Jarkko Ruottinen

HAAVOITTUVUUKSIEN HALLINTA-PROSESSI JA -JÄRJESTELMÄ KOHDEYRITYKSESSÄ

Opinnäytetyö

Insinööri (ylempi AMK)

Kyberturvallisuuden koulutus

2023

Kaakkois-Suomen ammattikorkeakoulu

South-Eastern Finland University of Applied Sciences

Tutkintonimike	Insinööri (ylempi AMK)
Tekijä/Tekijät	Jarkko Ruottinen
Työn nimi	Haavoittuvuuksien hallintaprosessi ja -järjestelmä kohdeyrityksessä
Toimeksiantaja	Kotimainen ICT-yritys
Vuosi	2023
Sivut	133 sivua, liitteitä 7 sivua
Työn ohjaaja(t)	Vesa Kankare

TIIVISTELMÄ

Yritysten laaja verkottuminen, etätöiden ja pilvipalveluiden lisääntynyt käyttö on lisännyt entisestään yritysten tietoturvan merkitystä. Tämä opinnäytetyö käsittelee kohdeyrityksen haavoittuvuuksien hallintaprosessin ja skannausjärjestelmän tutkimista ja edelleen kehittämistä. Tutkimusongelmana oli haavoittuvuuksien hallintaprosessin keskeneräinen toteutus. Tavoitteena oli päivittää toimeksiantajan haavoittuvuuksien hallintaprosessi, lisätä ohjeistuksia ja selkeyttää prosessivaiheet. Haavoittuvuuksien skannausjärjestelmän osalta tavoitteena oli opinnäytetyön aikana lisätä vähintään yksi uusi verkkosegmentti skannauksen piiriin ja selvittää varmuuskopioinnin hallinta.

Tutkimuksen tutkimuskysymykset liittyivät haavoittuvuuksien hallintaprosessin osalta prosessin kehittämiseen, haavoittuvuustikettien ja nollapäivähaavoittuvuustilanteen käsittelyyn. Lisäksi pyrittiin löytämään keinoja sille, kuinka voisi pienentää löydettyjen väärien positiivisten haavoittuvuuksien määrää. Tutkimuskysymysten ja kehittämisaiheiden yhteinen päämäärä oli saada organisaation haavoittuvuuksien hallintaprosessi paremmaksi.

Tässä opinnäytetyössä tutkittiin todellista tilannetta yrityksessä ja pyrittiin kehittämään sitä paremmaksi, ja siksi tutkimusmenetelmäksi oli valittu toimintatutkimus. Tutkimus oli myös empiiristä tutkimusta, koska sen teon vaiheet sopivat tähän tutkimukseen. Tutkimuksen primäärisinä tiedonkeruumenetelminä käytettiin teemahaastattelua, kyselylomaketta, havainnointia ja testaamista. Haastatteluihin valittiin mukaan alan asiantuntijoita. Tutkimustulosten ja organisaation tilanteen analysointiin käytettiin sisällön- ja tilanneanalyysia.

Kaikkiin tutkimuskysymyksiin löydettiin vastaukset. Haavoittuvuuksien hallintaprosessista saatiin työn aikana tuloksena yhtenäinen kokonaisuus, jonka toimintoja kuvattiin työssä. Haavoittuvuusskanneriin liitettiin suunnitellusti yksi iso verkkoalue lisää, ja haavoittuvuusskannerin dokumentointia kehitettiin työn aikana. Haavoittuvuuksien seurantaan määritelty KPI-mittari osoitti tutkimuksen loppuvaiheessa, että prosessi toimi oikein ja haavoittuvuusskannausta on syytä tehdä säännöllisesti.

Asiasanat: haavoittuvuuksien hallintaprosessi, haavoittuvuusskanneri, kyberturvallisuus, Outpost24, toimintatutkimus

South-Eastern Finland University of Applied Sciences

Degree title	Master of Engineering
Author	Jarkko Ruottinen
Thesis title	Vulnerability management process and system at company
Commissioned by	Domestic ICT company
Time	2023
Pages	133 pages, 7 pages of appendices
Supervisor	Vesa Kankare

ABSTRACT

The extensive networking of companies, the increased use of remote work and cloud services has further increased the importance of companies' information security. This thesis deals with the research and further development of the target company's vulnerability management process and scanning system. The research problem of the thesis was the unfinished implementation of the vulnerability management process. The goal was to update the organization's vulnerability management process and clarify the principles of functional escalation and clarify the process steps. A parallel issue with the partial was also the lack of documentation for the vulnerability scanner. Regarding the vulnerability scanner system, the goal during the thesis was to add at least one new network segment to the scope of scanning and to find out how to manage the backup.

The research questions of the study were related to the development of the vulnerability management process, the handling of vulnerability tags and the zero-day vulnerability situation. In addition, efforts were made to find ways to reduce the number of false positive vulnerabilities found. The common goal of the research questions and development topics was to improve the organization's vulnerability management process.

In this thesis, the real situation in the company was investigated and an effort was made to develop it better, and that is why the selected research method was action research. The study was also an empirical study. Theme challenges, a questionnaire, observation, and testing were used as the primary data collection methods of the study. Experts related to the operation of the vulnerability process were selected for the interviews. Content and situation analysis was used to analyze the research results and the organization's situation.

All research questions were answered. The vulnerability management process was completed, and its functions were described in the work. One more large network area was connected to the vulnerability scanner as planned, and the documentation of the vulnerability scanner was developed during the work. The KPI metric defined for monitoring vulnerabilities showed at the end of the study that the process worked correctly, and that vulnerability scanning should be done regularly.

Keywords: vulnerability management process, thesis, cyber risk management, Outpost24, research

SISÄLLYS

1 JOHDANTO 10

1.1 Opinnäytetyön aiheen kuvaus 10

1.2 Kohdeorganisaation kuvaus ja lähtökohta toimeksiannolle 11

1.3 Opinnäytetyön tavoitteet ja rajaus 11

1.4 Aikaisemmat tutkimukset 12

1.5 Opinnäytetyön luottamuksellisuus ja eettiset kysymykset 14

2 OPINNÄYTETYÖN TOTEUTUS 14

2.1 Tutkimusmenetelmä, -ongelma ja -kysymykset 15

2.2 Tiedonkeruumenetelmät 21

2.3 Analysointimenetelmät 22

2.4 Teoreettinen viitekehys ja tutkimusmenetelmät 23

2.5 Keskeiset käsitteet 23

2.6 Kirjallisuuskatsaus ja tärkeimmät lähteet 24

2.7 Resursointi 26

3 TEOREETTINEN VIITEKEHYS 27

3.1 Yrityksen turvallisuusperiaatteiden merkitys 27

3.2 Haavoittuvuuksien hallintaprosessi 28

3.3 Haavoittuvuuksien hallinnan viitekehykset ja ohjeistukset 29

3.3.1 SFS ISO/IEC-standardit 30

3.3.2 NIST Special Publication 800-53 Revision 5 36

3.3.3 CIS Critical Security Controls Version 8 37

3.3.4 OVMG - OWASP Vulnerability Management Guide 38

3.4 KPI-mittari tavoitteiden seurannassa 39

3.5 Haavoittuvuuksiin liittyvät käsitteet 40

3.6 Haavoittuvuuksien skannausjärjestelmät 44

3.7 Kohdeorganisaation käyttämä haavoittuvuusskanneri 54

4 AINEISTON KERUU JA TUTKIMUSRAPORTTI 56

4.1 Tiedonkeräys teemahaastattelun ja kenttäpäiväkirjan avulla 56
4.2 Havainnoinnit 58
4.3 Teema 1 - Millä tavalla yrityksen sisäistä haavoittuvuuksien hallintaprosessia kannattaisi kehittää paremmaksi? 58
4.4 Teema 2 - Haavoittuvuustikettien käsittelyn parannusideat? 61
4.5 Teema 3 - Kuinka täytyisi reagoida nollapäivähaavoittuvuuksiin? 62
4.6 Teema 4 - Kuinka voidaan pienentää haavoittuvuusskannerin löytämien väärien positiivisten määrää? 63
4.7 Haavoittuvuuksien hallintaprosessit 68
4.7.1 PwC:n haavoittuvuuksien hallinta 68
4.7.2 Taniumin korjausprosessi 70
4.7.3 Hafkampin tutkimus 73
4.7.4 Liaisonin tietoturvapäivitysprosessi 75
5 AINEISTON ANALYSOINTI 76
6 HAAVOITTUVUUKSIEN HALLINTAPROSESSIN TOTEUTUS 78
6.1 RACI 82
6.2 KPI-mittari 83
6.3 SOC-palvelun kuvaus kohdeorganisaatiossa 85
6.4 Yleinen ohjeistus organisaation haavoittuvuustikettien luontiin 86
6.5 SOC:n toimintaohjeistus haavoittuvuustikettien käsittelyyn 87
7 HAAVOITTUVUUSSKANNERIIN LIITTYVÄ TOTEUTUS 88
7.1 Yrityksen omien järjestelmien seuranta skannerilla 88
7.2 Uuden verkkosegmentin lisääminen skannaukseen 89
7.3 Outpost24 HIAB:n varmuuskopiointi 90
7.4 Outpost24 HIAB:n varmuuskopioinnin palautus 93
8 TUTKIMUSTULOKSET JA TULOSTEN ANALYSOINTI 94
8.1 Millä tavalla yrityksen sisäistä haavoittuvuuksien hallintaprosessia kannattaisi kehittää paremmaksi? 94
8.2 Haavoittuvuustikettien käsittelyn parannuskeinot? 98

8.3 Kuinka täytyisi reagoida nollapäivän haavoittuvuuksiin? 99

8.4 Kuinka voidaan pienentää haavoittuvuusskannerin löytämien väärien positiivisten määrää? 101

8.5 Kehityskohteiden tulosten analysointi 103

9 JOHTOPÄÄTÖKSET 104

10 POHDINTA JA REFLEKTOINTI 106

10.1 Tutkimuksen luotettavuus ja hyödynnettävyys 108

10.2 Jatkotutkimusmahdollisuudet 111

LÄHTEET 113

KUVALUETTELO

LIITTEET

Liite 1. Kyselyn ja teemahaastattelun alustus

Liite 2. Teemahaastattelun kyselypohja

Liite 3. Lähetettävä kyselypohja

Liite 4. Teemahaastatteluihin liittyvä kenttäpäiväkirja

Liite 5. RACI-matriisiesimerkki rooleille ja vastuille (PwC 2022, 12)

LYHENTEET JA TERMIT

CERT	Computer Emergency Response Team. Tietoturvaloukkausten ennaltaehkäisyyn ja torjuntaan keskittyvä tiimi.
CIA-malli	Tietoturvallisuuden käsitemalli, joka perustuu luottamuksellisuuteen, eheyteen ja saatavuuteen.
CM	Change Management. Muutostenhallinta.
CVE	Common Vulnerabilities and Exposures. Tietoturvahaavoittuvuuksien hallintajärjestelmä.
CWE	Common Weakness Enumeration. Haavoittuvuuksien luokittelujärjestelmä.
CVSS	Common Vulnerability Scoring System. Tietoturvahaavoittuvuuksien vakavuuksien pisteytysjärjestelmä.
CMDB	Configuration Management Database. Konfigurointien hallinnointitietokanta.
DNS	Domain Name System. Nimipalvelujärjestelmä.
DoS	Denial of Service. Palvelunestohyökkäys.
ENISA	European Union Agency for Cybersecurity. Euroopan unionin verkko- ja tietoturvaviranomainen.
FIRST	Forum of Incident Response and Security Teams. Kansainvälinen tietoturvatiimien järjestö.
FTP	File Transfer Protocol. Tiedonsiirtoprotokolla.
HTTP	Hypertext Transfer Protocol. Tiedonsiirtomenetelmä.
IDM	Identity Management. Identiteetin ja pääsynhallinnan hallintajärjestelmä.
ICMP	Internet Control Message Protocol. Tietoliikenteen kontrolliprotokolla.
IP	Internet Protocol. IP-osoite on yksilöivä osoite, jonka perusteella laite tunnistetaan internetissä tai paikallisessa verkossa.
ISMS	Information Security Management System. Tietoturvallisuuden hallintajärjestelmä.
ISO	International Organization for Standardization. Kansainvälinen standardisoimisjärjestö.
ITOC	Information Technology Operations Center. Ryhmä, joka valvoo yrityksen IT-järjestelmiä ja palveluita reaaliaikaisesti.
KPI	Key Performance indicator. Suorituskykyindikaattorit (KPI) tarjoavat arvokkaita oivalluksia, jotka osoittavat tietoturvan hallinnan onnistumisen ja auttavat tekemään tärkeitä päätöksiä organisaation kyberturvallisuusstrategian parantamiseksi.
MFA	Multi-Factor Authentication. Monivaiheinen tunnistautuminen.
MIM	Major Incident Management. Laajavaikutteisten häiriöiden hallinta.
MOD	Manager On Duty. Päivystävä johtaja.

NCSC	National Cyber Security Centre. Britannian kyberturvallisuuskeskus.
NIST	National Institute of Standards and Technology. Yhdysvaltalainen standardivirasto.
NMAP	Porttiskannerikomento tai -ohjelma.
Outpost24	Ruotsalainen kaupallinen pilvipohjainen haavoittuvuusskanneriohjelmisto.
Pulsar	Pulsar on tuotannon työnohjausjärjestelmä, jossa tiketöinnin lisäksi sijaitsee muun muassa laitekanta, lista palveluista, sekä tuotannon dokumentaatiota.
RCA	Root Cause Analysis. Prosessi, jossa tunnistetaan tapahtumaan johtaneet juurisyyt, ja pyritään estämään vastaavanlaiset tapahtumat.
RACI	Responsible, Accountable, Consulted and Informed matrix. Tapa varmistaa, että kaikki ymmärtävät roolit ja vastuut, on käyttää vastuullista, konsultoitua ja tietoista RACI-matriisia. RACI-matriisi on yleinen tapa toteuttaa päätösoikeuskehys, joka selventää avainprosessien rooleja ja vastuita.
SI	Security Incident. Tietoturvatapahtuma.
SO	System Owner. Järjestelmäomistaja.
SOC	Security Operation Center. Tietoturvanhallintakeskus. Keskitetty toiminto organisaatiossa, joka valvoo ja analysoi seurannassa olevalla alueella tapahtuvia kyberturvallisuushäiriöitä.
Sec Tech-tiimi	Security Technology on tiimi, joka toimii SOC:n teknisenä järjestelmätukena. Se asentaa, muokkaa ja kehittää SOC:n käytössä olevia tietoturvajärjestelmiä.
SIEM	Security Information and Event Management. Tietoturvatiedon havannointijärjestelmä.
SIM	Security Information Management. Tietoturvatietojen hallinta (SIM) on käytäntö, jossa kerätään, seurataan ja analysoidaan tietoturvaan liittyviä tietoja tietokoneen lokeista ja useista muista tietolähteistä.
SIRT	Security Incident Response Team. Tietoturvatapahtumiin reagoiva ryhmä.
SMTP	Simple Mail Transfer Protocol. Sähköpostiprotokolla.
SOAR	Security Orchestration, Automation and Response. Ohjelmisto, jolla voi automatisoida ennalta määrättyjä työnkulkuja. SAR toimii usein SIEM:n apuna. Vähentää tietoturvaresurssien kuormitusta.
SSH	Secure Shell Protocol. Salatun tietoliikenteen protokolla.
TCP	Transmission Control Protocol. TCP on tietoliikenneprotokolla tietokoneiden väliseen luotettavaan tiedonsiirtoon.
TRIAGE-vaihe	Triage on lähestymistapa, jota käytetään kyberhäiriöiden reagoinnissa verkkohälytysten tutkimiseen. Triage auttaa tutkimaan verkon päätepisteitä keräämällä tietoja sekä analysoimalla sen perusteella haittaohjelmia ja epäilyttävää toimintaa.

TSAO	Technical system area owner. Tekninen järjestelmäalueen omistaja
UDP	User Datagram Protocol. UDP on yhteydetön tietoliikenneprotokolla, joka ei vaadi yhteyttä laitteiden välille, mutta se mahdollistaa tiedonsiirron.
VPR	Vulnerability Priority Rating. Tenablen käyttämä tietoturvahaavoittuvuuksien vakavuuksien pisteytysjärjestelmä.

1 JOHDANTO

1.1 Opinnäytetyön aiheen kuvaus

Yritysten laaja verkottuminen, etätöiden ja pilvipalveluiden lisääntynyt käyttö on lisännyt entisestään yritysten IT-ympäristön haasteita (Nuojua 2021). Hyökkäyspinta-ala on laajentunut ja hyökkääjillä on entistä enemmän kohteita, ja järjestelmien ylläpitäjillä on vastaavasti enemmän suojattavaa. Kyberympäristön uhkataso on kohonnut myös viime aikoina kansainvälisen turvallisuustilanteen ja lisääntyneen verkkorikollisuuden takia. (Traficom 2022.)

Vuoden 2022 aikana on tullut esille muun muassa yhdeksän nollapäivähaavoittuvuutta pelkästään Chrome-selaimessa, joka osoittaa, että sovellutuksista löytyy edelleen merkittäviä haavoittuvuuksia (Spiceworks 2022). Vuonna 2022 ovat Suomessa lukuisat yritykset, kuten Osuuspankki, Savonia AMK, eduskunta, Valtra, STT, S-pankki, YLE Areena, Keuda, Uponor ja KELA, olleet kyberhyökkäyksen kohteena (Rousku 2022). Edellä mainitut asiat ovat esimerkkiä sille, miksi yritysten on syytä panostaa riskienhallintaprosesseihin ja näin vähentää epävarmuutta organisaation tavoitteiden toteutumisesta. Mikä tahansa riski voi realisoitua. Riski voi olla tiedostettu tai tiedostamaton riski, mutta täytyy varautua pahimpaan (Rousku 2022). Suunnitelmilla ja prosesseilla voidaan varautua paremmin riskitilanteisiin. Tämän opinnäytetyön aiheena oleva haavoittuvuuksien hallintaprosessi on tärkeä osa-alue organisaation tietoturvallisuuden hallinnassa.

Haavoittuvuuksien hallintaprosessi on jatkuva prosessi, jonka avulla voidaan ennakoida, tunnistaa, arvioida, priorisoida ja korjata tietokonejärjestelmien, verkon ja ohjelmistojen haavoittuvuuksia. Tämä prosessi on tärkeä osa yritysten ja organisaatioiden kyberturvallisuuden hallintaa, koska se auttaa varmistamaan, että järjestelmät ja ohjelmistot ovat turvallisia ja suojattuja haitallisilta hyökkäyksiltä. Haavoittuvuuksien hallintaprosessi voidaan jakaa useisiin eri vaiheisiin, kuten haavoittuvuuksien tunnistamiseen, arviointiin, priorisoimiseen ja korjaamiseen. Näiden vaiheiden avulla voidaan varmistaa, että haavoittuvuudet tunnistetaan ja pyritään korjaamaan niiden vakavuuksien perusteella mahdollisimman nopeasti ja tehokkaasti. (Microsoft 2022.)

Haavoittuvuusskanneri on tehokas työkalu, jolla voi löytää yrityksen tietojärjestelmissä ja laitteissa olevia haavoittuvuuksia. Skannerilla on mahdollista skannata organisaation verkkoa sekä ulkoapäin että sisäpuolella, ja lisäksi yksityiskohtaisemmin palvelimia, sovelluksia ja käyttöjärjestelmää sisältäpäin (Mint-Security 2019). Haavoittuvuuksien varhainen löytäminen ja korjaaminen auttaa ennaltaehkäisemään tehokkaasti mahdollisia hyökkäyksiä. Haavoittuvuusskannaus mahdollistaa suunnitelmallisen prosessin verkkoalueiden ja infrastruktuurin haavoittuvuushallintaan, ja siksi se on otettu tähän opinnäytetyöhön mukaan tukemaan haavoittuvuuksien hallintaprosessin toimintaa ja kuvausta.

1.2 Kohdeorganisaation kuvaus ja lähtökohta toimeksiannolle

Opinnäytetyön toimeksiantaja on tietoliikenneyritys, joka tarjoaa ICT-palveluita korkealla tietoturvalla ulkoisille asiakkaille ja hyödyntää haavoittuvuuksien hallintajärjestelmiä myös omassa organisaatiossaan. Olin aloittanut työurani kohdeyrityksen tietoturvatiimissä kesäkuussa 2022.

Toimeksiantaja halusi kehittää opinnäytetyön avulla yrityksen omaa haavoittuvuuksien hallintaprosessia ja laajentaa haavoittuvuuksien skannausjärjestelmäksi valitun Outpost24-ohjelmiston käyttöä. Hallintaprosessi oli jo kuvattu ylätasolla, mutta siihen kaivattiin täydennystä, kehittämistä ja parempaa dokumentointia.

Toimeksiantajan nykyinen haavoittuvuuksien skannausjärjestelmä oli otettu käyttöön vuoden 2021 lopussa yhdellä verkkoalueella, mutta sitä oli tarkoitus laajentaa muillekin verkkoalueille. Samalla oli tarkoitus ottaa laajemmin sen ominaisuuksia käyttöön ja tehdä dokumentointia ylläpitäjille ja järjestelmäomistajille, jotta he voivat käydä itse tutkimassa skannaustuloksia ja luoda raportit omasta vastuualueestaan.

1.3 Opinnäytetyön tavoitteet ja rajaus

Opinnäytetyön tarkoituksena oli päivittää toimeksiantajan haavoittuvuuksien hallintaprosessi kuvaamalla ja täsmentämällä toiminnallisen eskalaation periaatteet ja työohjeet. Tavoitteena oli luoda selkeät prosessivaiheet, jonka lopputuloksena luodaan myös prosessin jonkin osa-alueen tehokkuutta kuvaava

KPI-mittari (Key Performance Indicator). KPI edustaa yleensä joukkoa toimenpiteitä, jotka keskittyvät niihin organisaation suorituskyvyn näkökohtiin, jotka ovat kriittisimmät organisaation nykyiselle ja tulevalle menestykselle (Parmenter 2010).

Kokonaistavoitteena oli parantaa organisaation tietoturvaa ja tehostaa toimintaa erityisesti kriittisten haavoittuvuustilanteiden suhteen. Näin yritys välttää mahdollisten tietoturvaloukkausten takia syntyviä mainehaittoja ja taloudellisia menetyksiä. Muut prosessit, kuten esimerkiksi muutoksenhallinta, ongelmanhallinta ja tietoturvahäiriöiden hallinta, on rajattu pois tästä työstä. Haavoittuvuuksien tutkimisessa keskitytään tutkimuksessa vain sisäiseen verkkoympäristöön ja siinä oleviin palvelimiin.

Haavoittuvuusskannerin laajentamisen tavoitteena oli opinnäytetyön aikana lisätä vähintään yksi verkkoaluekokonaisuus skannauksen piiriin ja tehdä sisäistä ohjeistusta järjestelmäomistajille ja ylläpitäjille sekä löytää vastauksia tutkimuskysymyksiin. Tarkoitus oli myös tuoda esille haavoittuvuusskannerin merkitys haavoittuvuuksien hallintaprosessissa. Haavoittuvuusskannereiden tarkempi käsittely rajataan Outpost24:een, johon organisaatiossa panostetaan lähitulevaisuudessa eniten.

Opinnäytetyön tuloksia tullaan hyödyntämään mahdollisimman nopeasti, jos ne todetaan käyttökelpoiseksi sisäisessä katselmoinnissa. Työ oli ajankohtainen ja tarpeen myös siksi, että yrityksen sisäiset verkot ja palvelut olivat muutosvaiheessa ja oli olemassa haavoittuvuusriski sekä uusissa että myös vanhemmissa hieman huomiotta jääneissä kohteissa. Mahdollisesti lopputyötä voidaan hyödyntää muissakin vastaavissa yrityksissä. Tämä tutkimustyön tarkoituksena oli myös edistää kehittymistäni organisaation työntekijänä, nopeuttaa tutustumista tärkeimpiin sidosryhmiin ja antaa hyvät jatkomahdollisuudet toimia teknisenä vastuuhenkilönä työssä kuvatun järjestelmän parissa.

1.4 Aikaisemmat tutkimukset

Aiemmat vastaavanlaiset opinnäytetyöt ja tutkimukset pyrittiin kartoittamaan Google Scholarin, Kaakkurin ja hakukoneiden avulla. Täysin vastaavalla ta-

valla käsiteltyjä töitä ei löytynyt, mutta joitakin opinnäytetöitä löytyi, joissa tutkittiin tai vertailtiin samoja osa-alueita. Joissakin töissä käsiteltiin haavoittuvuuksien hallintaprosessia ja osassa haavoittuvuusskannereita yleisellä tasolla. Haavoittuvuusskannereita tutkivissa töissä keskityttiin lähinnä haavoittuvuusskannauksiin tai verkkosovellutuksien skannauksiin. Tarkempia kuvauksia yritysten haavoittuvuuksien hallintaprosesseista ei löytynyt. Tämän työn tutkimusraporttia käsittelevässä luvussa mainitaan muutamia tutkimuksia, joista saatavaa tietoa hyödynnettiin jonkin verran tässä tutkimuksessa.

Tiina Nikumaan vuonna 2022 tekemä opinnäytetyö ”Vulnerability Management Process” käsittelee yleisesti haavoittuvuuksien hallintaprosesseja. Anssi Ylätalon (2019) opinnäytetyö ”Development of process and tools for vulnerability management” on samaan aiheeseen liittyvä tutkimus myös prosessin kehittämisen näkökulmasta. Tämän työn tutkiminen jäi tutkijalla avain oman tutkimuksen loppuvaiheeseen. Ylätalon työssä ja tässä tutkimuksessa käsitellään paljon samoja asioita, mutta tutkimuskysymykset ovat erilaisia ja aihealueet käsitellään melko eri tavoin.

Juho Salmen (2021) diplomityö käsittelee haavoittuvuusskannauksia osana organisaation tietoturvallisuuden kehittämistä. Salmen työ tutki yleisellä tasolla haavoittuvuusskannauksia ja tietoturvaa, eikä käsitellyt haavoittuvuuden hallintaprosesseja. Skannereista tarkempaan käsittelyyn oli otettu Nessus Professional, joten se antoi hyvän vertailukohdan omassa tutkimuksessa käytetylle eri tuotteelle.

Pro gradu -tutkielma ”Verkkosovelluksen haavoittuvuustestaus” käsittelee tutkimuskysymyksenä verkkosovellusten haavoittuvuuksien testaamista ja tietoturvallisuuden parantamista niiltä osin (Salminen 2020). Omassa työssäni verkkosovellusten skannaukset rajataan kokonaan pois. Kuitenkin tämä työ tuo esille joitakin asioita, jotka toimivat myös muidenkin haavoittuvuuskohteiden kanssa.

AMK-opinnäytetyö ”Tietoturvatapahtumien hallinta – Operaattoritoiminta JYVSECTEC-projektissa” oli kehittämisprojekti, jossa suunniteltiin tietoturvatapahtumien hallintaprosessi, tikettijärjestelmä ja dokumentaatio operaattoritoi-

mintaa varten (Viinikainen 2014). Viinikaisen työ käsittelee osittain samaa aihetta, mutta se eroaa tästä työstä muun muassa erilaisten organisaatio- ja prosessirakenteiden takia.

1.5 Opinnäytetyön luottamuksellisuus ja eettiset kysymykset

Eettisesti hyvä tutkimus edellyttää, että tutkimuksen teossa noudatetaan hyvää tieteellistä käytäntöä (Hirsjärvi ym. 2009, 23.) Ennen opinnäytetyön aloitusta perehdyttiin hyvän tieteellisen käytännön, tutkimusetiikan ja eettisen ennakkoarvioinnin ohjeistuksiin (TENK 2023).

Tämän opinnäytetyön tulosten julkaisemiseen ja luottamuksellisuuteen liittyvät sopimusehdot oli ohjeistettu allekirjoitetussa sopimuksessa. Työnantajan määrittämiä salassa pidettäviä asioita ei julkaista opinnäytetyössä. Toimeksiantajan työnohjaaja tarkisti tutkimuksen julkaistavan raportin. Tähän opinnäytetyöhön ei tarvinnut erillistä eettistä lupaa, koska tutkittavana ei ollut suoranaisesti ihmiset. Haastateltavilta kysyttiin ennakkoon lupa, heille selvitettiin haastattelun syy ja he ovat nähneet ennen haastattelua kysymykset.

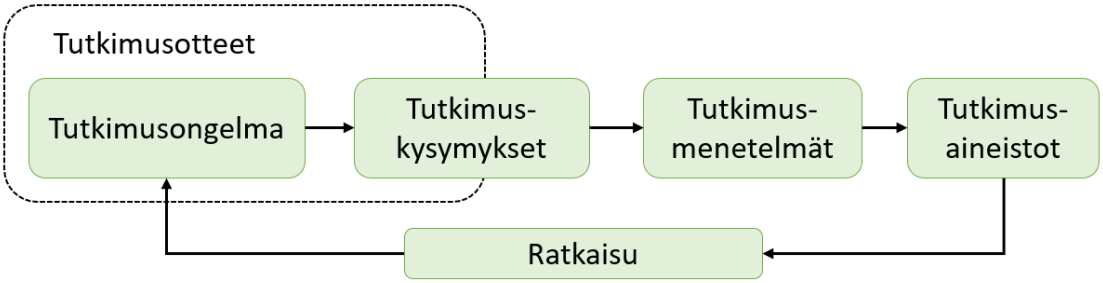
2 OPINNÄYTETYÖN TOTEUTUS

Tutkimusasetelma muodostuu tutkimusongelman, empiiristen aineistojen ja analyysimenetelmien kokonaisuudesta. Teoreettinen viitekehys ja siihen liittyvät keskeiset käsitteet liittyvät myös tutkimusasetelmaan. Tutkimusasetelmalla pyritään löytämään vastauksia asetettuihin tutkimusongelmiin. (Ronkainen ym. 2011, 63–70.)

Tutkimusasetelmia voi olla useita erilaisia, kuten vertailuasetelma, pitkittäisasetelma, poikkileikkausasetelma, tapaustutkimus, toimintatutkimus ja arviointitutkimus. Tutkimusasetelman valintaan vaikuttaa muun muassa olemassa oleva aineisto, konteksti ja ajankohdat. Tutkimusasetelman valinnalla tehdään samalla ratkaisuja analyysitavasta. (Vuori 2021.) Seuraavissa kappaleissa käydään opinnäytetyön tutkimussuunnitelmaan liittyviä vaiheita läpi.

2.1 Tutkimusmenetelmä, -ongelma ja -kysymykset

Tässä opinnäytetyössä tutkittiin todellista tilannetta yrityksessä ja pyrittiin kehittämään sitä paremmaksi ja siksi tutkimusmenetelmäksi valittiin toimintatutkimus, joka on yksi tutkimusasetelman muoto (Vuori 2021) ja kvalitatiivisen tutkimuksen laji (Hirsjärvi ym. 2009, 162). Tutkimus oli myös empiiristä tutkimusta, koska sen teon vaiheet sopivat tähän tutkimukseen. Empiiriseen tutkimukseen kuuluvat tutkimuksen suunnittelu, aineiston kerääminen, aineiston analysointi ja tulosten raportointi (Nummenmaa 2009). Kanasen (2014) mukaan toimintatutkimuksessa tutkimusongelma ja siihen perustuvat tutkimuskysymykset ratkaistaan tutkimusmenetelmillä erilaisten aineistojen avulla (Kuva 1).



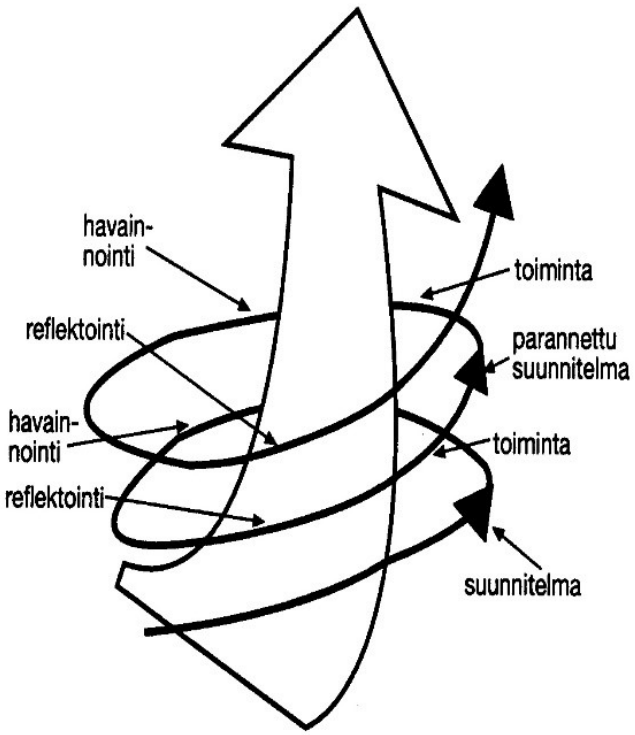
Kuva 1. Valitun tutkimusotteen kautta siirrytään tutkimismenetelmien ja aineiston tutkimisen kautta ratkaisuun (Kananen 2014, 30)

Toimintatutkimusta sovelletaan yleisesti monilla akateemisilla tieteen- ja tutkimusaloilla ja työelämän kehitysaloilla. Toimintatutkimuksen tavoite on parantaa paikallisia toimivia ratkaisuja, ja teorian luomista ei pidetä niin tärkeänä. Tässä työssä oli tarkoitus tutkia ja muuttaa nykyisiä käytäntöjä tehokkaammiksi aidossa työympäristössä ongelmanratkaisun keinoin. Tutkimus pidettiin yhteistoiminnallisena ja käytännönläheisenä, koska prosessiin ja järjestelmään liittyvä kommunikointi tapahtui osittain toimintaan liittyvien jäsenten välillä sekä opinnäytetyön tekijän kanssa. (Koski ym. 2019; Kananen 2014, 29.)

Heikkisen ym. (1999) mukaan toimintatutkimus etenee spiraalinomaisesti kehänä (Kuva 2), jolloin toimintaa voidaan havainnoida välillä ja parantaa edelleen jatkossakin (Jyrkämä s.a.). Tämän tyylisen syklisen etenemisen ensimmäinen vaihe on suunnittelu, johon kuuluu nykytilanteen arviointi ja kehitystoimenpiteiden suunnittelu. Seuraavaksi tulee toimintavaihe, joka on suunniteltu-

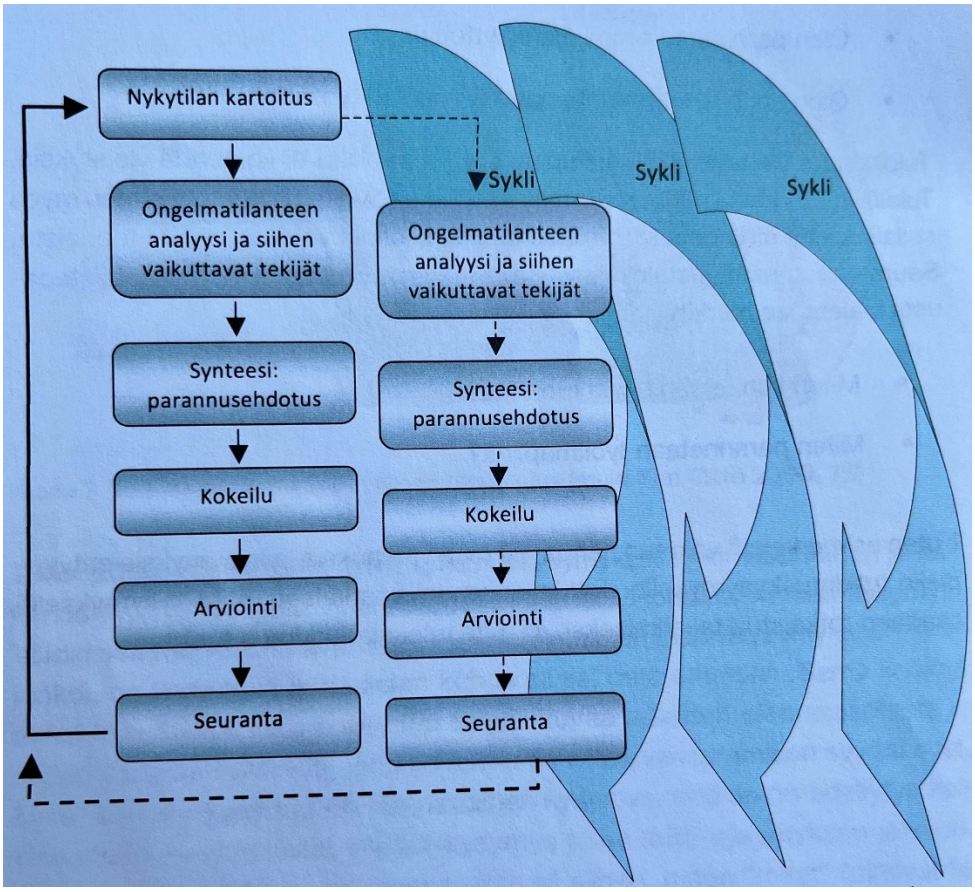
jen toimenpiteiden toteuttamista käytännössä. Kolmannessa havainnointivaiheessa toimintaa havainnoidaan. Viimeisessä vaiheessa arvioidaan ja reflektoidaan suunniteltu toiminta ja aikaansaadut seuraukset. (Koski ym. 2019.)

Opinnäytetyön aikana pyrittiin tekemään toimintatutkimuksen ensimmäiset vaiheet reflektointiin asti. Pienemmissä tutkimuksen toimintavaiheissa pyrittiin hyödyntämään tutkimuksellisen kehittämisen sykliä useampikin kierros. Kehitystyötä on tarkoitus jatkaa myöhemminkin Leanin oppien mukaisesti jatkuvan parantamisen tapaan (Torkkola 2015), joka sopii useisiin työelämän käytäntöihin.



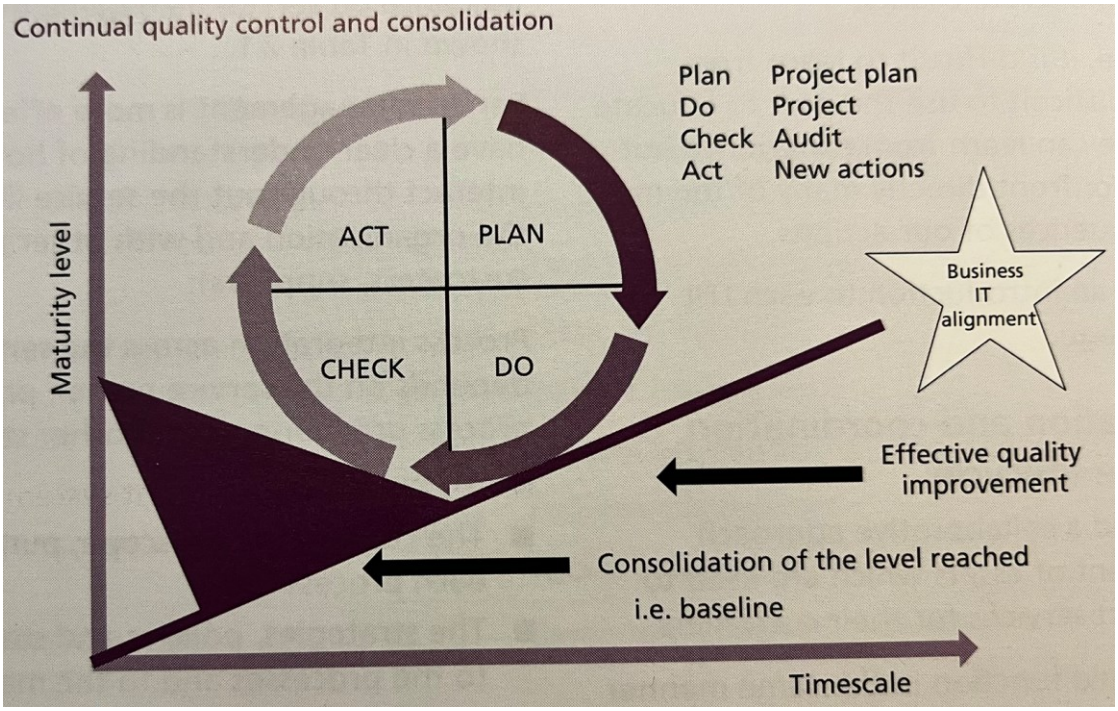
Kuva 2. Toimintatutkimuksen perusmalli (Heikkinen ym. 1999)

Kuva 3 esittelee seuraavaksi Kanasen näkemyksen toimintatutkimuksen vaiheista ja syklisyydestä (Kananen 2014).



