäjän tietokonetta viruksilta, madoilta, troijalaisilta (Trojan horse), näppäimistön kirjaajilta (keystroke loggers) sekä piilohallintaohjelmilta (rootkit.) (Check Point, 2019) Tunnistamisessa hyödynnetään digitaalisia allekirjoituksia (signatures),

käyttäytymisen estoa (behavior blockers) sekä heuristista analyysia (heuristic analysis) (Check Point, 2017.)

Allekirjoitusten tunnistamisessa skannattujen tiedostojen tunnisteita vertaillaan jo tunnettujen haittaohjelmien tunnisteisiin (Kaspersky, n.d.) Käyttäytymisen estolla tarkoitetaan jonkin tietyn toiminnan estämistä, esimerkiksi järjestelmän rekisterin muuttamista tai tiedoston ajamista. Käyttäytymisen estoon sovelletaan hiekkalaatikkoa, jossa ensin testataan koodin tai ohjelman toiminta. Jos testaus ei aiheuta hälytystä, voidaan tiedosto ajaa rajoitetussa ympäristössä, jossa jokaista mahdollisesti haitallista toimintoa tutkaillaan dynaamisin tarkistuksin. Monitasoisilla arvioinneilla ja testauksilla saadaan tehokkaasti haitallisia koodinpätkiä kiinni. (National Institute of Standards and Technology, 2003) Heuristisessa analyysissa on useita tapoja lähestyä tutkittavaa ohjelmaa. Staattisessa heuristisessa analyysissa tutkittava ohjelma puretaan ja sen lähdekoodia tutkitaan ja vertaillaan heuristiseen tietokantaan. Kun riittävän suuresta osasta ohjelman lähdekoodia löytyy samankaltaisuuksia tietokannan kanssa, merkitään tutkittava ohjelma mahdollisesti haitalliseksi. Dynaamisessa heuristiikassa hyödynnetään hiekkalaatikkoa tai emulointia tutkittavien lähdekoodien ja koodin pätkien koettelemiseksi. (Kaspersky, n.d.)

Lunnasohjelmien torjunta (anti-ransomware), kuuluu Harmony Basic-paketeista ylöspäin. Lunnasohjelmien torjunnassa hyödynnetään Check Pointin omaa Endpoint Behavioral Guard-työkalua, joka tunnistettuaan poikkeavaa käyttäytymistä estää ja korjaa hyökkäysketjun. (Check Point, 2021) Lunnasohjelmia tunnistetaan myös niiden käyttäytymisen perusteella. Tunnistukseen ei vaadita allekirjoituksia ja toiminto toimii myös yhteydettömässä tilassa. (Check Point, 2019) Jotkin vähemmän kehittyneet lunnasohjelmat jäävät kiinni haittaohjelmien torjunnan tutkaimeen joko allekirjoituksen tai heuristisen raportin vuoksi (PCMag UK, 2020.) Harmony Endpoint käyttää paikalliselle koneelle luotua holvia (Harmony Endpoint Vault), johon laitteen muilla prosesseilla ei ole pääsyä. Holvia käytetään, jos haittaohjelma pyrkii poistamaan volyymin varjokopion (shadow copy.) (Check Point, 2021) Shadow copy on Windowsin varmuuskopiointitekniikka, jolla luodaan palautuspisteitä (snapshot) (Personaldatasecurity, n.d.)

Zero-Day Phishing Protection kuuluu Harmony Basic-paketeista ylöspäin. Se toimii reaaliaikaisesti hyödyntäen dynaamista analyysia sekä staattisia ja heuristisia tunnistusmekanismeja verkkosivuilla, joilla vaaditaan käyttäjän syötettä. Havaittuaan haitallisia elementtejä, estää toiminto käyttäjää antamasta syötettä sivulle, ilmoittaa käyttäjälle mahdollisesta uhkasta ja luo

raportin portaaliin. (Check Point, 2021) Termi Zero-Day Phishing viittaa sananmukaisesti nollaan päivään, eli haavoittuvuutta tai uhkaa ei ole tavattu aikaisemmin ja ratkaisua kehitetty (Norton, 2019.) Phishing-hyökkäyksessä käyttäjää yritetään johtaa harhaan johtamalla käyttäjä esimerkiksi tekaistulle verkkosivulle antamaan käyttäjätunnuksensa yleensä tuttuun palveluun (FBI, n.d.)

Edistynyt uhkien ehkäisy käsittää Anti-Bot toiminnon, joka kuuluu Harmony Basic-paketeista ylöspäin (Check Point, 2021.) Anti-Bot estää prosessien kommunikoinnin C&C -palvelimien kanssa. C&C on lyhennys sanoista ”command and control,” joka tarkoittaa etäpalvelinta, eli tässä tapauksessa bottien isäntää (host) tai ohjaajaa (controller). Anti-Botin havainnointi tapahtuu seuraamalla kaikkien työaseman prosessien verkkoliikennettä. Varsinainen uhkien tunnistaminen tapahtuu kaksiosaisesti: ensin verkkoliikenteestä poimittuja allekirjoituksia verrataan tunnettuihin haitallisten toimijoiden allekirjoituksiin sekä verraten IP-osoitteita ja verkkotunnuksia Check Point Threat Cloud -pilvitietokantaan. Kun hälytys haitallisesta yhteydestä saadaan, Anti-Bot estää yhteyden, pysäyttää yhteyttä käyttäneen prosessin ja siirtää prosessin tiedostoineen karanteeniin, jonka jälkeen tapahtumasta kirjataan lokitiedosto omalle lokipalvelimelle. (Check Point, 2019) Harmony käyttää hyväksi tunnetuksi tullutta MITRE ATT&CK® -runkoa (framework.) Infinity portaalista voidaan valita tunnettu hyökkäys ja etsiä siitä kirjattuja raportteja (Check Point, 2021.) MITRE ATT&CK® on tietopohja tai kirjasto, joka sisältää tietoturvatestaajille taktiikoita ja tekniikoita, joita oikeat haittaohjelmat ja haitalliset toimijat käyttävät (MITRE ATT&CK, 2021.)

Päätepisteen havainnointi ja vaste (Endpoint Detection and Response), EDR on toiminnallinen kokonaisuus, jolla kerätään jatkuvasti dataa työasemien toiminnasta ja tilasta. EDR kuuluu Harmony Standard-paketeista ylöspäin. Kerätyn datan pohjalta voidaan tehdä analyysejä ja vertailla dataa työasemien välillä. EDR raportoi keskitetylle järjestelmälle, josta voi yhtä konsolia tutkimalla nähdä koko verkon työasemien tilan. EDR on tarkoitettu automatisoimaan datan keräys, käsittely, raporttien muodostus ja vastatoimien aloitus uhan ilmestyessä. Automatisoinnin lisäksi EDR on muokattavissa ja sille voidaan antaa sääntöjä, joiden mukaan uhkatilanteissa toimitaan. Omat säännöt vähentävät työhön sidotun henkilöstön kuormaa. (Check Point, n.d.)

Uhkaemulointi ja uhkien poisto -ominaisuudet (Threat Emulation and Threat Extraction) kuuluvat Harmony Advanced-paketeista ylöspäin. Uhkaemuloinnissa jokainen verkkoselaimella ladattu tiedosto viedään uhkaemuloinnin tai hiekkalaatikon läpi, jossa tiedostoa tarkastellaan aidatussa ympäristössä. (Check Point, 2019) Emuloinnissa imitoidaan resurssia, jota ei ole tosiasiallisesti

olemassa. Imitoitavat resurssit voivat olla ohjelmia, fyysisiä laitteita tai kokonaisia alustoja. (Techopedia, 2013) Uhkan poisto pitää huolen, että käyttäjä saa vain tarkistettuja ja puhtaita tiedostoja. Ladatusta tiedostosta poistetaan haitalliset komponentit, esimerkiksi Exel-taulukon makrot. Puhdistuksen jälkeen tiedosto välitetään käyttäjälle ja käyttäjä voi käyttää tiedostoa normaalisti sekä tarvittaessa pääsee käsiksi alkuperäiseen tiedostoon. (Check Point, 2019) Uhkien poisto käyttää Check Pointin uutta Content Disarm & Reconstruction teknologiaa (Check Point, 2021.)