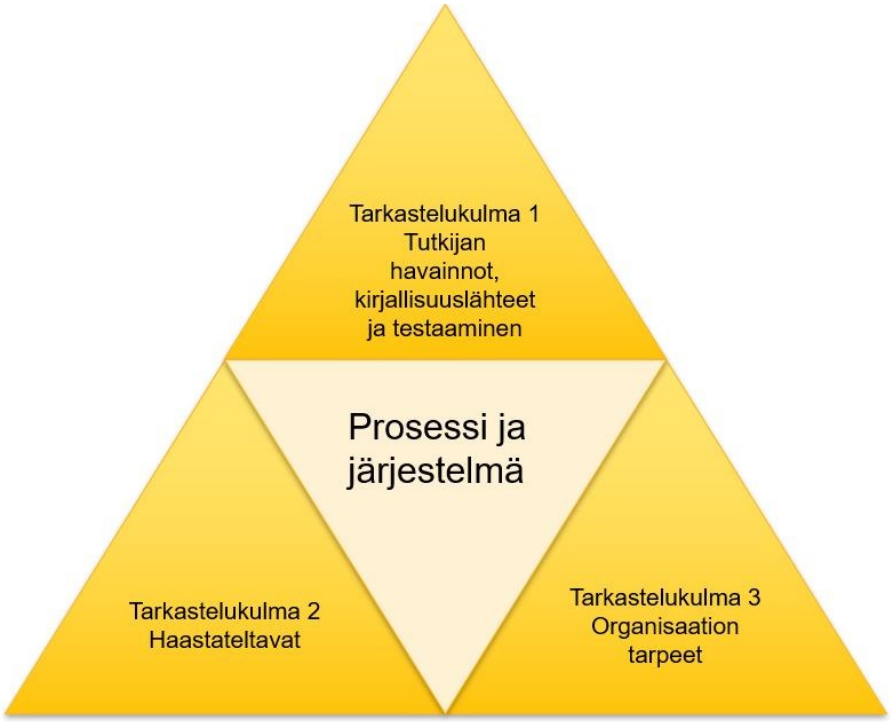
Kuva 3.Toimintatutkimuksen vaiheet (Kananen 2014, 34)

Toimintatutkimuksen perusmallia melko paljon vastaavaa kehittämismallia edustaa myös William Edwards Demingin kehittämä PDCA-malli, jota käytetään yleisesti laatujohtamisessa ja hallintajärjestelmien prosessien kehittämisessä. PDCA-mallin nimi tulee vaiheista suunnittele (plan), toteuta (do), arvioi (check) ja toimi (act) (Andreasson ym. 2013, 42–43). Kuva 4 näyttää vaihtoehtoisesti ITIL:n tulkinnan PDCA-syklistä jatkuvassa laadunvalvonnassa ja konsolidoinnissa (ITIL 2011a, 27).



Kuva 4. Plan-Do-Check-Act -syklin kuvaus (ITIL 2011a, 27)

Tutkimuksen objektiivisuutta eli puolueettomuutta pyrittiin lisäämään käyttämällä erilaisia menetelmiä. Tähän sopi triangulaatio eli monimetodinen tutkimusmenetelmä, jolla tarkasteltiin asetettuja tutkimuskysymyksiä useista eri näkökulmista. Laadullisessa tutkimuksessa tutkija tarkkailee tutkimusta tehdessään organisaation toimintaa havaintojen avulla. Toisena osa-alueena on tulosten tulkinta. (Grönfors 2011.) Tämän lisämenetelmän haettiin työhön parempaa validiteettia. Monimetodinen tutkimusasetelma mahdollistaa laadullisen analysoinnin, kuten myös määrällisen analysoinnin, mutta tässä työssä ei ollut kuitenkaan tarvetta määrälliselle analyysille. Kuva 5 näyttää kuinka triangulaatiossa tutkittavaa kohdetta voi tarkastella useista eri näkökulmista. Tässä työssä käytettiin tutkimustapana aineistotriangulaatiota, jossa hyödynnetään useita eri aineistoja tutkimuskysymyksiin vastattaessa ja metodologista triangulaatiota, jossa hankittiin aineistoja erilaisin tavoin tarvittaessa tutkimusmenetelmiä yhdistäen. Aineistotriangulaation avulla tehdylle raportille olisi hyvä saada haettua myös vahvistukset tietolähteiltä. (Viinamäki 2007, 181–185; Kananen 2014, 134.)



Kuva 5. Tutkimuksen triangulaation tarkastelunäkökulmat

Tutkimustehtävänä oli tarkoitus selvittää prosessin omistajalta ja käyttäjiltä haavoittuvuuden hallintaprosessin puutteet. Nämä puutteet liittyivät lähinnä siihen, ettei kaikille tilanteille ollut vielä selkeitä toimintaohjeita. Tutkimus perustui päteviin lähdetietoihin, aiempaan tietämykseen ja kehitystoiveita haettiin ja tarkasteltiin useammasta näkökulmasta. Tutkimuksessa tutkittiin myös yleisesti käyttöön otetut kirjallisuuden ja muiden organisaatioiden vastaavat prosessimallit ja pyrittiin hyödyntämään niistä löytyviä sopivia toimintamalleja. Prosessin rakennetta käytiin läpi niin, että se noudatti mahdollisimman hyvin SFS-tietoturvastandardeja ja ITIL4:n suosituksia niin, että se soveltui kohdeyrityksen eri osastojen toimintaan kuitenkin hyvin. Tohtori Hafkamp käsitteli ITIL-prosessien toimintaa tutkimuksessaan jo vuonna 2006. Hän piti ITIL:n IT-hallintaprosesseja jo siinä vaiheessa hyvinä, ja niitä on kehitetty jatkuvasta siitäkin lähtien (Hafkamp 2006). Tutkimuksen aikana käytiin haavoittuvuuden hallintaprosessin kaikki vaiheet läpi ja tarkennettiin niitä tutkimuksen edetessä. Samalla tehtiin yrityksen sisäiseen käyttöön tarkempaa ohjeistusta. Tutkimustyön edetessä selvitettiin lähdeviittaukset prosessin eri osa-alueille.

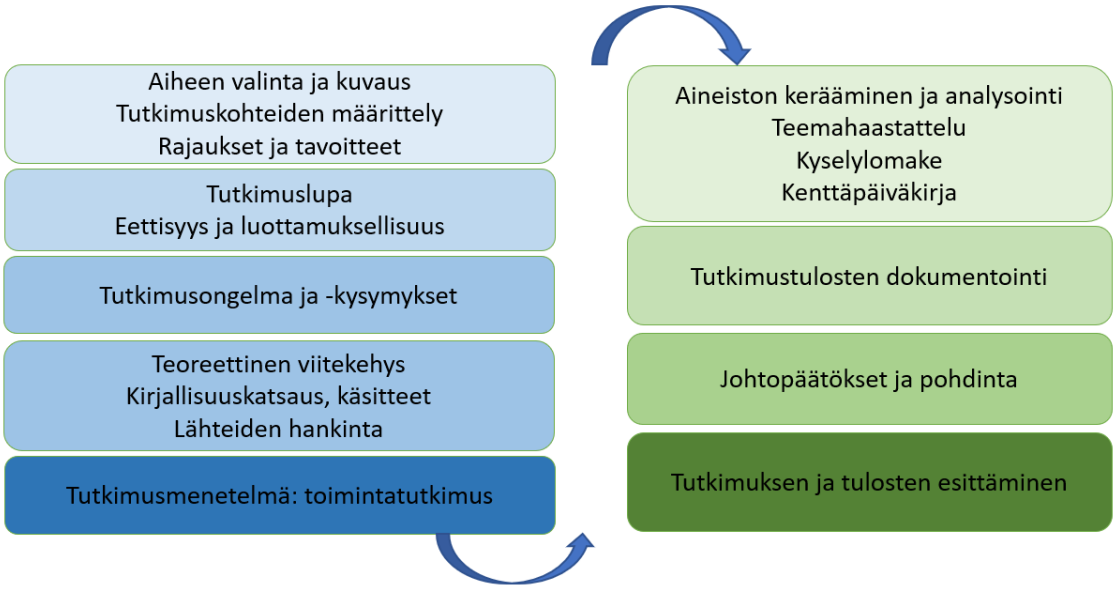
Haavoittuvuusjärjestelmän kehittäminen tehtiin järjestelmäomistajien ja SOC:n toiveiden mukaisesti ja pyrkien samalla tekemään siitä helposti ylläpidettävän.

Muutosehdotukset ja kehitysideat otetaan käyttöön, jos ne todetaan katselmoinnissa järkeviksi. Tavoitteena oli entistä selkeämpi toimintatapa koko organisaatiossa haavoittuvuuden hallintaprosessin osalta. Hallintaprosessin toiminnan mittarina voitaisiin käyttää KPI-mittaria. KPI-mittarin suunnittelu pyrittiin yhdistämään tähän työhön mukaan, jos se todettaisiin toteuttamiskelpoiseksi työn loppuvaiheissa jonkin osa-alueen suhteen. KPI-mittarin tulosten avulla selviää kuinka hyvin järjestelmä toteuttaa sille asetetut tehtävät.

Opinnäytetyön tutkimusongelmana oli haavoittuvuuksien hallintaprosessin keskeneräinen toteutus ja sen kuvaaminen organisaatiolle, jossa toimii useita ryhmiä ja käytössä on erilaisia tikettijärjestelmiä ja sovelluksia. Organisaatiolta puuttuvat myös haavoittuvuuksiin käsittelyyn liittyvät toiminnalliset eskalaation periaatteet ja työohjeet, joita on tarkoitus myös suunnitella. Tutkimuksen alkuvaiheeseen kuului nykytilanteen selvittäminen eli se, kuka päättää ja tietää mistäkin asiasta ja mitä kaikkia työkaluja ja toimintatapoja voidaan hyödyntää toiminnan parantamisessa, ja mitkä ovat kehityskohteet.

Haavoittuvuusprosessiin liittyvänä osittaisena ongelmana oli myös haavoittuvuusskannerin dokumentoinnin puute. Palveluiden järjestelmäomistajat tarvitsivat selkeät käyttöohjeet haavoittuvuusraporttien tarkastelua varten. Haavoittuvuusskannerin ylläpitäjiä varten täytyi testata skannerin varmuuskopiointien hoitaminen käytännössä ja näiden toimintojen dokumentointi.

Kuva 6 esittää yhteenvetona tämän opinnäytetyön kulun prosessikuvana.



Kuva 6. Opinnäytetyön prosessikuvaus

Tutkimukselle oli määritelty seuraavat tutkimuskysymykset:

1. Millä tavalla yrityksen sisäistä haavoittuvuuksien hallintaprosessia kannattaisi kehittää paremmaksi?
    a. Mitkä ovat nykyisen haavoittuvuuksien hallintaprosessin heikkoudet tai puutteet?
2. Haavoittuvuustikettien käsittelyn parannuskeinot?
3. Kuinka täytyisi reagoida nollapäivähaavoittuvuuksiin?
4. Kuinka voidaan pienentää haavoittuvuusskannerin löytämien väärien positiivisten määrää?

Kehittämiskysymyksinä tai -alueina oli lisäksi haavoittuvuuksien hallintaprosessin päivitys ja ohjeistaminen sekä Outpost24-skannerin tietojen varmuuskopioinnin ja palautuksen testaaminen ja ohjeistaminen yritykselle. Näihin asioihin liittyvä toteutus käsitellään työssä omissa luvuissaan.

2.2 Tiedonkeruumenetelmät

Haastattelua pidetään kvalitatiivisessa tutkimuksessa usein päämenetelmänä (Hirsjärvi ym. 2009, 205). Haastattelukeinoina voitaisiin käyttää lomakehaastattelua, avointa haastattelua ja teemahaastattelua (Hirsjärvi ym. 2009, 208–209). Tähän työhön valittiin päätiedonkeruumenetelmäksi teemahaastattelu, koska siinä haastateltava voi vastata kysymyksiin vapaasti, kuten avoimessakin haastattelussa, jolloin esille voi tulla uusia huomioitavia asioita aiheesta ja samalla ehkä tarkemman vastauksen. Teemahaastattelussa käydään läpi joustavasti ennalta valmisteltuja kysymyksiä tai aihealueita haastateltavien kanssa, joille teemaan liittyvä aihepiiri on ennestään tuttu (Hirsjärvi ym. 2009, 208). Valitusta aiheesta pyritään keskustelemaan vapaasti ja tutkija tekee samalla muistiinpanoja tai käyttää äänentallenninta. Haastateltavaksi valitaan sellaiset ihmiset, joiden oletetaan tietävän asiasta eniten, ja joita aihe koskettaa muutenkin heidän työtehtävässään. (Saaranen-Kauppinen ym. 2006.)

Laajemmalle ryhmälle, kuten SOC:lle ja järjestelmäomistajille, voitaisiin toteuttaa lisäksi myös kyselytutkimus, jos teemahaastattelulla ei saada katettua tarpeeksi laajaa joukkoa tarpeeksi nopealla aikataululla. Sen kautta pyritään saamaan tarkkaan mietittyihin kysymyksiin vastaukset ilman haastattelijan apua (Vehkalahti 2014, 11). Mukaan on hyvä liittää hyvin laadittu saatekirje, joka selvittää tutkimuksen aiheen, syyn ja tarkoituksen (Vehkalahti 2014, 47). Ky-

selytutkimuksiin ei todennäköisesti saada työkiireiden tai vähäisen kiinnostuksen takia kovin helposti vastauksia kaikilta (Hirsjärvi ym. 2009, 195) tai vastauksien sisältöön ei välttämättä panosteta niin hyvin kuin teemahaastattelussa, joten motivoivalla saatekirjeellä voidaan yrittää nostaa kiinnostusta (Vehkalahti 2014, 48).

Teemahaastattelun vastaukset kirjoitetaan pääasiassa vastauslomakkeeseen, mutta sen lisäksi tässä työssä on tarkoitus kirjata muita lisähavaintoja ja toimenpiteitä kenttäpäiväkirjaan. Kenttäpäiväkirjaa käytetään tutkimuksen yleisen kulun, metodologisten ja menetelmällisten seikkojen ja tutkijan omien havaintojen kirjaamiseen (Kallinen ym. s.a.).

Haavoittuvuusskannerin osalta selvitetään haastatteluiden tai kyselylomakkeen avulla SOC:n analyytikkojen ja raportteja tutkivien järjestelmäomistajien käyttökokemuksia. Skanneriin liittyvät kysymykset esitetään samalla kertaa, kun kysellään haavoittuvuuksien hallintaprosessiin liittyviä asioita. Opinnäytetyön tutkimuskysymykset ovat luonteeltaan pääasiassa sellaisia, että niihin haetaan vapaamuotoista vastausta ja selityksiä, joten strukturoitu lomakehaastattelu valmiine vastausvaihtoehtoineen ei sovi tähän käyttöön. (Saaranen-Kauppinen ym. 2006.)

2.3 Analysointimenetelmät

Tutkimuksen ydinasioita ovat aineiston analyysi, tulkinta ja johtopäätösten teko. Eskolan ym. (2014) mukaan analyysin avulla aineistoon pyritään luomaan selkeyttä, ja sillä pyritään tiivistämään sisältöä kadottamatta informaatiota. Analyysivaiheessa selviää, minkälaisia vastauksia tutkija saa tutkimusongelmille asetettuihin kysymyksiin. (Hirsjärvi ym. 2009, 221.) Teemahaastattelun tulosten ja organisaation tilanteen analysointiin sopii sisällön- ja tilanneanalyysi. Sisällönanalyysiä voi käyttää kirjallisuuteen, haastatteluihin ja aiheen teemojen käsittelyyn (Vuori s.a.). Tuomen (2018) mukaan sisällönanalyysin tavoite on luoda sanallinen ja selkeä kuvaus tutkittavasta ilmiöstä, joten se sopi hyvin tähän työhön. Organisaation haavoittuvuuksien hallintaan liittyvien toimintojen analysointiin valittiin lisäksi tilanneanalyysi, siten että päivittäiseen toimintaan vaikuttavat tekijät otettiin huomioon. Näin saatiin selville nykytilanne ja voitiin luoda tarvittaessa uusia tavoitteita. (Kokonat 2022.)

Toimintatutkimuksen tulosten tulkintaa ja analysointia tehtiin jatkuvasti prosessin edetessä ja tulokset johtivat rakentaviin kokonaisuuksiin ja johtopäätöksiin Kiviniemen (1999) mukaisesti. Aineiston keräämisen jälkeen aineistoa jäsenneltiin teemoittain ja samalla tarkistettiin sisältöä. Tarvittaessa pyydettiin haastateltavilta tietojen täsmennystä ja käyttökelvottomat vastaukset voitiin poistaa. Seuraavassa vaiheessa aineisto järjesteltiin ja kirjoitettiin puhtaaksi eli litteroitiin. (Hirsjärvi ym. 2009, 222.)

2.4 Teoreettinen viitekehys ja tutkimusmenetelmät

Teoreettinen viitekehys ja kysymyksenasettelu ohjaavat aineiston ja tutkimusmenetelmien valintaa. Tämän tutkimuksen teoreettinen viitekehys muodostui niin, että yrityksen aikaisemmista prosessimalleista ja käytännöistä, teemahaastatteluista, kyselyistä, kirjallisuuden tarjoamista tiedoista ja aikaisemmista tutkimuksista pyrittiin löytämään parhaiten haavoittuvuuksien hallintaprosessin kehittämistä tukeva tieto.

Opinnäytetyön teoreettinen viitekehys jaettiin kahteen osa-alueeseen ja peruskäsitteeseen, joista on pyritty luomaan kokonaiskuva opinnäytetyön johdannossa. Ensimmäinen laajempi osa-alue on haavoittuvuuksien hallintaprosessi ja toinen osa-alue on haavoittuvuuksien skannaukseen käytetty järjestelmä eli haavoittuvuusskanneri. Opinnäytetyöhön liittyvää tutkimustyötä tehtiin haavoittuvuuksien hallintaprosessin omistajan ja organisaation työntekijöiden näkökulmasta.

2.5 Keskeiset käsitteet

Teoreettisilla käsitteillä pyritään kuvaamaan asioiden tai ilmiöiden olemusta ja tunkeutumaan välittömän havainnon taakse (Hirsjärvi ym. 2009, 150). Tämän opinnäytetyön keskeisiä käsitteitä ovat haavoittuvuuksien hallintaprosessi ja haavoittuvuusskanneri, jotka on kuvattu johdannossa. Peruskäsitteisiin liittyvät lähikäsitteet haavoittuvuuksien hallinta, tietoturvatapahtuma, tietoturvapoikkeama ja haavoittuvuus, jotka kuvataan tarkemmin seuraavissa kappaleissa.

Haavoittuvuuksien hallinta tarkoittaa Microsoftin (2022) mukaan jatkuvaa, ennakoivaa ja useimmiten automaattista prosessia, joka suojaa järjestelmiä kyberhyökkäyksiltä ja tietomurroilta. Sen tavoite on vähentää yrityksen riskialttiutta poistamalla mahdollisimman monta haavoittuvuutta. Haavoittuvuus määritellään tietoturvapuolella alttiudeksi turvallisuutta uhkaaville tekijöille. Se voi olla puute tai heikkous turvatoimissa, suojauksessa, tietojärjestelmissä, prosesseissa ja ihmisen toiminnassa (Valtiovarainministeriö 2017, 54). Ohjelmistoissa oleva haavoittuvuus mahdollistaa järjestelmän väärinkäytön (Termipankki s.a.).

Tietoturvapoikkeama on tapahtuma, joka on tahallinen tai tahaton. Se voi aiheuttaa yrityksen tietojen ja palveluiden eheyden, luottamuksellisuuden tai käytettävyystason vaarantamisen. Tietoturvapoikkeamaksi voidaan kutsua muun muassa palvelunestohyökkäystä, tietovuotoa ja matkapuhelimen salakuuntelua. Tietoturvapoikkeama voi johtua myös haavoittuvuudesta. (Valtiovarainministeriö 2017, 12, 54.) Tietoturvatapahtuma on taas tapahtuma tai havainto, joka voi vaikuttaa vahingollisesti organisaation toimintaan. Esimerkkinä tietoturvatapahtumasta voidaan mainita läheltä-piti-tilanteet. (Valtiovarainministeriö 2017, 12, 52.)

2.6 Kirjallisuuskatsaus ja tärkeimmät lähteet

Lähtökohtana kirjallisuuskatsaukselle ovat tutkimuskysymykset. Kirjallisuuskatsauksessa hahmotetaan opinnäytetyön aihepiirin kokonaisuutta keräämällä yhteen olemassa olevaa tietoa tietystä aiheesta tai ongelmasta (Hirsjärvi ym. 2009, 121). Kirjallisuuden valinnassa täytyy käyttää lähdekritiikkiä, jotta aineisto olisi kelvollista. Lähdetiedon tulkinta vaatii myös kriittisyyttä. Lähteitä valittaessa huomioidaan kirjoittajan tunnettuus, arvostettavuus, lähteen ikä, lähdetiedon alkuperä, lähteen uskottavuus, totuudellisuus ja puolueettomuus. (Hirsjärvi ym. 2009, 113–114.)

Tässä opinnäytetyössä käytettiin menetelmällisenä ratkaisuna integratiivista kirjallisuuskatsausta, koska se voi sisältää sekä empiiristä että teoreettista kirjallisuutta (Jamk 2022). Tutkimuksen aiheeseen tutustuttiin tutkimalla ensin toimeksiantajan intranetsivut ja selvittämällä asiaan liittyviä perustietoja yrityksen työntekijöiltä. Tutkimukseen haettiin tietoa mahdollisimman luotettavista

lähteistä verkosta, kirjallisuudesta ja tutkimuksista sekä pyrittiin tutkimaan myös muiden organisaatioiden julkaistuja prosesseja ja artikkeleita. Lisäksi tutkittiin alan viralliset standardit ja suositukset.

Päätutkimuskohteena oli haavoittuvuuksien hallintaprosessi, johon liittyy useita sisäisiä toimintoja ja rajapintoja muihin prosesseihin. Käsitteelle haavoittuvuuksien hallinta löytyi melko paljon erilaista tietoa, mutta prosessien julkaistut kuvaukset olivat hyvin ylätasolla esitettyjä, joten niistä ei saanut helppoja malleja tähän työhön. Prosessin erilliset toiminnot täytyi tutkimuksessa käydä tapauskohtaisesti läpi ja yhdistää ne mukaan prosessikokonaisuuteen.

Prosessin rakennetta kehitettäessä perehdyttiin seuraaviin viitekehyksiin ja suosituksiin: SFS-tietoturvastandardit, ENISA (European Union Agency for Network and Information Security) ja ITIL (Information Technology Infrastructure Library). Näistä löytyviä käytäntöjä ja suosituksia voitiin hyödyntää niiltä osin, kun ne sopivat organisaation prosessien rakenteeseen ja eivät ole liian monimutkaisia ja kalliita ratkaisuiltaan.

Euroopan unionin verkko- ja tietoturvavirasto (ENISA) on Euroopan unionin (EU), sen jäsenvaltioiden, yksityisen sektorin ja Euroopan kansalaisten verkko- ja tietoturvaosaamisen keskus (ENISA 2016, 2). ENISA antaa Euroopan alueella yleisiä kyberturvallisuuden suosituksia, joita pyrittiin hyödyntämään prosessimallia pohdittaessa, mutta sieltä ei kuitenkaan löytynyt varsinaista apua.

ITIL on kokoelma pitkään kehitettyjä parhaita käytäntöjä IT-palveluiden hallintaan ja johtamiseen (CIO 2022). ITIL ja uudempi ITIL4 keskittyy jatkuvaan mittaamiseen ja laadun parantamiseen sekä liiketoiminnan että asiakkaan näkökulmasta. ITIL:n käytäntöjä tutkimalla pyrittiin löytämään apuja lähinnä hallintaprosessin kehittämiseen. Organisaation muita prosesseja oli toteutettu useimmiten ITIL:n mukaisesti, joten tässäkin työssä perusperiaatteet toiminnalle pyritään hakemaan ITIL:stä, jotta toimintatavoissa olisi eri prosessienkin kesken yhteneväinen tapa.

Käsitteelle haavoittuvuusskanneri löytyi yleistason tietoa, mutta niissä keskitytään useimmiten valmistajien tuotteiden mainostamiseen tai kuvaamiseen.

Niitä löytyy paljon erilaisia ominaisuuksiltaan, kattavuuksiltaan ja monesta eri hintaluokasta. Skannereista annetaan tässä työssä myöhemmin yleisluonteista kuvausta jonkin verran, ja sitten keskitytään tarkemmin organisaation skanneria koskeviin tutkimuskysymyksiin. Paras tieto valitun skannerin suhteen saadaan järjestelmän kehittäjän sivustoilta ja lisätietoja voi kysyä myös heidän teknisestä tuestaan. Haavoittuvuuksista löytyy paljon tietoa, mutta niistä on tarkoitus ottaa työssä käsittelyyn lähinnä vain niiden luokittelu, niihin liittyvät tietokannat ja haavoittuvuusluokkien huomiointi eri prosessivaiheissa.

Tärkeimmät tutkimusaiheeseen liittyvät lähteet:

- Calder, A. 2020. Cyber Security: Essential principles to secure your organization.
- Cavelty, M.C. & Wenger, A. 2022. Cyber Security Politics.
- Kerzner, H. 2017. Project Management Metrics, KPIs, and Dashboards: A Guide to Measuring and Monitoring Project Performance.
- Maglaras, L. ym. 2022. Cyber Security and Critical Infrastructures.
- NIST Cybersecurity Framework. NIST Vulnerability Database.
- Outpost24 Knowledge base documentation. 2022.
- OWASP. 2020. OWASP Vulnerability Management Guide (OVMG).
- Pricop, E. ym. 2021. Advanced Topics in Systems Safety and Security.
- Scott, J. 2022. Cyber Peace.
- Stewart, J. & Chapple M. & Gibson, D. 2012. CISSP: Certified Information Systems Security Professional Study Guide.
- Torkkola, S. 2015. Lean asiantuntijatyön johtamisessa.
- Wei, L. 2021. Cyber Security.

Lisäksi lähteinä käytettiin useita SFS-standardeja ja kriteeristöjä, mutta niitä voidaan pitää lähinnä sekundäärisinä lähteinä. Edellä mainittujen lähteiden tarkemmat saatavuustiedot ja muut lähteet löytyvät dokumentin lopussa olevasta lähdeluettelosta.

2.7 Resursointi

Tätä opinnäytetyötä varten ei tarvinnut tehdä lisähankintoja, koska tutkimuksessa käytettiin olemassa olevia laitteistoja ja ohjelmistoja. Yrityksen haavoittuvuuden hallintaprosessin ja haavoittuvuusskannerin kehittämiseen ja palavereihin pyrittiin käyttämään sovitusti korkeintaan yksi työpäivä työaikaa ja muu opinnäytetyöhön liittyvä toiminta tehtiin vapaa-ajalla. Opinnäytetyöhön ja Outpost24:een liittyen järjestettiin viikoittain seurantapalaveri opinnäyte-

työnohjaajan ja kahden muun henkilön kanssa. Näin pysyttiin hyvin ajan tasalla työn etenemisen suhteen ja samalla keskusteltiin sen hetkisistä ongelmista ja seuraavista vaiheista. Toimeksiantajan järjestelmäomistajien sekä verkko- ja palomuuriasiantuntijoiden apua tarvittiin verkon skannauksen laajentamisvaiheissa, joten heidän työaikaansa käytettiin tarpeen vaatiessa.

3 TEOREETTINEN VIITEKEHYS

3.1 Yrityksen turvallisuusperiaatteiden merkitys

Yrityksen tietoturvallisuutta pystytään parantamaan riskienhallintaprosessilla ja monilla muilla prosesseilla, joista nyt oli otettu tutkimuksen aiheeksi haavoittuvuuksien hallintaprosessi. Ilman kunnollisia suunnitelmia organisaatio saattaa käyttää liikaa resursseja tietoturvariskien hallintaan tai sitten vaihtoehtoisesti riskejä ei huomioida tarpeeksi. Tämän takia on tarpeen luoda sellaiset prosessit, jotka auttavat ymmärtämään ja priorisoimaan yrityksen tietoturvallisuuden kannalta tärkeimmät seikat. Ihmisten, prosessien ja tekniikan luoma kokonaisuus luo pohjan yrityksen tietoturvallisuudelle. (Keskuskauppakamari 2020.)

Tietoturvatoimenpiteissä täytyy aluksi keskittyä SFS 27001 standardin (2017) mukaan tärkeimpien tietojen ja järjestelmien suojaamiseen, niin ettei luottamuksellisuus, eheys tai käytettävyys vaarantuisi ja aiheuttaisi vakavaa haittaa yritykselle. Täytyy huomioida, että kaikki tiedonkäsittelyn vaiheet on suojattu asiallisesti eli tietojen käsittely, tiedonsiirto ja säilytys (Infosec 2023). Ulkoisiin järjestelmiin kytkeytyminen aiheuttaa aina lisäriskin, joten niiden suhteen täytyy toteuttaa turvatoimenpiteet joko fyysisin tai loogisin keinoin riskivaatimustasojen mukaisesti (Infosec 2023). Useimmiten voidaan todeta, että riskien täydellinen poistaminen ei ole kustannustehokasta. Kun pääasiat ovat kunnossa, niin sen jälkeen säännöllisen seurannan ja toimintojen hienosäätämisen kautta voidaan myös pienempiä riskejä vähentää vähitellen ja tehostaa samalla toimintaa. (Keskuskauppakamari 2020.)

Organisaation täytyy myös varautua ennakkoon tietoturvamurtoihin ja tietojen menetykseen. Tätä varten täytyy olla valmiit toimintaprosessit ja ohjeistukset. On tärkeää myös arvioida näitä ohjeistuksia säännöllisesti. Arvioinnit voi tehdä sisäisillä tai ulkoisilla arvioinneilla ja auditoinneilla, joihin voi sisällyttää erilaisia

testauksia. Auditointien ja yritysturvallisuusarviointien tueksi on kehitetty muun muassa Katakri (2020) ja pilvipalveluiden puolelle löytyy Traficomin kehittämä pilviturvallisuuden arviointikriteeristö PiTuKri (Traficom. 2020). Näillä molemmilla on tavoitteena edistää salassa pidettävän tiedon turvallisuutta ja ne soveltuvat myös itse yrityksen toimintojen kehittämiseen. Myös fyysinen turvallisuus täytyy organisaatioissa huomioida ja sen analysointiin voisi käyttää vaikka Tureanin tunkeutumisreittianalyysia (Peltonen 2003). Tietoturvaloukkausten varalta yrityksen täytyisi tehdä varautumissuunnitelma, jotta toiminta olisi jo valmiiksi suunniteltua myös riskien toteutuessa (Keskuskauppakamari 2020).

Organisaation tehokkaan tietoturvan kannalta on tärkeää, että yrityksen johto ymmärtää ja tukee riskienhallintaa ja siihen liittyviä prosesseja. Kaikille prosesseille on hyvä nimetä vastuullinen omistaja ja tietoturvatoimintojen tilanne olisi syytä raportoida johtoryhmälle vähintään kerran vuodessa. Lisäksi koko henkilöstölle on syytä kouluttaa kohtuullinen tietoturvaosaaminen ja tuoda esille yrityksen tietoturvapolitiikka ja oikeat työntekijää koskevat toimintatavat. (Keskuskauppakamari 2020.)

3.2 Haavoittuvuuksien hallintaprosessi

Prosessin tavoite on tunnistaa ja vähentää haavoittuvuuksien määrä IT-ympäristössä, samalla vähentäen järjestelmätietomurron ja muun järjestelmähyväksikäytön riskiä. Prosessi tunnistaa ja analysoi haavoittuvuuksia laitteiden ja järjestelmien muodostamassa teknisessä ympäristössä. Tunnistuksen ja analysoinnin pohjalta käynnistetään korjaavia toimenpiteitä esimerkiksi muutoksenhallinnan kautta. Tunnistamisen apuna käytetään teknisiä järjestelmiä, kuten haavoittuvuusskannereita ja ulkoisia tietolähteitä, kuten valmistajien dokumentaatiota, tietoturvauutisia ja työntekijöiden havaintoja. (Stewart ym. 2012, 552.)

Ilman järjestelmälokeja ja lokitietoja analysoivaa prosessia, teknisten haavoittuvuuksien tuntemusta ja IT-järjestelmien perusteellisempaa tarkastelua realistinen riskinarviointi ei ole mahdollista. Prosessin puuttuminen tai sen puutteet eivät myöskään mahdollista riskien hyväksymiskriteerien laatimista tai riskitasojen määrittämistä - kuten ISO 27001 -standardissa edellytetään. ISO

27001 -standardi edellyttää vähintään neljännesvuosittain tapahtuvan ulkoisen ja sisäisen haavoittuvuustarkistuksen järjestelmiin. Organisaation muut vaatimustasot ja tavoitteet voivat edellyttää useamminkin tapahtuvat haavoittuvuusskannaukset. (SFS27001 2017.)

Infrastruktuurin optimaalisen turvaamiseen kuuluu kaikkien järjestelmien säännöllinen, järjestelmällinen, verkko-ohjattu skannaus ja tunkeutumistestaus teknisten haavoittuvuuksien varalta. Tässä yhteydessä tekniset haavoittuvuudet on priorisoitava vakavuuden mukaan (CVSS / Common Vulnerability Scoring System) ja lopulta korjattava. Jäljellä olevista teknisistä haavoittuvuuksista jäävän jäännösriskin arviointi ja lopulta riskin hyväksyminen ovat osa ISO 27001 -standardin mukaista haavoittuvuuksien hallintaa. (SFS27001 2017).

Seuraavat asiat saattavat tulla eteen prosessin arvioinnin tai auditoinnin aikana, joten niihin kannattaa kiinnittää huomiota:

- Onko roolit ja vastuut määritelty teknisten haavoittuvuuksien käsittelyä ja seurantaa varten?
- Onko teknisten haavoittuvuuksien tunnistamiseen liittyviin tietolähteisiin tutustuttu?
- Mikä on määräaika sille, että haavoittuvuus otetaan käsittelyyn sen havainnon jälkeen?
- Onko tehty riskiarviointi haavoittuvuuksista yrityksen omaisuuden kannalta?
- Tunnistetaanko tekniset haavoittuvuudet? (SFS-ISO/IEC27001 2017.)

Edellä esitetyt kysymykset tulivat esille myös kohdeorganisaation toiminnan tarkastelussa. Osa asioista oli hoidettu hyvin, mutta teemahaastatteluissa ja tutkimuskysymyksiä listattaessa tuli esille kaksi kysymystä siinä mielessä, että asiat eivät olleet täysin kunnossa niiden osalta. Nämä asiat tuodaan esille ohjeistuksissa.

3.3 Haavoittuvuuksien hallinnan viitekehykset ja ohjeistukset

Haavoittuvuuksien hallintaprosessi suunnitellaan organisaation omien palveluiden, resurssien, tavoitteiden ja muiden prosessien mukaan, mutta suunnitteluvaiheessa on hyvä tutustua haavoittuvuuden hallinnan eri menetelmien

perusteisiin. Tähän lukuun on koottu haavoittuvuuksien hallintaa käsitteleviä viitekehyksiä ja ohjeistuksia.

3.3.1 SFS ISO/IEC-standardit

SFS on Suomen standardisoimisliiton vahvistaman asiakirjan tunnus ja SFS-standardi on kansallisesti laadittu standardi kotimaiseen käyttöön (SFS-opas 2022, 5). Myös eurooppalaiset (EN) ja maailmanlaajuiset (ISO tai IEC) standardit saavat etuliitteen SFS, jos ne on vahvistettu Suomessa (SFS-opas 2022, 5). SFS-standardit lisäävät tuotteiden ja palvelujen laatua, turvallisuutta ja yhteensopivuutta. Ne edistävät tutkitusti yritysten liiketoimintaa ja kasvattavat asiakkaiden luottamusta, joten näillä perusteilla SFS-standardeja kannattaa hyödyntää, jos niistä saa käyttökelpoista ohjeistusta prosessin toimintaan.

SFS ISO/IEC 27000

Eurooppalainen EN SFS ISO/IEC 27000:2020 on vahvistettu Suomessa kansalliseksi standardiksi. Tämän standardin mukaan täytyy seurata ja arvioida säännöllisesti toteutettujen menettelytapojen vaikuttuvuutta, tunnistaa uudet riskit ja kehittää valittuja hallintakeinoja tarpeiden mukaisesti. Tietoturvallisuuden hallintajärjestelmä (ISMS) on lähestymistapa yrityksen tietoturvallisuuden suunnittelemiseen, toteuttamiseen, seurantaan, auditointiin, ylläpitoon ja parantamiseen liiketoimintaan liittyvien tavoitteiden saavuttamiseksi. (SFS-ISO/IEC27000 2020.)

ISMS perustuu riskienhallintaan ja määriteltyihin riskien hyväksyntätasoihin. Tietoturvallisuuden hallintajärjestelmän toteutusta edesautetaan analysoimalla tieto-omaisuuden suojausvaatimukset ja toteutetaan hallintakeinot suojauksien varmistamiseksi. Seuraavat perusperiaatteet luovat pohjan onnistuneelle tietoturvallisuuden hallintajärjestelmälle:

- Tiedostetaan tietoturvallisuuden tarve.
- Määritellään tietoturvallisuuteen liittyvät vastuut.
- Johto sidosryhmineen sitoutuu tietoturvallisuuden tavoitteluun.
- Tuetaan yhteiskunnan arvoja.
- Määritellään hallintakeinot, joilla saavutetaan hyväksytyt riskitasot.
- Huomioidaan turvallisuus olennaisena osana tietojärjestelmä- ja verkkoratkaisuja.
- Ehkäistään ja havainnoidaan aktiivisesti tietoturvahäiriöitä.
- Varmistetaan tietoturvallisuuden hallinnan kattava toimintamalli.

- Tehdään jatkuvaa seurantaa ja parantamista tarpeen niin vaatiessa. (SFS-ISO/IEC27000 2020.)

Standardien avulla yrityksissä voidaan valmistautua tietoturvallisuuden hallintajärjestelmän riippumattomaan arviointiin. Eri SFS-standardit keskittyvät hieman eri osa-alueisiin, mutta ne voivat myös osittain täydentää toisiaan. Seuraavaksi esitettävät SFS ISO/IEC 27001 - ISO/IEC 27005 määrittävät enemmän tietoturvallisuuden hallintajärjestelmien käyttöä ja tietoturvariskien huomioimista ja siksi ne ovatkin tärkeitä standardeja organisaatioiden tietoturvan määrittämisessä.

SFS ISO/IEC 27001

Tämä standardi määrittelee tietoturvallisuuden hallintajärjestelmän suunnittelua, toteuttamista, johtamista, ylläpitämistä, tukitoimia, resursseja, dokumentointia, sisäistä auditointia, viestintää ja jatkuvaa parantamista koskevat vaatimukset. Mukana on myös tietoturvariskien arviointiin ja käsittelyyn liittyviä vaatimuksia. Jos yritys ilmoittaa noudattavansa tätä standardia, niin standardissa esitetyt vaatimukset täytyy olla kunnossa auditoinneissa. (SFS-ISO/IEC27001 2017.)

Edellisessä luvussa mainittu ISMS yhdistetään myös ISO/IEC 27001 standardiin, koska myös siinä määritellään ISMS vaatimukset. ISO/IEC 27001 auttaa organisaatioita tiedostamaan riskejä sekä tunnistamaan ja korjaamaan ennakoivasti heikkouksia (ISO 2022).

SFS-EN ISO/IEC 27002

Tämä standardi sopii lisäohjeistukseksi yrityksille, jotka noudattavat standardiin ISO/IEC 27001 perustuvia yleisesti hyväksyttyjä tietoturvallisuuden hallintakeinoja. Tämä standardi erityisesti ohjeistaa kuinka ISO/IEC 27001 standardin tietoturvallisuuden hallintajärjestelmän tietoturvariskien poistokeinoja voitaisiin määrittää ja toteuttaa.