Datan suojaus kuuluu Harmony Complete -pakettiin. Datan suojaus tarjoaa täyden kryptauksen työasemalle ja siirrettäville medioille, kuten USB-massamuisteille. Kryptauksella estetään datan hyödynnettävyys väärissä käsissä salaamalla se. Tieto, palvelu tai data on käyttökelvotonta kryptauksen jälkeen ilman oikeaa salausavainta. (Check Point, 2021)

4.2 Cisco Umbrellalla turvallisuutta nimipalvelusta

Ciscon Umbrella DNS Security on täysin pilvipalveluna toimiva nimepalvelin. DNS Security-pakettia tarjotaan kolmena eri tasoisena kokonaisuutena: Essentials, Advantage ja Secure Internet Gateway (SIG) Essentials. Umbrella DNS Security ei vaadi päivityksiä tai asennettavia sovelluksia pilvipalvelurakenteensa vuoksi. Se käyttää unicast-lähetystä, jolloin lähin datakeskus vastaa lähetettyyn palvelupyyntöön, mikä käytännössä poistaa palvelukatkon riskin. Data-keskuksia oli työn kirjoittamisen aikoihin ilmoitettu olevan noin 30 kappaletta ympäri maailman. (Cisco, n.d.)

Umbrellan mukana tarjotaan Cisco Talos uhkatietopalvelu. Umbrella käyttää staattisia ja koneoppimiseen perustuvia tekniikoita uusien uhkien löytämiseksi ja torjumiseksi. Umbrella Investigate konsolin ja API:n avulla tarjoavat reaaliaikaista tilannekuvaa uhkista sekä nopean reagoinnin uhkiin ja niiden tutkimiseen. Verkosta irti olevia tietokoneita suojaa kevyt roaming client-ohjelma tai laitteelle asennettava Ciscon AnyConnect-ohjelma. Umbrella tarjoaa suojaa myös mobiililaitteille. (Cisco, 2020) Umbrella Investigate tarjoaa verkkokonsolin tarkempia tutkimuksia varten. Rajapinnan avulla on mahdollista tukea muita työkaluja ja järjestelmiä Investigaten URL-, IP- ja tiedostojen uhka-analysointityökalulla. Verkkokonsolista näkee pisteytettynä uhka-arvion, kuvaajan DNS-pyynnöistä sekä tilannekuvan nimipalvelun päätapahtumista. (Cisco, n.d.)

Umbrella toimii nimipalvelimena yrityksen palvelimen ja työntekijöiden välissä tarkkaillen ja estäen haitallista liikennettä ennen tiedon siirtämistä loppukäyttäjälle. Nimipalvelimena ja IP-tasolla toimiminen mahdollistavat haitallisten yhteyksien estämisen jo yhteyspyyntöjen aikana ennen yhteyden muodostamista. Nimipalvelupyyntöjen seuranta auttaa tunnistamaan haavoittuneita järjestelmiä sekä estämään C&C-yhteyksien muodostuksen. Umbrella DNS Securityn avulla saadaan kuva organisaation verkkoon kytketyistä päätelaitteista ja niillä käytettävistä muista pilvipalveluista sekä siitä, kuka niitä käyttää. Umbrella DNS Securityn avulla kyetään kartoittamaan palvelun mahdollisia riskejä ja estämään palvelun käyttö. (Cisco, 2020)

Umbrella DNS Security estää verkkotunnuksiin yhdistämisen, jotka luokitellaan liittyvän haittaohjelmiin, tietojen kalasteluun ja botnetteihin. Hallintatyökalu antaa ylläpidolle mahdollisuuden estää, suodattaa ja kategorisoida verkkotunnuksia. Verkkotunnuksien seurantaan

perustuen kyetään havaitsemaan ja estämään niin kutsuttua C&C-yhteyksiä ja varjo- tai harmaa-IT:tä (shadow IT.) (Cisco, n.d.)

Umbrella DNS Securityn integrointi Windowsin aktiivihakemiston kanssa mahdollistaa käytäntöjen ja sääntöjen luomisen, raporttien seuraamisen ja toimialueen tehokkaan hallinnan. API-rajapinta mahdollistaa muiden olemassa olevien työkalujen ja työkulkujen valvonnan, raportoinnin, hallinnan sekä käyttöönoton. Cisco Threat Response on mahdollista yhdistää kaikkiin Ciscon tuotteisiin. Lokitiedostoja voidaan säilyttää Amazonin web-palvelussa joko käyttäjän tai Ciscon hallitsemassa S3-ämpärissä (Amazon Simple Storage Service). (Cisco, n.d.)

Advantage -paketti mahdollistaa estämään suorat, nimipalvelun ohittavat yhteydenotot verkon IP-osoitteisiin. Advantage tarjoaa myös valikoivan välityspalvelimen (Selective Proxy) sekä Umbrella Investigate-palvelun. Valikoivalle välityspalvelimelle ohjataan mahdollisesti haitalliseksi liputetut verkkotunnukset tarkempaan URL ja tiedostojen tarkasteluun käyttäen Ciscon viruksentorjuntaohjelmistoja, AV ja Ciscon edistynyttä haittaohjelmasuojausta, AMP (Advanced Malware Protection.) Valikoiva välityspalvelin mahdollistaa myös liikennöinnin kryptauksen sekä TLS-salatun liikenteen tarkkailun epäilyttäviin verkkotunnuksiin. (Cisco, n.d.)

SIG-paketti sisältää Essentials -paketin, Advantage -paketin ominaisuudet sekä muutamia lisäominaisuuksia. Kuten paketin nimi viittaa, tarjoaa SIG verkkoyhdyskäytävän suojaamiseksi DNS Security Advantage-paketista paranneltuja palveluita. SIG mahdollistaa kaiken verkkoliikenteen ohjaamisen välityspalvelimelle URL ja tiedoston tarkasteluun sekä kaiken liikenteen kryptaamisen ja kaiken TLS-salatun liikenteen tarkastelun. Myös liikenteen suodattamista on paranneltu Advantage-paketista: liikennettä voidaan suodattaa perustuen verkkotunnukseen, URL-osoitteeseen tai kategoriaan. SIG tarjoaa ympäristön Cisco Threat Grid -pilvihiekkalaatikolle, jossa epäilyttäviä tiedostoja voidaan tutkia ja analysoida. Paketissa on myös mahdollisuus tarkastella takautuvasti tapahtumia, joissa tiedostoa ei pidetty haitallisena, mutta liputettiin haitalliseksi myöhemmin. (Cisco, n.d.)

SIG mahdollistaa pilvipohjaisen palomuurin luonnin, joka toimii OSI-mallin tasoilla 3 ja 4 estäen halutut IP-osoitteet ja osoitealueet, portit sekä protokollat. (Cisco, n.d.) OSI-malli, eli Open Systems Interconnection Reference Model kuvaa tiedonsiirtoa jaettuna seitsemään kerrokseen. Kolmas kerros kuvaa verkkokerrosta, jonka tehtävänä on välittää kerroksien 4–7

tietoliikennepaketteja laitteiden välillä. Neljäs kerros kuvaa kuljetuskerrosta, jonka tehtävänä on vuonhallinta ja huolehtia pakettien pääsystä perille oikeassa järjestyksessä. (OSI-model, n.d.)