Organisaation on tunnistettava turvallisuusvaatimuksensa, joilla on kolme päälähdettä:

1. Riskienarviointi, jossa huomioidaan yleinen liiketoimintastrategia ja yleiset tavoitteet. Tunnistetaan omaisuuteen kohdistuvat uhkat, haavoittuvuudet, todennäköisyydet ja arvioidaan niiden mahdolliset vaikutukset toimintaan.
2. Lakiin, asetuksiin ja viranomaisvaatimuksiin ja sopimuksiin liittyvät vaatimukset, joita yrityksen on kumppaneineen noudatettava.
3. Tiedon tallentamista, viestimistä ja arkistointia koskevat periaatteet, tavoitteet ja liiketoimintavaatimukset, jotka yritys on kehittänyt omien toimintojensa tueksi. (SFS-ISO/IEC27002 2017.)

Tässä standardissa ohjeistetaan tietoturvallisia keinoja ja ohjeita projektityöhön, mobiililaitteiden käyttöön, etätyöhön, henkilöturvallisuuden huomiointiin, työsopimuksiin, johdon vastuisiin, tietoturvakoulutuksiin, suojattavan omaisuuden hallintaan, tietojen luokitteluun, tiedon merkintään, suojattavan omaisuuden käsittelyyn, tietovälineiden käsittelyyn, erilaisiin pääsynhallintoihin, salasanojen hallintajärjestelmään, käyttäjien vastuisiin, hallintasovellutuksiin, salauksen hallintaan, kulunvalvontaan, käyttöturvallisuuteen, muutoksenhallintaan, kapasiteetinhallintaan, varmuuskopiointiin, kirjaamiseen, seurantaan, teknisten haavoittuvuuksien hallintaan, viestintäturvallisuuteen, järjestelmien hankintaan, tietojen siirtämiseen, toimittajasuhteiden huomiointiin, tietoturvahäiriöiden hallintaan, liiketoiminnan jatkuvuuden hallintaan, vikasietoisuuden huomiointiin ja vaatimustenmukaisuuden noudattamiseen. (SFS-ISO/IEC27002 2017.)

SFS-ISO/IEC 27005

Tämä asiakirja ohjeistaa tietoturvariskien hallintaa yrityksessä. Tässä standardissa ei esitetä malliksi mitään tiettyä tietoturvariskien hallintamenetelmää, vaan kunkin yrityksen oletetaan määrittelevän itse omat toimintamallinsa, koska siihen vaikuttaa tietoturvallisuuden hallintajärjestelmän laajuus, toimintaympäristö ja yrityksen toimiala. Riskienhallintaprosessi ja tietoturvariskien hallintaprosessi kuvataan tässä standardissa yleisellä tasolla, ja ohjeistus antaa mahdollisuuden soveltaa ohjeita erityyppisissä yrityksissä. Riskien käsittely on standardin mukaan jatkuva prosessi, joka koostuu riskien arvioinnista, jäännösriskien tason hyväksynnän arvioinnista ja uudesta riskien käsittelyn aloittamisesta, jos aiemmat riskitasot eivät olleet hyväksyttäviä. Lopuksi arvioidaan riskien käsittelyn toimivuus. (SFS-ISO/IEC27005 2018.)

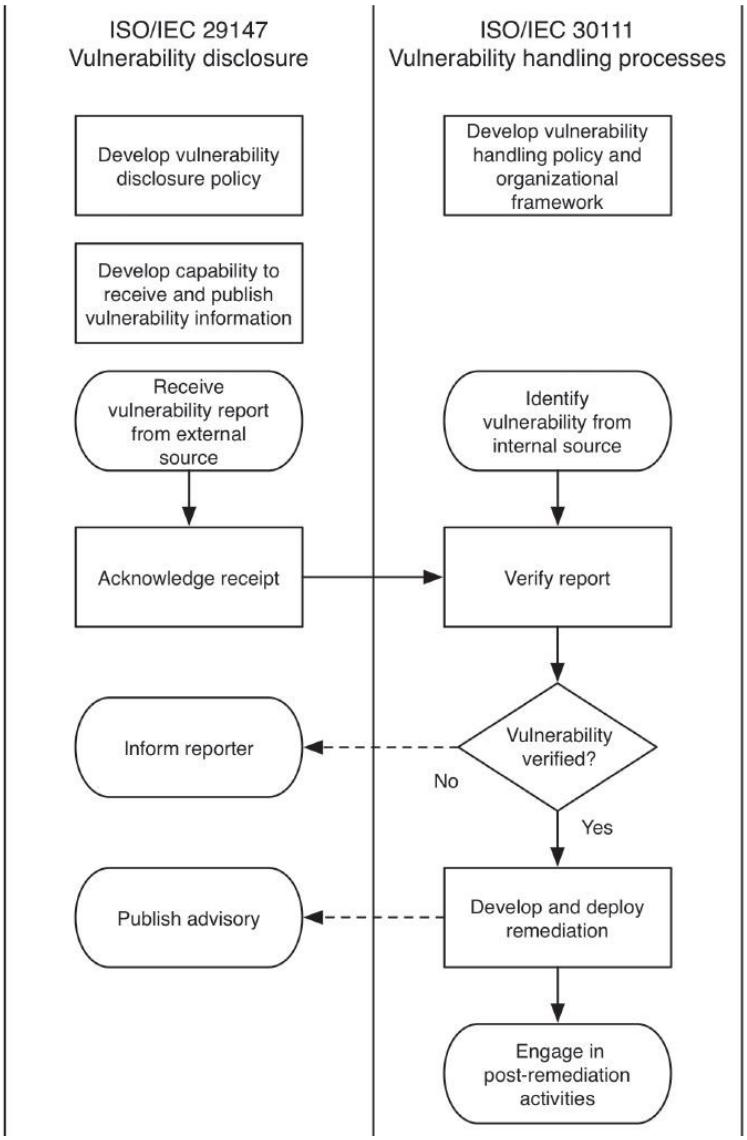
Tämä standardi tarjoaa vaihtoehdon SFS-ISO/IEC27002 standardille, koska siinä käsitellään standardin tietoturvallisuuden hallintajärjestelmän tietoturvariskien poistokeinoja. Tämän standardin tehokas hyödyntäminen edellyttää kuitenkin, että edellisten standardien käsitteet ja prosessit ovat jo tuttuja. (SFS-ISO/IEC27005 2018.)

SFS-ISO/IEC 27035 ja SFS-ISO/IEC 27043

Tämä standardi käsittelee tietoturvahäiriöiden hallinnan periaatteita ISO/IEC 27035-1:ssa ja ohjeistusta häiriövasteiden suunnitteluun ISO/IEC 27035-2:ssa. Standardi käsittelee lähinnä tietoturvahäiriöiden hallintaa, mutta siinä on mukana myös hiukan tietoturvahaavoittuvuuksiin liittyviä asioita. Enemmän haavoittuvuuksien paljastamiseen ja järjestelmätoimittajien käsittelytapoihin liittyviä asioita käsitellään vastaavissa standardeissa ISO/IEC 27147 ja ISO/IEC 30111. Standardi ISO/IEC 27043 liittyy myös tietoturvahäiriöiden tutkinnan periaatteiden ja prosessien käsittelyyn, joten sitä ei käydä tässä enempää läpi. (SFS-ISO/IEC27035 2016; SFS-ISO/IEC27043 2016.)

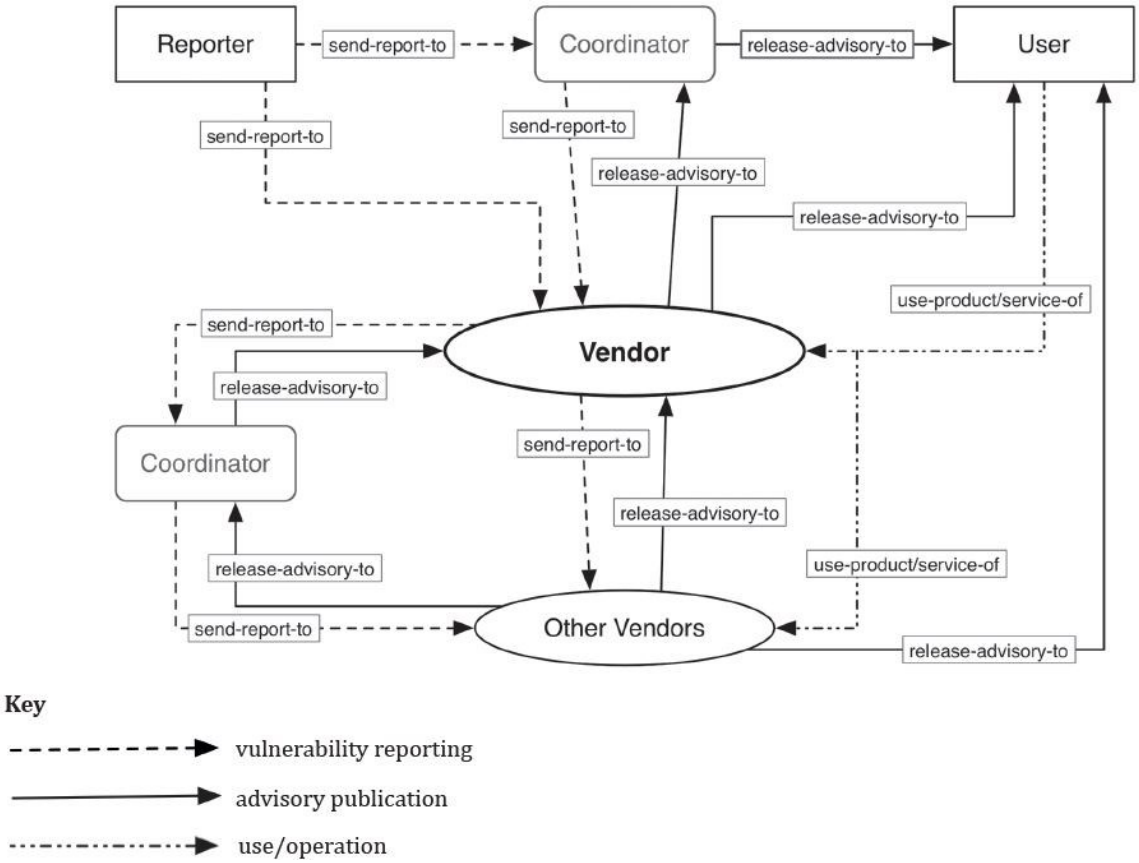
SFS-ISO/IEC 29147

SFS-ISO/IEC 29147 esittää vaatimuksia ja suosituksia ohjelmistovalmistajille tuotteiden ja palveluiden haavoittuvuuksien paljastamiseksi (engl. vulnerability disclosure). Haavoittuvuuden paljastaminen tarkoittaa tietokoneohjelmiston tai -laitteiston tietoturvapuutteiden ilmoittamista. Tietoturvatutkijat, IT-tietoturvatiimit, sisäiset kehittäjät, kolmannen osapuolen kehittäjät ja muut haavoittuvien järjestelmien kanssa työskentelevät voivat paljastaa haavoittuvuuksia suoraan virheellisistä järjestelmistä vastuussa oleville osapuolille (TechTarget s.a.). Tämä standardi liittyy läheisesti standardiin SFS-ISO/IEC 30111. Kuva 7 esittää standardien SFS-ISO/IEC 29147 ja SFS-ISO/IEC 30111 välistä suhdetta, jossa kuvataan samalla haavoittuvuuksien paljastamiseen ja käsittelyyn liittyvää prosessia. Standardissa kehotetaan tutkimaan haavoittuvuustyyppien osalta lisätietoja CWE:sta ja OWASP:sta. (SFS-ISO/IEC29147 2020.)



Kuva 7. Standardien ISO/IEC 29147 ja ISO/IEC 30111 välinen suhde (SFS-ISO/IEC29147 2020) haavoittuvuuksien käsittelyprosessissa

Kuva 8 esittää tiedonkulkua haavoittuvuuden paljastumisprosessissa.



Kuva 8. Tiedonkulku haavoittuvuuden paljastumisprosessissa (SFS-ISO/IEC29147 2020)

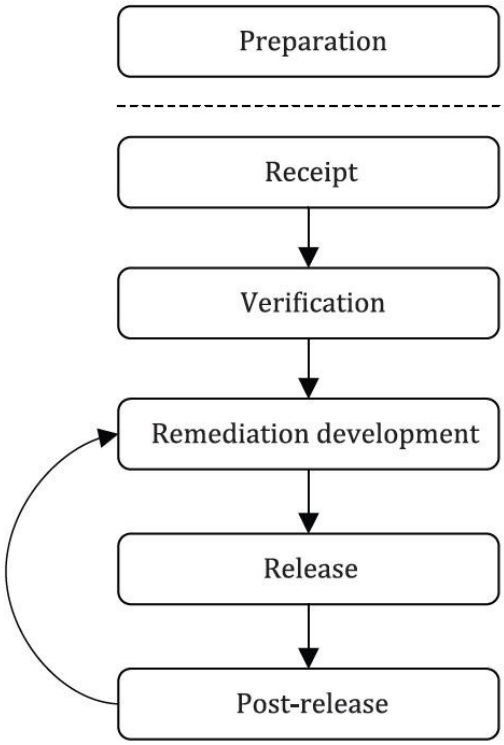
Raportoijan haavoittuvuusilmoitus tiedotetaan suoraan tai koordinoijan kautta ohjelmistotoimittajalle. Toimittaja ilmoittaa haavoittuvuudesta muille toimittajille, ja lopuksi alkuperäinen toimittaja tai muu vastuussa oleva toimittaja julkaisee korjauspäivityksen käyttäjille, kunhan se on saatavilla. (SFS-ISO/IEC29147 2020.)

SFS-ISO/IEC 30111

SFS-ISO/IEC 30111 sisältää vaatimuksia ja suosituksia ilmoitettujen mahdollisten haavoittuvuuksien käsittelemiseksi ja korjaamiseksi. Tämä asiakirja koskee ohjelmistovalmistajia ja sidosryhmiä, jotka ovat mukana haavoittuvuuksien käsittelyssä.

Standardin mukaan haavoittuvuuden hallinnan prosessit täytyy dokumentoida, niin että ne ovat toistettavissa. Dokumentoinnin täytyy kuvata menetelmät, joilla seurataan ilmoitettuja haavoittuvuuksia. Johdon täytyy varmistaa, että haavoittuvuuksien hallintaan liittyvät vastuut ja roolit on määritelty ja tiedotettu. Organisaation täytyy perustaa yhteyskanava, jota kautta hoidetaan kommunikoinnin ulkoisten osapuolien kanssa haavoittuvuuksiin liittyen. Yhteyshenkilö

voisi olla esimerkiksi ohjelmistovalmistajien CSIRT-tiimistä (Computer Security Incident Response Team) tai PSIRT- tiimistä (Product Security Incident Response Team). (SFS-ISO/IEC30111 2020.)



Kuva 9. Yhteenveto ohjelmistovalmistajien haavoittuvuuksien hallintaprosessista (SFS-ISO/IEC30111 2020)

Kuva 9 näyttää yksinkertaistetun kuvan SFS-ISO/IEC 30111:n ohjelmistovalmistajien haavoittuvuuksien hallintaprosessin vaiheista. Näiden vaiheiden ymmärtäminen on tarpeen myös muiden organisaatioiden haavoittuvuuksien hallintaprosessia suunniteltaessa.

3.3.2 NIST Special Publication 800-53 Revision 5

Tämän NIST-julkaisun pyrkimyksenä on ollut kehittää seuraavan sukupolven tietoturva- ja yksityisyydenhallintaohjeistuksia yritysten käyttöön. Ohjeet on mukautettavissa ja säädettävissä, ja niitä voidaan käyttää osana koko yrityksen riskienhallintaa. Tämä julkaisu käsittelee erityisesti haavoittuvuuksien hallintaa ja tarkistusta. (NIST 2020.)

Uusien haavoittuvuuksien tunnistamisessa on tärkeää, että haavoittuvuuksien seurantatyökaluja on mahdollista päivittää nopeasti, kun uusia haavoittuvuuksia tunnistetaan, ja kun luodaan uusia tarkistustekniikoita. Räätälöityjen ohjelmistojen seurantaan ja analysointiin voidaan tarvita myös lisätapoja, kuten staattinen analyysi, dynaaminen analyysi, binäärianalyysi tai näiden kolmen yhdistelmä. Näitä menetelmiä voidaan käyttää lähdekooditarkistuksissa sekä verkkopohjaisissa ohjelmistoanalysaattoreissa, staattisissa analyysiohjelmistoissa ja binääriskannereissa. (NIST 2020.)

Haavoittuvuuksien valvontaan täytyisi kuulua ohjelmistopäivitysten seuranta, ylimääräisten avoimien porttien, protokollien ja palveluiden etsiminen sekä virheellisesti asennettujen tai väärin toimivien vuonhallintamekanismien valvonta. Verkkokomponenttien telemetriatietojen seuraaminen olisi myös jatkuvan haavoittuvuuden seurantaratkaisu. Agenttipohjaisilla ratkaisuilla pystytään parantamaan haavoittuvuustietoisuutta, ja niitä voidaan käyttää yrityksissä ilman skannauksiakin. Security Content Automated Protocol (SCAP)-protokollaa tukevat valvontatekniikat voivat parantaa yhteensopivuutta haavoittuvuuksien tarkkailussa (NIST 2018). Open Vulnerability Assessment Language (OVAL) -kieltä ja Common Vulnerabilities and Exposures (CVE) -nimeämisjärjestelmää käyttävillä haavoittuvuusskannereilla saa automaattisesti hyvät tiedot haavoittuvuuksista. Erilaisilla turvallisuustestausharjoituksilla, kuten penetraatiotestaus-, Red Team tai ”Bug Bounty”-harjoituksilla, voisi saada myös hyvää uutta tietoa organisaation haavoittuvuuksista. (NIST 2020.)

3.3.3 CIS Critical Security Controls Version 8

CIS Controls on kansainvälinen vapaaehtoistyöntekijöiden ja -instituutioiden verkosto, jota johtaa Center for Internet Security. Critical Security Controls Versio 8 sisältää 18 ohjeistusta, jotka liittyvät tietoturvallisuuden hallintaan. Jokaista ohjeistusta voidaan soveltaa kolmella eri tasolla, joita kutsutaan toteutusryhmiksi: IG1, IG2 ja IG3. IG1 on tarkoitettu pienille ja keskisuurille yrityksille. IG2-tason yrityksillä on omia työntekijöitä, jotka vastaavat IT-infrastruktuurin hallinnasta ja suojaamisesta. IG2-suojauksia käyttävät yritykset käsittelevät yleensä arkaluontoisia asiakas- tai yritystietoja ja selviävät lyhyistä pal-

velukatkoksista. IG3-suojaustason yrityksillä on kyberturvallisuuden asiantuntijoita eri osa-alueilla. IG3-yrityksen on huomioitava palveluiden saatavuus sekä kriittisten tietojen turvallisuus ja eheys. (CIS 2021.)

CIS:n ohjeistus 07 käsittelee jatkuvaa haavoittuvuuksien hallintaa. Ohjeistuksen mukaan skannaustoimintojen tiheyden pitäisi lisääntyä, kun yrityksen omaisuuden monimuotoisuus lisääntyy, jotta voidaan ottaa huomioon kunkin valmistajan vaihtelevat päivitysjaksot. Haavoittuvuuksien tarkistustyökaluissa kannattaa käyttää todennettuja skannauksia, jotta saadaan kattavammat tulokset. Korjausta vaativien haavoittuvuuksien käsittely kannattaa tehdä tiketöintijärjestelmän kautta, jos mahdollista, jotta haavoittuvuuksien korjaamisen edistymistä voidaan seurata ja tuoda helpommin esille myös ylimmälle johdolle. (CIS 2021.)

Valitessaan korjattavia haavoittuvuuksia tai korjauksia, yrityksen tulisi täydentää NIST:n yleistä haavoittuvuuspisteytysjärjestelmää (CVSS) tiedoilla, jotka koskevat haavoittuvuutta hyödyntävän uhkatekijän todennäköisyyttä tai hyväksikäytön mahdollisia vaikutuksia yritykseen. Tietoa hyväksikäytön todennäköisyydestä tulee myös päivittää säännöllisesti uusimpien uhkatietojen perusteella. Uuden haavoittuvuuden hyödyntämisen tai haavoittuvuuden hyödyntämiseen liittyvän uuden tiedon julkaiseminen saattaa muuttaa korjaustarpeen prioriteettia. Saatavilla on erilaisia kaupallisia järjestelmiä, joiden avulla yritys voi automatisoida ja ylläpitää tätä prosessia skaalautuvalla tavalla. (CIS 2021, 28.)

3.3.4 OVMG - OWASP Vulnerability Management Guide

OVMG-oppaan tavoitteena on vähentää tietoturvapuutteita esittämällä monimutkaiset ongelmat yksinkertaisilla, toistuvilla jaksoilla: havaitseminen, raportointi ja korjaaminen. Käsikirja keskittyy syklisen prosessihallinnan kehittämiseen. Menettelytapoja omaksuttaessa kehotetaan aloittamaan perusasioista ja sitten kehittämään yksittäisiä toimintoja asteittain ja johdonmukaisesti syklisissä vaiheissa. Jokainen sykli on luokka, joka koostuu neljästä päämekanismista. Jokainen työnkulku on prosessi, johon on liitetty tehtäväluettelo. Tämä opas käy melko tarkkaan haavoittuvuuden hallintaa läpi, joten se tarjoaa useita selkeitä keinoja haavoittuvuuksien hallintaprosessiin. Opasta ei käydä

tässä tutkimuksesta kuitenkaan tarkkaan läpi, mutta sitä on käytetty lähteenä tämän tutkimuksen toimintojen kuvaamiseen jonkin verran (OWASP 2020.)

3.4 KPI-mittari tavoitteiden seurannassa

KPI-mittareiden käyttö sopii hyvin prosessissa määriteltyjen tavoitteiden seurantaan, mutta niiden suunnittelu vaatii asiantuntemusta. Seuraavaksi listataan erilaisia ominaisuuksia, joita hyvin suunniteltujen ja tehokkaiden KPI-mittareiden tulisi täyttää:

1. Yhdenmukaisuus. KPI-mittareiden tulisi olla aina organisaation strategian ja tavoitteiden mukaisia.
2. Ennustettavuus. KPI-mittarit ovat organisaation suorituskyvyn indikaattoreita, jotka mittaavat liiketoiminnan arvoa.
3. Toimintakyky. Mittareiden tulosten täytyisi olla ajantasaisia sekä käytännöllisiä, jotta henkilöstö voi parantaa niiden perusteella suoritustaan.
4. Määrä. Mittareita ei ole syytä tehdä liikaa, ettei niiden seuraaminen ja noudattaminen kuluttaisi liikaa henkilöstön energiaa.
5. Selkeä ja ymmärrettävä. Mittareiden tulisi olla yksinkertaisia sekä helposti ymmärrettäviä.
6. Tasapainoinen ja toisiinsa tukeutuva. KPI-mittareiden tulisi olla tasapainossa toisiinsa nähden, jos niitä on useita.
7. Muutosten aikaansaanti. KPI-mittarin käyttöönoton tulisi käynnistää positiivisten muutosten ketjureaktio organisaatiossa, erityisesti silloin kun sitä seurataan toimitusjohtajatasolla.
8. Standardoitu. KPI-mittareiden tulisi perustua yhtenäisiin sääntöihin, laskelmiin sekä määritelmiin, jotta ne voidaan integroida yrityksen muihinkin mittaristoihin.
9. Johdettu asiayhteydestä. KPI-mittari ohjaa toimintaa hyödyntämällä suorituskyvylle asetettuja tavoitteita ja kynnysarvoja, jotta henkilöstö voi arvioida niiden edistymistä ajan kuluessa.
10. Motivoi kannustimilla. Yritys voi tehostaa KPI-mittareiden toimintaa liittämällä niihin erillisiä kannustimia ja vaikka taloudellisia korvauksia. Kannustimien käyttö sopii vain helposti ymmärrettäviin ja vakaisiin mittareihin.
11. Merkityksellisyys. KPI-mittareita täytyy tarkistaa ja uudistaa säännöllisesti, koska ne saattavat menettää ajan myötä merkityksensä.
12. Omistajuus. KPI-mittarin omistaa liiketoiminnan puolella oleva tulosvastuullinen henkilö tai ryhmä. (Kerzner 2017.)

OWASP:n OVMG-oppaan mukaan haavoittuvuuksia voisi kuvata KPI-mittarilla, joka esittää haavoittuvien löydösten määrän ja prosenttiosuuden. Samoja tietoja voisi myös täydentää ottamalla mukaan haavoittuvuuden vakavuus- ja CVSS-tiedon. Tuoreimmille haavoittuvuuksille voisi tehdä samanlaisen mittarin. Lisäksi muita seurantatietoja voidaan jakaa alaryhmiin seuraavien rajausten mukaan: vakavuusluokitus, toiminnallinen ryhmä, toimintaympäristö, CVE-

numerointi, haavoittuvuustyyppi ja ikä. Mittarina voisi olla myös haavoittuvien löydösten hyödynnettävyys vakavuuden, lukumäärän tai prosenttiosuuden mukaan. Yksi näkökulma olisi esittää trendikäyrää käyttämällä KPI:tä, jolla on merkitystä yrityksen riskien ja vaatimustenmukaisuuden kannalta. (OWASP 2020, 9.)

3.5 Haavoittuvuuksiin liittyvät käsitteet

Yleisesti haavoittuvuudella tietotekniikassa tarkoitetaan ohjelmistossa tai järjestelmässä olevaa aukkoa, virhettä tai puutetta, joka mahdollistaa hyökkäyksen järjestelmään. Jos ohjelmistossa on piilevä haavoittuvuus, useimmiten ohjelmiston toimittaja tekee ohjelmistoon korjaavan päivityksen ja julkaisee sen. Tietokoneissa olevat turhat avoimet portit, käyttöjärjestelmä- ja ohjelmistovalinnat vaikuttavat haavoittuvuuksien määrään oleellisesti. Näitä voi tuoda esille hyvillä haavoittuvuusskannereilla ja pienentää haavoittuvuuksia sitten tarkkaan mietityllä konfiguroinnilla, poistamalla turhat ohjelmat, pitämällä päivitykset kunnossa ajurien, sovellusten ja käyttöjärjestelmän osalta ja tietysti verkkotasolla voi tehdä monenlaisia lisäsuojauksia. (Manzuik 2006, 8–9.)

Internetin kautta voi etsiä helposti useista paikoista tietoja haavoittuvuuksista. Seuraavissa kappaleissa käydään läpi tärkeimmät haavoittuvuuksien selvittelyyn sopivat lähteet. Eri lähteet ovat painottuneet eri alueille ja tarjoavat erilaista tietoa, mutta tietoturva-ammattilaisen on syytä olla niistä kaikista tietoinen saadakseen hyvät valmiudet haavoittuvuuksien tutkimiseen.

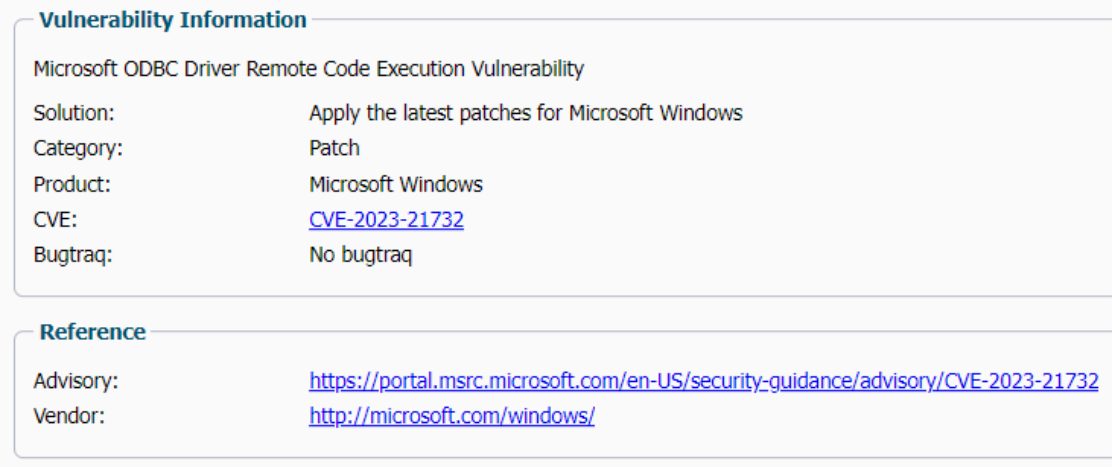
NVD

NVD (engl. National Vulnerability Database) on Yhdysvaltain hallituksen kokoelma haavoittuvuuksien hallintatiedoista, jotka perustuvat standardeihin ja edustavat Security Content Automation Protocol (SCAP) -protokollaa. NVD:tä ylläpitää Yhdysvaltain standardisointi- ja teknologiainstituutti (engl. National Institute of Standards and Technology, NIST). Näillä tiedoilla mahdollistetaan haavoittuvuuksien hallinnan, turvallisuuden mittaamisen ja vaatimustenmukaisuuden automatisointi. NVD sisältää tietokantoja turvatarkistusluetteloista, tietoturvaan liittyvistä ohjelmistovirheistä, virheellisistä määrityksistä, tuotteiden nimistä ja vaikutusmittareista. (NIST 2022a.)

CVE

CVE (engl. Common Vulnerabilities and Exposures) on yhdysvaltalaisen Mitren hallinnoima haavoittuvuuksien hallintaan kehitetty järjestelmä. CVE-järjestelmän tehtävänä on tunnistaa, määritellä ja luetteloida julkisesti julkistetut kyberturvallisuuden haavoittuvuudet. CVE hoitaa haavoittuvuustietojen välityksen työkalujen, tietokantojen ja ihmisten välillä. NVD:n haavoittuvuustietokanta on synkronoitu CVE:n haavoittuvuuslistojen kanssa. (CVE 2023a.)

Useat haavoittuvuusskannerit tarjoavat haavoittuvuustiedon yhteydessä viittauksen julkaistuun haavoittuvuustietoon eli CVE-tunnisteeseen. Kuva 10 on tästä esimerkki, jossa Outpost24-ohjelma näyttää löydetyn haavoittuvuuden raporttitiedoissa CVE-tunnisteen linkkitiedon. CVE-tunniste muodostuu CVE-alkuosasta, vuosiluvusta ja juoksevasta numerosta (CVE 2023b).



Vulnerability Information

Microsoft ODBC Driver Remote Code Execution Vulnerability

Solution:	Apply the latest patches for Microsoft Windows
Category:	Patch
Product:	Microsoft Windows
CVE:	CVE-2023-21732
Bugtraq:	No bugtraq

Reference

Advisory:	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21732
Vendor:	http://microsoft.com/windows/

Kuva 10. Esimerkki Outpost24-ohjelman CVE-linkistä ODBC Driver Remote Code Execution-haavoittuvuudelle

CVE-linkin kautta avautuu www-sivu, johon on koottu kyseisestä haavoittuvuudesta kerätyt tiedot.

CWE

CWE (Common Weakness Enumeration) on yhteisön kehittämä luokittelujärjestelmä ohjelmistojen ja laitteistojen heikkouksista ja haavoittuvuuksista. Sen tavoitteena on tunnistaa ohjelmisto- ja laitteistovikoja ja luoda automaattisia työkaluja, joiden avulla voidaan tunnistaa, korjata ja ehkäistä kyseiset puut-

teet. Heikkouksien vakavuus voidaan pisteyttää käyttämällä heikkouksien pisteytysjärjestelmää CWSS (Common Weakness Scoring System). (CWE 2022.)

CWE:tä ylläpitää tällä hetkellä MITRE Corporation, jonka sivustolta on saatavissa CWE-listaukset. Jokainen yksittäinen CWE edustaa yhtä haavoittuvuustyyppiä. NVD hyödyntää CWE:tä luokitusmekanismina CVE-haavoittuvuuksien pisteytyksessä ja haavoittuvuustyyppien erottelussa. (NIST 2022c.)

OWASP

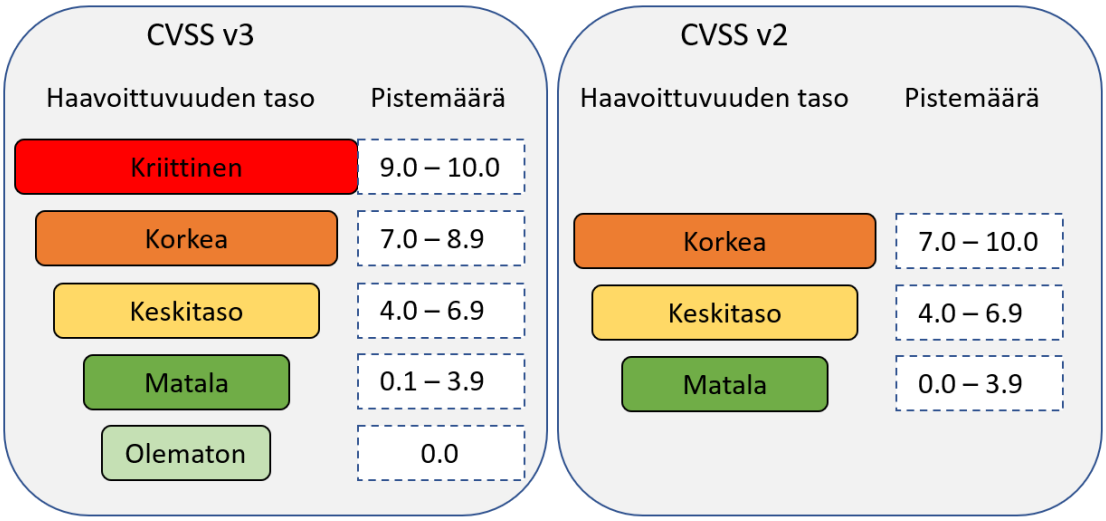
OWASP (Open Web Application Security Project) on verkkoyhteisö, joka tuottaa ilmaiseksi artikkeleita, menetelmiä, dokumentaatiota, työkaluja ja teknologioita tietoturvan alalla. Sitä johtaa OWASP Foundation, joka on voittoa tavoittelematon järjestö. (OWASP 2023a.)

OWASP tarjoaa muun muassa verkkosovellusten haavoittuvuuksien etsimiseen ilmaisen OWASP ZAP (Zed Attack Proxy) penetraatiotestaustyökalun, jota päivitetään aktiivisesti vapaaehtoisvoimin. Se on suunniteltu kokeneiden tietoturva-alan ihmisten käyttöön. (OWASP 2023b.)

CVSS - Haavoittuvuuden vakavuuden luokittelu

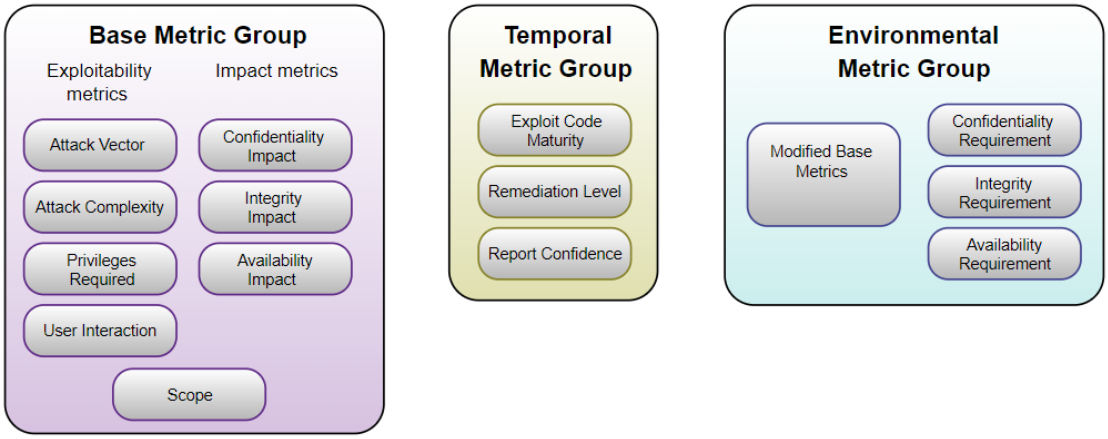
Haavoittuvuuden vakavuuden luokittelu lähtee useimmiten CVSS-arvosta. Se on maailmanlaajuinen, valmistajariippumaton haavoittuvuuksien vakavuuden luokitusmenetelmä. Sen tarkoituksena on esittää loppukäyttäjälle selkeä lukuarvo, joka ilmaisee haavoittuvuuden vakavuuden ja sillä perusteella voidaan priorisoida korjaustoimenpiteet organisaation sisällä. Tätä järjestelmää ylläpitää FIRST-järjestö (engl. Forum of Incident Response and Security Teams). Suomessa siihen kuuluu Kyberturvallisuuskeskus. (Laurio 2014.)

NVD tuottaa CVSS-pisteytykset lähes kaikille tunnetuille haavoittuvuuksille. NVD tukee sekä v2.0 että v3.x -standardien CVSS-pisteytystä. CVSS-arvo on määritelty välille 0,0–10,0. Kuva 11 esittää pistemääriä vastaavat haavoittuvuuksien tasot. (Vulnerability Metrics s.a.)



Kuva 11. Haavoittuvuuksien tasot ja pistemäärät CVSS-järjestelmässä

Haavoittuvuuden kokonaispistemäärä lasketaan monen eri tekijän perusteella. CVSS v3:ssa perusmittaristo koostuu kahdeksasta perustekijästä. Lisäksi laskennassa huomioidaan ajalliset ja ympäristöön sidotut tekijät (FIRST 2022). Kuva 12 näyttää FIRST:n määrittämät CVSS-järjestelmän pisteytykseen vaikuttavat tekijät.



Kuva 12. CVSS-järjestelmän pisteytykseen vaikuttavat tekijät (FIRST 2022)

CVSS-arvojen määritykseen käytetyt perustekijät kuvaavat haavoittuvuudesta seuraavanlaisia ominaisuuksia:

1. Hyökkäystapa (Attack Vector)
2. Hyökkäyksen monimutkaisuus (Attack Complexity)
3. Vaaditut käyttöoikeudet (Privileges Required)
4. Käyttäjän vuorovaikutus (User Interaction)
5. Luottamuksellisuus (Confidentiality Impact)
6. Eheys (Integrity Impact)
7. Saatavuus (Availability Impact) (FIRST 2022.)

CVSS-arvo voi muuttua, jos esimerkiksi aiemmin todetulle haavoittuvuudelle julkaistaan esimerkiksi uusi tehokkaampi hyödynnettävyystapa (CIS 2021, 28). Ajallinen mittaristo koostuu tekijöistä, jotka voivat muuttaa pisteytystä ajan myötä:

1. Hyökkäyskoodin kypsyys (Exploit Code Maturity)
2. Haavoittuvuuden korjattavuus (Remediation Level)
3. Haavoittuvuustiedon luotettavuus (Report Confidence) (FIRST 2022.)

Ympäristöön sidotut tekijät ovat ympäristö- ja organisaatiokohtaisia. Tämä mittaristo antaa mahdollisuuden säätää haavoittuvuuden vakavuusarvoa omaan organisaation sopivaksi, jos halutaan määritellä tietyille haavoittuvuuksille erilaiset prioriteetit. Vakavuusarvoa voidaan säätää perusmittariston ominaisuuksien, luottamuksellisuuden, eheyden ja saatavuuden turvaamisen näkökulmista eri tasoille. CVSS:n dokumentaatio tarjoaa tarkat laskukaavat pisteytyksille, ja tätä varten löytyy myös valmiita CVSS-laskureita. (FIRST 2022.)

Useimmat kaupalliset skannausohjelmat hakevat tuoreimmat CVSS-arvot automaattisesti NVD:n kansainvälisestä haavoittuvuuksien tietokannasta (NIST 2022b).