Advantage-paketeista varjo-IT:n torjumista on paranneltu: varjo-IT:n havainnointi ja esto voidaan tehdä URL-tasolla, riippumatta verkkotunnuksesta. SIG tarjoaa suoraan käännettynä ”rakeista hallintaa” (granular control tai fine-grained control.) (Cisco, n.d.) Granular control tarkoittaa hyvin yksityiskohtaista hallintaa. Tietoturvallisuudessa tämä voi tarkoittaa kirjautumisen hallinnassa tarkkoja vaatimuksia, joiden puitteissa järjestelmään voidaan kirjautua tai muutoksia voidaan tehdä. Vaatimuksia, joiden tulee täyttyä samanaikaisesti, voisivat olla, että tapahtuma tapahtuu tietyssä aikaikkunassa, identifiointi on kaksivaiheinen, esimerkiksi salasanan ja toimikortin yhdistelmä, identifioidulla käyttäjällä on oikeutus toimiin, toimi suoritetaan tietyllä tavalla, esimerkiksi tietyllä sovelluksella, toimi suoritetaan tietyssä paikassa tai paikasta, esimerkiksi sisäverkon tietty IP-osoite ja MAC-osoite. Edellä esitettyjä vaatimuksia on hyökkääjän yhtäaikaisesti vaikea saada itselleen. (Helpsystems, 2018) SIG tarjoaa siis tarkkoja tapoja rajata toimintaa verkossa, esimerkiksi estäen tiedostojen lataamisen (upload) verkkoon, liitetiedostojen avaamisen ja lataamisen sekä viestien lähettämisen sosiaalisen median alustoilla. (Cisco, n.d.)

4.3 Microsoft Defender päätepisteille ja pilvipalveluturvallisuus

Microsoft Defender for Endpoint (MDE) sekä Cloud App Security ovat pilvipohjaisia palveluita. Microsoft tarjoaa useita erilaisia ja monipuolisia paketteja etätyöaseman ja yhteyden suojaamiseksi. Tutkittavana oleva Windows Defender for Endpoint tunnettiin ennen Microsoft Defender Advanced Threat Protection (ATP). MDE kuuluu osana Microsoft 365 Enterprise E5, Business Premium ja Education A5 -paketteja, mutta on myös saatavana itsenäisenä palveluna. Myös Cloud App Security on saatavilla itsenäisenä tuotteena, sekä integroituna Microsoft 365 E5 ja A5 -paketeissa. (Microsoft, n.d.)

Hallinnan ja toimintojen pohjana ja portaalina toimii Microsoft Defender Security Center, suojauskeskus (MDSC). MDE tarjoaa riskeihin pohjautuvien haavoittuvuuksien hallintaa ja arviointia, hyökkäyspinta-alan rajauksen, päätepisteiden tunnistuksen ja käsittelyn (EDR), automaattisen tutkinnan ja korjauksen (AIR) sekä hallitut etsintäpalvelut. Suojaus perustuu käyttäytymisen tunnistamiseen. (Microsoft, n.d.)

Päätepisteiden käytöksen tunnistamisen sensorit ovat osa Windows 10 -käyttöjärjestelmää. Sensorit havainnoivat ja keräävät merkkejä käyttöjärjestelmältä prosessien käyttäytymisestä ja lähettävät datan erilliseen, rajattuun Defender for Endpoint -pilvitilaan. Kaikessa tiedonsiirrossa käytetään vähimmäisvaatimuksena 256-bittistä AES-suojausta. (Microsoft, n.d.)

Uhkien ja haavoittuvuuksien hallinta toimii infrastruktuurina organisaation altistumisen vähentämiseen, päätelaitteiden koventamiseen ja organisaation sietokyvyn lisäämiseen. MDE:hen liitetyt laitteet lähettävät automaattisesti raportteja keskitetylle hallinnalle haavoittuvuuksista ja suojauskokoonpanoista, jotka esitetään hallintapaneelissa toimintasuosituksineen. Uhkien ja haavoittuvuuksien hallinta parantaa näkyvyyttä organisaation ohjelmistoluetteloon, muutoksiin ohjelmistoissa, ohjelmistojen käyttömalleihin sekä organisaation tietoturvan kokoonpanoon. (Microsoft, n.d.)

Hyödyntämällä big-dataa, koneoppimista sekä havainnoimalla Microsoft-optiikkaa Windowsin-ekosysteemissä, yritysten pilvipalvelutuotteissa ja verkkoresursseissa saadaan käyttäytymisen tunnistamisessa saatu data muunnettua oivalluksiksi (insights), havainnoiksi ja suositelluiksi toimiksi uhkiin vastaamiseksi. Reaaliaikaisella havainnoinnilla voidaan havaita haavoittuvuuksia ja virheitä määrityksissä ilman erillisiä agentteja tai säännöllisesti ajettavia tarkistuksia. Haavoittuvuuden löytyessä, tehdään priorisointi uhka-alueen, tehtyjen havaintojen, vaarassa olevan datan ja liiketoimintaympäristön pohjalta. (Microsoft, n.d.)

Microsoftin tietoturvatiimien tuottama uhkatiedustelutieto (threat intelligence) ja sitä kumppanien uhkatiedolla parantelu auttavat MDE:tä tunnistamaan haitallisia toimijoita niiden käyttämien työkalujen, tekniikoiden ja menettelytapojen perusteella. MDE mahdollistaa automaattisen hälytyksen luonnin, kun kerättyjen tietojen perusteella tunnistetaan haitallinen toimija. (Microsoft, n.d.)

Käytettynä yhdessä Microsoft Intune -palvelun kanssa, on uhkien ja haavoittuvuuksien hallinnalla mahdollista luoda korjaustehtäviä tietyistä tietoturvasuosituksista. Suositukset voivat ehdottaa muun muassa kokoonpanomuutoksia ohjelmistojen haavoittuvuuksiin liittyvien riskien pienentämiseksi. Uhkien ja haavoittuvuuksien hallinta mahdollistaa korjaustoimien tilan ja edistymisen reaaliaikaisen seurannan koko organisaation laajuudelta. (Microsoft, n.d.)

Microsoft 365 E5 -lisenssin kanssa käytettävät seuranta-, analytiikka-, työnkulku-, raportointi- ja määritystyökalut auttavat pienentämään hyökkäyspinta-alaa. Hyökkäyspinta-alaa voidaan

pienentää hallitsemalla pääsemistä haitallisille IP-osoitteille, verkkotunnuksille ja URL-linkeille sekä asettamalla sääntöjä ohjelmistoille estämään haittaohjelmistotartuntoja. Hyökkäyspinta-alaa rajaavat säännöt voivat vaikuttaa esimerkiksi ajettaviin tiedostoihin ja skripteihin, jotka yrittävät ladata tai ajaa tiedostoja tai toimivat tavallisuudesta poikkeavasti, esimerkiksi pyrkivät erikoisena aikana ajamaan tiedostoa. Ennen sääntöjen käyttöönottoa voidaan arvioida sääntöjen vaikutuksia verkkoympäristöön ja organisaatioon auditointimoodissa. Auditointi on hyödyllinen työkalu, kun arvioidaan sääntöjen vaikutusta kolmannen osapuolen prosesseihin, joiden toimet saattavat joutua liputetuksi haitallisena. Auditoinnin tarkoituksena on auttaa luomaan tehokkaita sääntöjä vaikuttamatta tuotantoon ja käytettävyyteen. Uusimpien Windows 10 versioiden (1908) kanssa yhteensopivana on saatavissa varoitusmoodi (warn mode), joka antaa käyttäjälle varoituksen sisällön estämisestä sekä mahdollisuuden väliaikaisesti purkaa eston. Vanhemmissa Windows 10 versioissa varoitusmoodi ajetaan estomoodissa. Kaikki varoitukset ja hälytykset ovat tarkasteltavissa Microsoft Defender suojauskeskuksessa. (Microsoft, n.d.)