3.6 Haavoittuvuuksien skannausjärjestelmät

Tässä luvussa kuvataan lähinnä yrityskäyttöön tarkoitettuja kaupallisia ohjelmia yleisellä tasolla. Haavoittuvuusskanneri on tietokoneohjelma, joka on suunniteltu arvioimaan tietokoneiden, verkkojen tai sovellusten tunnettuja heikkouksia. Skannereita käytetään tietyn järjestelmän heikkouksien havaitsemiseen. Niitä käytetään sellaisten haavoittuvuuksien tunnistamiseen ja havaitsemiseen, jotka johtuvat virheellisistä määrityksistä tai virheellisestä ohjelmoinnista verkkopohjaisessa resurssissa, kuten palomuurissa, reitittimessä, verkkopalvelimessa ja sovelluspalvelimessa. Nykyaikaiset skannerit ovat tyypillisesti saatavilla SaaS-muodossa (Software as a Service), ne tarjotaan Internetin kautta ja toimitetaan verkkosovelluksena. (NIST 2022d.)

Haavoittuvuusskannauksien ensisijaisena etuna on se, että sillä saa nopean ja laadukkaan katsauksen kohdealueen haavoittuvuuksista. Skannaukset ovat tunkeutumistestaukseen (engl. penetration testing) verrattuna edullisempi ja

nopeampi ratkaisu, vaikka ne eivät vastaakaan täysin toisiaan. Skannaukset voidaan helposti automatisoida toimimaan halutuin aikavälein. (Securitymetrics s.a.)

Haavoittuvuusskannauksien haittapuolina voidaan todeta, että kaupallisten haavoittuvuusskannereiden käyttö maksaa jonkin verran ja niiden ylläpitoon ja tulosten tarkasteluun joudutaan käyttämään työresursseja. Jotkut skannerit tuottavat paljon ”vääriä positiivisia” -tuloksia ja niiden läpikäynti vie aikaa, mutta jotkut kehittyneemmät skannerit osaavat myös poistaa näitä turhia löydöksiä hyvin automaattisesti. Kaikki skannerit eivät kerro, voiko haavoittuvuutta hyödyntää ja sen tutkiminen vie aikaa. Osa skannereista osaa kuitenkin tämänkin kertoa raporteissaan. (Securitymetrics s.a.; Outpost24 2023a.)

Todentamattomat (eng. unauthenticated) tarkistukset ovat menetelmä, joka voi johtaa suureen määrään vääriä positiivisia tuloksia, eikä se pysty antamaan yksityiskohtaisia tietoja käyttöjärjestelmästä ja asennetuista ohjelmistoista. Tätä menetelmää käyttävät tyypillisesti tietoturva-analyytikot, jotka yrittävät selvittää ulkoisesti saatavilla olevat tiedot. Tähän menetelmään joudutaan joskus tyytymään, jos kohteisiin ei ole saatavilla erillisiä testaustunnuksia sisäänkirjautumista varten. (NIST 2022d.)

Todennettujen (eng. authenticated) tarkistusten avulla skanneri voi hyödyntää suoraan verkkopohjaisia resursseja käyttämällä etähallintaprotokollia, kuten Secure Shell (SSH) tai Remote Desktop Protocol (RDP), ja todentaa käyttämällä toimitettuja järjestelmän valtuustietoja. Tämän ansiosta haavoittuvuusskanneri voi käyttää matalan tason tietoja, kuten tiettyjä palveluita ja isäntäkäyttöjärjestelmän määritystietoja. Sen jälkeen se pystyy tarjoamaan yksityiskohtaisia ja tarkkoja tietoja käyttöjärjestelmästä ja asennetuista ohjelmistoista, mukaan lukien määritysongelmista ja puuttuvista tietoturvakorjauksista. (NIST 2022d.)

Edellä mainitut kirjautumisoikeudet ja porttiavaukset skannerille aiheuttavat samalla uuden turvallisuusriskin, koska joku muukin voisi hyödyntää tätä ylimääräistä kirjautumismahdollisuutta ja avattuja portteja. Siksi kirjautumistunnuksen täytyy olla vaikea ja hyvässä tallessa. Laajemmissa verkoissa rajauksia yhteydenottoon voi tehdä palomuurin avulla. SSH-yhteyksissä kannattaa

käyttää esimerkiksi RSA-avainta autentikointiin (IBM 2021). Yhteyden turvallisuutta voi varmistaa lisää myös IP-rajauksella, niin että yhteys saa tulla vain yhdestä IP-osoitteesta eli skannerin suunnasta (StackExchange 2021). Tutkija huomasi omassa työssään, että tämä IP-osoitteen rajauksen käyttö RSA-avaimessa voi aiheuttaa myös järjestelmien vaihdon yhteydessä lisätöitä. Kohteissa olevat RSA-avaimet joudutaan päivittämään jokaiseen kohteeseen, jos skanneri on vaihdettu myöhemmin toiseen IP-osoitteeseen esimerkiksi tuotteen vaihdon yhteydessä. Tallaisissa järjestelmävaihdoissa olisi siis helpointa pyrkiä käyttämään samaa IP-osoitetta uudessakin skannerissa.

Haavoittuvuusohjelmiston kohteena voi olla yksi tai useampi kohde samaan aikaan, sisäinen verkko tai internet. Haavoittuvuusskannerit käyttävät seuraavanlaisia toimintatapoja:

- Kartoitetaan aktiiviset kohteet. Selvitetään, antaako kohde ICMP-, ARP, tai TCP-vastauksen. ICMP (engl. Internet Control Message Protocol) on TCP/IP-pinon kontrolliprotokolla, jolla lähetetään viestejä koneesta toiseen. ARP (engl. Address Resolution Protocol) on protokolla, jolla Ethernet-verkoissa selvitetään loogista osoitetta vastaava fyysinen osoite. TCP (engl. Transmission Control Protocol) on tietoliikenneprotokolla tietokoneiden väliseen luotettavaan tiedonsiirtoon. (Kabelova ym. 2006.)
- Tehdään porttiskannaus eli tunnistetaan kohteen TCP- ja UDP-portit ja niiden tilat. Jos porttiskannaus löytää NetBIOS / SMB-portit 139 tai 445, niin se tietää kohteen olevan Windows-laite. UNIX-kone tunnistetaan yleensä portin 22 kautta. (IBM 2022b.)
- Tunnistetaan aktiiviset palvelut (SSH, HTTP, FTP ja niin edelleen).
- Käynnistetään turvamoduulit.
- Yritetään kirjautua kohteeseen sisään, jos toimenpide on aktivoitu.
- Luodaan turvallisuusraportti. (Frwiki s.a.)

Haavoittuvuusskanneri pystyy teoriassa testaamaan minkä tahansa IP-osoitteella toimivan kohteen, joita voi olla muun muassa: tietokone, palvelin, reititin, kytkin, palomuuri, älypuhelin, verkkosivusto, automaatti, robotti, kone tai IP-kamera. (Frwiki s.a.)

Haavoittuvuusskannerit voidaan luokitella seuraaviin tyyppeihin niiden toiminnan perusteella:

- Pilvipohjaisia (cloud-based) haavoittuvuusskannereita käytetään haavoittuvuuksien etsimiseen pilvipohjaisista järjestelmistä, kuten verkkosovelluksista, WordPressistä ja Joomlasta (PhoenixNAP 2020).

- Palvelinpohjaisia (host-based) haavoittuvuusskannereita käytetään haavoittuvuuksien etsimiseen yksittäisestä tietokoneesta, verkkolaitteesta, kytkimestä, runkoreitittimestä tai järjestelmästä (PhoenixNAP 2020).
- Verkkopohjaisia (network-based) haavoittuvuusskannereita käytetään sisäisen verkon haavoittuvuuksien etsimiseen etsimällä avoimia portteja. Avoimissa porteissa toimivat palvelut määrittelevät työkalun avulla, onko niissä haavoittuvuuksia vai ei. (PhoenixNAP 2020.)
- Tietokantapohjaisia (database-based) haavoittuvuusskannereita käytetään haavoittuvuuksien etsimiseen tietokannan hallintajärjestelmistä. Tietokannat ovat jokaisen arkaluonteista tietoa tallentavan järjestelmän selkäranka. Haavoittuvuustarkistus suoritetaan tietokantajärjestelmissä SQL-injektion kaltaisten hyökkäysten estämiseksi. (PhoenixNAP 2020.)
- Langattomat (wireless) haavoittuvuusskannerit (SoftwareTestingHelp 2023).

Haavoittuvuusskannerit voivat tarjota laajan valikoiman ominaisuuksia ja tässä on lueteltuna muutamia markkinoiden yleisimpiä ominaisuuksia:

- Verkkokartoitusominaisuudet (Network mapping) tarjoavat visuaalisen näkymän verkkoresursseista, mukaan lukien päätepisteet, palvelimet ja mobiililaitteet.
- Web-tarkastusominaisuuksia (Web inspection) käytetään arvioimaan verkkosovelluksen turvallisuutta saatavuuden näkökulmasta. Tämä sisältää sivuston navigoinnin, taksonomiat, skriptit ja muut verkkopohjaiset toiminnot.
- Vikojen ja ongelmien seurantatoiminto (Defect tracking) auttaa käyttäjiä löytämään ja dokumentoimaan haavoittuvuuksia ja jäljittämään ne niiden lähteeseen ratkaisuprosessin aikana.
- Vuorovaikutteisen skannauksen (Interactive scanning) tai interaktiivisten sovellusten suojaustestausominaisuuksien avulla käyttäjä voi olla suoraan mukana skannausprosessissa, seurata testejä reaaliajassa ja suorittaa ad hoc -testejä.
- Kehäskannaus (Perimeter scanning) analysoi verkko- tai pilviympäristöön yhdistetyt kohteet haavoittuvuuksien varalta.
- Black box -skannauksella tarkoitetaan hakkerin näkökulmasta tehtyjä testejä. Black box -skannaus tutkii toimivia sovelluksia ulkoisesti haavoittuvuuksien, kuten SQL-injektion tai XSS:n varalta.
- Jatkuvan valvonnan (Continuous monitoring) avulla käyttäjät voivat määrittää toiminnon ja unohtaa sen. Tämän ominaisuuden avulla skannerit voivat olla toiminnassa koko ajan ja ne varoittavat käyttäjiä uusista haavoittuvuuksista.
- Vaatimustenmukaisuuteen (Compliance monitoring) liittyvien valvontaominaisuuksien avulla seurataan tietojen laatua ja lähetetään hälytyksiä rikkomuksista tai väärinkäytöstä.
- IT-kohteiden etsintä (Asset Discovery) ominaisuudet paljastavat käytössä olevat sovellukset ja resurssiliikenteeseen, pääsyyn ja käyttöön liittyvät trendit.
- Lokidokumentaatio ja raportointiominaisuudet tarjoavat tarvittavat raportit vianmääritystä ja auditointia varten.
- Uhkatietojen (Threat intelligence) käsittelyominaisuudet integroivat tai tallentavat tietoja, jotka liittyvät yleisiin uhkiin ja niiden ratkaisutapoihin.

- Riskipisteytys- ja riskianalyysiominaisuudet tunnistavat, pisteyttävät ja priorisoivat tietoturvariskit, haavoittuvuudet ja hyökkäysten ja rikkomusten vaikutukset vaatimustenmukaisuuteen.
- Laajennettavuus- ja integrointiominaisuudet mahdollistavat alustan tai tuotteen laajentamisen lisäominaisuuksien ja toimintojen lisäämiseksi. (G2 2023.)

Haavoittuvuusskannereilla voi olla monenlaisia käyttäjiä. Ilmaisia tai edullisimpia versioita voi käyttää kotonakin melko pienellä opettelulla. Haavoittuvuusskannereiden tyypillisimpiä käyttäjiä yrityspuolella ovat IT-ammattilaiset, kyberturvallisuusinsinöörit, tietoturva-analyytikot, penetraatiotestaajat ja verkkopuolen järjestelmävalvojat (Sourceforge 2023).

Haavoittuvuusskannerin valintaperusteita

Haavoittuvuusskannerin valintaa tehdessä kannattaa tutkia, löytyykö siitä halutut ominaisuudet, tarjoaako se riittävästi kapasiteettia yrityksen verkkojen testaukseen ja minkälaisia skannauskustannukset ovat. Seuraavaan listaan on koottu asioita, jotka kannattaa huomioida haavoittuvuusskanneria valitessa:

- Huomioidaan, minkä tyyppisiä haavoittuvuusskannauksia skannerilla halutaan tehdä. (PhoenixNAP 2020).
- Varmistetaan, että pystyykö skannerilla skannaamaan sekä sisä- että ulkoverkon (Securitymetrics 2015a).
- ASV- ja ulkoverkkoskannauksia saa tehdä vain PCI hyväksytty skannausvalmistaja (engl. PCI Approved Scanning Vendor) (PCI DSS GUIDE 2020).
- Täyttääkö skanneri PCI DSS-vaatimukset ja vaaditaanko niitä yrityksessä? Ilmaiset haavoittuvuusskannerit eivät yleensä täytä näitä vaatimuksia (Securitymetrics 2015b). Kaikkien yrityksien, jotka tallentavat, käsittelevät tai lähettävät kortinhaltijatietoja, on oltava PCI DSS:n mukaisia (ControlCase 2021).
- Halutaanko haavoittuvuusskanneri integroida johonkin organisaation käyttämiin järjestelmään ja löytyykö siihen tuki (Astra 2023)?
- Missä skanneriohjelmisto ja skannaustulokset sijaitsevat?
- Voiko skanneria käyttää sekä paikallisella palvelimella että pilvessä? Jotkut yritykset välttävät pilvipohjaista tallennuspaikkaa.
- Kuinka tulosten varmuuskopiointi on toteutettavissa?
- Kuinka usein skannerin päivitykset tapahtuvat (Securitymetrics 2015a)?
- Mitä liitännäisiä skanneri tarjoaa ja toimivatko niiden päivitykset riittävän hyvin (Securitymetrics 2015a)?
- Osaako skanneri poistaa turhat false-positive-haavat automaattisesti, jos käyttäjä niin haluaa (Astra 2023)?
- Kuinka isoa haavoittuvuuskirjastoa skanneri hyödyntää (Securitymetrics 2015a)?

- Onko ohjelmisto riittävän helppokäyttöinen?
- Saako järjestelmää testata ennen ostopäätöstä (Securitymetrics 2015a)?
- Minkä tasoinen dokumentointi järjestelmään löytyy?
- Miten yksityiskohtaisia ja tasokkaita haavoittuvuusraportit ovat ja antavatko ne korjausohjeita (Securitymetrics 2015a)?
- Saako raportit lähetettyä automaattisesti eteenpäin?
- Minkälaiset ajastusominaisuudet skannerista löytyvät?
- Pystyykö skanneri tutkimaan useampaa kohdetta yhtä aikaa ja pystyykö skannereita lisäämään suuriin verkkoympäristöihin rinnakkaisajoa varten?
- Kuinka isoja verkkokokonaisuuksia skanneri voi hallita maksimissaan?
- Millainen on skannausjärjestelmän oma suojaustaso? Jos hakkerit näkevät skannaustulokset ja kohteet, he tietävät samalla järjestelmän heikkoudet. (Securitymetrics 2015a.)
- Onko teknistä tukea saatavilla, minkälaisella vasteajalla ja maksaako sen palvelu? (Astra 2023.)
- Mikä on järjestelmän hankintahinta tai lisenssien hinta yrityksen skannausmäärillä? (Astra 2023.)

Edellä olevassa listassa ilman lähdeviitettä olevilla riveillä oleva tieto perustuu tutkijan omiin havaintoihin haavoittuvuusskannereiden tärkeistä ja käyttökelpoisista ominaisuuksista. Kaikki listassa esille tuodut toiminnot eivät ole tarpeen tai pakollisia kaikille. Listan tarkoitus on tuoda esille eri näkökulmat ja ominaisuudet, jotta haavoittuvuusskannerin valinta tulisi tehtyä harkiten.

Ilmaiset haavoittuvuusskannerit

Tähän kappaleeseen on koottu muutamia lähinnä kotikäyttöön tai pienen yrityksen satunnaiseen käyttöön suunnattuja ilmaisia skannausohjelmia ja esitelty ne lyhyesti. Näille skannereille on yhteistä se, että ne on helppo ottaa käyttöön, mutta niiden tarjoamat ominaisuudet ovat melko rajalliset kaupallisiin skannereihin verrattuna. Näistäkin ohjelmistoista suurin osa osaa etsiä ja varoittaa monista erilaisista uhista ja haavoittuvuuksista: niitä ovat avoimet portit, heikot salasanat sekä oletussalasanat, vanhentuneet ohjelmistot, haavoittuvat asetukset sekä vanhentuneet tekniikat. Verkkoskannerin asennus kannattaa, jos käyttäjä ei ole täysin tietoinen verkkoonsa kytketyn tietokoneen, mobiililaitteen, reitittimen, digiboksin, äly-tv:n, verkkotulostimen tai valvontakameran asetuksista, ohjelmistoversiosta ja käyttäjätunnuksesta. (Mikrobitti 2019.)

Nessus Essentials on ilmainen ja hyviä ominaisuuksia sisältävä haavoittuvuusskanneri maksimissaan 16 IP-osoitteen verkolle, joka tarjoaa samalla mahdollisuuden tutustua Tenablen ekosysteemiin. Ohjelma on päivitettävissä myöhemmin kattavampaan ja maksulliseen Nessus Professional-ohjelmistoon. Tuotteen optimointia varten on mahdollista saada apua Tenable-yhteisön kautta. (Tenable 2019.)

Bitdefender Home Scanner on ilmainen ja nopea verkkoskanneri, joka kartoittaa verkkolaitteet, skannaa portit ja heikot salasanat. Bitdefender Home Scanner tarkistaa kuinka laitteista kerätyt tiedot korreloivat sen online-haavoittuvuustietokannan kanssa. Loppuraportissaan se kertoo haavoittuneet laitteet, heikot salasanat ja tarjoaa yksityiskohtaisia suojaussuosituksia. (Bitdefender 2023.)

Nmap (Network Mapper) on avoimen lähdekoodin tietoturvaskanneri verkkojen ja tietoturvapuutteiden tarkasteluun. Se on ilmainen, hyvin dokumentoitu ja saatavissa monelle käyttöjärjestelmälle. Nmap:n skannauksella saa selville laitteiden suojaustasosta riippuen muun muassa laitteiden IP-osoitteet, käyttöjärjestelmätiedot, sovellusten nimi- ja versiotiedot ja porttitiedot. Nmap toimii komentorivin kautta, mutta sille löytyy myös edistyneempi graafinen versio Zenmap. (Nmap s.a.)

Zed Attack Proxy (ZAP) on ilmainen avoimen lähdekoodin haavoittuvuus- ja penetraatiotestaustyökalu, joka on kehitetty OWASP:ssa (Open Web Application Security Project). ZAP on suunniteltu erityisesti verkkosovellusten testaukseen, ja se on sekä joustava että laajennettavissa. Se on saatavilla seuraaville käyttöjärjestelmille: Windows, Linux ja macOS. (ZAP 2023.)

ZAP tarjoaa seuraavat testausominaisuudet:

- Haavoittuvuuksien arviointi: Järjestelmä tarkistetaan ja analysoidaan tietoturvaongelmien varalta.
- Penetraatiotestaus: Järjestelmä käy läpi analyysin ja hyökkäyksen simuloiduilta haitallisilta hyökkääjiltä.
- Ajonaikainen testaus: Järjestelmä käy läpi analyysia ja tietoturvatestausta loppukäyttäjän koneella.
- Koodin tarkistus: Järjestelmäkoodi käy läpi tarkistuksen ja analyysin, jossa etsitään erityisesti tietoturva-aukkoja. (ZAP 2023.)

ZAP:n ytimessä on niin sanottu "man-in-the-middle-välityspalvelin". Se sijaitsee testaajan selaimen ja verkkosovelluksen välissä, jolloin se voi siepata ja tarkastaa selaimen ja verkkosovelluksen välillä lähetetyt viestit, muokata niiden sisältöä tarvittaessa ja välittää paketit sitten edelleen kohteeseen. Sitä voidaan käyttää erillisenä sovelluksena ja käyttöjärjestelmäprosessina. Penetraatiotestauksen etuna on se, että se on tarkempi, koska se tuottaa vähemmän vääriä positiivisia tuloksia, mutta sen suorittaminen voi viedä aikaa. Väärillä positiivisilla (engl. false positive) tarkoitetaan sellaisia tuloksia, jotka ilmoittavat haavoittuvuudesta, jota ei todellisuudessa ole. (ZAP 2023.)

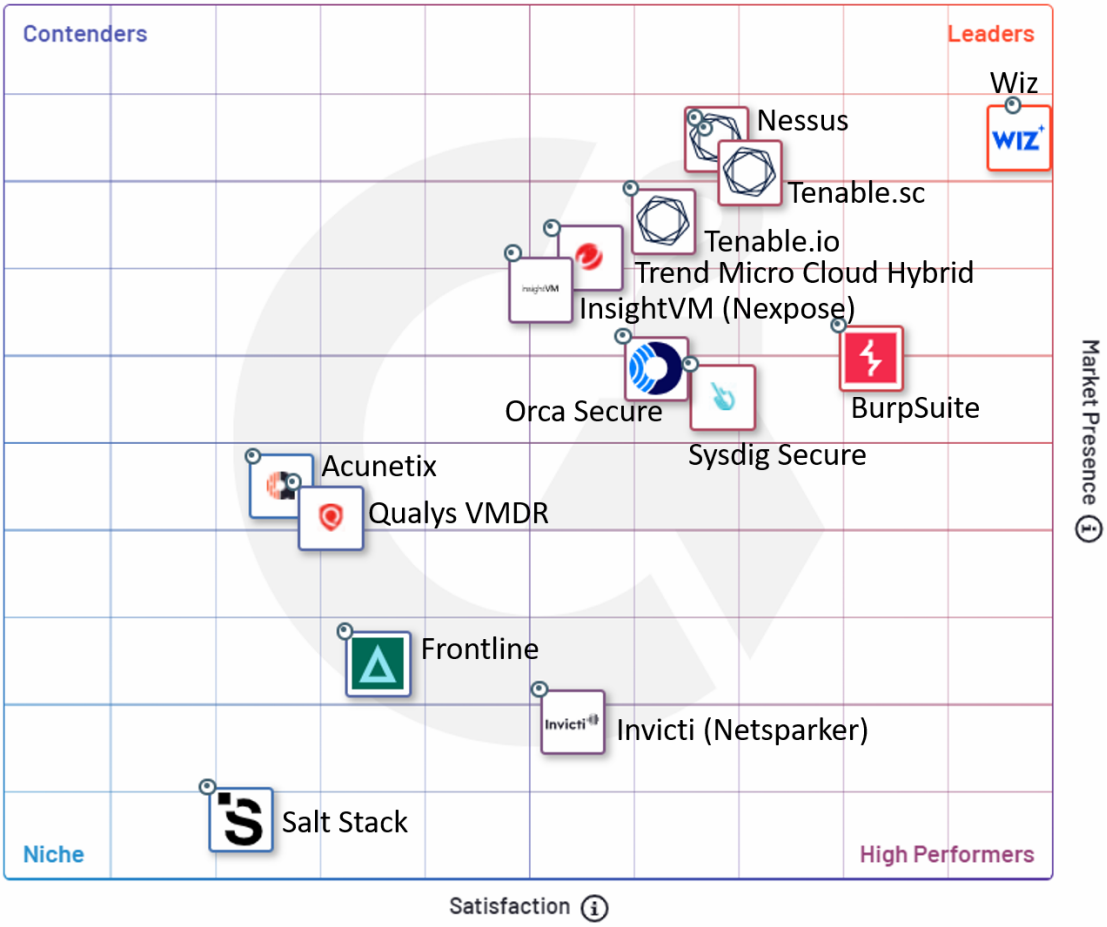
Edellä on mainittu vain pieni osa markkinoiden tarjonnasta ja nämäkin tuotteet olivat melko erilaisia toisiinsa verrattuna. Ilmaisuuden takia niitä voi ainakin helposti koekäyttää ja todeta, että ovatko ominaisuudet riittävät esimerkiksi kotiverkkoon. Koekäytön jälkeen tulee ehkä mieleen lisää ominaisuuksia, joita skannerilta voisi haluta ja sitten siltä pohjalta voi hakea internetistä muita vaihtoehtoja. Laajemmista lisäominaisuuksista ja paremmasta kattavuudesta joutuu usein maksamaan, joten sitten voi harkita myös kaupallisia versioita.

Kaupalliset haavoittuvuusskannerit

Tähän kappaleeseen on koottu yleistietoja suosituimmista yrityskäyttöön suunnatuista haavoittuvuusskannereista ja niiden markkinaosuuksista. Markkinoilta löytyy jo paljon erilaisia haavoittuvuusskannereita, joten tässä työssä ei lähdetä niitä kaikkia vertailemaan yksityiskohtaisesti. Kuva 13 näyttää suuryritysten käyttöön soveltuvien haavoittuvuusskannereiden markkinaosuudet G2:n tutkimuksen mukaan. G2 kokoaa erilaisten ohjelmistojen käyttäjäarvosteluita ja pisteyttää tuotteet niiden perusteella. G2:n tutkimukset eivät ole tieteellisiä, vaan esitetyt tiedot perustuvat yrityksen mukaan mahdollisimman luotettaviin lähteisiin ja arviot kuluttajakokemuksiin. G2 on toiminut vuodesta 2014 lähtien ja käyttäjämäärät ovat olleet vuosittain suuria. (G2 2023a.)

Kuvassa oikeaan yläkulmaan sijoittuvat tämänhetkiset markkinajohtajat. G2:n vuonna 2023 tehdyssä vertailussa oli otettu mukaan 139 haavoittuvuusskanneria, ja enterprise (suuryritys) luokituksella mukana oli 14 tuotetta. Koska vertailussa ei ollut mukana tässä opinnäytetyössä mainittua Outpost24:ia, voidaan todeta, ettei vertailu kata ainakaan kaikkia mahdollisia valmistajia. G2:n

tutkimuksen pisteytykseen liittyvien arvosteluiden määrä vaihteli tässä enterprise-luokassa välillä 12–332 arvostelua tuotteesta riippuen. Johtavassa asemassa olevat tuotteet saivat ääniä 47–332 kappaletta, joten niiden sijoittuminen voidaan arvioida kohtuullisen hyvin suuntaa antavaksi. Yleisesti voidaan sanoa, että keskiarvoa määritellessä otoskoon eli tässä tapauksessa arvosteluiden määrän olisi hyvä olla vähintään 30 kappaletta (Taanila 2019).



Kuva 13. Suuryritysten käyttöön soveltuvien haavoittuvuusskannereiden markkinaosuudet G2:n tutkimuksen mukaan (G2 2023)

Kuva 14 näyttää opinnäytetyön tekijän tekemän koosteen Gartnerin vuonna 2023 tehdyn asiakastutkimuksen tuloksista, jotka koskivat keskikokoisten ja suurten yritysten haavoittuvuusskannerikokemuksia maailmanlaajuisesti. Arvosteluiden pistemääriä tarkastellessa on syytä huomioida myös arvosteluiden määrä. Gartner tuottaa kaupallista puolueetonta tutkimusmateriaalia, mutta ei tee varsinaisesti tieteellistä tutkimusta. Gartnerin tutkimuksia voidaan pitää melko luotettavana aineistona, koska se on kansainvälisesti tunnustettu johtava ICT-teknologian tutkimus- ja konsultointiyritys (Gartner 2023b).

Tuote	Valmistaja	Pisteiden keskiarvo	Arvostelu-määrä
Cycognito	Cycognito	5,0	5
NopSec Unified VRM	NopSec	5,0	3
ArmorCode	ArmorCode	5,0	1
Intruder	Intruder	5,0	1
Balbix Security Cloud	Balbix	5,0	1
StorageGuard	Conntinuity	4,9	12
RidgeBot	Ridge Security	4,8	18
Artic Wolf managed Risk	Arctic Wolf	4,7	39
Falcon Spotlight	CrowdStrike	4,7	13
ESOF	TAC Security	4,7	5
Camel 360	Camel Secure	4,7	3
Frontline Vulnerability Manager	Digital Defense	4,6	39
Nessus	Tenable	4,5	391
Tenable.sc	Tenable	4,5	171
Skybox	Skybox Security	4,5	4
Tenable.io	Tenable	4,4	137
Titania Nipper	Titania	4,5	13
GFI Langaurd	Aurea SMB	4,4	69
Qualys (VMDR)	Qualys	4,4	316
BreachLock	BreachLock	4,4	51
Holm Security VMP	Holm Security	4,4	42
Alert Logic (MDR)	Alert Logic	4,4	30
SecPod SanerNow	SecPod	4,4	21
InsightVM (Nexpose)	Rapid7	4,3	415
WithSecure	WithSecure	4,3	63
Cortex Xpanse Expander	Palo Alto Networks	4,3	31
Microsoft Defender for Endpoint	Microsoft	4,3	25
Greenbone Vulnerability Management	Greenbone Networks	4,3	22
beSECURE	HelpSystems	4,3	18
BeyondTrust Network Security Scanner	BeyondTrust	4,3	9
Tripwire IP360	Tripwire	4,1	82
Outpost24 HIAB	Outpost24	4,1	5

Kuva 14. Gartnerin tutkimuksesta kerätyt arvostelupistemäärät eri haavoittuvuusskannereille (Gartner 2023)

Gartnerin tutkimuksen pisteiden keskiarvoon oli otettu mukaan asiakkaan arvosanat seuraaville asioille: sopimusasiat, integrointi, käyttöönotto, asiakaspalvelu, tekninen tuki ja tuotteen ominaisuudet (Gartner 2023a). Gartnerin tutkimuksen pisteiden keskiarvojen reliabiliteettia ei voi todeta kovin hyväksi kaikkien tuotteiden osalta, koska arvioiden määrä oli hyvin pieni.

Näiden tutkimusten perusteella voidaan karkeasti päätellä, että suosituimmat yrityskäyttöön suunnitellut haavoittuvuusskannerit olivat vuonna 2023 seuraa-

vat tuotteet, jos otetaan huomioon riittävä arvostelumäärä eli vähintään 30 arvostelua saanut tuote: Wiz, Tenablen tuotteet, Trend Micro ja Rapid7 InsightVM. Outpost24-skanneria ei näy G2:n tuloksissa ollenkaan ja Gartnerin tutkimuksessa se on saanut melko vähän arvioita, ja on lisäksi esitetyn listan lopussa. Tälle oli vaikea löytää helposti selkeitä syitä. Tätä asiaa tutkija analysoi jonkin verran kahden muun haavoittuvuusasiantuntijan kanssa. Yksi syy voi olla Outpost24:n vähäisempi tunnettuus, varsinkin Tenablen tuotteisiin verrattuna, jolla on useita tuotteita eri käyttöön hyvin ominaisuuksin. Outpost24 on toiminut alkuun lähinnä Pohjoismaissa ja se on ollut melko pieni toimija. Outpost24:lla ei ole ilmaista tai kevyempää versiota kotikäyttöä tai pientä verkkoa varten, kuten Tenablella on, joka vaikuttaa tunnettuuteen varsinkin harrastajien keskuudessa. Gartnerin listoille pääsy vaatii yleensä myös hyvää näkyvyyttä USA:ssa.

3.7 Kohdeorganisaation käyttämä haavoittuvuusskanneri

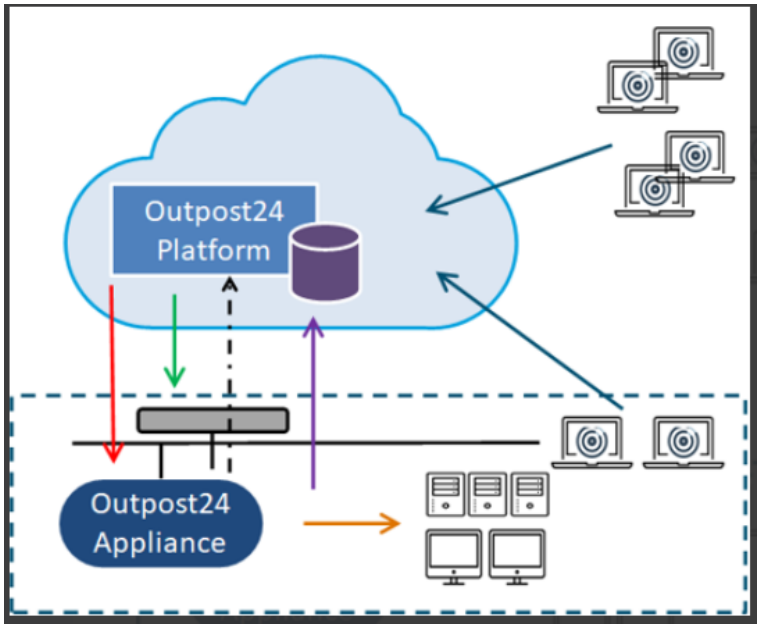
Yritykseen oli valittu ennen tätä tutkimustyötä haavoittuvuusskanneriksi Outpost24-ohjelmisto. Outpost24 on ruotsalaisen tietoturvayrityksen kaupallinen pilvipohjainen tuote, joka tukee myös on-premises-asennustapaa, joka tarkoittaa paikalliseen verkkoon asennettavaa järjestelmää (Outpost24 2023a). Sen valintaan vaikuttivat sopivat ominaisuudet, monipuoliset asennustapavaihtoehdot, laajennettavuus, hallittavuus, soveltuvuus erilaisten asiakkaiden käyttöön, tekninen tuki ja hinnoittelutapa. Yrityksessä oli myös ennestään käyttökokemusta seuraavista haavoittuvuusskannereista: Rapid7, Tenable Nessus ja Tenable.sc. Tutkijan ja muiden asiantuntijoiden kokemuksen perusteella Tenable on monipuolinen tuote, mutta monimutkaisempi ja käyttökustannuksiltaan kalliimpi tuote kuin Outpost24.

Haavoittuvuusskannerin arkkitehtuuri kohdeorganisaatiossa

Yrityksen Outpost24 -asennuksissa käytetty arkkitehtuuri on nimeltään Outscan Remote Control (RC) eli Outscan Internal. Tässä asennustavassa Outpost24 sovellus toimii pilvessä ja sillä hoidetaan skannausten ajastukset,

raporttien tuottaminen, käyttäjien ja sisäverkon skannereiden hallinta. (Outpost24 2023a).

Toimeksiantajalle valitussa asennuskonfiguraatiotavassa (Kuva 15) pilvi toimii palvelun pääsijaintina, ja kaikki tieto tallennetaan valmistajan pilveen. Outpost olisi mahdollista asentaa myös on-premise-asennuksena. Valitussa asennustavassa on se etu, että kohdeverkon skannaus voidaan tehdä verkon ulkopuolelta, jolloin tulee testattua verkon ulkopuolelle näkyvät portit ja palvelut. Tämä tapa mahdollistaa sisäverkon skannereiden sekä koneille asennettavien agenttien liittämisen systeemiin. (Outpost24 2023a.)



Kuva 15. Outpost24 asennuksen arkkitehtuurikuva toimeksiantajalla

Jos yrityksessä on tarkkaan rajattuja sisäisiä verkkoja, niin on myös mahdollista asentaa niihin erilliset skannerit, joita ohjataan pilvessä olevalla Outpost-ohjelmistolla. Kuvassa (Kuva 15) oleva Outpost24 Appliance tarkoittaa sisäverkon skanneriohjelmistoa ja sitä voidaan kutsua myös nimellä HIAB. HIAB™ (hacker-in-a-box) on automatisoitu sisäinen haavoittuvuuksien hallintajärjestelmä, joka sisältää verkon haavoittuvuuksien skannerin ja verkkosovellusskannerin (Outpost24 2023e).

Yhdelläkin skannerilla voi hallita usean sadan palvelimen verkkoja, mutta ajastetut skannaukset voi olla hyvä ajoittaa osittain eri aikoihin eri verkkoalueisiin, ettei skannaustapahtuma kestä liian pitkään, jolloin Outpostin Scheduler saattaa katkaista skannauksen. Käytännössä näin saattaa tapahtua, jos skannaus

kestää yli määritellyn skannausikkunan, mutta tämän aikaikkunan voi määritellä myös asetuksissa suuremmaksi. Olisi kuitenkin huomioitava, ettei skannausta mielellään päästetä tapahtumaan kesken työpäivän, jolloin se voi haitata joidenkin palvelimien toimintaa. Jos skanneri on liitetty pilvessä olevaan OUTSCAN-instanssiin, niin kaikki skannaustietokin tallentuu pilveen. (Outpost24 2023f.)

4 AINEISTON KERUU JA TUTKIMUSRAPORTTI

Tässä luvussa käydään aluksi läpi eri vaiheet, kuinka primääriaineistoa oli kerätty teemahaastatteluilla ja kyselyillä toimintatutkimuksen tapaan. Tämän jälkeen esitetään litteroituna tutkimuskysymyksiin haastatteluissa ja kyselyissä kerätyt tiedot. Empiirisen tutkimuksen mukaisesti aluksi tehtiin aineiston tietojen tarkistus, sitten täydennettiin tietoja lisäkyselyin ja erilaisia lähteitä tutkimalla ja kolmantena vaiheena aineisto järjestettiin analyyseja varten (Hirsjärvi ym. 2007). Aineistoa kerättiin myös teknisellä havainnoilla ja osallistuvalla havainnoinnilla, ja ne kirjattiin kyselylomakkeisiin tai ohjauspalavereiden osalta palaverimuistioihin (Eskola ym. 2014, 99–101). Sekundääristä aineistoa kerättiin kirjallisuudesta, organisaation intranet-sivuilta ja yleisiltä internet-sivuilta. Osa haavoittuvuusskanneriin liittyvästä aineistosta kerättiin kokeilemalla, joka kuuluu Kanasen (2017) mukaan primäärisen aineiston keruumenetelmiin.

4.1 Tiedonkeräys teemahaastattelun ja kenttäpäiväkirjan avulla

Opinnäytetyön tutkimuskysymyksiin kerättiin primääritutkimusaineistoa teemahaastattelun ja siihen liittyvän kenttäpäiväkirjan (liite 4) avulla. Kenttäpäiväkirjaa käytettiin tässä työssä lähinnä haastatteluihin liittyvän toiminnan, yllättävien tietojen ja omien arvioivien kommenttien kirjaamiseen, mutta sen käyttö ei ollut aivan päivittäistä ajankäytöllisistä syistä, kuten yleensä kenttäpäiväkirjaa käytettäessä (Grönfors 2011).

Teemahaastatteluun ja -kyselyyn osallistui organisaation sidosryhmiin kuuluvia asiantuntijoita, joiden oletettiin tietävän käsiteltävästä aiheesta mahdollisimman paljon. Haastatteluun valittiin alan kokeneimmat ja melko pitkään tässä samassa organisaatiossa työskennelleet ihmiset. Haastateltavat edustivat yrityksen tietohallintoa tai kyberturvallisuusosastoa. Tutkija tunsi osan

haastateltavista hyvin ennakkoon taustoiltaan ja osa valikoitiin muiden kokeneempien asiantuntijoiden ehdotuksesta.

Yrityksen lähtötilanne haavoittuvuuden hallintaprosessin ja haavoittuvuusskannerin osalta oli selvitetty aiemmin tutkimalla intranettiin kootut tiedot, ja haastattelemalla näiden aiheiden parissa työskennelleitä ihmisiä. Teemahaastattelussa kysyttiin haastatteluun valituilta ihmisiltä suurin osa työn tutkimuskysymyksiksi valituista kysymyksistä. Teemahaastatteluiden primääriaineisto koottiin kyselylomakkeisiin (liite 2), jotka oli tehty jokaiselle haastateltavalle erikseen. Kaikki alakysymykset eivät varsinaisesti soveltuneet kysyttäväksi muilta, koska ne vaativat syvää järjestelmäosaamista ja käyttökokemusta ja ne täytyi selvittää itse kirjallisuus- ja internet-lähteitä tutkimalla ja kokeilemalla käytännössä. Teemahaastatteluissa saadut vastaukset koottiin lopuksi yhteen, analysoitiin ja käytettiin hyväksi tutkimustulosten muodostamisessa. Vastausinnokkuutta todennäköisesti pudotti selvityksen alkuvaiheessa alkaneet YT-neuvottelut ja organisaation muutossuunnitelmat, jotka kohdistuivat kahteen valitsemaani henkilöön. Kysymykset ja haastattelupyynnöt esitettiin kolmelletoista henkilölle ja seitsemän kanssa asia päästiin käymään läpi.