Advanced Hunting, joka on kyselypohjainen työkalu, mahdollistaa raakadatan tutkimisen 30 päivään asti. Tämä mahdollistaa verkon tapahtumien tutkimisen ja kyselyiden tekemisen Microsoft Defender Security Centerissä. Hyökkäyspinta-alaa rajaavien sääntöjen tapahtumien tarkastelu on mahdollista myös Windows Event Viewerillä, joka löytyy jokaiselta Windows 10 -käyttöjärjestelmältä ja on käytettävissä ilman E5-lisenssiä. (Microsoft, n.d.)

Advanced Protection -työkalu huolehtii suojautumisesta haittaohjelmia (malware) vastaan skannaamalla järjestelmään saapuvia ajettavia tiedostoja. Jos skannauksessa löydetään haittaohjelmia muistuttavia elementtejä, eikä tiedosto ole poikkeuksien listalla tai luotettu toimija, estetään tiedoston toiminta säännöllä. (Microsoft, n.d.)

Microsoft Defender Antivirus tarjoaa big-datan analyysiin, koneoppimiseen ja pilvipohjaiseen infrastruktuuriin pohjautuvan virusturvan. Defender Antivirus hyödyntää uhkien etsinnässä käyttäytymiseen pohjaavaa heuristiikkaa ja sekä skannaa jatkuvasti käytettäviä tiedostoja. Se toimii reaaliaikaisesti estäen myös mahdollisesti haitallisten sovellusten ajamisen, joita ei liputettaisi lähtökohtaisesti haittaohjelmina. Pilvipohjaisuus mahdollistaa ajantasaisen tiedon uhkista ja uusista päivityksistä. (Microsoft, n.d.)

Päätepisteen havainnointi ja vaste (Endpoint Detection and Response) auttavat havaitsemaan, tutkimaan ja vastaamaan uhkiin, jotka eivät jää kiinni ja pääsevät järjestelmän sisälle. Taustalla on

ajattelu siitä, että mikään järjestelmä tai suojaus ei ole murtamaton. EDR kerää jatkuvasti tietoverkkomittauksia prosesseista, verkon tapahtumista, kernelistä, muistinhallinnasta, kirjautumisenhallinnasta, rekistereistä sekä muutoksista järjestelmätiedostoista. Tietoja säilytetään kuusi kuukautta. EDR auttaa löytämään kyselyitä hyväksi käyttäen murtokohtia ja itse luotuja havaintoja. EDR auttaa tietoturvavastaavia priorisoimaan hälytyksiä, saamaan paremman kokonaiskuvan murrosta ja vastaamaan tehokkaammin havaittuun murtoon tai uhkaan. (Microsoft, n.d.)

Automaattinen tutkinta ja korjaus (Auto investigation and remediation), AIR perustuu turvallisuusanalyytikoiden käyttämiin prosesseihin ja erilaisiin tarkastusalgoritmeihin. AIR helpottaa tietoturvahenkilöstön työtä vapauttamalla resursseja automatisoimalla hälytyksiin vastaamista ja toimiin ryhtymistä. Automaattinen tutkinta voidaan aloittaa myös manuaalisesti. Vireillä olevia ja valmiita toimia voidaan seurata toimintakeskuksessa (action center), jossa toimia voidaan hyväksyä tai hylätä sekä valmiit toimet voidaan tarvittaessa kumota. Korjaustoimet voidaan asettaa alkamaan automaattisesti tai vaatimaan erillisen hyväksynnän. (Microsoft, n.d.)

Microsoftin uhka-asiantuntija (Microsoft Threat Experts) tarjoaa asiantuntijatason monitorointia ja analysointia varmistamaan, että asiakkaan yksilöllisen ympäristön uhat eivät jää huomioimatta. Uhka-asiantuntija auttaa ennaltaehkäisemään vaikeimmilta verkon uhilta, kuten inhimillisen toimijan toteuttamilta murroilta, ihmisen ohjaamilta kiristyshyökkäyksiltä ja kybervakoilulta. Asiakas voi jättää tiketin Microsoftin Defender suojauskeskukseen ottaakseen yhteyttä Microsoftin tietoturva-asiantuntijaan. (Microsoft, n.d.)

Laitteiden yhdistäminen on integroitu Microsoft Endpoint Manageriin, Microsoft Intune for client -laitteisiin ja Azure Security Center palvelinlaitteisiin. Integraatio mahdollistaa monitoroinnin, kokonaiskuvan kokoonpanoista sekä laitteiden, sovellusten ja sääntöjen käyttöönotosta. Roolipohjaisen käyttöoikeuksien hallinnan avulla Defender for Endpoint tarjoaa mahdollisuuden vaikuttaa siihen, mitä portaalin käyttäjät voivat nähdä tai tehdä. Roolipohjainen käyttöoikeuksien hallinta mahdollistaa globaalisti hajautetut organisaatiot ja tietoturvaryhmät, porrastetut tietoturvatoimintaryhmät sekä yhdellä keskitetyllä turvallisuusoperaatioryhmällä johdetut täysin erilliset osastot. (Microsoft, n.d.)

Defender for Endpoint tarjoaa monikerroksisen API-mallin, jolla tietoja ja ominaisuuksia voidaan jakaa. API:t (application programming interface) voidaan jakaa kolmeen kerrokseen: Microsoft

Defender for Endpoint API:t, Raw data streaming API ja SIEM integraatio. SIEM integraatio mahdollistaa tietoturvatietojen ja tapahtumien hallinnan jakamisen. Microsoft Defender for Endpoint on mahdollista integroida myös muiden Microsoftin tuotteiden kanssa. (Microsoft, n.d.)

Microsoft CloudApp Security tunnetaan myös nimellä Cloud Access Security Broker (CASB.) Lisänimen mukaisesti palvelu toimii välikätenä pilviresurssien ja yrityksen työntekijän välissä. CloudApp auttaa ylläpitämään yrityksen tietoturvakäytänteitä ja havaitsemaan varjo-IT:tä. CASB:n avulla voidaan seurata käyttäjiä poikkeavan käyttäytymisen havaitsemiseksi sekä hallita pääsyä yrityksen resursseihin. Tällä voidaan parantaa datan luottamuksellisuutta ja estää tietovuotoja. (Microsoft, n.d.)

5 Metodit ja työn tarkoitus

Työn menetelmä on tutkimuksellinen vertailu. Erillisistä yhteydenotoista ei ole erikseen tilaajan kanssa sovittu, vaan työn edistymisestä vaihdetaan tarvittaessa sähköposteja. Työn tärkein fokus on avata etätyöskentely-yhteyksien suojaamiseksi hyödynnettyjä tekniikoita ja työkaluja sekä vertailla toivottujen ratkaisujen tekniikoita. Työn aikana tarkentui vielä valinnainen fokus liittyen tietohallinnon luottamuksellisuuteen ja tietosuojaan: ketkä tietohallinnossa pääsevät seuraaman hyvinkin yksilöllisiä tietoja organisaation työntekijöiden laitteista ja tekemisistä käytettäessä tutkittavia ratkaisuja? Työn lopputuloksen tulee tarjota tukea teknisistä ratkaisuista kiinnostuneille, yritysten hankinnasta vastaaville henkilöille. Työn on tarjottava lyhyt aiheeseen perehdyttävä teoriaosuus, joka antaa taustatietoa tietoturvasta ja etätyöskentelystä ratkaisuiden teknistä tarkastelua varten.

Tilaajan toiveesta työ toimii tukena erilaisille etätyötä harjoittaville yrityksille ja organisaatioille, ei vain Hämeen ammattikorkeakoulukeskusta varten, sillä ratkaisut ovat yleismaailmallisia ja soveltuvat niin oppilaitoksille, kuin kaupallisille yrityksillekin. Tästä syystä ratkaisuiden läpikäymisen on oltava riittävän helposti ymmärrettävää.

Työn painopiste on teoriaosuudessa ja olemassa olevien arvosteluiden sekä tarkasteluiden läpikäynnissä. Käytännön osuus jää lyhyeksi, sillä ratkaisuiden käytännönläheinen kokeileminen teettäisi työtä toisen opinnäytetyön verran laboratorioympäristön rakentamisen ja ratkaisuiden lisenssien tai demoversioiden hankkimisen vuoksi. Tämän vuoksi tukeudutaan olemassa olevaan dokumentaatioon ja tarvittaessa kolmannen osapuolen opastusvideoihin palveluiden käytöstä ja käyttöönotosta.

6 Työn suunnittelu ja toteutus

Tilaajan ehdotettua aihetta, aloitettiin rajojen vetäminen aiheen ympärille ja aiheen suuntaa antava kartoitus. Aihealueen tarkennuttua tilaaja esitti tarkasteltaviksi toivotut ratkaisut: Check Point Sandblast Endpoint Agent, Cisco Umbrella DNS Security sekä Microsoft Defender ATP & CloudApp security. Työn fokukseksi lukittui ratkaisujen teknisten ominaisuuksien tarkastelu. Myöhemmin valinnaiseksi tarkastelun aiheeksi otettiin kysymys siitä, ketkä tietohallinnossa pääsevät seuraaman hyvinkin yksilöllisiä tietoja organisaation työntekijöiden laitteista ja tekemisistä käytettäessä tutkittavia ratkaisuja.

Työn varsinainen suunnittelu tapahtui työn edetessä ja rakentuessa tarkasteltavien ratkaisujen ympärille. Ratkaisuja tutkittaessa kävi ilmeiseksi, että teoriaosuudessa lukijalle on avattava tietoturvan käsitettä, eli mitä ratkaisuilla pyritään kattamaan. Teoriaosuudessa oli myös sivuttava lyhyesti joitakin etätyöskentelyyn käytettyjä tekniikoita. Tiedonkeruun edetessä hahmottui myös teoriaosuuden rakenne. Kerätyn tiedon suuren määrän vuoksi lopullisen tuotoksen teoriaosuutta oli leikattava.

Toteutusvaiheessa kolmea edellä mainittua ratkaisua verrattiin keskenään. Pyrkimys oli korostaa ominaisuuksia, joita ei muista ratkaisuista löydy tai ominaisuus voitiin katsoa ylivoimaiseksi muihin verrokkeihin verrattuna. Pohjana vertailulle toimi työtä varten ratkaisuista kerätty tietoaineisto. Koska kaikista kolmessa ratkaisusta oli tarjolla useita eritasoisia paketteja, tyydyttiin vertaamaan laajimpia ja kokonaisvaltaisimpia paketteja, Checkpoint Harmony Endpoint Complete, Cisco Umbrella Secure Internet Gateway Essentials ja Microsoft 365 E5 -lisenssille Microsoft Defender for Endpoint.

Käyttötarkoitukset ratkaisuiden välillä olivat pääosin yhtenevät, sekä jopa se, miten ratkaisut oli toteutettu. Pohjaratkaisuna kaikki ratkaisut hyödyntävät vahvasti pilvipalveluita toimintoihinsa: Check Point Threat Cloud, Cisco Threat Grid, MITRE ATT&CK framework, Selective Proxy, CASB. Jokaista ratkaisua ohjataan keskitetystä portaalista: Check Point Infinity, Cisco Umbrella dashboard ja Microsoft Defender suojauskeskuksesta. Kaikki ratkaisut tukevat rajapintaa Windowsin aktiivihakemistojen ja muiden Windowsin palveluiden kanssa joko suoraan tai ohjelmointirajapintaa hyödyntäen. Kaikista ratkaisuista löytyi pääsynhallinnan ominaisuuksia. Ratkaisuista Microsoft Defender for Endpoint oli eniten lähellä paikallista palvelua, suurimman

osan päätepisteen työkaluista ja ominaisuuksista kuuluessa osana Windows 10 käyttöjärjestelmää, CloudApp Securityn tuodessa pilvipalvelua vahvemmin mukaan. Check Point Harmony client-ohjelma tuottaa pääsynhallintaa, porttien suojausta ja vaatimustenmukaisuuden tarkistuksia päätepisteellä. Cisco Umbrella tekee pääsynhallintaa ja verkkoliikenteen suodatusta nimipalvelimelta käsin. Microsoft Defender for Endpoint mahdollistaa sääntöjen ja CloudApp Securityn kautta pääsynhallinnan. Endpoint-palveluista vain Check Point Harmony tarjoaa työasemien ja laitteiden kryptaamista. Cisco Umbrella tarjoaa kaiken valikoivalle välityspalvelimelle ohjattavan liikenteen kryptaamista.

Kaikki ratkaisut tarjoavat haittaohjelmien torjumisen työkaluja. Check Point Harmony tarjoaa kuitenkin laajimmat ja monipuolisimmat työkalut, mahdollistaen tehokkaan suojan yhteydettömässä tilassa sekä tarjoaa Harmony Endpoint Vault -säilön. Harmony hyödyntää myös tehokkaasti haittaohjelmien torjunnassa uhkaemulaatiota ja hiekkalaatikkoa, käyttäen omaa uhkanpoistoa, Content Disarm & Reconstruction technology. Harmony ja Umbrella käyttävät tehokkaasti käyttäytymisen estoa ja jatkuvaa prosessien tarkkailua. Defender for Endpoint hyödyntää jatkuvaa Windows-ekosysteemin tarkkailua käyttöjärjestelmästä käsin.

Cisco Umbrellan haittaohjelmien torjuntaratkaisu säästää käyttäjän koneen resursseja tehdessään tiedostojen ja URL:ien tarkastelun valikoivalla välityspalvelimella sekä toimiessaan nimipalvelimena työntekijän ja yrityksen resurssien välissä. Harmony, että Umbrella tuottavat molemmat ATP-palvelua, jolla seurataan verkkoliikennettä ja kyetään estämään suorat yhteydenotot, C&C. CloudApp Security toimii niin välittäjänä työntekijän ja verkkoresurssien välissä auttaen löytämään varjo-IT:n ja estämään C&C-yhteyksiä. Cisco Umbrella ATP hyödyntää palvelussaan Amazonin web-palvelua lokipalvelimena, vaihtoehtoisesti voidaan käyttää asiakkaan omaa tai Ciscon tarjoamaa lokipalvelinta.

Cisco, Check Point ja Microsoft Defender for Endpoint tuottavat näkyvää ja laadukasta EDR- ja AIR-palvelua, joilla suoritetaan päätepisteiden datankeruu, analysointi, keskitetyt vastatoimet ja IT-forensiikka. AIR-palvelu tekee kaikkien ratkaisujen osalta datankeruusta, analysoinnista, suosituksista ja vastatoimista automaattisia. Cisco Umbrella ja Check Point etsivät EDR-palvelujaan käyttäen varjo-IT:tä. Microsoft Defender for Endpoint tarjoaa Threat Expert-palvelua, joka tuottaa lisää monitorointia ja uhkan etsintää auttavaa Targeted Attack Notification. Microsoft Defender suojauskeskuksen kautta asiakas voi konsultoida Microsoftin tietoturvaeksperttien kanssa. Vastaavaa palvelua tarjoaa Cisco Talos osana Cisco Umbrellaa.

Defender for Endpoint ja Cisco Umbrella mahdollistavat rakeisen hallinnan suoraan portaaleissaan. Lopulta myös Check Point Harmony saadaan toteuttamaan vastaavaa hallintaa, vaikka ominaisuutta ei ole otettu osaksi paketteja. Harmonylla tämä on mahdollista saada toteutettua ottamalla käyttöön yhteyksiä ja käyttäjän toimintaa koskevia sääntöjä. Defender for Endpointin auditointiominaisuus auttaa kartoittamaan sääntöjen vaikutuksia. Saman toiminnon vastaavasti hoitaa Check Point Harmonyn EDR.