Teemahaastatteluiden nopeuttamiseksi ja paremman valmistautumisen takia aiheeseen liittyvä teema-aihelista (liitteet 1 ja 2) tai selkeämpi kysymyslista (liitteet 1 ja 3) lähetettiin ennakkoon, ja pyydettiin myös palauttamaan se ennen haastattelua. Osa kysymyksiin liittyvästä kommunikaatiosta käytiin myös jo ennakkoon Teamsin välityksellä, jos vastaaja halusi tehdä tarkentavia kysymyksiä. Kaikkien kanssa ei pidetty haastattelua, jos sille ei nähty tarvetta. Itse haastattelut pidettiin myös Teamsin kautta, koska suuri osa ihmisistä työskenteli etänä. Teams tarjoaa mahdollisuuden samalla tallettaa tapahtuman jälkikuuntelua varten, joka korvaakin kätevästi vanhemman tavan käyttää jotain muuta äänentallennustapaa. Haastattelun aikana tehtiin myös muistiinpanoja. Tutkimusraportti ja työ annettiin haastateltaville arvioitavaksi ennen tutkimustyön julkistamista, koska tällä parannetaan toimintatutkimusraportin luotettavuutta.

4.2 Havainnoinnit

Aineistoa kerättiin myös teknisellä ja osallistuvalla havainnoinnilla. Havainnointi on tieteellisen tutkimuksen perusmetodi ja sitä käytetään tietojen keräämiseen tutkimuksessa ja se sopii hyvin myös laadulliseen tutkimusmenetelmään. Teknistä ja osallistuvaa havainnointia tutkija pystyi tekemään lähinnä haavoittuvuusskannerin uusien asennuksien ja uusien verkkojen lisäämisen yhteydessä sekä kuukausittaisissa haavoittuvuuspalavereissa. (Grönfors 2011.)

Tutkija toimi itsekin teknisenä asiantuntijana prosessin piiriin kuuluvalla osastolla, joten hän pystyi tekemään hyvin omia havaintoja useimmista toimenpiteistä ja prosessin toimivuudesta koko tutkimuksen ajan. Haastattelujen edetessä tutkimuksen tekijälle kehittyi koko ajan parempi tilannekuva prosessin nykytilanteesta ja sen kehitystarpeista, ja vähitellen hän osasi tehdä parempia tarkentavia kysymyksiä uusille haastateltaville. Kysymyspohjaa muokattiin myös hiukan haastatteluiden puolivälissä. Haastattelut suoritettiin Teamsin välityksellä työpäivän aikana.

Lähes viikoittain pidettävät opinnäytetyön ja haavoittuvuusskannerin seurantapalaverit auttoivat tarkentamaan toimintatapoja työn edistämiseksi. Palavereissa esitetyt ja selvitetyt asiat kirjattiin ylös tutkijan palaverimuistioihin. Seurantapalaverit auttoivat samalla toteuttamaan pienimuotoisesti tutkimuksellisen kehittämisen sykliä, josta Kananen (2015) kertoo kirjassaan, ja tämä soveltuu myös toimintatutkimuksen spiraalin muotoisen perusmallin noudattamiseen (Heikkinen ym. 1999).

4.3 Teema 1 - Millä tavalla yrityksen sisäistä haavoittuvuuksien hallintaprosessia kannattaisi kehittää paremmaksi?

Tämän päätutkimuskysymyksen alakysymyksenä oli myös ”Haavoittuvuuksien hallintaprosessin selkeimmät heikkoudet tai puutteet?” Nämä kaksi kysymystä liittyivät läheisesti samaan aiheeseen, joten ne käsitellään tässä samassa kappaleessa. Tässä kappaleessa käydään läpi kooste vastauksista tutkimuskysymykseen, mutta näitä vastauksia ei pidetä vielä tämän työn tuloksina.

Haavoittuvuuksien havainnointi todettiin puutteelliseksi ja usein tieto haavoittuvuudesta saattaa tulla myös asiakkailta. Laitteita ja alustateknologioita ei tunnisteta riittävällä tarkkuudella, ja tämä johtaa siihen, että osa laitteista sekä alustoista jää päivittämättä. Proaktiivinen toiminta vaikuttaa vähäiselle. Tämän parantamista varten oli otettu 1.1.2023 käyttöön vuosikello, jonka tarkoituksena on käydä teknologioiden päivitystä läpi proaktiivisesti. Tutkimushetkellä kuitenkin vuosikellon dokumentaatio eri teknologioista oli hyvin puutteellinen ja sitä pitäisi täydentää pian.

Henkilöresursseja ei ollut kohdistettu laiteresursseihin riittävän tarkalla tasolla, ja tämän takia teknologiaspesifinen osaaminen oli heikohkoa. Prioriteetti 1-haavoittuvuuksien kohdalla oli usein ongelmana työvoimaresurssien jatkuva metsästys. Prioriteetti 1-tasolla kuvataan tietoturvatapahtumissa yleisesti asian korkeaa tai kriittistä tärkeystasoa (Buildahelpdesk 2022). Haasteena oli, ettei tiedetty kunnolla, että kuka osasi mitäkin teknologiaa ja näin ollen päivitysresurssien etsimiseen kului tuhottomasti aikaa.

Ohjelmistopäivitysten teosta tuotiin esille tällainen kommentti ”Prosessissa pitäisi tuoda vahvemmin ilmi järjestelmäomistajien vastuu sekä päivityksistä vastaavien vastuu ja tekeminen. SOC:n roolia pitäisi jopa ehkä kuvata pois, koska tämä prosessi ei vaadi SOC:ia sen toimimiseen ja olemassaoloon.” Muistutettiin myös, että järjestelmäomistajien pitäisi seurata säännöllisesti haavoittuvuuksia, jotka liittyvät heidän järjestelmiinsä. Prosessi ei toimi sisäisesti, koska päivityksistä vastaavat tahot ja SOC eivät toimi yhteistyössä tässä asiassa. Monet luulevat, että haavoittuvuuksien korjaaminen on SOC:n vastuulla, ja että SOC:n pitäisi osata kertoa haavoittuvuudesta kuin haavoittuvuudesta, miten se korjataan, vaikka haavoittuvuudet ovat järjestelmissä, joita he eivät omista teknisesti eivätkä välttämättä ymmärrä tarpeeksi hyvin.

Tärkeänä korjaavana toimenpiteenä todettiin, että järjestelmänomistajille allokoidaan riittävästi aikaa valvoa ja parantaa vastuullaan olevaa järjestelmää. Aika- ja resurssipula oli todettu monen järjestelmänomistajan ongelmaksi. Yksi ehdotus oli, että määritellään organisaation sisäisille tiketeille SLA (Service Level Agreement), jolla olisi korkeampi prioriteetti kuin asiakkailla, koska

kaikki mitä tehdään organisaatiossa sisäisesti, liittyy myös epäsuorasti asiakkaisiin. SOC:n työntekijät taas suhtautuivat hiukan negatiivisesti uusiin SLA-määrityksiin, koska se luo painetta ajankäytön suhteen.

Kokonaisprosessin omistajuus oli organisaatiossa tutkimuksen haastatteluiden aikoihin epäselvä, mutta sille löydettiin kuitenkin omistaja aivan tutkimuksen loppuvaiheessa. Järjestelmäpuolen todettiin skannausten suhteen kehittyneen, mutta toiveena oli sen laajentaminen edelleen ja parempi kattavuus verkoista.

Jotkut toivoivat, että SOC:n tutkimista sisäisistä asioista jäisi aina jälki ja heidän tiketteihinsä olisi parempi näkyvyys organisaation sisällä. Tämän esteenä on ollut erot SOC:n ja muiden ryhmien tietoturvatasoissa. Järjestelmäomistajien ja SOC:n sisäistä yhteistyötä täytyisi parantaa ja laajentaa. SOC:n ulkopuolisesta näkökulmasta katsottuna todettiin, että SOC:lla on hieman heikko kyky korreloida haavoittuvuudet organisaation palveluihin. Esimerkkinä tästä kysymys: ”Koskeeko MariaDB-haavoittuvuus Pulsar-järjestelmää?” Pulsar on yrityksen oma tuotannon työnohjausjärjestelmä, jossa tiketöinnin lisäksi sijaitsee muun muassa laitekanta, lista palveluista, sekä tuotannon dokumentaatiota. Pulsar perustuu ServiceNow:n tiketöintijärjestelmään. CMDB:n (Configuration Management Database) heikohko hyödynnettävyys nähtiin myös heikkoudeksi. CMDB on tietokanta-arkisto, johon voi tallentaa tietoja IT-infrastruktuurin eri komponenteista (Motadata 2023).

Heikkouksiksi mainittiin myös haavoittuvuusskannerin seurannan ulkopuolelle jääneet kohteet, jotka olivat vielä vanhalla verkkoalueella sekä puutteet CMDB:n tiedoissa tai kokonaan dokumentoimattomat laitteet ja järjestelmät. Tietojen selvittämistä vaikeutti se, että dokumentointi oli hajautunut useaan järjestelmään. Yhtenä parannuskeinona joihinkin toimintoihin nähtiin automaatio, esimerkiksi SOAR (engl. Security Orchestration, Automation and Response). SOAR on ohjelmisto, jolla voi automatisoida ennalta määrättyjä työnkulkuja. Organisaatiolla pitäisi olla myös CISO, joka voisi eskaloida sekä seurata asioita. CISO onkin ollut aiemmin, mutta hänen lähdettyään tilalle ei ole löytynyt uutta sopivaa henkilöä ja tutkimuksen aikoihin tilalle perustettiin tietoturvatiimi organisaation muista henkilöistä.

Yksi epäilyn aihe oli se, että näkyvätkö rogue-laitteet haavoittuvuusskanne-rissa. Rogue-laite tarkoittaa IT-infrastruktuurissa olevaa luvatonta tai järjestelmälle tuntematonta laitetta (Securiwiser 2021). Nämä laitteet tulevat kyllä esille verkkoalueiden laitteiden etsintäskannauksessa automaattisesti ja uusi laite otetaan samalla haavoittuvuusskannaukseen mukaan. Tämä herättää kuitenkin uuden kysymyksen, kuinka uusi laite erottuu verkon muiden laitteiden raporttien seasta selkeästi, koska Outpost24-skanneri ei sitä varsinaisesti korosta mitenkään tuloksissaan. Jos skannaustuloksia tutkii tarkemmin, sieltä voi kyllä nähdä, ettei laitteeseen pääse kirjautumaan sisään testaustunnuksilla, jos tunnuksia ei sinne ole aiemmin määritelty. Mahdollisesti hälytys uudesta laitteesta voi tulla myös jonkin muun järjestelmän kautta, mutta tätä näkökulmaa ei oteta tässä työssä tarkemmin esille turvallisuussyistä.

4.4 Teema 2 - Haavoittuvuustikettien käsittelyn parannusideat?

Toinen tutkimuskysymys tarkasteli haavoittuvuustikettien tekemistä, eskalointia ja seurannan parantamista. Tässä kappaleessa käydään läpi kooste analysoimattomista vastauksista tutkimuskysymykseen, mutta näitä vastauksia ei pidetä vielä tämän työn tuloksina. Haavoittuvuustikettien käsittelyssä todettiin yleisesti melko monen mielestä parantamisen varaa aiemmin mainittujen hallintaprosessin heikkouksien takia.

Toivottiin, että SOC käsittelisi enemmän ohjelmistopäivitysten hallintaa palavereissa, ja että heillä olisi tiiviimpi liitos tähän prosessissakin. Ohjelmistopäivityksillä voitaisiin poistaa monet haavoittuvuudet (Intel s.a.a.). Haavoittuvuuksien hallintaprosessissa ei ole kuvattu vielä minkäänlaista yhteyttä SOC:n palvelupäälliköihin, mutta ei perusteltu, että olisiko se tarpeen ja millä tavalla. SOC-tiketteihin on tällä hetkellä hyvin rajattu näkyvyys organisaation sisällä ja se perustuu tarkastelijan rooliin. Tikettien tarkastelu kiinnostaisi ainakin osaa johtajista ja järjestelmänomistajista, mutta pääsy on rajattu turvallisuusrajausten takia. Toivottiin myös mahdollisuutta varata aikaa järjestelmäomistajien puolelta tarjottuihin työkeikkoihin.

Prosessin alkuvaiheisiin toivottiin tarkennuksia. Haluttiin nähdä, miten tieto haavoittuvuuksista tavoittaa SOC-analyytikon, ja millaisella päätöksellä ulkoisista lähteistä nousevista ilmoituksista luodaan SI-tiketti (Security Incident).

SOC avaa SI-tiketin yhteydessä normaalisti muutostiketin, mutta vaihtoehdoksi nähtiin muutostiketin sijasta palvelupyyntötiketti ITOC:lle, koska siinä on automaattisesti jonoseuranta, joka muutostiketistä nyt puuttuu. Palvelupyyntötiketissä pitäisi olla samalla linkitys SI-tikettiin. Service line hoitaisi tikettiin kuuluvat muutokset ja SOC tukisi taustalla. Kaikki ilmoitukset tuskin päätyvät SI-tiketiksi, joten ymmärrys SI-tikettien arvoisista ilmoituksista olisi hyvä avata ohjeistukseen. Olisi myös hyvä selvittää, kuinka usein ja säännöllisesti näitä ulkoisia lähteitä analysoidaan. Samat kuvaukset voisivat sopia myös haavoittuvuusskannerin tuloksien tulkintaan. Kuinka usein analysoidaan, ja millä logiikalla löydöksestä avataan SI-tiketti?
Voitaisiin ohjeistaa mitkä korkean tason haavat (engl. high-risk) voidaan jättää odottamaan toistuvaa kuukausittaista kontrollikokousta, ja mihin täytyy reagoida nopeammin. Haavoittuneen koneen järjestelmäomistaja voitaisiin selvittää Pulsar-järjestelmän kautta ja ilmoittaa hänelle pahiten haavoittuneista koneista.

Ainakin osalle haastateltavista oli myös epäselvää, löytyykö haavoittuvuustikettien luonnille, seurannalle ja tikettien eskaloinnille selviä ohjeita. Edellä mainittujen tietojen tutkiminen voi ollakin SOC:n ulkopuolisille sidosryhmille vaikeaa tai mahdotonta, koska SOC:lla on suuri osa sisäisestä dokumentoinnista sellaisessa paikassa, jonne muilla ei ole pääsyä. Tämä hankaloittaa myös tällaisen tutkimuksen tekemistä, vaikka tutkija kuuluukin SOC:n lähimpään sidosryhmään.

4.5 Teema 3 - Kuinka täytyisi reagoida nollapäivähaavoittuvuuksiin?

Kolmanneksi kysyttiin, kuinka täytyisi reagoida nollapäivähaavoittuvuuksiin. Nollapäivähaavoittuvuus (engl. zero-day vulnerability) tarkoittaa haavoittuvuutta, johon ei ole vielä olemassa korjaavaa päivitystä (Intel s.a.b.). Yksi ehdotus tähän oli geneerinen tiedotuslistapohja, johon olisi listattu asiakkaat ja heidän käyttämänsä teknologiat. Näin voisi tiedottaa selkeämmin haavoittuneeseen teknologiaan liittyviä oikeita asiakkaita. Tämä voisi toimia sekä organisaation sisäisillä asiakkailla että ulkoisilla. Toisen vastaajan kommentti oli ”Haavoittuvuuden tietoisuuteen tulemisen jälkeen asia tulisi saada SOC:n kautta järjestelmäomistajien tutkintaan pikimmiten, ja kriittisyydestä riippuen myös SIRT:lle tai MOD:lle (Manager On Duty, päivystävä johtaja), niin että

SOC arvioi kriittisyyden.” Internettiin auki oleva haavoittuvuus on aina kriittisempi ja se pitää hoitaa heti. Sisäisessä järjestelmässä oleva haavoittuvuus ei ole niin kriittinen, mutta tämäkin riippuu myös itse haavoittuvuudesta.

Täytyisi löytää systemaattinen tapa reagoida nollapäivähaavoittuvuuksiin ja luoda siihen laaja näkyvyys organisaatiossa. Vastuu tulisi jalkauttaa koko organisaatiolle, ei vain SOC:lle, joka toki nämä lähes aina ensimmäisenä huomaa. Voisi olla jokin keskitetty paikka, johon kuka tahansa voi epäillyn (kriittisen) haavoittuvuuden ilmoittaa.

Yksi kommentti oli tähän kysymykseen, että pitäisikö luoda erillinen prosessikuva nollapäivähaavoittuvuuksien käsittelyyn. Pitäisi kuvata tarkasti roolit, vastuut sekä eskalointitavat. Määritellään tilanteet, jolloin täytyy hälyttää henkilöitä töihin. Hyvin tehdyt ohjeistukset toisivat toimintaan selkeyttä ja nopeutta, mutta turhaa panikointia täytyy myös välttää. Osaston täytyy täyttää palvelulupauksensa, jos sellainen on määritelty.

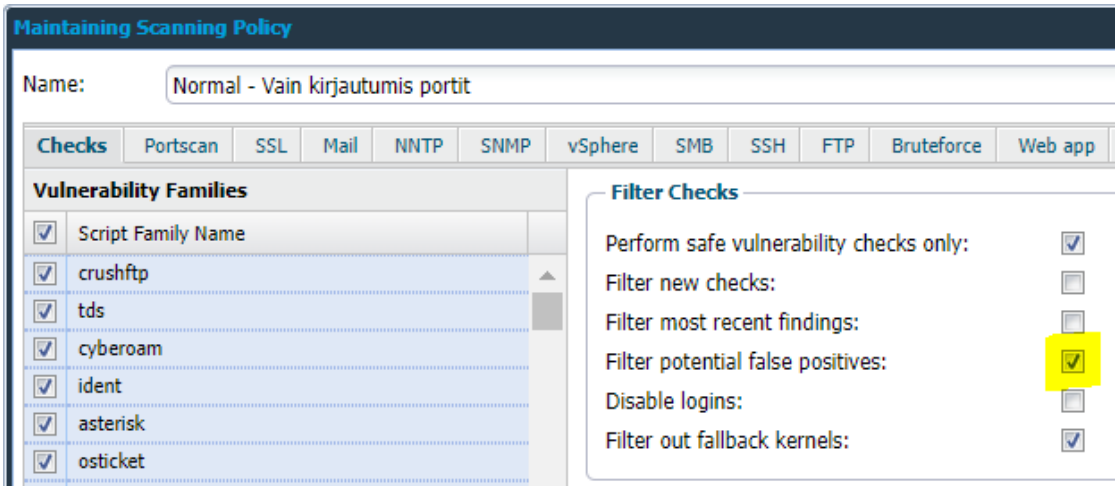
4.6 Teema 4 - Kuinka voidaan pienentää haavoittuvuusskannerin löytämien väärien positiivisten määrää?

Forresterin vuoden 2022 Total Economic Impact (TEI) -tutkimuksessa havaittiin, että InsightVM:n käyttämä toimintatapa vähensi vääriä positiivisia tuloksia 22 prosentilla, mikä vapautti osan ryhmästä kokonaan tutkimustyöstä ja nopeutti muiden haavoittuvuuksien korjausprosessia. Kolmen vuoden ennustejakson aikana Forrester ennusti 397 200 dollarin säästöjä yritykselle. Tämä on esimerkkinä väärien positiivisten haavoittuvuuksien vaikutuksesta kustannuksiin, jos yrityksessä oikeasti pyritään vähentämään haavoittuvuuksia aktiivisesti. (Forrester 2022.)

Tähän kysymykseen ei löytynyt haastatteluissa kovinkaan monelta mitään kommenttia. Toivottiin lähinnä, että SOC voisi mahdollisesti merkitä väärät positiiviset Outpostin raportteihin. Asiaa selviteltiin kuitenkin lähteitä tutkimalla ja haavoittuvuusskannerin toimintoja testaamalla. Yhtenä tehokkaana keinona haavoittuvuuksien määrän pienentämiseen on todettu järjestelmien aktiivinen ylläpito eli kaikki osa-alueet päivitetään säännöllisesti ja pyritään karsimaan

turhat ja rinnakkaiset järjestelmät ja sovellutukset pois (Intel s.a.a; Nordic-Defender 2022). Jotta nämä asiat onnistuisivat, niin järjestelmäomistajille ja ylläpitäjille täytyisi jättää tarpeeksi aikaa näiden asioiden hoitamiseen.

Outpost24:n haavoittuvuusskannerin asetuksista löytyy ”Filter potential false positives”-toiminto (Outpost24 2023a). Tätä käyttämällä turhien haavoittuvuuslöydösten määrä vähenee oleellisesti, ja se taas helpottaa ja varsinkin nopeuttaa kriittisempien haavoittuvuuksien tutkimista. Kuva 16 näyttää tämän ominaisuuden sijainnin Outpost24:n asetuksissa.



Kuva 16. Väärien positiivisten haavoittuvuuksien suodatus Outpost24:ssa

Toimintoa testattiin yhden Windows-palvelimen kanssa. Aktivoidun ”false positives” -valinnan kanssa tuli 14 ilmoitusriviä, joista 12 oli informatiivisia löydöksiä ja 2 oli keskitason haavoittuvuutta. Valinnan deaktivoinnin jälkeen suoritettiin uusi skannaus ja ilmoitusrivejä tuli raporttiin 2706 kappaletta, jossa oli mukana myös paljon korkean ja kriittisen tason haavoittuvuuksia. Kuva 17 näyttää kokeilussa käytetyn palvelimen haavoittuvuuslöydösten historiatiedot kahden viikon ajalta ja alin rivi näyttää haavoittuvuudet kokeilupäivänä. Varmuuden vuoksi skannaus suoritettiin uudestaan suodatin aktivoituna ja jälleen raporttiin tuli vain 14 ilmoitusriviä.

Date	Low	Medium	High
2023-02-08	0	2	0
2023-02-16	0	2	0
2023-02-23	0	2	0
2023-02-26	154	649	546

Kuva 17. Esimerkkinä toimineen Windows-palvelimen haavoittuvuuksien historianäkymä

Vakaviksi määriteltyjen haavoittuvuuksien suuri määrä herättää epäilyksen valmistajan kehittämän suodattimen oikeanlaisesta toiminnasta. Analysoitavaa olisi tässäkin tapauksessa niin paljon, että se veisi todella paljon aikaa. Castsoftwaren (2017) mukaan jotkut skannausohjelmistot osaavat päätellä ohjelmistokomponenttien ”kuolleen koodin”, ja kirjastot, joita ei kutsuta, jolloin näitä puutteita ei tarvitse huomioida ja ne eivät ole potentiaalisia uhkia. Kokeilutulosten takia selvitettiin valmistajan teknisen tuen kautta, miten Outpost24:n suodatus tehdään. Vastauksen perusteella he käyttävät tämän suhteen hyväksi omaa tietokantaansa. He voivat tarkistaa sovellusten otsikkotiedot, versiot, kirjastot ja rekisterit. Joissakin harvinaisissa tapauksissa, kuten Log4J:n suhteen, tehdään tiedostoindeksointia haavoittuvuuksien havaitsemiseksi, mutta he eivät kuitenkaan tarkistele ohjelmistojen koodeja.

Haavoittuvuusskannerin löytämät väärät positiiviset voivat johtua Tenablen (2020) mukaan skannerin tarkistuskäytäntöasetuksista, virheellisistä korjauksista, vääristä tai puuttuvista kirjautumistiedoista tai ongelmasta ohjelmistoliitännäisen (engl. plugin) kanssa. Skanneri tekee ohjelmistoversioita tutkiessaan seuraavat tarkistustoimenpiteet:

- Verrataan kohdelaitteessa olevan päivitystiedoston versiota tai ohjelmistoversiota valmistajan ilmoittamaan korjausversioon.
- Tarkistetaan, onko päivitystiedosto (esimerkiksi Microsoft KB) asennettu.
- Tarkistetaan, vastaako rekisteriavain toimittajan asettamaa arvoa. (Tenable 2020.)

Name	Type	CVSS	CVSS V3 Sev	Risk Level	Port	Accepted	False Positive	Age (Days)	Exploit Available
n Vulnerability (1)									
Microsoft Internet Explorer: XML Exter...	Vulnerability	4.7	Medium	Medium risk	445	No	No	0	No
OS Detection	Information	0.0		Information	Generic	No	No	0	No
Patches Installed	Information	0.0		Information	Generic	No	No	0	No

Kuva 18. Outpost24:n False Positive -sarake

Kuva 18 osoittaa, että Outpost24 antaa mahdollisuuden merkitä todetut väärät aktiiviset löydökset. Löydökset voi merkitä halutessaan niin, että ne pysyvät merkittyinä myös seuraavissa skannausraporteissa. SOC:n analyytikot voisivat käyttää tätä ominaisuutta hyväkseen. Väärien positiivisten tietojen manuaaliseen selvittelyyn voi käyttää aluksi skannerin tuottamia alkutietoja. Jos skannauskohteeseen ei ole päässyt kirjautumaan sisään, löydös voi jäädä vääräksi positiiviseksi, koska silloin skanneri ei pysty tunnistamaan kaikkia asennettuja sovelluksia ja versiotietoja varmuudella oikein. Tämän voi korjata hankkimalla kohteeseen järjestelmänhaltijatason (admin tai sudo) testaustunnukset, jolloin skanneri pystyy tutkimaan kohdetta tarkemmin. Testaustunnuksella pitäisi olla myös täydet oikeudet koneen rekistereihin. Windows-koneiden OVAL-skannauksissa olisi päästävä käyttämään WMI:tä (Windows Management Instrumentation). Open Vulnerability and Assessment Language (OVAL) on kansainvälinen tietoturvayhteisön perusstandardi, joka on suunniteltu tarkistamaan tietokonejärjestelmien haavoittuvuuksia (OVAL 2016). Näiden toimenpiteiden ohittaminen aiheuttaa lisää vääriä positiivisia löydöksiä. (IBM 2022.)

Yksi hieman monimutkaisempi keino selvittää vääriä positiivisia on käyttää penetraatiotestausta. Jotkut haavoittuvuusskannerit antavat tämän ominaisuuden lisäoptiona. Tällöin skanneri tarkistaa automaattisesti epäselvän löydöksensä hyödyntämällä havaittuja puutteita ja ilmoittaa tuloksen automaattisesti raporttiin (Castsoftware 2017). Erilliseen penetraatiotestaukseen löytyy automaattisia ohjelmistoja, apuohjelmia ja manuaalisia keinoja, mutta niiden hyödyntäminen vaatii myös aikaa ja asiantuntijuutta. Näitä erilliskeinoja käytettäessä lopputulos täytyisi päivittää manuaalisesti haavoittuvuusskannerin raportteihin, jos se halutaan myös pitää ajan tasalla. Lopputuloksen luotettavuus riippuu asiantuntijan ammattitaidosta (Castsoftware 2017.)

Linux- ja macOS-käyttöjärjestelmissä melko yleinen syy väärille positiivisille löydöksille on backporting-toimenpiteen käyttö (HolmSecurity 2022). Backporting on toimenpide, jossa osia ohjelmistojärjestelmän tai ohjelmistokomponentin uudemmasta versiosta otetaan käyttöön saman ohjelmiston vanhemmassa versiossa. Se on osa ohjelmistokehitysprosessin ylläpitovaihetta, ja sitä käytetään yleisesti ohjelmiston vanhempien versioiden tietoturvaongelmien korjaamiseen ja myös uusien ominaisuuksien tarjoamiseen vanhemmille versioille.

Vanhempaa ohjelmistoversiota saatetaan joutua käyttämään järjestelmässä jonkin ajurin tai muun yhteensopivuusongelman takia. Skannauksen yhteydessä ongelma syntyy siinä, kun haavoittuvuusskanneri yrittää yksinkertaisesti havaita ohjelmiston version ja luetteloida siihen liittyvät haavoittuvuudet sen sijaan, että yrittäisi löytää tiettyä haavoittuvuutta ja tämä kasvattaa väärän positiivisen tuloksen todennäköisyyttä. (RedHat 2023.)

OWASP:n OVMG-opas suosittaa väärien positiivisten haavoittuvuuksien tutkimiseen seuraavia keinoja:

- Varmistetaan kohteen eheys. Hankitaan lisätodisteita lähteestä, kuten esimerkiksi kuvakaappaus ja kooditulostus.
- Pyritään rakentamaan tästä toistettavissa oleva prosessi.
- Dokumentoidaan eri työvaiheet.
- Voidaan selvittää ulkopuolisista lähteistä ja yrityksistä, voiko joku muu vahvistaa löydöksen vääräksi positiiviseksi haavoittuvuudeksi.
- Asetetaan aikakehys, jolloin väärä positiivinen löydös tulee arvioida uudelleen. Tämä aika voi olla kuusi kuukautta tai vuosi. Käytetään lakisääteisiä ja vaatimustenmukaisuutta koskevia ohjeita ajan määrittämiseen.
- Dokumentoidaan jokainen väärä positiivinen löydös, ja tallennetaan se myöhemmin auditoitavaan arkistoon.
- Luodaan sopiva toimintapolitiikka toiminnalle ja päivitetään pääkohdat haavoittuvuuksien hallintaohjeistuksiin.
- Tiedotetaan sovitusta toimintapolitiikasta vastuullisille henkilöille ja tiimeille. (OWASP 2020, 14–15.)

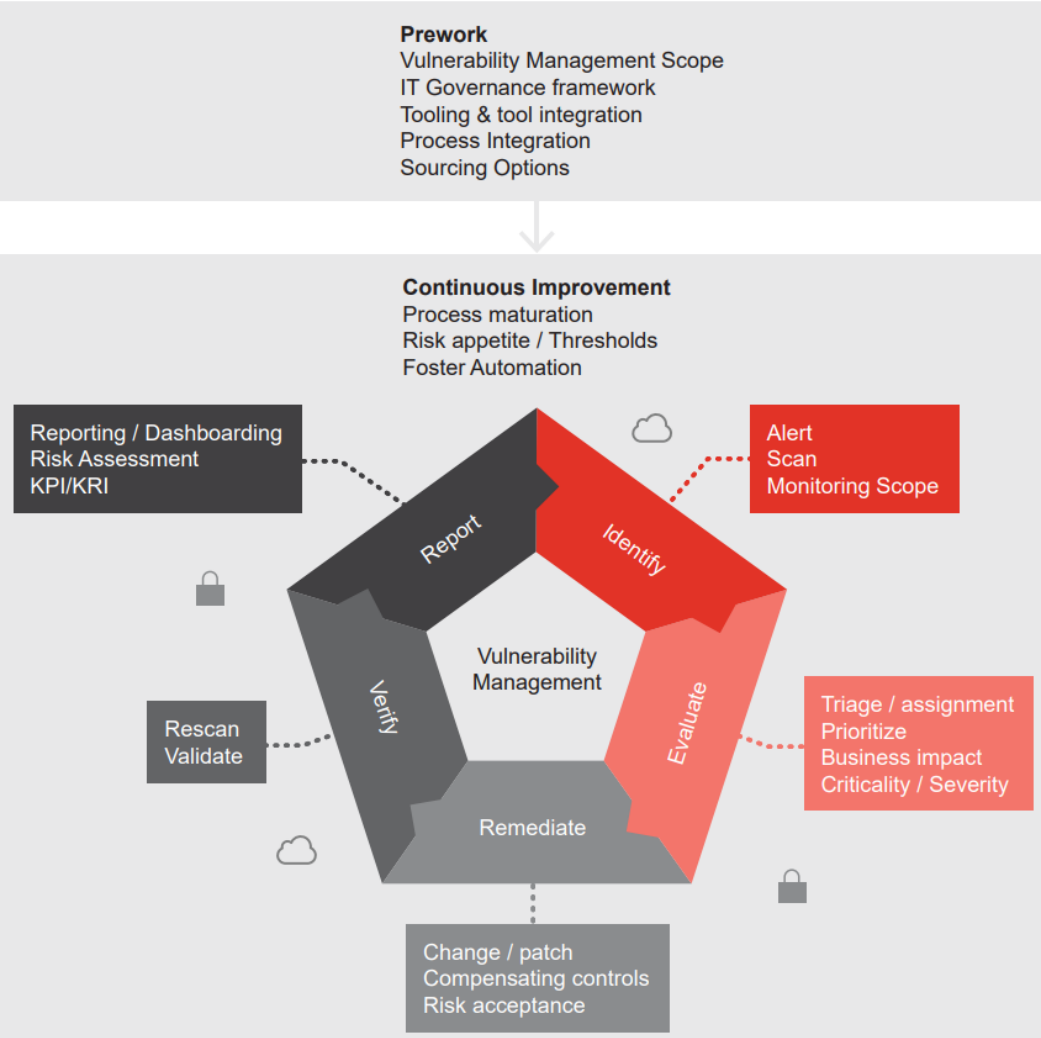
Edellä mainitut keinot liittyvät lähinnä korjaustoimenpiteisiin, mutta niiden toteuttaminen kunnolla dokumentoiden vähentää uusien löydösten löytymistä, jos tiedot päivitetään myös haavoittuvuusskannerin löydöksiin. Aineistosta päätellen tutkimusten ja tuotekehityksen myötä on löydetty useita tapoja pienentää väärien positiivisten määrää käyttämällä oikeanlaista toimintatapaa; konfiguroidaan skanneri oikein ja pidetään päivitykset ohjelmistoissa, käyttöjärjestelmissä ja ajureissa ajan tasalla. Myös todennetuilla skannauksilla ja penetraatiotestauksella saadaan pienennettyä väärien positiivisten määriä huomattavasti.

4.7 Haavoittuvuuksien hallintaprosessit

Tähän lukuun on koottu muutamia kuvauksia lähteistä löydetyille haavoittuvuuden hallintaprosesseille, joita on voitu osittain hyödyntää kohdeorganisaation prosessin muodostamisessa. Käytännössä organisaation prosessi täytyy kuitenkin suunnitella omien tarpeiden, tavoitteiden ja valmiuksien mukaan.

4.7.1 PwC:n haavoittuvuuksien hallinta

PwC on yksi maailman johtavista asiantuntijapalveluorganisaatioista, jolla on maailmanlaajuisesti lähes 328 000 työntekijää 152 maassa. PwC viittaa PricewaterhouseCoopers International Limitedin jäsenyritysten verkostoon. Kuva 19 esittää PwC:n kuvailemaa haavoittuvuuksien hallintaprosessia, joka muodostuu useiden toimintojen kiertokulusta. Alkuvaiheisiin kuuluu haavoittuvuuksien hallinta-alueen rajaaminen, IT-hallintakehyksen muodostaminen, työkalujen ja työkalujen integrointi, prosessien ja hankintavaihtoehtojen integrointi. Syklisiin toimintoihin kuuluu tunnistamis-, arviointi-, korjaus-, todentamis- ja raportointivaiheet. Samalla tapahtuu jatkuvaa kehittymistä, toimintojen automatisointia ja riskirajojen määrittelyä. (PwC 2022).



Kuva 19. PwC:n esittämä haavoittuvuuksien hallintaprosessi (PwC 2022)

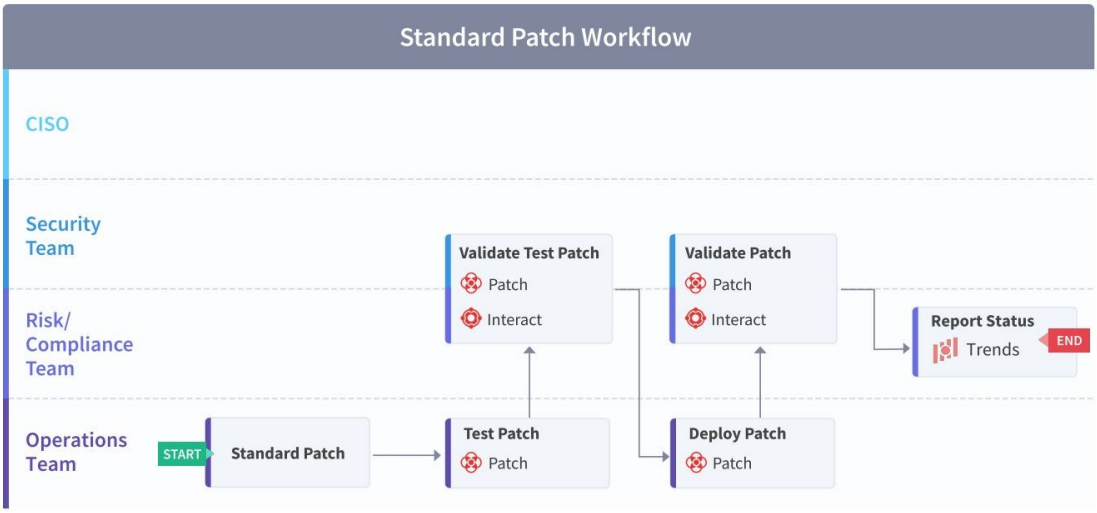
PwC:n haavoittuvuuksien hallintaprosessin kuvaus on kuvassa 19 hyvin tiivistetysti esitetty. Samoja toiminnallisuuksia on tuotu kohdeorganisaationkin hallintaprosessiin, mutta siinä toiminnot integroitiin yhteen isoksi prosessikaavioksi, jotta kokonaisuuden hahmottaisi paremmin. Jotkut toiminnot on sitten jaettu aliprosesseihin, ettei kaaviosta tulisi liian laaja.

PwC tuo esille myös eri työkalujen ja ohjelmistojen integroinnin tärkeyden prosessin ja järjestelmien suunnittelussa. PwC:n mielestä IT-palvelut kannattaisi hoitaa tiketöintijärjestelmän kautta, joka olisi yhdistetty CMDB:hen tai muuhun laitetietokantaan, sekä toimintoja kannattaisi automatisoida mahdollisimman paljon esimerkiksi SOAR:n avulla. (PwC 2022). Edellä mainittuja asioita kohdeorganisaatiossa jo hyödynnetäänkin melko tehokkaasti ja niiden ohjeistuksia on parannettu tutkimuksen aikana. SOAR on myös työkaluna olemassa

joissakin toiminnoissa, mutta sitä ei ole vielä integroitu nykyiseen haavoittuvuusskanneriin, koska se ei ole suoraan mahdollista nykyisillä järjestelmillä. SOAR:n ja haavoittuvuuksien seurantaa voi kuitenkin tehostaa kohdeorganisaatiossa käytössä olevan SIEM-järjestelmänkin avustuksella, mutta tätä vaihtoehtoa ei käsitellä tässä työssä sen tarkemmin.

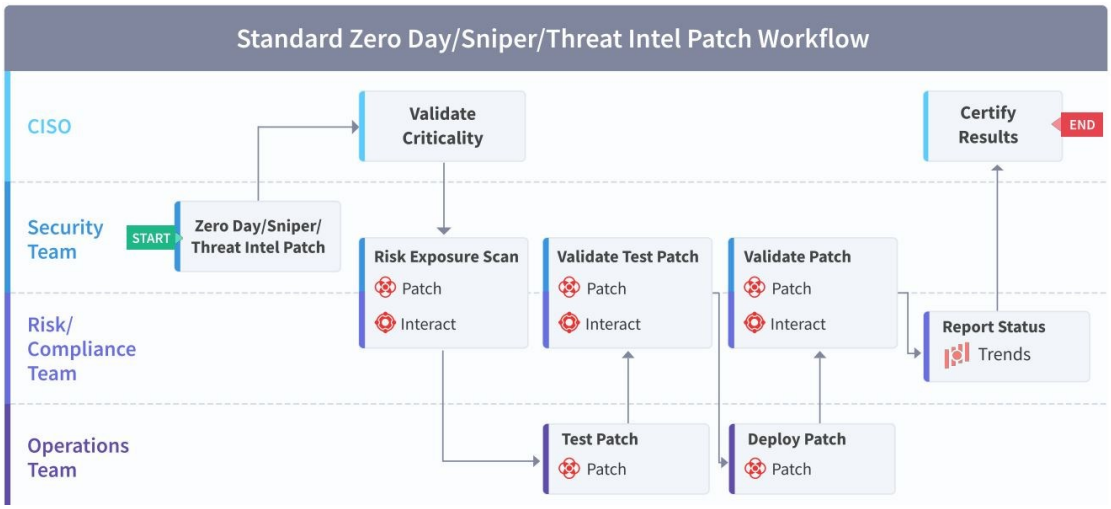
4.7.2 Taniumin korjausprosessi

Haavoittuvuuksien hallintaprosessiin kuuluu myös oleellisesti haavoittuvuuksien korjausprosessi ja ohjelmistojen päivitysprosessi. Korjausprosesseille voi olla erilaisia lähestymistapoja ja vaiheita. Kuva 20 näyttää Taninumin (2022) ratkaisun standardille korjausprosessille. Organisaation haavoittuvuuden hallintaprosessiin korjausprosessia ei ole tarkoitus kuvata tarkasti, mutta sen toiminta kannattaa ymmärtää vähintään ylätasolla ja siksi se tuodaan tässäkin esille.