Microsoftin dokumentaatiosta löytyi ohjeita IT-hallinnon roolien asettamiseksi käyttäen Azuren aktiivihakemistoa. Tällä hetkellä odotetaan vielä tulevaksi ominaisuutta hallita rooleja Microsoft suojauskeskuksessa ilman menemistä Azuren aktiivihakemistoon. Myöskin roolien kustomointi on tulossa 18. helmikuuta 2021 julkaistun dokumentin mukaan. (Microsoft, 2021) Vastaavaa on mahdollista tehdä Ciscon portaalissa luomalla useita ohjausnäkymiä, joille asetetaan erillisellä Cisco Umbrella for MSSPs tuotteella pääkäyttäjiä ja rajoitetaan pääkäyttäjien näkymät vain tiettyihin näkymiin (Umbrella, 2020.) Check Point mahdollistaa pääkäyttäjien hallinnan ohjelmointirajapinnan kautta käyttäen SmartConsolen graafista käyttöliittymää ja Management rajapintaa. (Check Point, n.d.)

7 Johtopäätökset ja pohdinta

Muutamista eroavaisuuksista huolimatta ratkaisut ovat laajimpia paketteja tarkastellessa hyvin samankaltaisia. Eroja tuli tarkasteltaessa virtualisoinnin hyödyntämistä osana ratkaisuja: käytetäänkö hiekkalaatikkoa tai emulointia osana uhkien tarkistusta. Kaikki ratkaisut hyödyntävät MITRE ATT&CK frameworkia, joka tarjoaa laajan tietopohjan tavatuista haavoittuvuuksista, uhkista ja haitallisten toimijoiden toimintatavoista ja taktiikoista. Tutkittaessa ratkaisuja käyttävien yritysten arvosteluja sivustoilla, kuten esimerkiksi TrustRadius, oli Check Point Harmonyn ja Cisco Umbrellan ratkaisujen palaute pääosin positiivista, pois lukien hinta kaikkien kolmen ratkaisun kohdalla. Microsoft Defender for Endpoint sai samalla sivustolla hieman muita ratkaisuja alhaisempia arvosteluita.

Vain Check Point tarjosi paikallisten resurssien ja siirrettävien medioiden kryptaamista osana päätepisteen suojauksen ratkaisua. Ciscon ratkaisussa kaikki välityspalvelimelle ohjattava liikenne voidaan kryptata. Microsoft mahdollistaa bitlockerin käytön useissa Windows versioissa, joten erillisen endpoint-ratkaisun käyttö kryptaamiseen lienee turhaa. Näkemys kryptaamiseen saattaa olla osoitus tavasta mieltää ja toteuttaa suojausta. Ajatus voi olla, että mikään haitallinen ei tule koskemaan etäpistettä, kun kaikki yhteydet suojataan. Microsoft ilmoittaa mieltävänsä toteutuvan tietoturvauhkan olevan ennemmin ajan kysymys, tämän vuoksi on myös korjaaviin ja palauttaviin työkaluihin panostettu. Tällaisesta ominaisuudesta hyvä esimerkki on Check Point Harmony Endpoint Vault, johon shadow volume siirretään havaittaessa kiristysohjelma.

Selkein huomio haittaohjelmien ja uhkien löytämisessä on metodien painottumisen siirtyminen reaktiivisesta toiminnasta proaktiiviseen etsintään. Enää ei siis vain odoteta, että haitalliseksi tiedetty allekirjoitus skannataan, vaan aktiivisesti käytetään uhkien emulointia ja heuristista analyysia tiedostoja ja verkko-osoitteita tutkittaessa. Jatkuva käyttäytymisen seuranta, prosessien liikenteen seuranta ja käyttäytymisen esto kasvattavat painoarvoaan, perustellusti. Esimerkiksi hiljaisen ja pienehkön prosessin yhtäkkinen muistin, suorittimen tai verkkoyhteyden käytön kasvu voivat kieliä siitä, että kaikki ei ole kunnossa. Useat haitalliset ohjelmat kykenevät sulauttamaan prosessinsa osaksi uhrin järjestelmän prosesseja, tässä käyttäytymisen seuranta on omiaan paljastamaan haittoja. Digitaalisten allekirjoitusten etsiminen ei ole kuitenkaan kadonnut toimenpideluettelosta. Haittaohjelmien ja uhkien määrä vain kasvaa jatkuvasti, eikä kaikkien uhkien allekirjoituksia ole saatu kerätyksi.

Kerätyn materiaalin perusteella Check Point Harmony soveltuu parhaiten tilanteessa, jossa ei vaadita jatkuvaa tiedonsiirtoa yrityksen palvelimen ja etäpisteen välillä. Harmony sisältää kyllä VPN-etäyhteyden muodostuksen, mutta Cisco Umbrella suojaa siirrettävän tiedon tehokkaammin ohjatessaan liikenteen välityspalvelimelle kryptattuna ja jatkuvan tarkkailun alaisena. Cisco Umbrella on myös etäpisteelle hieman kevyempi vaihtoehto, suojaustoimien tapahtuessa pilvipalvelussa. Umbrella on hyvä ratkaisu korkean automatisaation, pilvipohjaisena nimipalvelimena ja palomuurina toimisen vuoksi yritykselle, jolla ei ole varsinaista IT-hallintoa.

Microsoft Defender for Endpoint on parhaimmillaan Windows-ympäristössä, vaikkakin tuki muille käyttöjärjestelmille ja alustoille kasvaa hiljalleen. Defender for Endpoint toimii luotettavasti yhdessä muiden Microsoft-tuotteiden kanssa. Paras hyöty saadaan, kun otetaan CloudApp Security osaksi ratkaisua täydentämään verkkoliikenteen suojausta.

8 Yhteenveto

Tietoturvauhkien määrä ei ota laskeakseen, mikä lisää suojaavien ratkaisuiden tarvetta ja kilpailua. Hyvä esimerkki tästä on työn palautuksen kanssa samalla viikolla, 10.3.2012, Supon (suojelupoliisi) ilmoittama havainto ulkomaisten tiedustelupalveluiden käyttäneen suomalaisten yksityishenkilöiden ja yritysten verkkolaitteita ja palvelimia osana suurempaa kybervakoiluoperaatiota. Supon ilmoituksesta uutisoi muun muassa Iltalehti.

Tutkimuskysymykset levisivät sisällöllisesti suureksi kokonaisuudeksi, jolloin tutkittavien tekniikoiden määrä nousi korkeaksi ja laadullinen panostus laski omasta tavoitteestani. Kaikkia palveluntarjoajien esittelemiä tekniikoita ja palveluita on pyritty avaamaan vähintään parilla lauseella. Kiinnostuneen kannattaa upottaa aikaa tutkimukseen, esimerkiksi etätyöpisteiden suojaamiseksi. Työn aikana tuli kantapään kautta selväksi Check Point Endpoint Agentin muuttuessa Harmonyksi, että ratkaisut ja tarjotut kokonaisuudet muuttuvat ja kehittyvät jatkuvasti. Myöskin mitä suurempi palveluntarjoaja, sitä pirstaleisemmaksi tarjottujen palveluiden kenttä hajoaa.

Kuten työn teoriaosuudesta käy ilmi, on tietoturva vain palanen suurempaa kokonaisuutta, työkalu tiedon tai palvelun suojaamiseksi. Työn painopiste oli tietoturvassa, mutta tietoturvasta vastaava ei saa unohtaa muita turvallisuuden aspekteja, esimerkiksi sosiaalinen manipulaatio (social engineering), jatkuvuuden turvaaminen sekä fyysinen turvallisuus. Hankintaa suunnittelevan tulisi tutustua alansa tietoturvan ja tietosuojan vaatimuksiin, sekä kartoittaa verkkoinfrastruktuurinsa ja selvittää suojattavien etäpisteiden määrä ja laatu, kuten käyttöjärjestelmät ja käytetyt tallennustilat.