Kuva 20. Taniumin standardi korjausprosessi (Tanium 2022, 29)

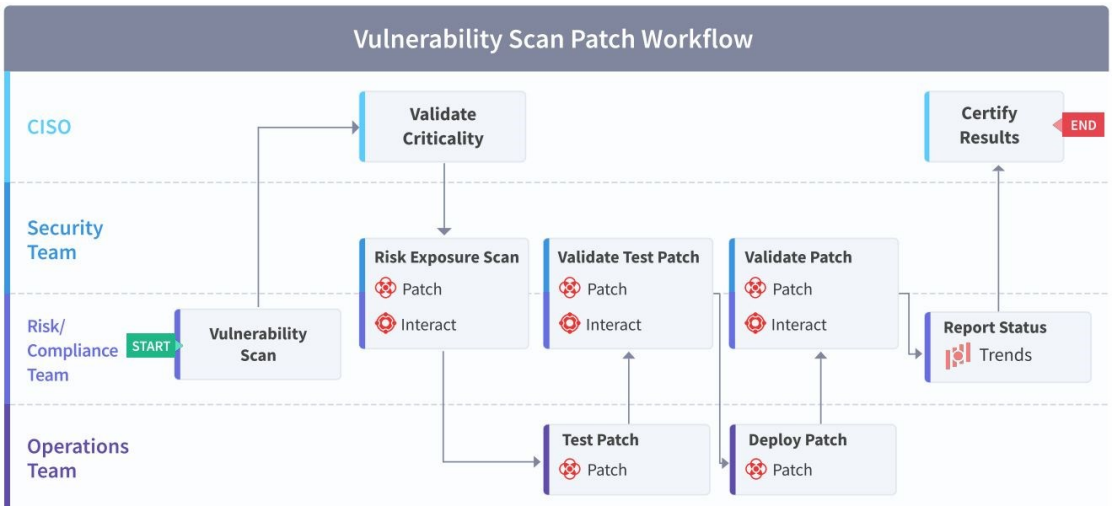
Kuva 21 näyttää toimintatavan nollapäiväkorjauksessa, jossa on mukana CISO tai tietoturvatiimi.



Kuva 21. Taniumin korjausprosessikuvaus nollapäivän haavoittuvuudelle (Tanium 2022, 29)

Kun tietoturvatiimi havaitsee nollapäivän haavoittuvuuden, otetaan yhteyttä CISO:on ja hän validoi haavoittuvuuden kriittisyyden käyttäen mahdollisesti apuna SOC-tiimiä. Sen jälkeen turvallisuustiimi suorittaa riskialtistusskannauksen yhteistyössä riski- ja vaatimustenmukaisuustiimin kanssa. Seuraavat vaiheet ovat kuten tavallisessa korjaustyönkulussa, jolloin tapahtuu testikorjaus operaatiotiimin toimesta, testikorjauksen validointi ja raportointi turvallisuustiimin ja riski- ja vaatimustenmukaisuustiimin toimesta.

Kuva 22 näyttää Taniumin (2022, 30) korjausprosessin siinä tapauksessa, jos haavoittuvuus löytyy haavoittuvuusskannerin kautta. Skannerit löytävät paljon eri tasoisia haavoittuvuuksia, joten käytännössä kaikkia haavoittuvuuksia ei voi tutkituttaa CISO:lla, vaan organisaation täytyisi määrittää haavoittuvuuden kriittisyysaste tutkimisen aloittamiselle.



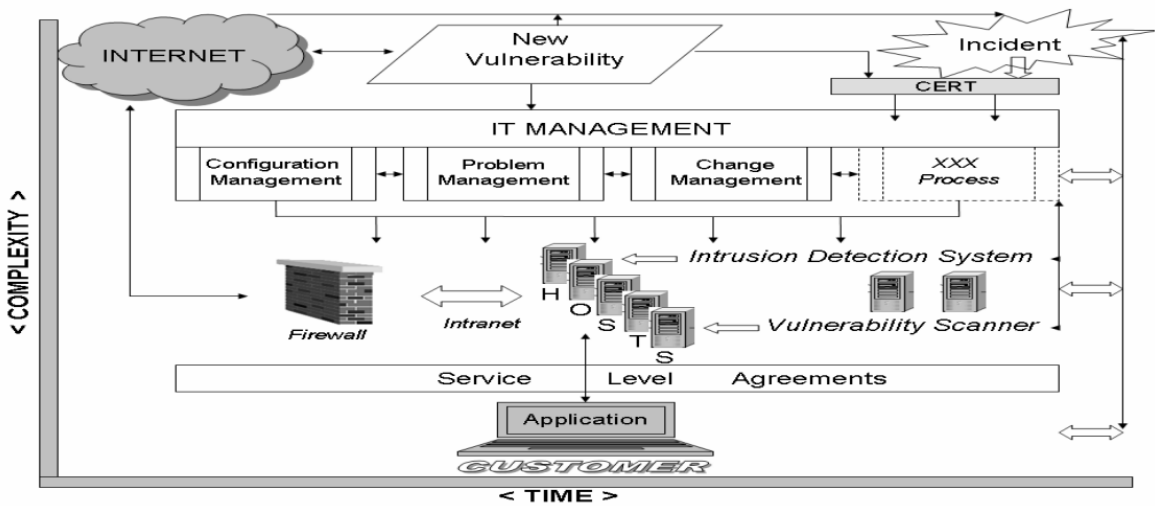
Kuva 22. Taniumin korjausprosessikuvaus haavoittuvuusskannerin avulla löydetylle haavoittuvuudelle (Tanium 2022, 30)

Käyttöönotto tapahtuu operatiivisen ryhmän toimesta, korjaustiedoston validointi turvallisuus-, riski- ja vaatimustenmukaisuustiimin toimesta ja tilaraportointi riski- ja vaatimustenmukaisuustiimin toimesta. Standardikorjauksen työnkulku on valmis tässä vaiheessa, mutta nollapäivän korjaustyönkulun viimeinen vaihe on CISO:n tai tietoturvatiimin suorittama tulosten varmentaminen. (Tanium 2022.)

Haavoittuvuuksien korjaus- ja päivitysprosessi on kuvattu melko eri tavalla kohdeorganisaation kaaviossa, koska siinä ohjelmistojen päivitysten validointi ja itse päivitysprosessi tehdään muutostiketteinä muutoksenhallintaprosessin sisällä. Standardiohjelmistojen päivitysprosessi ja nollapäivähaavoittuvuuksien käsittely etenee Taniumin kuvauksessa (Tanium 2022, 29) ja kohdeorganisaatiossa tavallaan samalla tavalla, mutta kohdeorganisaation kuvassa on tuotu esille tikettien käsittelyä. Kohdeorganisaation nollapäivähaavoittuvuuksien käsittelyssä on huomioitu lisäksi muun muassa haavoittuneiden palveluiden vastuukysymykset, eri ryhmien toiminta ja jälkitutkinta. Haavoittuvuusskannerin tuloksien tarkastelun hoitaa pääasiassa kohdeorganisaatiossa SOC-ryhmä ja järjestelmänomistajat. Yleisellä tasolla skannerin tuottamia raportteja tarkastellaan vielä kuukausipalaverissa siihen valikoidun ryhmän sisällä ja sitä kautta annetaan haavoittuvuuksien korjauskehotuksia eteenpäin.

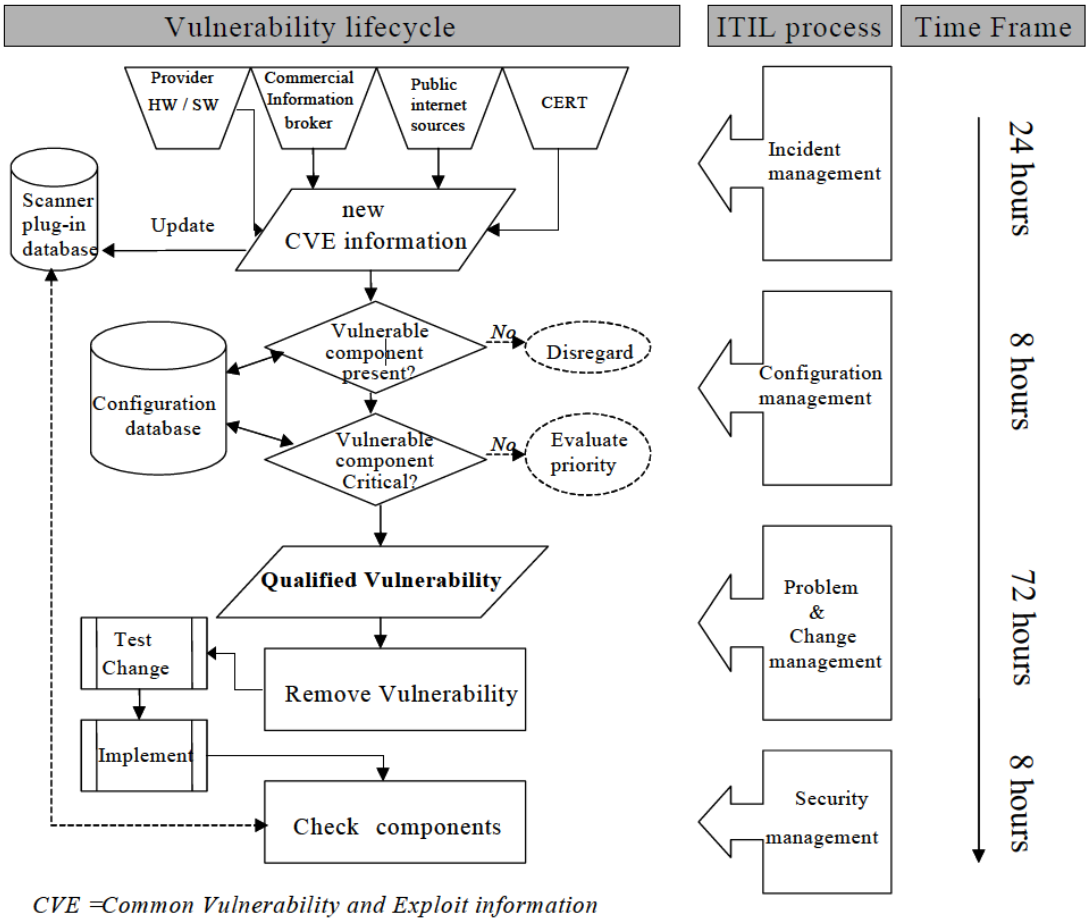
4.7.3 Hafkampin tutkimus

Hafkamp (2006) kuvailee hyvin tohtoritutkimuksessaan haavoittuvuuksien ja tietoturvatapahtumien hallintaa IT infrastruktuurin sisällä. Kuva 23 näyttää kuinka muut IT-prosessit ja palvelut liittyvät läheisesti uuden haavoittuvuuden käsittelyyn. Tutkimuksessa painotetaan, että vakaat muutostenhallintamenettelyt ovat tärkeitä sovittujen palvelutasosopimusten noudattamisen kannalta. Liian vahvat menettelytavat voivat kuitenkin estää nopean reagoinnin, jota tarvitaan tehokkaan IT-tietoturvan haavoittuvuuden ja tapausten hallinnan kannalta. (Hafkamp 2006.)



Kuva 23. Haavoittuvuuksien liittyminen IT-palveluiden hallintaprosesseihin (Hafkamp 2006)

Kuva 24 esittää haavoittuvuuden ja CVE-tiedon käsittelyn elinkaarta Hafkampin mukaisesti. Tämä vuokaavio osoittaa kuinka haavoittuvuus lähtee etenemään lähdetietojen perusteella määritellyllä CVE-tiedolla. Haavoittuvuuden tietoja täsmennetään konfigurointitietokannan ja testauksien kautta ja pyritään lopuksi poistamaan haavoittuvuus. (Hafkamp 2006, 8.)

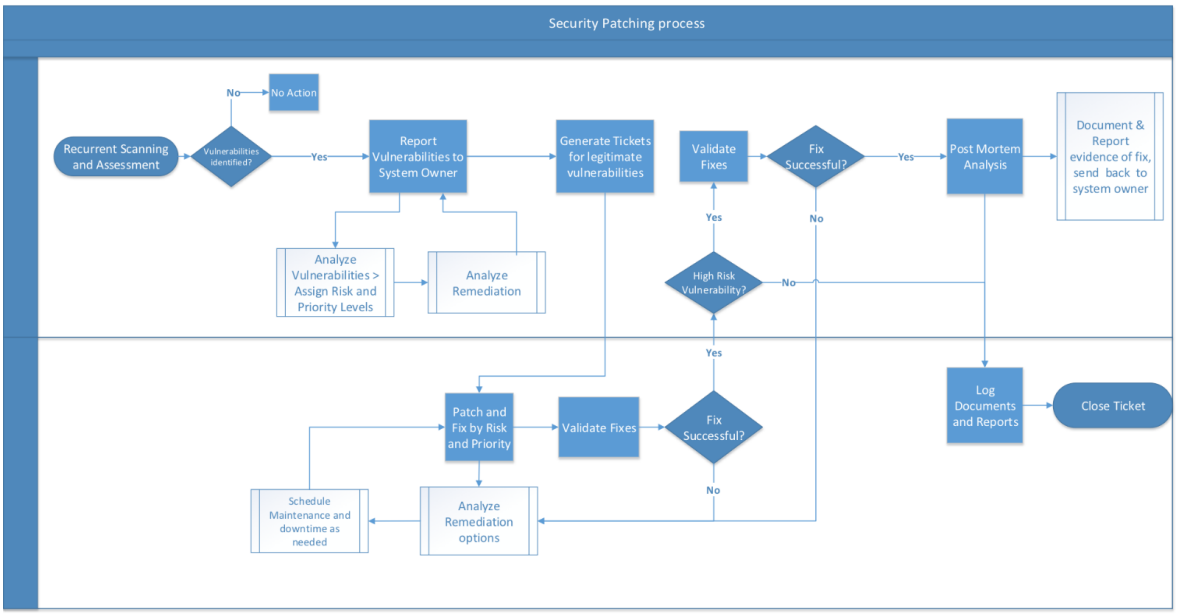


Kuva 24. Haavoittuvuuden elinkaari (Hafkamp 2006, 8)

Kuvassa 24 näkyy haavoittuvuuden käsittelytoimenpiteiden rinnalla käsittelyyn käytetty ITIL-prosessi ja suositeltu maksimikäsittelyaika Harfkampin mukaan. Haavoittuvuuksien ja tietoturvatapahtumien elinkaareen ja hallintaprosessiinkin vaikuttaa kohdeorganisaatiossa monet muut prosessit Hafkampin kuvan mukaisesti, ja ne ovat toteutettu ITIL:n mukaan. Alkuvaiheessa haavoittuvuudet tarkistetaan haavoittuvuuksien hallintaprosessin mukaisesti ja tietoturvahäiriöt taas erillisen tietoturvahäiriöiden hallinnan (eng. security incident management) kautta. Haavoittuvuuskomponentin tarkempi tarkistus ja kriittisyys tarkistetaan Hafkampin mukaan konfiguraationhallinnassa. Tämä toiminto löytyy myös kohdeorganisaatiosta, mutta haavoittuvuustarkistukset suorittaa kuitenkin SOC-tiimi. Haavoittuvuuden määrittely ja poisto tapahtuu Hafkampin mukaan ongelman- ja muutostenhallintaprosessissa, jotka löytyvät myös kohdeorganisaatiosta rinnakkaisprosesseina. Lopullisen haavoittuvuuden lopputarkastuksen tekee kohdeorganisaatiossa yhteistyössä tietoturvatiimi ja SOC haavoittuvuuden kriittisyyden mukaan. (Hafkamp 2006.)

4.7.4 Liaisonin tietoturvapäivitysprosessi

Liaison tuottaa erilaisia ohjeistuksia korkeakouluoppilaiden ja yhteistyökumppaneiden käyttöön. Liaisonin esittämää prosessikuvausta tietoturvapäivityksille voisi hyödyntää haavoittuvuuden hallintaprosessissa, koska siinä havainnoidaan haavoittuvuudet ja pyritään korjaamaan tilanne ohjelmistopäivityksillä, ja mahdollisesti muillakin korjaustavoilla. Kuva 25 näyttää Liaisonin kuvauksen tietoturvapäivitysprosessille. (Liaison 2017.)



Kuva 25. Liaisonin tietoturvapäivitysprosessi (Liaison 2017)

Päivitysprosessi etenee loppukäyttäjien koneella seuraavanlaisesti:

- Skannataan saatavilla olevat päivitykset.
- Ladataan tarpeelliset päivitykset luotettavasti lähteestä.
- Ajastetaan asennus.
- Suoritetaan päivitys. (Liaison 2017.)

Vastaava päivitysprosessi etenee tuotannossa näin:

- Hyväksytetään päivitykset ja otetaan ne käyttöön vaiheittain.
- Luodaan muutoksenhallintapyyntö ajoissa ennen huoltopäivää.
- Asiakastukitiimi julkaisee ylläpitoikkunan asiakasportaaliin.
- Suoritetaan päivitys.
- Ilmoitetaan pitkistä käyttökatkoista asianmukaisille tiimeille. Jos katkos ylittää ikkunan, asiakastuen on ilmoitettava siitä asiakkaille.
- Verifioidaan palveluiden toimivuus. (Liaison 2017.)

Poikkeuksien käsittelyyn Liaison ehdottaa seuraavia keinoja, jos haavoittuvuutta ei saada korjattua:

- Dokumentoidaan haavoittuvuuden tiedot ja perustelut korjaamattomuudelle. Perusteluina voi olla:
  - Valmistajan päivitys- tai korjaustiedostoa ei ole saatavilla.
  - Valmistajan tarjoama korjaustiedosto luo epävakautta järjestelmään; epävakaus on suurempi kuin riskit jättää päivitys asentamatta.
- Muokataan seuraavia toimintoja:
  - Verkon segmentointi.
  - Kulunvalvontaluettelot.
  - Tunkeutumisen estojärjestelmä.
- Järjestelmistä, jotka lähettävät tai tallentavat suojattuja tietoja ja joita ei voida korjata tunnetun haavoittuvuuden ratkaisemiseksi, tiedotetaan tietoturvavastaaville ja järjestelmäomistajille ja otetaan tarvittavat korvaavat hallintalaitteet käyttöön. (Liaison 2017.)

Liaison päivitysprosessi on periaatteellisella tasolla vastaava kuin kohdeorganisaatiossa onkin toimittu, ja kuva 25 auttoi lisää hahmottamaan päivitysprosessin toimintaa. Liaisonin (2017) kuvaus on hieman tarkempi kuin aiempi Taniumin (2022, 29) päivitysprosessin kuvaus ja siinä tuodaan lisäksi esille keinoja poikkeuksien käsittelyyn. Suoraan kohdeorganisaation haavoittuvuuksien hallintaprosessikuvaan tästä ei voinut tuoda asioita, koska ohjelmistojen päivitysten validointi ja päivitysprosessi tehdään muutostiketteinä muutoksenhallintaprosessin sisällä. Kuitenkin edellä mainituista prosessikuvauksista sai varmistuksia ja tietoa erilaisista toimintaperiaatteista, joita voi hyödyntää haavoittuvuuksien käsittelyssä, ohjeistuksissa ja eri prosessien kuvauksissa myös kohdeorganisaatiossa.

5 AINEISTON ANALYSOINTI

Laadullisen aineiston analysoinnilla pyritään tuomaan aineistoon selkeyttä ja tuottamaan uutta tietoa aiheesta (Eskola ym., 138). Edellisessä aineistonkeruuseen liittyvässä luvussa tehtiin osittaista aineiston analysointia jo aineiston keruu- ja litterointivaiheessa. Aineistoa kerättiin ja analysoitiin samanaikaisesti tutkimuksen edetessä, kuten on Hirsjärven (2007) mukaan mahdollista tehdä. Kirjallisuuden, haastatteluiden ja aiheen teemojen käsittelyyn käytettiin tilanne- ja sisällönanalyysiä. Teemahaastattelut tehtiin aihealueesta kokeneiden asiantuntijoiden kanssa. Tutkimusvastauksiin valittiin ja järjesteltiin sisäl-

lönanalyysissä mukaan lähinnä sellaiset vastaukset, jotka tulivat esille useamman haastateltavan kanssa (Grönfors 2011, 104). Kylläänytymisen avulla haettiin parempaa luotettavuutta vastauksiin. Yksittäiset vastaukset huomioitiin tutkimusvastauksissa, jos lähdekirjallisuus, organisaation sisäiset lähteet ja tutkijan omat havainnot tukivat samaa asiaa. Muutamia asioita käsiteltiin myös viikoittain pidetyissä opinnäytetyön, haavoittuvuusskannerin laajennustyön ja prosessin kehittämisen ohjauspalavereissa, jonka perusteella saatiin hyvää täydentävää tietoa tutkimusvastauksiin ja itse haavoittuvuuden hallinnan prosessin kehittämiseen. Sisällönanalyysiin on yhdistetty tässä vaiheessa myös kontekstianalyysiä, jonka avulla tarkistettiin asioiden konteksti, jossa ne esiintyvät (Grönfors 2011, 104).

Organisaation haavoittuvuuksien hallintaan liittyvien toimintojen analysointiin käytettiin tilanneanalyysiä, jolla huomioitiin päivittäiseen toimintaan vaikuttavat tekijät yleisiä havaintoja tekemällä yrityksen normaalissa toiminnassa, haavoittuvuuspalavereissa ja prosessia koskevissa seurantapalavereissa. Näin saatiin selville nykytilanne ja voitiin luoda tarvittaessa uusia tavoitteita. (Kokonat 2022.)

Erilaisissa rooleissa toimivat haastateltavat hahmottavat asioiden merkityksiä eri tavoin. Toisen ryhmän toimintatapoja arvosteltiin hieman voimakkaammin ja ehdotettiin heille lisää töitä. Vastaavasti oman ryhmän toimintaan ei haluttu yleensä lisävastuuta, mutta ilmoitettiin kyllä epäkohdista ja ongelmista hyvin. Selkeästi ja toistuvasti esille tulleet epäkohdat tuodaan tässä työssä objektiivisesti esille, niin että ratkaisun mahdollisille jatkotoimenpiteille tekevät myöhemmin siihen sopivat esihenkilöt.

Prosessin ja tutkimuskysymysten analysointiin käytettiin myös ymmärtämiseen perustuvaa lähestymistapaa ja laadullista analyysia, koska sen koettiin tuovan selkeimmän kuvan kokonaisuudesta (Hirsjärvi ym. 2007, 219). Alkuvaiheessa haavoittuvuuden hallintaprosessin osalta oli vaikea ymmärtää prosessin osien toiminta ja siihen liittyvät monet eri käsitteet. Asiat selvisivät vähitellen kyselemällä, tutkimalla yrityksen palvelukuvauksia sekä aiheeseen liittyvän kirjallisuuden avulla. Tulosten lopulliseen muodostamiseen käytettiin lopuksi tutkijan omia tulkintoja, jotka pyrittiin perustamaan kirjallisuuslähteisiin, jos

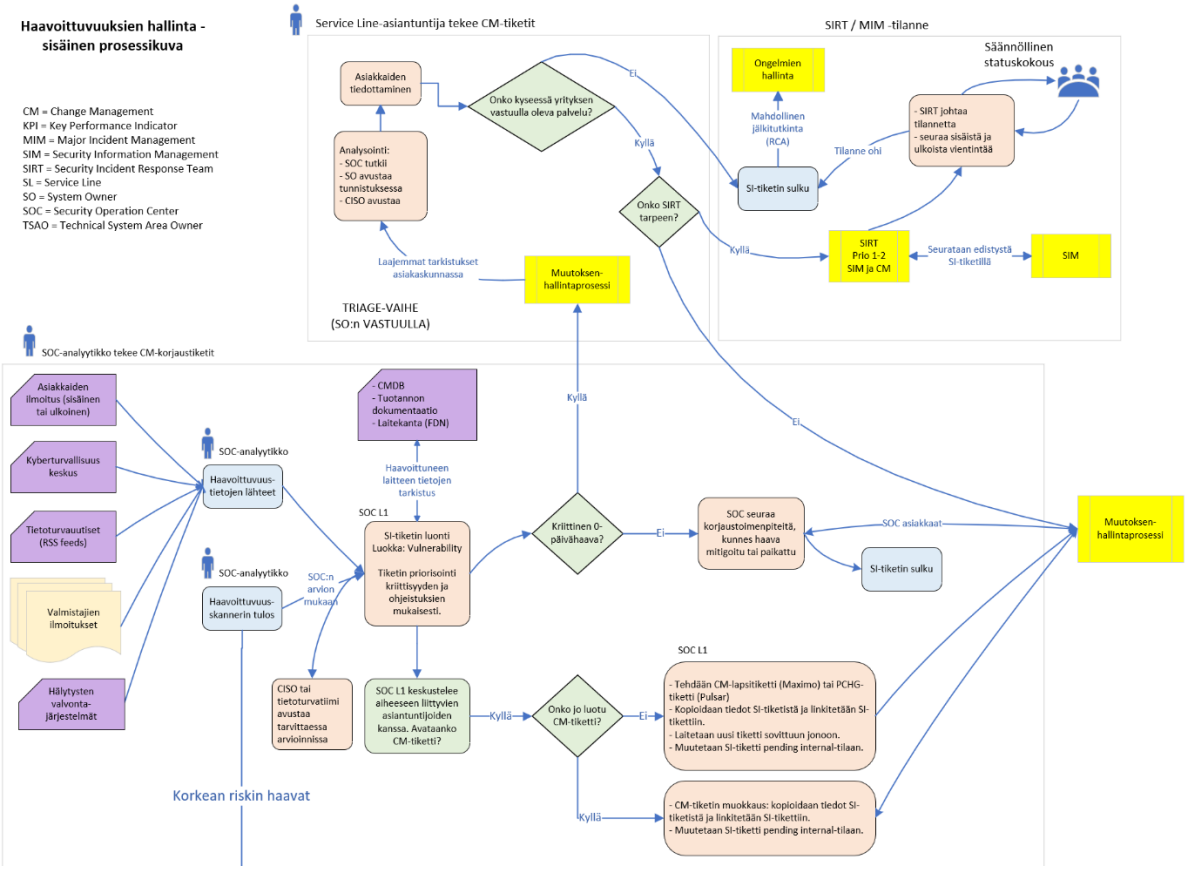
mahdollista. Erilaisilla analysointitavoilla on pyritty hakemaan löydetyille asioille ja tulkinnoille varmistuksia ja luotettavuutta.

6 HAAVOITTUVUUKSIEN HALLINTAPROSESSIN TOTEUTUS

Täysin valmista ja suoraan sopivaa haavoittuvuuksien hallintaprosessia ei ollut saatavilla, koska jokaisella organisaatiolla on omat tarpeensa, ja organisaatiot eivät yleensä julkaise tarkasti kuvattuja prosessejaan. Erilaisia ohjeita ja esimerkkejä prosessivaiheista kuitenkin löytyi. Haavoittuvuuksien hallintaprosessissa on hankala kuvata kaikkia toimintoja yhdessä, joten se vaatii useita ali- tai rinnakkaisprosesseja. Tämä kappale kuvaa yritykselle kehitettyä hallintaprosessia, jonka muutokset tai lisäykset perustuvat teemahaastatteluissa saatuihin tietoihin ja aiemmin esitettyihin kirjallisuuslähteisiin. Tutkimuskysymyksissä selvitettyjen asioiden ja lähtötietojen synteesissä saatiin muodostettua lopullinen kuvaus haavoittuvuuden hallintaprosessista.

Prosessi käynnistyy, kun SOC saa syötteen uudesta haavoittuvuudesta. Haavoittuvuuksien hallintaprosessin kuuluu oleellisesti korjausprosessi. Jos haavoittuvuuden kriittisyys ylittää sovitun tason, tiketöidään työ ja analysoidaan vaikutus ympäristöittäin. Näin saadaan ajankohtaista tietoa, onko haavoittuvuus hyväksikäytettävissä kyseisessä ympäristössä. Huomioidaan myös se, onko haavoittuvuus ulkoverkossa vai sisäverkossa, ja onko haavoittuvuus hyödynnettävissä (engl. exploit available). Jos laitteet tai järjestelmä todetaan haavoittuvaiseksi, käynnistetään korjaavat toimenpiteet. Toimenpiteinä voidaan tehdä järjestelmiin konfiguraatiomuutoksia, päivittää laitteen tai järjestelmän ohjelmisto, jos saatavilla on korjaava päivitys, tai viime kädessä eristetään tai suljetaan kyseinen järjestelmä. SOC tiedottaa ja analysoi kriittiset haavoittuvuudet järjestelmäomistajille, tietoturvatiimille ja CISO:lle. Kuva 26 näyttää haavoittuvuuksien hallintaprosessin toiminnan SOC:n analyytikon ja Service Line:n asiantuntijan toiminnan osalta.

Prosessikuvassa CM-tikettien käsittely tapahtuu muutostenhallintaprosessin (eng. Change Management Process) sisällä. Muutostenhallintaprosessi oli jo organisaatiossa kuvattu ja päivitetty ajan tasalle aiemmin ja sitä ei käydä tässä työssä läpi.



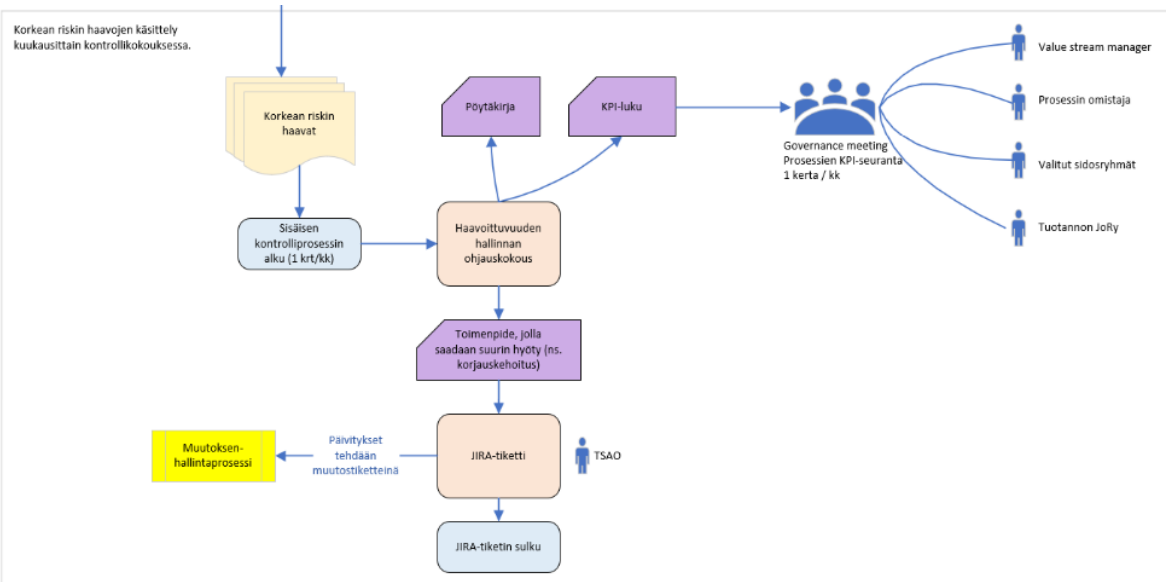
Kuva 26. Haavoittuvuuksien hallinnan prosessikuva SOC:n ja SL:n osalta

SIRT-tilanteessa haavoittuvuus on kohdistunut yrityksen vastuulla olevaan palveluun. Viimeistään tässä vaiheessa avataan haavoittuvuustiketti ITOC:lle, jos sitä ei ole jo tehty. ITOC (Information Technology Operations Center) on ryhmä, joka valvoo IT-järjestelmien ja palveluiden toimintaa. Alkuvaiheessa muodostetaan tilannekuva, jossa selvitetään tilanteen vakavuus, laajuus, aika-kriittisyys, asiakasvaikutukset ja tekninen vaikutus toimintaan. Sitten pyritään selvittämään tarkemmin, mistä on kyse ja miten poikkeaman tai vikatilanteen voisi todeta. Seuraavaksi selvitetään, ketkä ovat olleet tekemisissä aiemmin vastaavan tilanteen kanssa, ja mistä saa lisätietoja. ITOC:lle täytyy tässä vaiheessa ilmoittaa sen hetkisen SIRT/MIM-vastaavan tiedot. MIM (Major Incident Management) tarkoittaa tässä laajavaikutteisten häiriöiden hallintaa. Seuraavaksi aloitetaan aikaleimalokitietojen pitäminen, ja päivitetään tilanteesta myös tiketille säännöllisesti yhteenvedot. Tilanteeseen liittyvä viestintä täytyy hoitaa sisäiselle MIM-kanavalle, myynnille, asiakkuustiimeille, palvelupäällikköille, henkilöstölle laajemmin ja tarvittaessa asiakkaille ja viranomaisille. Tilanteen loppuvaiheena aloitetaan säännöllisten tilannekatsauksien pitäminen,

kunnes tilanne saadaan hoidetuksi. (SFS-ISO/IEC30111 2020; Hafkamp 2006, 4; Kohdeyritys 2022.)

Tietoturvahäiriön hallinnan (SIM, Security Incident Management) tehtävänä on hallita tietoturvapoikkeamia, jotka voivat vaikuttaa organisaation tai sen asiakkaiden tietojärjestelmien tai niiden käsittelemien tietojen luotettavuuteen, eheyteen tai saatavuuteen (CIA, Confidentially-Integrity-Availability). Tavoitteena oli, että hallintaprosessin avulla tietoturvapoikkeamilta voidaan mahdollisimman tehokkaasti puolustautua, pysäyttää ne ja toipua normaalitilanteeseen. Kun tietoturvapoikkeama on ratkaistu, SI-tiketti suljetaan. Jos kyseessä on ollut prioriteetin 1 poikkeama, SIRT-tiimin vetäjä järjestää loppuarvioinnin tilanteesta. Loppuarvioinnissa (engl. Root Cause Analysis, RCA) käsitellään muun muassa poikkeaman juurisyy ja ehkäisevät toimenpiteet sekä arvioidaan tietoturvapoikkeaman hallintaprosessin tehokkuutta ja kehitystarpeita. Myös prioriteetin 2 ja 3 poikkeamille on hyvä pitää loppuarviointi SIRT-tiimin, SOC-managerin ja tarvittavien SOC-analyytikkojen kesken. SIM-prosessi on aliprosessi, jota ei käsitellä tässä tutkimuksessa tämän tarkemmin. Edellä mainitut tietoturvahäiriöiden hallintavaiheet selvitettiin kohdeorganisaation dokumentaatiosta.

Kuva 27 näyttää prosessin etenemisen silloin, kun haavoittuvuus on määritelty korkean riskin (engl. high risk) haavoittuvuusluokkaan.



Kuva 27. Korkean riskin haavojen käsittely haavoittuvuuksien hallintaprosessissa

Eri prosessien KPI-mittarit käydään kerran kuukaudessa läpi Governance-kokouksessa. Governance pyrkii noudattamaan ITIL4:n mukaista ohjeistusta. KPI-mittareiden perusteella voidaan päätellä prosessien toiminnan tehokkuus verrattuna tavoitetilaan ja trendiin. Haavoittuvuuksien osalta yhtenä seurantakohteena on otettu käyttöön kriittisten haavoittuvuusmäärien seuranta kuukausittain. Tiedon saa haavoittuvuusskannerin raporttiosiosta valitsemalla trendkohdan. Tavoitteena on, että pidetään taso vähintään tasaisena tai mieluiten vähitellen pienennetään haavoittuvuuksien määrää, joka näkyy laskevana käyränä trendissä. Governance määrittelee organisaation IT-puolen rakenteen ja suunnan varmistaakseen, että koko organisaatio työskentelee kohti yhteisiä tavoitteita ja noudattaa yhdenmukaista strategiaa ja järjestelmien hallintaa. Asetetut tavoitteet ja luotu strategia suunnitellaan varmistamaan organisaation pitkän aikavälin toimintakyky. Kokouksessa tunnistetaan osa-alueet, joissa suoriutuminen ei ole ollut tavoitetason mukaista sekä suunnitellaan ja vastuutetaan sen perusteella seuraavat operatiiviset toimenpiteet. (ITIL4 2020a, 200.)

Governance asettaa toimintojen suunnan tarkastelemalla ja hyväksymällä toimintapolitiikan ja toimintakehyksen. Se varmistaa riskien optimoinnin hyväksymällä hyväksyttävät riskikynnykset ja yrityksen riskienhallinnan puitteet sekä hyväksymällä jäännösriskit. Governance delegoi vastuuta perustamalla tarvittavia uusia rakenteita ja varmistaa, että niiden roolit ja vastuut määritellään ja allokoidaan. Tällä hallintatavalla varmistetaan, että politiikat ja strategia on todella viety käytäntöön, ja vaadittuja prosesseja noudatetaan. Hallintatapa sisältää roolien ja vastuiden määrittelyn, mittaamisen ja raportoinnin, sekä tarvittavien toimenpiteiden käynnistämisen esille tulleiden kysymysten ratkaisemiseksi. (ITIL4 2020b, 20; BusinessBeam s.a.)

Tarkoituksena on noudattaa jatkuvan parantamisen keinoja ja pyritään parantamaan kokouskäytäntöjä, yleisiä toimintatapoja ja työohjeita. Seurataan prosessien, teknologioiden, järjestelmien, palveluiden kehityskohteita ja saatua asiakaspalautetta. Reagoidaan puutteisiin suunnittelemalla niille kehityssuunnitelma ja asettamalla seuraava tavoitetila Leanin oppien mukaisesti. (ITIL4 2020b, 74–86; Torkkola 2015.)

Organisaation Governancen pääperiaatteet:

- Laitetaan painopiste siihen mikä tuottaa eniten arvoa.
  - Tunnistetaan iso kuva ja pidetään se mielessä.
  - Helpot kivet käännetään ensin eli saavutetaan pienellä työmäärällä kohtuullisen suuri hyöty.
- Tunnistettava, ymmärrettävä ja kuvattava ensin millä tasolla eri osa-alueilla ollaan.
  - Tuloksena ymmärrettävä ja dokumentoitu nykytila, että voidaan kehittyä.
- Vaalitaan jatkuvaa kehitystä.
  - Pientä kehitystä jatkuvasti mieluummin kuin isoa muutosta harvoin.
  - Automatisoidaan ja yksinkertaistetaan aina kuin on mahdollista.
  - Pidetään dokumentaatio ajan tasalla, etenkin silloin kuin muutetaan asioita.
- Korostetaan näkyvyyttä, tiedon eheyttä ja yhteistyötä, johdetaan toimintaa tiedon pohjalta.
  - Mitataan prosesseja, tekemistä ja laatua.
  - Ymmärretään järjestelmien elinkaaren tila.
  - Jaetaan aktiivisesti tietoa esimerkiksi tiekarttojen avulla.
  - Data ja tieto toimii asioiden polttoaineena, joten pidetään se eheänä ja puhtaana.
  - Korostetaan toimivan yhteistyön ja vastuunottamisen merkitystä.
- Pidetään asiat ymmärrettävinä, käytännöllisinä ja yksinkertaisina.
  - Ihmisten tulee ymmärtää miten tulisi toimia. (ITIL4 2020b.)

Governance ohjaa TSAO-tiimien toimintaa prosessien näkökulmasta. Näihin toimintoihin kuuluu korjauspäivitysten hallinta (engl. patch management), varmuuskopioinnit, riittävän kapasiteetin varmistaminen, lisenssimäärien seuranta, jatkuvuussuunnitelmat ja -testaukset. TSAO:n tehtävä on johtaa aktiivisesti palveluiden teknistä toimivuutta ja tarkkailla mahdollisia puutteita järjestelmissään. TSAO ylläpitää tulevaisuuden etenemissuunnitelmaa (engl. roadmap) järjestelmiensä elinkaaren osalta. (Kohdeyritys 2022.)

6.1 RACI

Prosessien hallinnassa on tärkeä huomioida vastuunjako ja siihen liittyvä roolitus. Organisaation vastuunjaon kuvaamiseen sopii hyvin RACI-matriisi (PWC 2022, 20). Matriisin avulla voidaan varmistaa, että kaikki tietävät omat ja muiden vastuut, sekä mitä tehtäviä millekin roolille kuuluu ja kenen kanssa tehtävät tehdään. Myös ITIL4 suosittelee käytännöissään RACI-matriisin käyttöä (ITIL4 2020b, 110–111).

Rooli- ja vastuumatriisin (RACI) kirjaimet kuvaavat eri roolien vastuita seuraavasti:

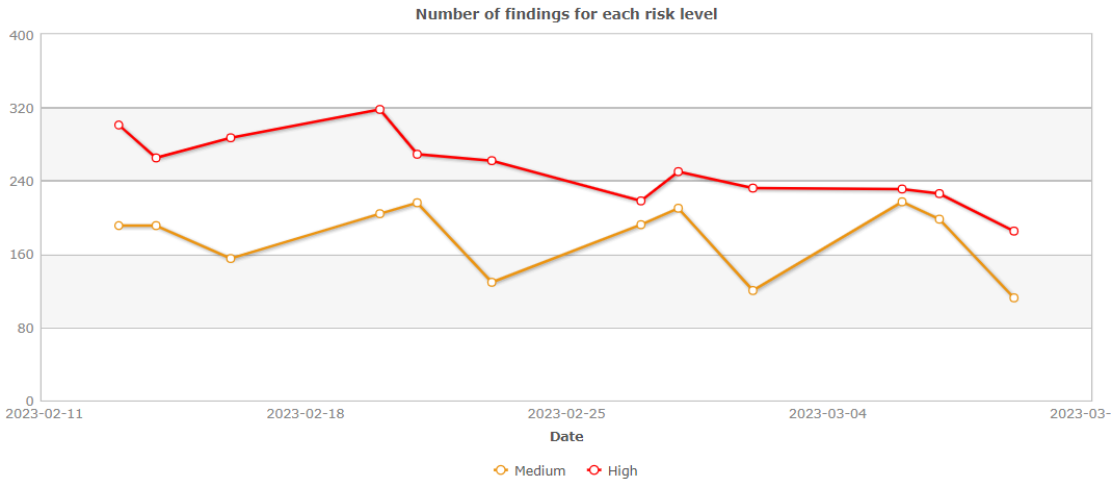
- R = Responsible = Vastuullinen. Rooli tai henkilö, joka on vastuussa tehtävän suorittamisesta.
- A = Accountable = Vastaava. Päätöksen tekijä, rooli tai henkilö, joka vastaa siitä, että tehtävä tulee tehdyksi.
- C = Consulted = Konsultoitava. Rooli tai henkilö, jolta kysytään mielipidettä ja neuvoa tehtävien tekemiseen. 2- suuntainen kommunikointi.
- I = Informed = Tiedotettava. Rooli tai henkilö, joka pidetään ajan tasalla tehtävistä. 1-suuntainen kommunikointi. (ITIL4 2020b, 110–111).

Tutkittavan organisaation haavoittuvuuden hallinnan RACI-kuvaus tehtiin pääosin tutkimuksen aikana. Organisaation haavoittuvuushallinnan tekninen omistaja puuttui tutkimuksen aikaan, ja se oli tiedostettu ongelma, mutta omistajuus löytyi aivan työn raportoinnin loppuvaiheessa. Haavoittuvuuksien tekniseen hallintaan liittyvät tehtävät jakautuivat palvelun kaupallisen omistajan ja osittain Security Technology-tiimin kesken. Tutkittavan organisaation RACI-kuvausta ei esitetä tässä, mutta haavoittuvuuksien hallintaan sopiva RACI-matriisiesimerkki löytyy liitteessä 5.

6.2 KPI-mittari

Sisäistä prosessia kontrolloidaan niin, että pyritään kuukaudesta toiseen vähentämään aktiivisten haavojen kokonaismäärää IT-ympäristössä. Haavoittuvuuksien osalta yhtenä seurantakohteena ja KPI-mittarina on otettu käyttöön uusien korkean tason haavoittuvuusmäärien seuranta kolmenkymmenen viimeisimmän päivän ajalta kuukausittain haavoittuvuuksien kontrollitapaamisessa (engl. Vulnerability Management Control Meeting). Palaverissa pyritään löytämään tehokkain tapa vähentää auki olevia haavoittuvuuksia, ja luodaan niistä erilliset JIRA-korjauskehotustiketit tekniselle palvelualueen omistajalle eli TSAO:lle. KPI-mittarit raportoidaan myös kuukausittaisessa johtotason Governance-palaverissa. KPI-mittarin käyttöä suositellaan muun muassa PwC:n, ja OVMG:n ohjeistuksissa (PwC 2022; OWASP 2020). ITIL on määritellyt useita eri nimisiä KPI-mittareita, joista tähän käyttöön sopisi myös prosessitason indikaattori (PLI), jota käytetään prosessin tehokkuuden seuraamiseen (Knowledgehut 2023).

Kuva 28 näyttää esimerkin haavoittuvuusskannerin Trend-näkymästä, kun on valittu seurantaan keskitason ja korkean tason riskit viimeisen kuukauden ajalta. Skannerin raporttitiedot voi viedä myös Exceliin ja tehdä siellä tarvittaessa haluamansa näköisen seurantakäyrän. Excelin avulla saa myös muokattua seurantakäyrästä hiukan tasaisemman viikkokohtaisesti, koska Outpost24:n kehityskäyrään tulee helposti päiväkohtaisia heilahduksia, jos eri verkkoalueiden skannauksia on jaettu eri päiville skannerinkuormituksen tasaamiseksi, kun skannattavia kohteita on useita satoja. Työaikaan suoritettuja skannauksia pyritään välttämään, ettei skannaus tuo mitään häiriöitä palvelimiin, eikä myöskään kuormita verkkokomponentteja liikaa.



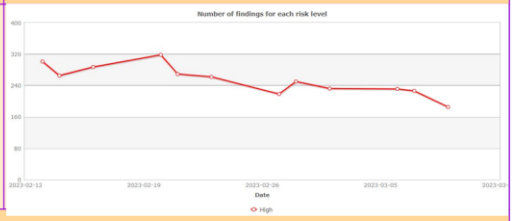
Kuva 28. Esimerkki verkkoalueen keskitason ja korkean riskien haavoittuvuusmäärien kehityksestä Outpost24:n trend-toiminnon kautta

Tavoitteena on pyrkiä pienentämään korkean tason haavoittuvuuksien määrää niin pitkään, kun niitä löytyy. Tämä näkyy laskevana käyränä kehityskäyrässä. Jos käyrä saadaan pidettyä jatkuvasti laskevana, niin se osoittaa prosessin toimivan hyvin. Jos käyrä ei laske tai jopa nousee, niin se osoittaa, että prosessiin olisi tehtävä jotain muutoksia tai ainakin täytyy löytää syy hetkittäisille muutoksille ja reagoitava niihin. Tällainen kehityskäyrän seuraaminen sopii KPI-mittariksi, koska se on visuaalisesti selkeä ja suunta on helposti tulkittavissa. Vertailuarvoksi voi ottaa myös aiempien kuukausien kehityksen. Kuva 29 näyttää esimerkin KPI-mittaritaulukosta, joka sopisi kohdeyrityksen käyttöön, jos seurataan viimeisen kuukauden kehityskäyrää korkean tason haavoittuvuuksien suhteen. Lisämittariksi voisi ottaa helposti samalla tavalla keskitason haavoittuvuuksien seurannan, kunhan ensin korkean tason haavoittuvuudet saadaan paremmalle tasolle.

HAAVOITTUVUUKSIEN HALLINTA

Prosessin tarkoitus: Pidetään korkean tason haavoittuvuuksien määrä mahdollisimman pienenä

PROSESSIOMISTAJA:
PROSESSIMANAGER:
Päivitetty: xx.xx.2023 (tekijä)

KPI Mittari	Tavoite	Status / Trendi
Korkean tason haavoittuvuuksien trendi viimeisen kuukauden aikana. High-risk-haavojen määrä tällä hetkellä = xxx	- Ei tällä hetkellä päätettyä tavoitearvoa - Laskeva trendi	
Analyysi	**Viimeisimmän kuukauden trendi-käyrä**	
Analyysi tuloksista tekstimuodossa. Trendi: Ollut laskeva. Status: Kokonaisuutena hyvä.		
Lisätietoja:		
Seuraavat vaiheet: (3. tärkeintä tehtävää prosessin/mittarin näkökulmasta)	**Päätökset / Nostot:** (tulosten perusteella)	
AP1: AP2:		

Kuva 29. Esimerkkikuva haavoittuvuuksien seurannan KPI-mittarista

Lisäksi kannattaa seurata haavoittuvuuksien määrää pidemmältäkin ajalta, jotta voidaan seuloa sieltä ainakin korkean tason haavoittuvuudet, joita ei ole saatu päivityksissä pois. Niiden selvittäminen vaatii tarkempaa selvitystyötä, joten niistä täytyy luoda JIRA-tiketti järjestelmänomistajille. Myös vanhojen haavoittuvuuksien seuraamisesta voisi tehdä käyttökelpoisen KPI-mittarin.

Jos haavoittuvuus- tai muutostikettien hoidossa olisi otettu käyttöön sisäiset palvelulupaukset (SLA:t) eli tikettien ratkaisuajoille olisi määritelty tavoitteet, niin tästäkin voisi tehdä seurattavan KPI-mittarin (Tiketöinti 2022). Tikettijärjestelmä tukisi tätä toimintoa, mutta tällä hetkellä kohdeorganisaatiossa ei haluta sisäisten tikettien vastaus- tai ratkaisuaikaa seurata.

6.3 SOC-palvelun kuvaus kohdeorganisaatiossa

Security Operations Center -palvelu (lyhenne SOC) tuottaa asiakkaalle todellisen tietoturvan tilannekuvan tietoturvapoikkeamien hallinnan (engl. Security Incident Management) avulla. SOC-palvelun tuottaa yrityksen oma SOC-funktio. SOC analysoi tietoturvajärjestelmien tuottamia hälytyksiä sekä raportteja ja tuottaa näistä kirjattuja tietoturvapoikkeamia priorisoidusti ja kategorisoidusti. Palvelun edellytyksenä on vähintään SIEM- (Security Information & Event Management) tai MDR-järjestelmän (Managed Detection and Response) käyttö. SOC vastaa tietoturvatapahtumien herätteiden käsittelystä, analysoinnista ja poikkeamatilanteen korjaavien tai niitä ennalta ehkäisevien

vastatoimenpiteiden suosittelemisesta muutoksista vastaavalle osapuolelle. Tietoturvatapahtumiin kuuluvat myös ulkoiset uhkatiedotteet.

SOC-palvelussa analysoidaan ja hallinnoidaan ympäristöstä esiin tulleita tietoturvapoikkeamia. SOC:n pääasiallinen tehtävä on valvoa erilaisia tietoturvapoikkeamia, joita koostetaan tietoturva-analysoijien sekä automatiikan avulla eri lähteiden tietoturvatapahtumista. Tietoturvapoikkeamien kirjaamisen sekä käsittelyn kautta SOC valvoo, reagoi ja kehittää oman organisaation tai asiakkaan tietoverkko- ja tietoturvapalveluita paremman tietoturvan aikaansaamiseksi organisaatioon helposti ymmärrettävässä muodossa. SOC reagoi tietoturvapoikkeamiin ennalta määritettyjen mallien mukaisesti ja tiedottaa eri osapuolia sovitulla tavalla.

6.4 Yleinen ohjeistus organisaation haavoittuvuustikettien luontiin

Asiakas tai mikä tahansa organisaation ryhmä voi tehdä tiketin yrityksen kohderyhmälle tai kohdistaa sen suoraan myös jollekin henkilölle. Jos tiketti tulee vahingossa tai tietämättömyyttä väärälle ryhmälle tai henkilölle, niin se voidaan uudelleen ohjata toiselle ryhmälle tai henkilölle. Kaikki tiketit näkyvät ryhmän tikettisivulla aluksi avoimina. Sieltä työntekijät voivat ottaa niitä käsittelyyn ja kohdistavat samalla tiketin itselleen. Kun tiketti on työn alla, niin se laitetaan ”in progress”-tilaan.

Tikettijärjestelmä tukee sähköpostien lähettämistä, joten sitä kautta voi laittaa myös kysymyksiä tiketin luojalle ja ne jäävät järjestelmään talteen. Järjestelmään kannattaa myös laittaa välihuomautuksia työtoimenpiteitä tehdessä, jos ne jäävät johonkin odotustilaan. Olisi suositeltavaa ryhmän ja tikettien hoitamisen kannalta myös käydä tikettien tilanne esimerkiksi 2 kertaa viikossa ryhmän kanssa yhdessä läpi. Joillakin ryhmillä voisi toimia myös toimintatapa, että yksi ryhmän jäsenistä on aina viikon kerrallaan tikettivastaavana ja hän hoitaa tikettien tekemistä ja ohjailua muille ensisijaisesti sillä viikolla ja käy läpi myös palaverissa tikettitilanteen. Tämä toimintatapa sopii ryhmille, joissa tehdään paljon myös muita erilaisia töitä kuten esimerkiksi kehitystöitä ja projekteja. Lopuksi hoidettu tiketti suljetaan kommentein. Tiketin luoneella henkilöllä on tässä vaiheessa vielä jonkin aikaa mahdollista reagoida tiketin sulkemiseen omin kommentein. Jos tiketin käsittelyssä on tullut esille jotain uutta tietoa,

jota ei ole dokumentoitu minnekään, tässä vaiheessa myös dokumentointia kannattaisi päivittää ryhmän kanssa sovituin tavoin.

6.5 SOC:n toimintaohjeistus haavoittuvuustikettien käsittelyyn

SOC seuraa ulkopuolisia lähteitä uusien vakavien haavoittuvuuksien varalta. SOC L1 -analysoija (tason 1 analysoija) avaa SI-tiketin (Security Incident-tiketti eli tietoturvapoikkeamatiketti) kategorialla Vulnerability (haavoittuvuuskategoria) ja priorisoi sen kriittisyyden ja SOC:n ohjeistuksien mukaisesti. SOC L1 -analysoija analysoi haavoittuvuuden ja huomioi myös haavoittuvuuden sijainnin verkossa (OWASP 2020).

Haavoittuneen laitteen tiedot voidaan tarkistaa CMDB:stä (engl. Configuration Management Database) tai tuotannon dokumentaatiosta. SOC L1 -analysoija keskustelee haavoittuvuudesta sisäisesti aiheeseen liittyvien asiantuntijoiden kanssa ennen mahdolliseen päivitykseen liittyvän muutostiketin avaamista. Näin vältytään tarpeettomilta tiketeiltä.

SOC L1 analysoija avaa Security Incident -tiketistä muutostiketin, joka on CM-tiketti Maximo:ssa (yrityksen tikettijärjestelmä) tai PCHG-tiketti Pulsar:ssa (tuotannon työnohjausjärjestelmä) ja kopioi tiedot SI-tiketistä sekä lisää muutostiketin kuvaukseen lyhyen selitteen siitä, mitä odotetaan tehtävän, mainitaan asiaan liittyvät laitteet ja laitetaan tiketti laitteesta vastaavan tahon jonoon. Jonon nimi on Maximo:ssa TIER1 tai keskustelussa sovittu muu jono. SI-tiketti laitetaan tässä vaiheessa ”pending internal” -tilaan (”odottaa sisäisesti”-tila), joka kuuluu prosessin ”Processing Stage Remediation”-osuuteen. Service Line-ryhmä toimii omien prosessiensa mukaisesti. Se varmistaa, että tiketillä on kaikki laitteet, joita haavoittuvuus koskee ja sulkee avatun muutostiketin, kun kaikki korjaukset on tehty.

SOC seuraa SI-tiketiltä lapsitiketin tilaa ja sulkee SI-tiketin omalta osaltaan, kun lapsitiketti on suljettu ja haavoittuvuus on korjattu. Tarvittaessa SOC kommentoi Security Incident -tiketille, mikäli SOC saa haavoittuvuuteen liittyen lisätietoja. SOC voi myös testata korjausten vaikuttavuutta tapauskohtaisesti.

Kriittisen nollapäivähaavoittuvuuden skenaario on muuten samanlainen, mutta tuotannon kanssa suoritetaan laajemmat tarkastukset ja otetaan SIRT mukaan, jos tarpeellista. SFS-suositusten mukaan SIRT:ssä tulisi olla vuororooli, joka vastaa herätteiden ja tikettien käsittelystä ja päättää jatkotoimenpiteistä. Herätteet voitaisiin toimittaa esimerkiksi sähköpostitse, puhelimitse tai SIRT:lle osoitetuilla raporteilla (SFS27035 2011, 26).

SOC ilmoittaa vapaamuotoisesti organisaation sisäisistä kriittisistä haavoittuvuuksista Teams:ssa kanavalla nimeltä: Production - General. Näin lisätään tiedon jakoa haavoittuvuuksista tuotannon kanssa. Yrityksen johtoa ja muitakin haavoittuvuustilannetta seuraavia henkilöitä kiinnostaa SOC-tikettien näkyvyys järjestelmässä, jotta voisi tarkkailla avattujen tikettien tilaa ja etenemistä. Tämä on kuitenkin siinä mielessä ongelmallista, että SOC-tikettien sisältö on rajattu yleensä vain SOC-ryhmälle tai ryhmän toimintaan liittyville henkilöille. SOC-asiakkaat vaativat erillisen turvallisuusselvityksen, jota ei ole teetetty kaikille organisaation henkilöille. Mahdollisesti tätä näkyvyyttä voisi kuitenkin suunnitella otettavaksi käyttöön, jos tiketti koskee vain organisaation omaa SOC-palvelua, sillä edellytyksellä, että organisaation oma turvallisuusselvitys on tehty ja vaadittu tietoturvataso saavutettu.

7 HAAVOITTUVUUSSKANNERIIN LIITTYVÄ TOTEUTUS

Tässä luvussa kerrotaan ensin haavoittuvuusskannerin käyttötapa ja -tarkoitus yrityksessä. Sitten esitellään, kuinka kehittämistavoitteena ollut yhden uuden verkkosegmentin lisääminen skannaukseen onnistui. Lopuksi selvitetään, kuinka kehittämistavoitteena ollut haavoittuvuusskannerin varmuuskopiointi ja sen palautus onnistui.

7.1 Yrityksen omien järjestelmien seuranta skannerilla

Yrityksen omien järjestelmien ja laitteiden haavoittuvuuksien tilaa seurataan Outpost24 haavoittuvuusskannerilla suoritettavien viikoittain toistuvien skannauksien avulla. Järjestelmän kattavuutta omaan infrastruktuuriin parannetaan jatkuvasti. Kerran kuukaudessa järjestetään Vulnerability Management Control -kokous, jossa seurataan haavoittuvuuksien kehitystä, sekä raportoidaan tilanne eli prosessin KPI-mittari Governance-kokouksessa, joka on myös kerran kuukaudessa tapahtuva johtotason keskustelupalaveri.

Haavoittuvuusskannerin raporttien tarkkailua varten haetaan oikeudet IDM:stä (Identity Management). IDM-käyttöoikeushallinnan avulla annetaan esimiehen tai järjestelmänomistajan hyväksynnän kautta käyttöoikeus sovelluksiin, intranet-sivuille tai muihin käyttöalueisiin (TechTarget 2021). Organisaation ohjeistuksen mukaan SOC:n lisäksi on tarkoitus, että jokainen TSAO seuraa omaa teknistä palvelualuetta suoraan järjestelmästä. Myös järjestelmäomistajat saavat hakea oikeudet työkaluun. Haavoittuvuuksien seuranta on luonnollinen osa järjestelmien ja teknisten palveluiden ylläpitoa.

7.2 Uuden verkkosegmentin lisääminen skannaukseen

Uuden verkkosegmentin lisääminen säännölliseen haavoittuvuusskannaukseen onnistui suunnitellusti. Tässä luvussa käydään läpi sen vaatimat vaiheet lyhyesti. Aluksi selvitettiin IT- ja kehityspäällikköjen kanssa oikean verkkoalueen toimintaympäristö ja tekninen omistaja. Sitten selvitettiin yrityksen verkkokuvien ja tarvittaessa verkkoasiantuntijoiden kanssa lisättävän verkkoalueen IP-osoitealueet. Kohdealueen järjestelmänomistajilta varmistettiin, saako kohteena olevan verkon ottaa mukaan skannaukseen. Seuraavaksi varmistettiin skannerin discovery-skannauksella pääsy kohteena olevalle verkkoalueelle. Yleensä pääsyä uuteen verkkoalueeseen ei ole, joten silloin otetaan yhteys palomuurien konfigurointia hoitaviin verkkopuolen henkilöihin ja ilmoitetaan mihin verkkoon sisäverkkoskannerin pitäisi päästä. Tätä varten kerrotaan sisäverkon skannerin IP-osoite ja käytettävien porttien tiedot, jotka ovat yleensä 22, 139 ja 445.

Kun palomuuriavaukset on tehty, voidaan syöttää verkkoalue skanneriin ja tehdään discovery-skannaus, joka ilmoittaa verkosta löytyneet aktiiviset IP-osoitteet (Outpost24 2023h). Jotkut IP-osoitteista voivat olla myös yhdyskäytävien osoitteita. Discovery-skannauksen löydöksistä voidaan tuottaa seuraavaksi listaus Report export -toiminnon avulla esimerkiksi Excel-tiedostoksi. Excel-listauksessa näkyville IP-osoitteille selvitetään seuraavaksi lisätietoja kohteista. Kohdeorganisaatiossa koneiden hallintatietoja voidaan hakea CMDB-järjestelmän kautta ja sitä kautta myös tarkistetaan järjestelmänomistajan nimi jokaiselle IP-osoitteelle. (Outpost24 2023g.)

Kun järjestelmäomistaja on tiedossa, otetaan häneen yhteyttä ja pyydetään häntä tai hänen alaistaan avuksi asentamaan haavoittuvuusskannerin testaustunnukset löydettyihin palvelimiin. Testaustunnukset toimitetaan vain asennusta tekevälle henkilölle, koska ne täytyy pitää hyvin salassa. Jotkut palvelimet saattavat vaatia erikoisluvan skannaukselle tai erityistunnuksen, joka hoidetaan tarvittaessa JIRA-tiketin kautta. Joissakin harvemmissa tapauksessa joku laite saatetaan joutua jättämään skannauksen ulkopuolelle. Tunnusten asennusvaihe saattaa kestää melko pitkäänkin, jos palvelimia on paljon, ja jos ne ovat usean eri järjestelmäomistajan hallinnassa.

Samaan aikaan, kun tunnuksia asennetaan kohdeverkon koneille, voi myös haavoittuvuusskannerin tunnukset määritellä valmiiksi kohdeverkon koneille. Haavoittuvuusskannerilla tunnukset määritellään skannauspolitiikan sisään. Jos kaikille koneille on sama testaustunnus, ne voidaan testata yhden skannauspolitiikan avulla. Jos tarvitaan johonkin kohteeseen erikoistunnus, voidaan näille koneille tehdä erilaiset tunnukset skannerillakin manuaalisesti tai jos koneita on hiukan enemmän, niitä varten voi tehdä myös yhden uuden skannauspolitiikan. (Outpost24 2023f.)

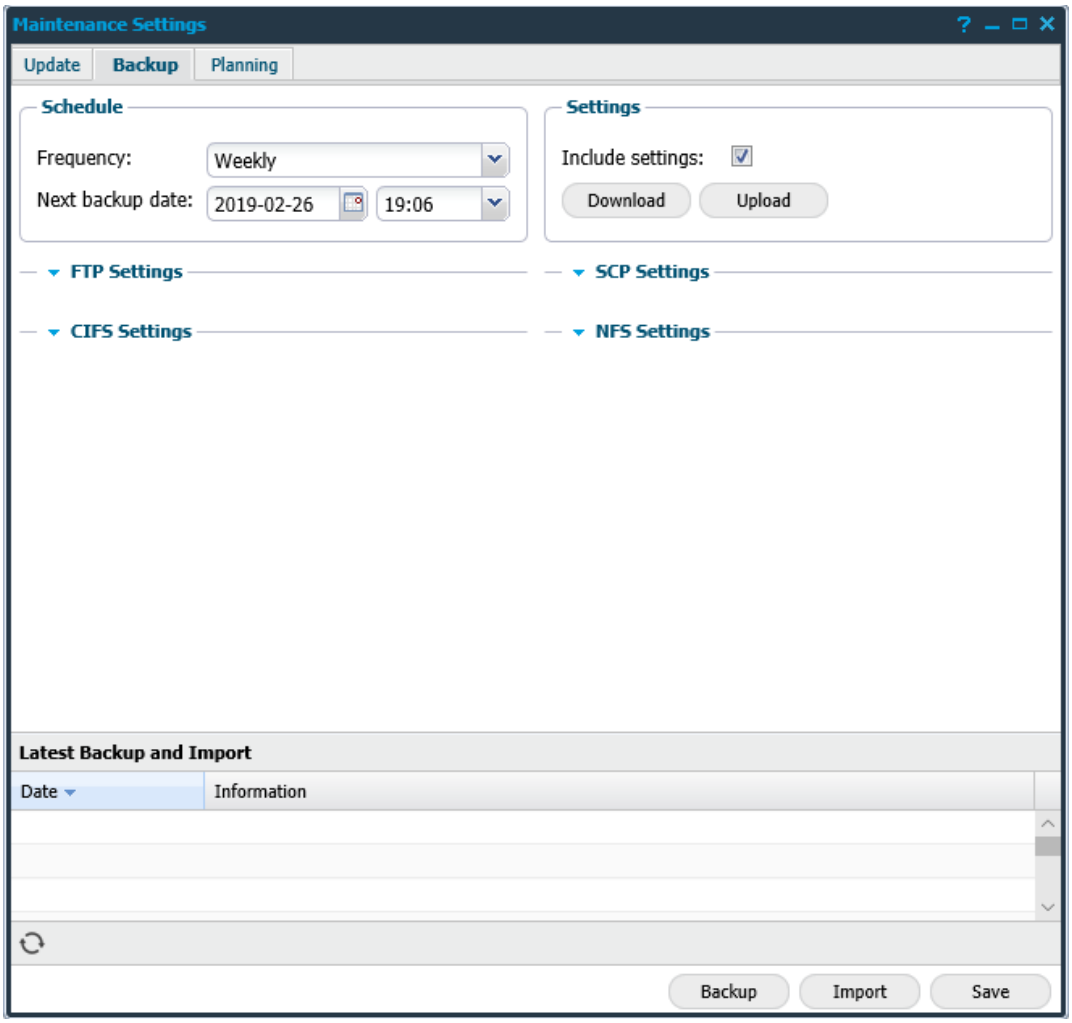
Tämän jälkeen voidaan tehdä skannaus koko verkolle joko heti tai ajastettuna haluttuun aikaan. Skannauksen jälkeen kannattaa kaikkien kohteiden raportti käydä läpi ja tarkistaa, onko sisäänkirjautuminen onnistunut ja selvittää syy, jos se ei ole onnistunut. Linux-palvelimissa käytetty SSH-kirjautuminen näkyy raportissa tekstinä ”SSH Authentication Failed”, jos testauskirjautumisen autentikointi epäonnistuu. Vastaavasti Windows-palvelimessa epäonnistunut SMB-kirjautuminen erottuu tekstinä ”SMB Supplied Login Credentials Failure”.

7.3 Outpost24 HIAB:n varmuuskopiointi

Yhtenä tutkimuskysymyksenä oli, miten haavoittuvuusskannerin järjestelmä varmuuskopioidaan ja miten se palautetaan varmuuskopiosta. Tämä koskee käytännössä vain Outpostin HIAB-scheduleria on-premise-asennettuna. HIAB-skanneria ei voi, eikä tarvitse, varmuuskopioida, koska se ei sisällä skannausdataa, eikä konfigurointitietoja. Sen pystyy asentamaan melko helposti uudes-

taan, jos se sattuisi hajoamaan. Myöskään pilvessä olevaa Outscan RC-asennusvaihtoehtoa ei voi itse varmuuskopioida. Outpost24:n teknisen tuen mukaan tuotteen valmistaja huolehtii tietokannan varmuuskopioinnista säännöllisesti ja palautus voidaan hoitaa sitä kautta, jos tietokanta sattuisi korruptoitumaan tai häviämään. Käyttäjillä ei ole pääsyä näihin varmuuskopioihin.

HIAB-schedulerista on kuitenkin mahdollista ottaa säännöllisiä varmuuskopioita (kuva 30Kuva 30), ja palauttaa tiedot varmuuskopiosta (Outpost24 2023c). Tässä kohtaa tuli aluksi ongelmaksi organisaation laboratorioympäristössä se, että siellä oli jo toisen henkilön tekemä HIAB-scheduler ja samaan verkkoinstanssiin ei voi luoda toista HIAB-scheduleria. Lopulta laboratorioympäristöön saatiin luoda toinen käyttäjätili, jolloin pystyttiin tekemään uusi HIAB-scheduler ja HIAB-skanneri varmuuskopioinnin testausta varten.

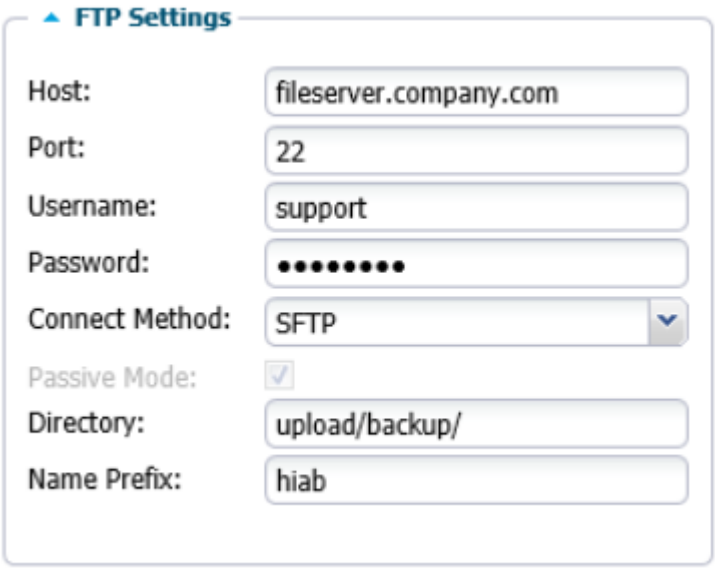


Kuva 30. HIAB:n ajastetun varmuuskopioinnin määritys (Outpost24 2023c)

Outpost24:n varmuuskopioinnissa voidaan käyttää seuraavia tiedostoserve-reitä (Outpost24 2023c):

- FTP (File Transfer Protocol). FTP on yleinen tiedostojen siirtämiseen menetelmä laitteiden ja käyttäjien välillä verkossa. FTP:tä käytetään useimmiten tiedostojen siirtämiseen isäntätietokoneen ja palvelimen tai verkkosivuston välillä.
- SCP (Secure Copy Protocol). SCP toimii Secure Shell-SSH-protokol-lalla, ja sitä voidaan käyttää tiedostojen siirtämiseen paikallisten ja etäisäntien välillä tai kahden etäisäntäkoneen välillä. SCP perustuu BSD RCP -protokollaan.
- CIFS (Common Internet File System). CIFS-protokollan avulla asiakas-järjestelmä voi kommunikoida palvelinjärjestelmän kanssa verkon kautta. CIFS on SMB:n (Server Message Block) erityinen toteutus.
- NFS (Network File System) on standardiprotokolla, jota käytetään ha-jautetussa tiedostojärjestelmässä. (Iplocation 2018.)

Testauksessa käytettiin SCP-siirtoa varmuuskopioinnin tallentamistapana toi-selle Linux-koneelle. Yhdistämismenetelmäksi voisi valita myös tavallisen FTP:n, FTPS:n (FTP Secure), implisiittisen FTPS:n tai SFTP:n (SSH FTP). Esimerkki FTP-asetuksista näkyy seuraavassa kuvassa (Kuva 31). Varmuus-kopion voi myös ottaa suoraan etähallintakoneen kovalevylle esimerkiksi tes-tausvaiheessa.



Kuva 31. Varmuuskopioinnin FTP-asetukset (Outpost24 2023c)

Lisävaihtoehto tilapäisen varmuuskopion ottamiseen on tehdä se VMwaren snapshot-toiminnon avulla. Tämä olisi lähinnä hyvä varatoimenpide silloin, kun kokeilee esimerkiksi HIAB:n oman varmuuskopioinnin toimivuutta ja palau-tusta. VMwaren snapshottien käyttöä ei kuitenkaan suositella käytettäväksi kuten normaaleja varmuuskopioita, ja ne täytyy poistaa testauksien jälkeen

(VMware 2021). Varmin ja ajallisesti helpoin keino on järjestää HIAB-schedulerin ja mahdollisesti myös HIAB-skannerin levyosiolle joku muu ulkopuolinen tapa. Tälle tulee perusteluita enemmän seuraavassa palautusosiossa.

Valmistajan ohjeistus HIAB:n varmuuskopiointiin löytyy tästä osoitteesta: https://kb.outpost24.com/kb/vulnerability-management-netsec/outscan-hiab/netsec-maintenance/hiab-backup.

7.4 Outpost24 HIAB:n varmuuskopioinnin palautus

Kopioinnin palauttamista ei kannata välttämättä testata todellisen ympäristön kanssa, koska silloin on riski menettää tai sekoittaa edelliset konfiguroinnit, jos jotain meneekin pieleen palautuksessa. Siksi testaus on pyrittävä tekemään virtuaalisessa testausympäristössä, laboratorioverkossa tai pienen erillisen verkon kanssa, jos se on mahdollista. Toimeksiantajalla on oma testausympäristö, johon voi pystyttää lähes vastaavan asennuskokoonpanon, joka mahdollistaa testauksen turvallisesti. Varmuuskopioita ja palautuksia tehdessä on syytä muistaa, että varmuuskopio on yhteensopiva vain saman HIAB-version kanssa, josta se on tehty (Outpost24 2023d). Varmuuskopion palautus onnistui valmistajan ohjeistuksen mukaan hyvin, kun olemassa oleva HIAB-scheduler oli edelleen käynnissä ja sillä pääsi vielä käyttämään varmuuskopiointitoimintoa.

Palautus menee monimutkaisemmaksi silloin, jos HIAB-scheduler on tuhoutunut kokonaan. Tällaista tapausta ei ole selvitetty valmistajan sivuilla varmuuskopiointiosuudessa, vaan tätä asiaa täytyi kokeilla ensin eri tavoin ja selvittää myös lisätietoja Outpost24:n teknisestä tuesta. Ongelmaksi tuli olemassa olevat aiemmin luodut lisenssivaraukset Outpostin serverillä. Jos HIAB-schedulerin yrittää luoda uudestaan alusta alkaen, siitä tulee automaattisesti uusi HIAB-skanneri. Syynä tähän on se, että yhdellä Outpost-tilillä voi olla vain yksi HIAB-scheduler, joka on aina ensimmäinen laite, joka luodaan ja kaikki seuraavat ovat HIAB-skannereita. Ongelman voi ohittaa vain niin, että pyydetään Outpost24:n asiakaspalvelua poistamaan hallintatilillä olevat lisenssit, ja sitten aloitetaan HIAB-schedulerin asennus alusta. Tämän jälkeen HIAB-schedulerin asennus sujuu oikein, kun sinne on päässyt kirjautumaan. Myös mahdollisen HIAB-skannerin joutuu asentamaan uudestaan, koska muuten sen lisenssi ei

päivity aiemmin tyhjennetylle hallintatilille. Näiden uudelleenasennuksien jälkeen voidaan hakea viimeisin varmuuskopio, joka palauttaa kaikki tiedot.

Valmistajan ohjeistus HIAB:n palautuksiin löytyy tästä osoitteesta: https://kb.outpost24.com/kb/vulnerability-management-netsec/outscan-hiab/netsec-maintenance/hiab-restore.

8 TUTKIMUSTULOKSET JA TULOSTEN ANALYSOINTI

Tässä luvussa esitellään vastaukset varsinaisiin tutkimuskysymyksiin. Vastaukset tarjoavat tässä työssä useita vaihtoehtoja vähentää tutkimuskysymyksissä todettua ongelmaa tai poistaa se kokonaan. Vastauksien jälkeen analysoidaan tutkimuskysymykseen saatuja tuloksia samassa luvussa. Kehityskohteiden lopputulosten tai löydösten analysointi on viimeisessä luvussa. Tutkimustuloksiin valitut tulokset perustuvat loppujen lopuksi toimintatutkimuksen mukaisesti tutkimuksen tekijän päätelmiin asioista, joten niissä on aina tekijän jälki. Tutkimustuloksista muodostetaan lopuksi synteesit, joissa kootaan yhteen pääasiat aiheesta ja joiden avulla vastataan tutkimusongelmaan luvussa johtopäätökset (Grönfors 2011, 100).

8.1 Millä tavalla yrityksen sisäistä haavoittuvuuksien hallintaprosessia kannattaisi kehittää paremmaksi?

Tämän päätutkimuskysymyksen alakysymyksenä oli myös ”Mitkä ovat nykyisen haavoittuvuuksien hallintaprosessin heikkoudet tai puutteet?” Nämä kaksi kysymystä liittyivät läheisesti samaan aiheeseen, joten ne käsitellään tässä samassa kappaleessa. Aihe on niin laaja, ettei tähän ole ihan lyhyttä vastausta, vaan vastaukseksi on koottu parannusehdotuksia ja toimintatapoja, jotka voisi ottaa käyttöön kohdeyrityksessä. Näitä kuvattuja toimintoja on esitetty ja selostettu myös jonkin verran haavoittuvuuksien hallintaprosessia koskevassa luvussa.

Haavoittuvuuksien havainnointi oli ajoittain todettu puutteelliseksi ja siksi siihen puoleen kannattaa kiinnittää huomiota. Laitteita ja alustateknologioita ei tunnistettu riittävällä tarkkuudella ja tämä johti siihen, että osa laitteista sekä alustoista saattoi jäädä päivittämättä. Tämän takia ryhmän vastuulla olevat eri-

laiset laitteet ja teknologiat pitäisi listata, jos niin ei ole jo tehty, ja selvittää ryhmän sisällä niihin liittyvät koulutustarpeet ryhmässä. SFS-standardeissa (SFS-ISO/IEC27000 2020; SFS-ISO/IEC27001 2017) ja ITIL4-viitekehyksessä (ITIL4 2020a) tuodaan toistuvasti esille vastuiden kuvaamisen tärkeys hallintajärjestelmissä ja yrityksen sisäisessä toimintaympäristössä. Vastuiden määrittely teknologioiden osalta voitaisiin määrittää tässä työssä aiemminkin mainitun RACI-taulukon avulla tai sitten liikennevalomallia käyttämällä, jolla voidaan tuoda selkeästi esille kyseisen teknologian päivitystilanne. Liikennevalomallista löytyy esimerkki muun muassa ERA:n johtamisen ja hallinnan kypsyysmallin oppaasta (ERA 2018, 16).

Proaktiivinen toiminta teknologioiden päivitysten suhteen vaikutti kyselyiden mukaan vähäiselle. Tämän parantamiseksi otettiin tutkimuksen aikana (1.1.2023) käyttöön vuosikello, jonka tarkoituksena on käydä teknologioiden päivitystä läpi proaktiivisesti. Tutkimuksen loppuvaiheessa vuosikellon dokumentaatio eri teknologioista oli vielä puutteellinen ja sitä pitäisi täydentää pian. Vuosikellon pohjan voi suunnitella itse ja sitä varten löytyy myös valmiita sovellutuksia. Muun muassa Aalto Yliopisto käyttää vuosikelloa suunnittelun ja kehityksen hallinnassa apuna (Aalto University 2023).

Henkilöresursseja ei ollut kohdistettu laiteresursseihin riittävän tarkalla tasolla, ja tämän takia teknologiaspesifinen osaaminen oli heikohkoa. Erityisesti prioriteetti 1-haavoittuvuuksien suhteen oli todettu ongelmaksi työvoimaresurssien jatkuva metsästys. Haasteena oli, ettei tiedetty, kuka osasi mitäkin teknologiaa ja näin ollen päivitysresurssien etsimiseen kului paljon aikaa. Tätä varten täytyisi tehdä ryhmän jäseniä koskeva teknologiaosaamislista, jota voisi käyttää päivitysresursseja etsiessä. Saman tai vastaavan listan kautta voisi määritellä myös osaamiseen liittyvät kehittämistarpeet. Yritys jo tukikin tiettyjen järjestelmien sertifikaattien suorittamista palkitsemalla niistä ja tätä kannattaa jatkaa ja mahdollisesti monipuolistaa entisestään.