Työtä varten suoritin verkkokursseina tietoturvan perusteet -kurssin sekä CISSP-sertifikaattiin valmistavan kurssin. Kurssit antoivat arvokasta näkökulmaa työtä varten, koska tietoturva ei ole pakollisena tietojenkäsittelyn koulutusohjelmassa. Työn aikana opin uutta tietoturvahaavoittuvuuksien etsinnästä, heuristiikasta ja aktiivisesta tarkkailusta. MITRE ATT&CK oli mielenkiintoinen tuttavuus, johon varmasti tulen tulevaisuudessa palaamaan. Tulevia jatkoprojekteja ajatellen olisi hedelmällistä valita tämän työn pohjalta esimerkiksi Check Point Harmony Endpoint ja toteuttaa ratkaisun käyttöönotto sekä tarkastella hallintaa rajatussa ympäristössä.

Lähteet

Ace Cloud Hosting. (2018). What Is VDI And How Does It Work? Haettu 10.3.2021 osoitteesta https://www.acecloudhosting.com/blog/what-is-vdi-how-it-work/

AT&T Cybersecurity. (2020). What is Endpoint Protection? Benefits, Solutions Explained. Haettu 15.2.2021 osoitteesta https://cybersecurity.att.com/blogs/security-essentials/endpoint-protection-explained

Bright Hub. (2009). Information Security Concepts: Authenticity. Haettu 28.1.2021 osoitteesta https://www.brighthub.com/computing/smb-security/articles/31234/

Cisco. (2021). Cisco Umbrella: DNS Security Advantage Package. (Haettu 24.2.2021 osoitteesta https://learn-umbrella.cisco.com/i/1153481-cisco-umbrella-dns-security-advantage-package/0?

Check Point. (2017) Advanced Endpoint Security. Haettu 20.2.2021 osoitteesta https://www.checkpoint.com/downloads/products/endpoint-security-datasheet.pdf

Check Point. (2017). Endpoint Security Anti-malware. Haettu 20.2.2021 osoitteesta https://www.checkpoint.com/downloads/products/ds-endpoint-antimalware.pdf

Check Point. (2021). Endpoint Security. (Haettu 24.2.2021 osoitteesta https://www.checkpoint.com/solutions/endpoint-security/

Check Point. (2020). SandBlast Agent. Haettu 20.2.2021 osoitteesta https://www.checkpoint.com/downloads/products/sandblast-agent-solution-brief.pdf

Check Point. (n.d.). EDR Security - What is Endpoint Detection and Response? Haettu 24.2.2021 osoitteesta https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-endpoint-detection-and-response/

Cisco. (n.d.). Compare Cisco Umbrella's Cloud Security Packages for Your Organization. Haettu 26.2.2021 osoitteesta https://umbrella.cisco.com/products/umbrella-enterprise-security-packages

Cisco. (n.d.). Cisco Umbrella - DNS Security Advantage Package. Haettu 10.2.2021 osoitteesta https://learn-umbrella.cisco.com/datasheets/cisco-umbrella-dns-advantage?utm_content=umb-content-datasheet-cisco-umbrella-dns-advantage

Cisco. (n.d.). Cisco Umbrella Investigate - Investigate Cyber Attacks Like Never Before. Haettu 26.2.2021 osoitteesta https://umbrella.cisco.com/products/umbrella-investigate

Cisco. (n.d.). Compare Cisco Umbrella's Cloud Security Packages for Your Organization. Haettu 10.2.2021 osoitteesta https://umbrella.cisco.com/products/umbrella-enterprise-security-

packages

Cisco. (n.d.). Datasheets - Cisco Umbrella DNS Security Advantage Package. Haettu 10.2.2021 osoitteesta https://learn-umbrella.cisco.com/i/1153481-cisco-umbrella-dns-security-advantage-package/0?

Cisco. (n.d.). Datasheets - Cisco Umbrella Secure Internet Gateway Essentials Package. Haettu 10.2.2021 osoitteesta https://learn-umbrella.cisco.com/i/1153736-cisco-umbrella-secure-internet-gateway-essentials-package/0?

Cisco. (n.d.) What Is Shadow IT? - Haettu 26.2.2021 osoitteesta https://www.cisco.com/c/en/us/products/security/what-is-shadow-it.html

Digital Guardian. (n.d.). What is the MITRE ATT&CK Framework? Haettu 11.3.2021 osoitteesta https://digitalguardian.com/blog/what-mitre-attck-framework FBI. (n.d.). Spoofing and Phishing. Haettu 25.2.2021 osoitteesta https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing

Forcepoint. (n.d.). What is Endpoint Security? Defined, Explained, and Explored. Haettu 10.2.2021. https://www.forcepoint.com/cyber-edu/endpoint-security

Geek-University. (n.d.) Confidentiality, Integrity, and Availability (CIA) triad. Haettu 27.1.2012 osoitteesta https://geek-university.com/ccna-security/confidentiality-integrity-and-availability-cia-triad/

Geek-University. (n.d.) AAA explained. Haettu 27.1.2012 osoitteesta https://geek-university.com/ccna-security/aaa-explained/

Grance T, Stevens M, Myers M. Special Publication 800-36 Guide to Selecting Information Technology Security Products Recommendations of the National Institute of Standards and Technology. Haettu 22.2.2021 osoitteesta https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151284

HelpSystems. (2018). The Six Ws of Granular Access Control. Haettu 27.2.2021 osoitteesta https://www.helpsystems.com/resources/articles/six-ws-granular-access-control

IBM. (n.d.) Authorization and security mechanisms for data access. Haettu 27.1.2021 osoitteesta https://www.ibm.com/support/knowledgecenter/en/SSEPEK_10.0.0/intro/src/tpc/db2z_authandsecurityfordataaccess.html

IBM. (2019). Virtualization. Haettu 22.2.2021 osoitteesta https://www.ibm.com/cloud/learn/virtualization-a-complete-guide

Iltalehti. (2021). Supo: ulkomaiset tiedustelupalvelut käyttävät suomalaisten verkkoreitittimiä.

Haettu 12.3.2021 osoitteesta https://www.iltalehti.fi/tietoturva/a/74c10020-0a6c-4833-bc56-19703bcff576

ISO. (2018). ISO/IEC 27000:2018(en). Haettu 27.1.2021 osoitteesta https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

Järvinen, P (2003). *Salausmenetelmät*. Jyväskylä: Docendo Finland Oy

Kaspersky. (n.d.). What is Heuristic Analysis? Haettu 22.2.2021 osoitteesta https://usa.kaspersky.com/resource-center/definitions/heuristic-analysis

Kyberturvallisuuskeskus. (n.d.) Tietoturva. Haettu 27.1.2021 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

Leijona Security. (2019). Tietoturvaa jonka ansaitset. Haettu 27.1.2012 osoitteesta https://www.leijonasecurity.fi/2019/07/26/tietoturva/

Microsoft. (2021). Integrate Microsoft Defender for Endpoint with other Microsoft solutions. Haettu 3.3.2021 osoitteesta https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/threat-protection-integration

Microsoft. (2021). Microsoft 365 Defender. Haettu 3.3.2021 osoitteesta https://docs.microsoft.com/en-us/microsoft-365/security/mtp/microsoft-threat-protection?view=o365-worldwide

Microsoft. (2021). Microsoft 365 Education - Service Descriptions. Haettu 6.3.2021 osoitteesta https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/microsoft-365-education

Microsoft. (n.d.). Microsoft Cloud App Security documentation. Haettu 3.3.2021 osoitteesta https://docs.microsoft.com/en-us/cloud-app-security/

Microsoft. (2021). Microsoft Defender for Endpoint. Haettu 3.3.2021 osoitteesta https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-advanced-threat-protection

Microsoft. (2021). Microsoft Defender for Endpoint data storage and privacy. Haettu 7.3.2021 osoitteesta https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/data-storage-privacy

Microsoft. (2021). Microsoft Secure Score for Devices. Haettu 3.3.2021 osoitteesta https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/tvm-microsoft-secure-score-devices

Microsoft. (2021). Microsoft Threat Experts. Haettu 3.3.2021 osoitteesta

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-threat-experts

Microsoft. (2020). Next-generation protection in Windows 10, Windows Server 2016, and Windows Server 2019. Haettu 3.3.2021 osoitteesta https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/microsoft-defender-antivirus-in-windows-10

Microsoft. (2021). Overview of attack surface reduction. Haettu 3.3.2021 osoitteesta https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/overview-attack-surface-reduction

Microsoft. (2021). Overview of endpoint detection and response capabilities. Haettu 3.3.2021 osoitteesta https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/overview-endpoint-detection-response

Microsoft. (2021). Overview of management and APIs. Haettu 3.3.2021 osoitteesta https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/management-apis

Microsoft. (2021). Permissions in the Microsoft 365 security and compliance centers. Haettu 11.3.2021 https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-microsoft-365-compliance-security?view=o365-worldwide

Microsoft. (2018). Remote Desktop Protocol. Haettu 10.2.2021 osoitteesta https://docs.microsoft.com/fi-fi/windows/win32/termserv/remote-desktop-protocol?redirectedfrom=MSDN

Microsoft. (2021). Threat and vulnerability management. Microsoft Docs. Haettu 3.3.2021 osoitteesta https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/next-gen-threat-and-vuln-mgt

Microsoft. (2021). Use automated investigations to investigate and remediate threats. Haettu 3.3.2021 osoitteesta https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/automated-investigations

Microsoft. (2021). What is Cloud App Security? Haettu 3.3.2021 osoitteesta https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security

Nextiva (n.d.). Telecommuting Technology: The Essentials for Remote Work. Haettu 10.3.2021 osoitteesta https://www.nextiva.com/blog/telecommuting-technology.html#tools

Norton. (2019). Zero-day vulnerability: What it is, and how it works. Haettu 25.2.2021 osoitteesta

https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html

Obiora Nweke L. PM World Journal Using the CIA and AAA Models to Explain Cybersecurity Activities Www.Pmworldjournal.Net Commentary by Livinus Obiora Nweke Using the CIA and AAA Models to Explain Cybersecurity Activities. Vol VI.; 2017. Accessed January 27, 2021. www.pmworldlibrary.net

OSI-malli. (n.d.). Haettu 27.2.2021 osoitteesta https://www.cs.tut.fi/etaopetus/titepk/luku19/OSI.html

Palo Alto Networks. (n.d.). What Is a Site-to-Site VPN? Haettu 2.2.2021 osoitteesta https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn

Palo Alto Networks. (n.d.). How to secure your remote workforce: The critical role of a secure VPN. Haettu 8.2.2021 osoitteesta https://www.paloaltonetworks.com/cyberpedia/how-to-secure-your-remote-workforce

PCMag. (2020). The Best Ransomware Protection for 2021. Haettu 23.2.2021 osoitteesta https://uk.pcmag.com/ransomware-protection/89011/the-best-ransomware-protection-for-2020

Pender-Bey G. (n.d.) *THE PARKERIAN HEXAD The CIA Triad Model Expanded*. Information Security Program. Lewis University. Haettu 12.1.2021 osoitteesta https://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf

Personaldatasecurity (n.d.). Volume Shadow Copy Service – mikä se on. Haettu 25.2.2021 osoitteesta https://personaldatasecurity.wordpress.com/volume-shadow-copy-service/

Päivärinta, E. (2020). *Tietoturvan riskitason määrittäminen Android-laitteissa sovellusten ohjelmointirajapintaa käyttäen.* Diplomityö. Tietotekniikan tutkimusohjelma. Oulun yliopisto. Haettu 27.1.2021. osoitteesta http://jultika.oulu.fi/files/nbnfioulu-202003171271.pdf

Sanasto K. SANASTOKESKUS TSK TERMINOLOGICENTRALEN TSK. Haettu 27.1.2021 osoitteesta https://www.huoltovarmuuskeskus.fi/

Sharma, T & Yadav, R. (2015). Security in Virtual private network. *International Journal of Innovations & Advancement in Computer Science* 4/2015. Haettu 2.2.2021 osoitteesta https://www.academicscience.co.in/admin/resources/project/paper/f201503111426090873.pdf

StaffHost Europe. (n.d.) Cybersecurity and the Parkerian Hexad. Haettu 27.1.2012 osoitteesta https://www.staffhosteurope.com/blog/2019/03/cybersecurity-and-the-parkerian-hexad

Techopedia. (n.d..) What is Emulation? Haettu 22.2.2021 osoitteesta https://www.techopedia.com/definition/4787/emulation

TechRadar. (2020). Remote access VPN: what are they, how do they work and which are the best. Haettu 10.3.2021 osoitteesta https://www.techradar.com/vpn/remote-access-vpn

The OSI-Model. (n.d.). Network Layer 3. Haettu 27.2.2021 osoitteesta https://osi-model.com/network-layer/

Tietoturvariskien arviointi. (n.d.) Tietoturvariskit ja niiden arviointi. Haettu 28.1.2021 osoittesta https://www.tietoturvariskienarviointi.fi/

Tietosuojavaltuutetun toimisto. (n.d.) Mitä tietosuoja on? - Haettu 27.1.2021. https://tietosuoja.fi/tietosuoja

Tietoturvatapahtuma. (n.d.) Mitä on kyberturvallisuus? Lue vastaukset usein kysyttyihin kysymyksiin. Haettu 27.1.2021 osoitteesta http://www.tietoturvatapahtuma.fi/kyberturvallisuus/mita-on-kyberturvallisuus-lue-vastaukset-usein-kysyttyihin-kysymyksiin/

Tivi. (2016). Varjo-IT on myrkkyä digitalisaatiolle. Haettu 26.2.2021 osoitteesta https://www.tivi.fi/kumppaniblogit/salesforce/varjo-it-on-myrkkya-digitalisaatiolle/623e32d9-fa6f-3c0e-ab03-b7f4cca0d041

Visma. (2019). Tietosuoja vai tietoturva? Haettu 27.1.2012 osoitteesta https://www.visma.fi/blog/tietosuoja-tietoturva/

VPNyhteys. (2021). VPN-yhteys: Mikä on VPN, hyödyt ja arvostelut. Haettu 10.3.2021 osoitteesta https://www.vpnyhteys.fi/

Webroot. (n.d). Endpoint Protection & Business Antivirus Solutions. Haettu 9.3.2021 osoitteesta https://www.webroot.com/us/en/business/smb/endpoint-protection

Liite 1: Aineistonhallintasuunnitelma

Tutkimuksellinen työ:

Työtä varten ei tehdä haastatteluja tai kyselyitä.

Työstä pidetään vähintään kolmea kappaletta ajantasaista versiota. Versiot ovat omalla tietokoneellani C: -asemalla, usb-tikulla sekä Teams-kansiossa. Paikalliset kopiot ajetaan automaattisesti Poweshell-skriptillä sekä wordin varmuuskopio-ominaisuutta hyödyntäen. Työskentelyn päätteeksi Teams-versio päivitetään.

Luovutan opinnäytetyön tulokset tilaajalle Hämeen ammattikorkeakoululle, Tietohallinnolle.

Käytetyt kuvat on varmistettu CC0 -oikeudelle.

Tutkimusaineistoa ei luovuteta eteenpäin.

Aineistoa ei ole tarpeen säilyttää, kaikki aineisto on julkisesti saatavilla lähdeluettelon mukaisesti.