Prosessissa täytyy tuoda selkeästi esille järjestelmäomistajien vastuu haavoittuvuuksien suhteen sekä päivityksistä vastaavien vastuu ja tekeminen, kuten ITIL4-ohjeistuksessa kehotetaan (ITIL4 2020a). Prosessista täytyy huomioida myös se, että SOC ei tee kaikkia vaiheita ja erotella ne selkeästi. Prosessikaa-

viossa tämä tuotiin esille niin, että SOC:n toiminnot näkyvät omassa lohkossaan. Päivityksistä vastaavien tahojen, järjestelmänomistajien ja SOC:in täytyisi toimia enemmän yhteistyössä. Tässä oli ongelmana, että myöskään SOC ei osaa antaa aina lisätietoa kaikista haavoittuvuuksista ja miten se korjataan, koska haavoittuvuudet voivat olla järjestelmissä, joita he eivät omista teknisesti eivätkä välttämättä ymmärrä tarpeeksi hyvin. Tämän takia päivityksiä tekevien henkilöiden on syytä ensisijaisesti selvittää itse päivitysten ja haavoittuvuuksien hallinta omissa teknisissä järjestelmissään, jos mahdollista. Todennäköisesti tämä tehtävänjako ja haavoittuvuuksien hallinta SOC:n ja päivityksien tekevien tiimien välillä täytyy selvittää tarkemmin. Tämä voitaisiin tehdä myös RACI-taulukon avulla, josta on esimerkkikuva liitteessä 5.

Tärkeänä korjaavana toimenpiteenä todettiin, että järjestelmänomistajille täytyisi allokoida riittävästi aikaa valvoa ja parantaa vastuullaan olevaa järjestelmäänsä. Aika- ja resurssipula oli todettu monen järjestelmänomistajan ongelmaksi. Yksi ehdotus olisi, että määritellään organisaation sisäisille tiketeille SLA (Service Level Agreement), jolla olisi korkeampi prioriteetti kuin asiakkailla, koska kaikki mitä tehdään organisaatiossa sisäisesti, liittyy myös epäsuorasti asiakkaisiin. SLA:n merkitys tuodaan esille ITIL4:ssa (2020b, 42–43), ja sen avulla voitaisiin tehdä tarvittaessa myös toiminnan tehokkuuden seurantaa. Johdolla oli myös toive, että SOC:n tutkimista asioista pitäisi jäädä aina jälki ja niihin olisi parempi näkyvyys sisäisen asiakkaan suuntaan organisaation sisällä. Joissakin järjestelmissä tämä seuranta onkin, mutta niihin eivät kaikki pääse käsiksi, ja tämä taas liittyy rajattuihin tietoturvaselvityksiin. Tämän asian jatkoselvittely olisi hyvä ottaa esille kehityspalavereissa.

Kokonaisprosessin omistajuus oli organisaatiossa tutkimuksen aikoihin epäselvä, koska edellinen CISO irtisanoutui. Hänen lähdettyään tilalle ei ole löytynyt tarpeeksi nopeasti uutta sopivaa henkilöä ja siksi tutkimuksen aikoihin tilalle perustettiin erillinen tietoturvatiimi organisaation muista henkilöistä hoitamaan CISO:n joitakin tehtäviä. Kokonaisprosessille nimettiin tutkimuksen loppuvaiheessa vastuullinen henkilö, kuten ITIL4-ohjeistuksessa (ITIL4 2020b, 111) edellytetään.

Organisaation CMDB ei sisällä vielä tietoja kaikista laitteista ja järjestelmistä, joten sitä pitäisi täydentää niiltä osin. Jokainen järjestelmäomistaja voisi käydä

läpi omat palvelunsa ja niihin kuuluvat verkko-osoitteet sekä tarkistaa, että vaaditut tiedot löytyvät CMDB:stä. Tietojen selvittämistä vaikeutti yleisesti se, että dokumentointi oli hajautunut useaan järjestelmään. Tähän olisi apuna järjestelmien opiskelu haavoittuvuudet huomioiden, dokumentoinnin parantaminen ja mahdollisesti rinnakkaisista järjestelmistä luopuminen.

Haavoittuvuuksien korjaaminen voi olla hidasta. Tämä ei sinänsä ole prosessin vika. Juurisyyt haavoittuvuuksien poistamisen hitaudelle tulisi tunnistaa, jotta haavoittuvuudet saadaan paikattua tulevaisuudessa mahdollisesti nopeammin. Yhtenä parannuskeinona joissakin toiminnoissa voisi olla automaatio, josta esimerkkinä on SOAR (engl. Security Orchestration, Automation and Response), jota on jo otettu käyttöön joillakin asiakkailla. SOAR on ohjelmisto, jolla voi automatisoida ennalta määrättyjä työnkulkuja. (PWC 2022, 15.)

Tutkimuskysymys 1 - Tulosten analysointi

Haavoittuvuuden hallintaprosessin kaikkien ongelmien poistumista ei pystynyt tutkimuksen loppuvaiheessa toteamaan, koska kaikkia toimintoja ei ollut vielä otettu käyttöön. Tavoitteena oli luoda yhtenäinen prosessikuva, selvittää heikkoudet ja löytää niille korjausehdotukset. Nämä tavoitteet saatiin tehtyä ja nyt ne voidaan viedä käytäntöön, joten siinä mielessä tutkimustyö onnistui. Ehdotukset saatiin koottua monimetodijärjestelmän mukaisesti useasta näkökulmasta tarkasteltuna. Toimintatutkimukseen liittyvä jatkuva seuranta ja kehitys jatkuu toimintatutkimuksen syklin mukaisesti, ja vasta myöhemmin voidaan todeta, miten ohjeistukset toimivat. Tässä vaiheessa arviointia ovat tekemässä ne henkilöt, jotka ovat prosessissa mukana toimintatutkimuksen periaatteiden mukaisesti (Kananen 2014, 137).

Tutkimuksen loppuvaiheessa myös haavoittuvuuden hallintaprosessille löytyi omistaja, joka puuttui alkuvaiheessa, joten se tavoite saavutettiin. Haavoittuvuusmääriä seuraavan KPI-mittarin trendikäyrä on ollut tutkimuksen ajan loivasti laskeva, vaikka uusiakin kohteita on lisätty skannauksen piiriin, joten sekin osoittaa, että prosessi toimii tältä osin.

8.2 Haavoittuvuustikettien käsittelyn parannuskeinot?

SOC voisi käsitellä enemmän palvelimien päivitysten hallintaa palavereissa ja olla yhteystyössä niiden ryhmien kanssa, jotka tekevät päivityksiä palvelimille. Päivitysten hallinnan koordinointia ja ryhmien välistä tiedonsiirtoa olisi hyvä olla valvomassa ja hoitamassa koordinaattori tai sisäinen palvelupäällikkö. SOC-tiketteihin oli heikko näkyvyys tai sitä ei ole ollenkaan organisaation sisällä tarkastelijan toimenkuvasta riippuen. Voisi selvittää, kuinka haavoittuvuus- ja päivitystikettien hoidosta vastaavat esimiehet voisivat saada oikeudet yrityksen sisäisten tikettien seurantaan, jos sitä ei jo ole. Organisaation IDM-järjestelmän saisi mahdollisesti tukemaan tätäkin asiaa. SOC:lle voisi resursoida aikaa myös järjestelmäomistajien puolelta otettaviin työkeikkoihin.

Selkeytetään SOC-analyytikon ohjeistukseen, millaisella päätöksellä tai rajauksella ulkoisista lähteistä nousevista ilmoituksista tai haavoittuvuusskannerin löydöksistä luodaan SI-tiketti (Security Incident eli tietoturvatapahtumatiketti). SOC:n toimintaohjeisiin olisi syytä määrittää, kuinka usein ja säännöllisesti ulkoisia lähteitä analysoidaan, ja ketkä sen tekevät. Yhtenä hyvänä tikettien seurantakeinona on todettu joissakin ryhmissä, että pidetään esimerkiksi kaksi kertaa viikossa ryhmän tikettipalaveri, jolloin keskustellaan avoimista ja kesken olevista tiketeistä ja pyritään hoitamaan ne mahdollisimman tehokkaasti eteenpäin jakamalla tarvittaessa tehtäviä.

Ohjeistuksessa täytyisi määritellä, mitkä korkean tason haavat (high-risk) voidaan jättää odottamaan toistuvaa kuukausittaista kontrollikokousta, ja mihin tulee reagoida nopeammin. Haavoittuneen koneen järjestelmäomistajan voi selvittää Pulsar-järjestelmän kautta ja hänelle tulisi ilmoittaa pahiten haavoittuneesta koneesta.

Tutkimuskysymys 2 - Tulosten analysointi

Haavoittuvuustikettien käsittelyyn oli tavoitteena löytää parannuskeinoja ja niitä löytyikin jonkin verran. Parannuskeinoehdotukset saatiin kerättyä haastatteluiden ja tutkijan havaintojen perusteella. Kanasen (2014, 139) mukaan toimintatutkimuksessa todellinen muutos saadaankin toteutetuksi paremmin, jos muutosehdotukset tulevat prosessiin tai toimintoihin osallistuvilta henkilöiltä.

Näille vastauksille oli vaikea löytää tukea kirjallisuuslähteistä, joten vastauksien osalta täytyy luottaa asiantuntijoiden lausuntoihin, ja heidän kokemukseensa käytännön toiminnoista.

Myös itse tutkija tulee osallistumaan kokonaisprosessin tiettyihin toimintavaiheisiin jatkossakin. Selvitetyt ehdotukset viedään esimiestasolla eteenpäin ja niiden käyttöönotto ja toimivuus tulee selviämään myöhemmin. Toimivuuden arviointiin sopii parhaiten SOC-ryhmä, sen esimies ja muut järjestelmäomistajat, jotka toimivat SOC:n kanssa yhteistyössä. Ryhmän koordinaattoritehtävään liittyvään toimenkuvaan sopivaa henkilöä on jo alettu etsiä, joten tämä asia alkoi edetä jo hyvin nopeasti.

8.3 Kuinka täytyisi reagoida nollapäivän haavoittuvuuksiin?

Nollapäivän haavoittuvuus on sellainen tietoturva-aukko verkossa tai tietokoneohjelmassa, jota ei ole havaittu aiemmin. Se on ohjelmistoihin tai laitteistoihin liittyvä virhe tai heikkous, johon ei ole sillä hetkellä korjaavaa päivitystä. Nollapäivän haavoittuvuus on korjattava ja ratkaistava kehittäjien ja kyberturvatiimien toimesta mahdollisimman nopeasti ennen kuin hyökkääjät käyttävät haavoittuvuutta hyväkseen. Hyökkääjät voivat onnistua hyökkäyksessään, jos yrityksellä ei ole suojausstrategiaa. (NordicDefender 2022.)

Yksi vaihtoehto toimintatavaksi olisi käyttää tiedotuslistaa, johon olisi SOC:n, CISO:n tai mahdollisen muun tietoturvatiimin lisäksi listattu yrityksen sisäiset järjestelmäomistajat ja heidän käyttämänsä teknologiat. Näin voisi tiedottaa selkeämmin oikeaan haavoittuneeseen teknologiaan liittyviä oikeita henkilöitä. Tämä voisi toimia sekä organisaation sisäisillä asiakkailla että ulkoisilla.

Haavoittuvuuden tietoisuuteen tulemisen jälkeen asia tulisi saada SOC:n kautta järjestelmäomistajien tutkintaan pikimmiten ja myös SIRT:lle, MOD:lle (Manager On Duty, päivystävä johtaja) ja CISO:lle. Tanium (2022) tuo esille ohjelmistopäivitys- ja haavoittuvuuksien tarkkailuohjeistuksessaan, kuinka SOC arvioi tarvittaessa yhteystyössä CISO:n kanssa haavoittuvuuden kriittisyyden.

Nollapäivähaavoittuvuuksista tulee luoda laaja näkyvyys organisaatiossa ja se olisi hyvä tiedottaa ainakin yleiselle Teams-kanavalle. Voisi myös harkita muutakin keskitettyä paikkaa, johon kuka tahansa voisi ilmoittaa epäillyn (kriittisen) haavoittuvuuden, ja josta näkee myös mahdollisesti aktiiviset vakavat haavoittuvuudet sillä hetkellä.

Nollapäivähaavoittuvuuksien käsittelylle voisi joko luoda oman aliprosessinsa tai muussa tapauksessa se täytyy olla huomioitu kokonaisprosessissa selkeästi. Pitäisi kuvata tarkasti roolit, vastuut sekä eskalointitavat. Määritellään myös tilanteet, milloin täytyy hälyttää henkilöitä töihin ja keitä he ovat. Hyvin tehdyt ohjeistukset toisivat toimintaan selkeyttä ja nopeutta. Osaston täytyy täyttää palvelulupauksensa, jos sellainen on määritelty.

Tutkimuskysymys 3 - Tulosten analysointi

Tutkimuskysymyksen tavoitteena oli selvittää organisaation oikeat toimintatavat tilanteeseen, kun tulee ilmi nollapäivän haavoittuvuus. Tähän aiheeseen ei löytynyt haastatteluissa kovin paljon parannusehdotuksia, mutta kuitenkin pari ideaa, jotka otettiin ehdotukseksi mukaan tuloksiin. Lisäksi tutkija vertaili eri lähteiden vastaavia toimintatapoja ja ne tuotiin myös esille tuloksissa. Uusia toimintatapaehdotuksia ei ole vielä otettu käyttöön, mutta ne esitetään vaihtoehtoina näistä asioista päättäville henkilöille. Ehdotusten toimivuus käytännössä selviää sitten myöhemmin.

Nollapäivän haavoittuvuuksien käsittelylle on kuvattu oma reittinsä prosessikaaviossa. Prosessi todettiin kokonaisuudessaan toimivaksi viimeksi tutkimuksen loppuvaiheessa, kun paljastui Outlook:n toimintaan liittyvä vakava nollapäivän haavoittuvuus (CVE-2023-23397). Tiedotus toimi tässä tapauksessa myös kohtuullisen hyvin, mutta siihen voi harkita myös lisäksi tuloksissa mainittuja ehdotuksia.

8.4 Kuinka voidaan pienentää haavoittuvuusskannerin löytämien väärien positiivisten määrää?

Tähän kysymykseen löytyi vastauksista tutkijan omilla kokeiluilla haavoittuvuusskannerin kanssa, valmistajan dokumentoinnista ja myös kysymällä suoraan tarkennuksia valmistajan teknisestä tuesta. Vahvistuksia vastauksiin ja muuta uutta tietoa löytyi myös lähteistä. Löydettyjen väärien positiivisten haavoittuvuuksien määrään voi vaikuttaa sekä skannerin päässä että kohteissa ja siksi vastaukset ovat jaettu kahteen eri listaan selvyyden vuoksi.

Seuraavat toimenpiteet vähentävät ylimääräisiä vääriä positiivisia haavoittuvuuksia skannerin päässä:

- Tarkistetaan ajoittain, että haavoittuvuusskannerin automaattiset päivitykset sen omalle ohjelmistolle ja liitännäisille ovat tapahtuneet säännöllisesti (Securitymetrics 2015a).
- Outpost24:n asetuksista löytyy ”Filter potential false positives”-valinta (Outpost24 2023a), joka on erittäin tehokas apukeino tähän ongelmaan. Toiminto perustuu Castsoftwaren (2017) mukaan joissakin skannereissa ohjelmistokomponenttien ”kuolleen koodin” ja kirjastojen tarkempaan tutkimiseen. Outpost24:n teknisen tuen mukaan heidän työkalussaan käytetään hyväksi heidän omaa tietokantaansa. He tarkistavat sovellusten otsikkotiedot, versiot, kirjastot ja rekisterit. Joissakin harvinaisissa tapauksissa, kuten Log4J:n suhteen, tehdään myös tiedostoindeksointia haavoittuvuuksien havaitsemiseksi.
- Asiantuntijoiden eri tavoin varmistamat väärät positiiviset löydökset voidaan merkitä skannerin raporttiin ”False Positive = Yes”, jolloin jatkossa tämä löydös on vahvistettu väärä positiivinen ja siitä ei tarvitse välittää. Merkitsemistapa on ohjeistettu Outpost24:n dokumentoinnissa (Outpost24 2023i).
- Useimmat löydökset voitaisiin vahvistaa vääriksi positiivisiksi penetraatiotestauksen avulla (Castsoftware 2017). Sen voi tehdä erilaisilla työkaluilla asiantuntijoiden toimesta, ja myös osa monipuolisimmista haavoittuvuusskannereista tukee tätä ominaisuutta. Metasploit Framework on hyvä esimerkki suositusta penetraatiotestaukseen soveltuvasta työkalusta (Shetty 2011).
- SIEM-järjestelmien korrelaatiotoimintojen avulla pystyttäisiin seulomaan väärien positiivisten löydösten määrää, kuten Hyvärinen (2013) toteaa tutkimuksessaan. Perinteisen SIEM-järjestelmän löytöjä ei pysty helposti yhdistämään automaattisesti haavoittuvuusskannereiden löydöksiin, jos haavoittuvuusskanneri ei tule sitä, mutta tätä vertailutyötä voi tehdä ainakin manuaalisesti. Myös SOAR/SIEM-järjestelmissä laajennetaan ominaisuuksia enemmän haavoittuvuusskannausten suuntaan, kuten Pedab (Pedab s.a.) mainostaa. He tarjoavat myös olemassa olevan haavoittuvuusskannerin integroinnin heidän omaan SIEM-ratkaisuunsa.

Seuraavat toimenpiteet skannauskohteissa vähentävät väärien positiivisten haavoittuvuuksien määrää:

- Pidetään ajureiden, ohjelmistojen ja liitännäisten päivitykset aktiivisesti ajan tasalla (Manzuik 2006, 8–9).
- Ei asenneta tai pidetä laitteissa ylimääräisiä ohjelmistoja (Manzuik 2006, 8–9).
- Skannattaviin kohteisiin täytyy olla testaustunnus skanneria varten järjestelmähaltijan oikeuksin. Myös kohteen rekistereihin täytyy olla pääsyoikeus. (IBM 2022.)
- Ei poisteta laitteista korjaus- ja päivitystiedostoja, koska skannerit voivat päätellä myös niiden perusteella versiotietoja.
- OVAL-skannauksissa WMI (Windows Management Instrumentation) on konfiguroitava oikein (IBM 2022).
- Backporting-ilmiön välttämiseksi pyritään käyttämään järjestelmässä mahdollisimman uusia ohjelmistoja ja ajureita, joihin saa suoraan uusia päivityksiä (HolmSecurity 2022; RedHat 2023).

Tyypillisestä haavoittuvuusskannereilla skannataan ennalta tuttua verkkoaluetta, varsinkin jos verkko on yrityksen oma. Asiakasverkkojen suhteen voi olla erilaisia rajoituksia varsinkin kirjautumistunnusten suhteen. Kohdeverkon laitteita ei välttämättä tarvitsisi valmistella mitenkään skannausta varten, mutta näin tehtynä tulokset eivät olisi hyviä aiemmin työssä mainituista syistä, ja myös vääriä positiivia löydöksiä tulisi turhan paljon.

Tutkimuskysymys 4 - Tulosten analysointi

Tässä tutkimuskysymyksessä oli tavoite löytää erilaisia keinoja pienentää haavoittuvuusskannerin löytämien väärien positiivisten löydösten määrää. Tähän kysymykseen ei löytynyt oikein apua teemahaastatteluista, koska kysymys vaati syvempää perehtymistä ongelmaan. Tavoite kuitenkin saavutettiin, koska lähteitä hyödyntämällä löydettiin useita erilaisia keinoja, joita kannattaa hyödyntää skannerin päässä sekä skannauskohteissa. Suurin osa toiminnoista myös testattiin ja todettiin toimiviksi jo käytännön testeissä, joka lisää tulosten luotettavuutta. Tuloksia pystyttiin tätä kautta myös tarkentamaan paremmin. Useiden tulosten osalta toteutui myös toimintatutkimuksen syklinen kehitys, koska ominaisuuksia päästiin testaamaan labra- ja tuotantoympäristössä. Joihinkin tuloksiin perustuvaa jatkotutkimusta organisaatiossa tullaan miettimään lähitulevaisuudessa lisää.

8.5 Kehityskohteiden tulosten analysointi

Tässä luvussa analysoidaan kehityskohteina olevien aihealueiden tuloksia ja löydöksiä. Haavoittuvuuden hallintaprosessin osalta tulee esille osittain samoja asioita, joita mainittiin jo ensimmäisenkin tutkimuskysymyksen kohdalla, jossa etsittiin parannuskeinoja hallintaprosessiin.

Haavoittuvuuden hallintaprosessin osalta oli tavoitteena täydentää prosessikaaviota lähinnä SOC:n osalta, ohjeistaa toimintatapoja ja löytää toiminnoille luotettavat lähteet. Nämä tavoitteet saavutettiin siinä mielessä, että prosessikaaviota ja ohjeistuksia täydennettiin haastatteluissa ja lähteissä esille tulleiden asioiden perusteella. Prosessin toiminta kuvattiin hallintaprosessin toteutusta kuvaavassa luvussa. Jatkuva seuranta ja kehitys jatkuu toimintatutkimuksen syklin mukaisesti, ja vasta myöhemmin voidaan todeta, että miten ohjeistukset toimivat. Myöhemmässä vaiheessa arviointia ovat tekemässä ne henkilöt, jotka ovat prosessissa mukana. Tulosten on tarkoitus palvella käytäntöä ja jos näillä muutoksilla saavutetaan jotain kehitystä, niin voidaan todeta, että tavoite on saavutettu. Käytännön toiveet oli kerätty monimetodisen tutkimusmenetelmän mukaisesti tutkijan havaintojen, teemahaastatteluiden ja organisaation tarpeiden perusteella.

Uusien verkkoalueiden ensimmäisessä skannauksessa paljastuu usein varsinkin Windows-palvelimissa huomattava määrä haavoittuvuuksia. Tämä johtuu useimmiten viivästyneistä päivityksistä. Koko verkon haavoittuvuusmääriä seuraavan KPI-mittarin trendikäyrä on ollut tutkimuksen ajan laskeva, joten se osoittaa, että prosessi toimii käytännössä tältä osin hyvin. Haavoittuvuusmääriä ei tuoda tässä työssä tarkemmin esille, koska mittauksia oli tehty melko vähän aikaa. Tulokset eivät olisi myöskään täysin vertailukelpoisia eri ajanjaksoina vielä tässä vaiheessa, koska skannauskohteiden määrä ei pysynyt vakiona tutkimuksen aikana, koska skannauksiin otettiin vähitellen lisää kohteita uusista verkoista.

Uusien verkkosegmenttien lisääminen skannauskohteiksi haavoittuvuusskannerissa etenee useimmiten samalla tavalla, joka kuvattiin tässä työssä ylätasolla. Tarkkaa yleiskäyttöistä ohjeistusta olisi vaikea tehdä, koska verkkolait-

teissa, palomuureissa ja skannauskohteissa on paljon eroja. Eniten työtä tuleekin juuri näissä avauksissa, konfiguroinneissa ja skannaustunnusten toimivuuden testaamisessa. Kehitystavoitteena olikin lisätä vähintään yksi verkkosegmentti skannaukseen mukaan ja se toteutui hyvissä ajoin. Ensimmäinen uusi verkkosegmentti ehti olla mukana tutkimuksen aikana neljä kuukautta viikoittaisissa skannauksissa ja sen haavoittuvuusmäärät tippuivat huomattavasti seuranta-aikana. Haavoittuvuusmäärien pudotuksen mahdollistivat toimiva skannausprosessi, seurantapalaverit ja aktiiviset haavoittuvuuksien korjaajat. Tässä toimintatutkimuksen syklinen kehitystyö näkyi parhaimmillaan. Toimintaa seurattiin ja hoidettiin myös jatkuvasti useasta näkökulmasta tarkastellen triangulaation mukaisesti.

Outpost24:n HIAB:n varmuuskopioinnin testaus oli myös tutkimusaiheena. Aluksi selvitettiin, että missä tapauksessa varmuuskopiot täytyy ottaa, ja minkälaisia vaihtoehtoja on tarjolla. Outpost24:n oma varmuuskopiointitoiminto oli melko selkeä toimenpide, joka on kuvattu omassa luvussaan. Varmuuskopion palautustoimenpide oli riskialttiimpi testata ja se toteutettiin laboratorioympäristössä. Testaus tehtiin myös kunnolla niin, että tuhottiin koko HIAB ja yritettiin palauttaa se alkuperäiseksi. Tämä aiheuttaa Outpost24:n suhteen ongelmia muun muassa lisenssien kanssa, ja tätä ongelmaa on käsitelty tarkemmin sen omassa luvussaan. Testaustulos osoittaa, että pahimmatkin skenaariot kannattaa testata ennakkoon.

Koska tutkimus perustuu toimintatutkimukseen ja haastatteluihin, niin tuloksia ei voida suoraan yleistää johonkin toiseen tilanteeseen. Tuloksista saatua tietoja voi hyödyntää muualla, mutta käytännössä tutkimusprosessi on muissakin kohteissa käytävä itse läpi, jotta sen tuoma kehittyminen olisi mahdollista.

9 JOHTOPÄÄTÖKSET

Tässä luvussa tuodaan esille tutkimuksen tulosten tärkeimmät huomiot, yhteenvedot ja päätelmät. Tutkimuksen alkuvaiheiden skannaustulokset osoittivat, että lähes kaikista palvelimista ja erityisesti Windows-palvelimista löytyy yllättävän paljon haavoittuvuuksia, jos niitä ei päivitetä säännöllisesti ja konfiguroida huolellisesti. Näitä haavoittuvuuksia ei huomata helposti ilman kunnollisia haavoittuvuusskannauksia. Haavoittuvuuden mahdollisimman aikainen

löytäminen ja poistaminen on tärkeää yritykselle, jotta voidaan välttää tietomurrot ja sen seurauksena aiheutuneet taloudelliset riskit ja mainehaitat.

Haavoittuvuusskannausten säännöllinen tarkkailu on tärkeää, koska tutkimuksen aikanakin haavoittuvuusmäärien huomattiin vaihtelevan melko paljon, vaikka seurantakohteet pysyivät samoina. Viikoittainen skannaus koko alueelle ja tulosten säännöllinen seuranta vaikutti oikealle toimintatavalle. Koska säännöllinen seuranta oli kuitenkin SOC:n ja järjestelmäomistajien omasta innokkuudesta kiinni, siksi todettiin tarpeelliseksi pitää kuukausittainen kartoitus yleisestä haavoittuvuustilanteesta, jossa otettiin jatkokäsittelyyn kriittisimmät kohteet. Haavoittuvuuksien poisto ja poikkeuksellisten tilanteiden tehokas hoitaminen vaatii toimivan prosessin. Prosessi osoittautui jo tutkimuksen aikana toimivaksi, koska tutkimuksen loppuvaiheen aikana löytyneen nollapäivähaavoittuvuuden hoitaminenkin sujui hienosti.

Haavoittuvuuksien hallintaprosessi on nyt kuvattu kokonaisuudeksi, joka huomioi erilaiset haavoittuvuustapaukset. Tutkimuksen tarkennetuista ohjeistuksista ja tutkimuskysymyksien tuloksista löytyy useita uusia tapoja tehostaa kokonaisprosessin toimintaa. Koko prosessia ei saada yhdellä muutoksella täydelliseksi, koska kokonaisuus on useiden tekijöiden ja vaiheiden summa. Muutoksia tehdään jatkossakin vähitellen, seurataan niiden vaikutuksia ja jatketaan jatkuvaa kehitystä.

Tutkimuksessa todettiin vääriä positiivisia haavoittuvuuksia tulevan paljon erilaisista eri syistä. Tämän takia on tärkeää valita harkiten haavoittuvuusskanneri ja tuntea väärien positiivisten haavoittuvuuksien vähentämistavat. Näillä asioilla on merkittävä vaikutus pitkien haavoittuvuusraporttien kautta SOC-analyytikkojen työmäärään, KPI-mittarin tuloksiin ja lopulta myös organisaation kustannuksiin.

Varmuuskopioinnin palautuksen testaus todettiin hyödylliseksi, koska se aiheutti yllättäviä ongelmia käytössä olevan haavoittuvuusskannerin osalta. Jatkossa varmuuskopioinnin palautusprosessi on selkeämpi ja sen vaatiman ajan osaa arvioida tarkemmin. Näiden töiden selvittäminen ja dokumentointi luo nyt

varmuutta, että toimintaa voi jatkaa edelleen myös muiden ylläpitäjien avustuksella ja kerätty historiadata skannaustuloksista sekä konfigurointitiedot säilyvät jatkossakin, vaikka palvelimille sattuisi jotain.

Haavoittuvuusskanneriin liitetyn uuden verkkoalueen haavoittuvuuksia on jo ehditty tutkimaan viimeisimmissä seurantapalavereissa. Toiminta on todettu tärkeäksi ja yrityksen palvelin- ja verkkoturvallisuus paranee KPI-mittarin seurantatulosten perusteella hyvää vauhtia, joka todistaa prosessin toimivan oikein.

10 POHDINTA JA REFLEKTOINTI

Tässä luvussa yhteen vedetään työn tuloksia, pohditaan työn merkitystä kokonaisuudessaan henkilökohtaisella tasolla ja kohdeorganisaation kannalta. Seuraavassa luvussa käydään läpi tutkimuksen luotettavuutta, hyödynnettävyyttä yleisellä tasolla ja tutkimusprosessin toimivuutta. Lopuksi tuodaan esille mahdollisia lisätutkimusaiheita tähän aihealueeseen liittyen.

Toimintatutkimus sopi hyvin työn tutkimusmenetelmäksi ja seurantapalaverit auttoivat samalla toteuttamaan pienimuotoisesti tutkimuksellisen kehittämisen sykliä. Prosessiin liittyvää toimintaa pyritään kehittämään jatkossakin organisaatiossa jatkuvan kehittämisen oppien tapaan. Haastattelut ja kyselyt soveltuivat hyvin tietojen keräämiseen valikoiduilta ihmisiltä. Haasteena oli aluksi löytää sopivat ihmiset ja hektinen työtahti yleisesti vaikutti siihen, ettei läheskään kaikkien kanssa saatu sovittua haastattelua suunnitellussa aikataulussa. Kenttäpäiväkirjan pitämisestä voi olla toimintatutkimuksissa hyötyä, mutta tässä tutkimuksessa se ei tuntunut kovin välttämättömälle, koska tutkimuksen aikana pystyttiin tekemään muutenkin jatkuvaa analysointia ja dokumentointia.

Haavoittuvuuden hallintaprosessi saatiin tutkittua ja kuvattua kokonaisuudessaan sekä sanallisesti että vuokaavioin tämän tutkimuksen aikana. Dokumentointia tullaan jatkamaan organisaation intranet-sivuille. Organisaation ryhmien ohjeistuksia kehitettiin ja täydennettiin tutkimuksen aikana myös jonkin verran muiden työntekijöiden toimesta. Kokonaisuuden toimivuus käytännössä tullaan toteamaan myöhemmin myöhemmissä palavereissa, ja tilanteen mukaan tehdään tarvittaessa uudestaan muutoksia tai tarkennuksia.

Yllättävää oli todeta vääriä positiivisia haavoittuvuuksia koskevan tutkimuskysymyksen kohdalla, että niitä voi tulla niin paljon ja erilaisista syistä. Tämän suhteen on hyvä tiedostaa, osaako haavoittuvuusskanneri analysoida niitä ja poistaa niistä osan ennakkoon ja tämä onneksi onnistuu kohdeorganisaation skannerilla. Lisäksi tutkimuksessa selvisi useita muita tapoja vähentää vääriä positiivia haavoittuvuuksia. Näillä asioilla on merkittävä vaikutus SOC-analyytikkojen työmäärään ja KPI-mittarin tuloksiinkin.

Työ on hyvin ajantasainen, koska maailmanlaajuisesti on löytynyt säännöllisesti uusia vakavia haavoittuvuuksia, ja itse tutkimuksen aikanakin pystyi toteamaan prosessin toimivuuden haavoittuvuusilmoitusten ja tikettien etenemisen suhteen. Näin ollen tutkimusta voidaan pitää näiltä osin onnistuneena. Aihetta käsitellään usein mediassa ja lehdissä sekä julkaisujen määrä vaikuttaa olevan kasvava.

Tutkimustyöllä on ollut hyödyllinen vaikutus tutkijan omaan kehittymiseen työtehtävissä, koska näin sai mahdollisuuden tutustua nopealla aikataululla sekä haavoittuvuuksien hallintaprosessiin, että muihin prosesseihin, ryhmien toimintatapoihin ja ihmisiin. Samalla tuli selvitettyä haavoittuvuusskanneriin liittyviä epäselvyyksiä, ja sai paljon uutta tietoa perehtymällä laajasti aiheen kirjallisuuteen ja tästä on hyötyä tällä alalla työskennellessä. Tutkimustyön aihealue oli melko laaja ja sitä olisi voinut käsitellä tarkemmin ja laajemminkin haavoittuvuusskannerin ja haavoittuvuuksien osalta, mutta työ oli tarkoitus rajata kuitenkin kohtuullisen pituiseksi. Työn eri aihealueiden jäsentäminen selkeäksi dokumentiksi tuntui hiukan vaikealle, koska työhön kuului useita eri osa-alueita ja tutkimuskysymyksiä. Tutkimustyön tekeminen opetti hyvin käytännönläheisesti, kuinka toimintatutkimus etenee ja mitä kaikkea siinä täytyy huomioida. Tutkimustyön tekeminen uudehkon työtehtävän rinnalla oli melko työläs ja rankka projekti, koska varsinaista työaikaa ei voinut paljoakaan käyttää tähän tutkimukseen ja organisaation toiminnot eivät olleet ennakkoon tuttuja, mutta loppujen lopuksi tämä tutkimus kannatti ehdottomasti tehdä oman kehittymisen kannalta.

Työn valvonnasta, aikataulujen seurannasta ja avustamisesta isot kiitokset opinnäytetyön valvojalle ja seurantaryhmälle yrityksessä, sekä esimiehelle tämän mahdollisuuden tarjoamisesta ja tukemisesta. Lisäksi täytyy kiittää ehdottomasti haastatteluihin, kyselyihin ja palavereihin osallistuneita, joita tehtiin useiden eri työvaiheiden yhteydessä. Hienoa, että uudet haastavat päivätyötkin sujuivat hyvin opiskeluiden ohessa ja siitä voi osaltaan kiittää hyviä työkavereita.

10.1 Tutkimuksen luotettavuus ja hyödynnettävyys

Hirsjärven ym. (2009) mukaan tutkimuksen teossa olisi hyvä lopuksi arvioida tutkimuksen luotettavuus ja pätevyys. Niitä voidaan tarkastella validiteetin ja reliabiliteetin avulla, joita voidaan pitää luotettavuusmittareina. Reliabiliteetti kuvaa sitä, että tutkimusta toistettaessa saadaan samat tulokset. Eskolan ym. (2014) mukaisesti aineisto voi olla reliaabeli, kun se ei sisällä ristiriitaista tietoa. Toimintatutkimuksessa tavoitellaan kehityksen kautta muutosta ja siksi sille on vaikea tehdä luotettavuusarviointia. Kyselyiden uusiminen samoille henkilöille todennäköisesti aiheuttaisi hiukan muuttuneita vastauksia, koska niihin saattaisi vaikuttaa aiempi kysely, yleinen keskustelu aiheesta ja mielipiteiden muokkaantuminen. Tällaisen tutkimuksessa täytyy käyttää kvalitatiivisen tutkimuksen luotettavuusarviointia, johon ei taas joidenkin näkemysten mukaan voi soveltaa validiteettia. Tutkimuksen arviointiperusteina voi käyttää aineiston riittävyyttä, analyysin kattavuutta ja analyysin toistettavuutta. Tämän työn aineiston määrän voi arvioida tutkimusraportin sisältävästä luvusta ja lähteiden määrästä. Aineiston ja analysoinnille on oma lukunsa ja tulokset ovat analysoitu luvussa tutkimustulokset. Tiedonkeruu-, analysointi- ja tutkimusmenetelmien valinta on perusteltu luvussa opinnäytetyön toteutus. (Kananen 2014, 125–131, 152–153.)

Tutkimuksen tekijä teki itse kaikki haastattelut ja kyselyt. Haastattelurungon testaus tehtiin aluksi työn ohjaajan kanssa, jolloin todettiin, että toimintatapaa ja kysymyksiä voisi hieman muokata. Todettiin, että kysymykset olisi hyvä lähettää ennakkoon haastateltaville, koska niihin ei ole erityisen helppo vastata nopeasti. Tutkimuksen validiteetti parani myös testauksen myötä. Tutkimuksessa oli teemahaastatteluissa mukana seitsemän henkilöä. Haastattelu-

pyyntö lähetettiin kolmelletoista henkilölle. Haastattelut tehtiin kokeneiden asiantuntijoiden kanssa, joten vastaukset ja kommentit sisälsivät hyvää kokemusperäistä tietoa, ja niihin pystyi kohtuullisen hyvin luottamaan. Laajemmin kyselyä ei oikein kannattanut tehdä, koska kysymykset liittyivät aiheisiin, joihin ei voinut olettaa kovin monella olevan tietoa. Alkuperäisiä alakysymyksiä oli kaksi enemmän. Koska niihin ei puolet osallistuneista osannut vastata mitään ja vastauksissa oli vaihtelua melko paljon, niin siksi niiden käsittely karsittiin pois työstä luotettavuussyistä. Aihealue liittyi haastattelussa joko haavoittuvuuksien hallintaprosessiin tai haavoittuvuusskanneriin tai haavoittuvuuksiin, joten se lisäsi haastattelun luotettavuutta, koska aihealue pysyi samana. Syvällisen tuntemuksen puute joillakin osa-alueilla aiheutti vaikeuksia joillekin haastateltaville, joten se taas huononsi luotettavuutta niiltä osin, mutta yleensä näissä tapauksissa ei saatu vastaustakaan.

Teemahaastattelulle on ominaista se piirre, että suurella ja vähemmän laadukkaalla otantamäärällä voi tulla mukaan vääriä näkemyksiä asioista, jos aiheesta ei ole tarpeeksi kokemusta. Eskolan ym. (2014, 62) mukaan aineiston määrällä ei ole suoraa vaikutusta laadullisen tutkimuksen onnistumiseen, joten näillä perusteilla saatu otantamäärä on riittävä. Muotion ym. (2022) esille tuoma asenteellisuus teemahaastatteluissa pyrittiin ottamaan huomioon analysoimalla vastaukset puolueettomasti, koska se pudottaisi vastausten luotettavuutta. Sitä ei onneksi esiintynyt havaintojen mukaan paljon, mutta tutkimuksen haastatteluissa korostui se, että SOC-ryhmälle laitettiin monenlaista painetta lisätöihin ja toimintojen tehostamiseen. SOC-ryhmä onkin haavoittuvuuksien hallinnassa hyvin tärkeässä roolissa. Heidän osaamisensa hyödyntäminen kiinnostaisi muitakin ryhmiä ja järjestelmäomistajia, mutta lisätyöt täytyy suhteuttaa työkuormaan, ja tämä täytyy esimiesten ja johdon myös ymmärtää.

Haastatteluihin tai osittain kyselyihin oli valmistauduttu ennakkoon lähettämällä haastattelukysymykset ennakkoon haastateltaville ja ne myös palautettiin haastattelijalle ennakkoon, joten molemmat osapuolet olivat tietoisia kysymyksistä ja vastauksista jo ennen haastattelua. Tällä toimenpiteellä pyrittiin parantamaan vastauksien laatua ja luotettavuutta, kun haastateltava pystyi rauhassa miettimään asiaa, ja sai myös mahdollisuuden tarkentaa tai korjata vastaustaan myöhemmin. Valmiin tutkimusraportin sisällölle pyrittiin hake-

maan työn loppuvaiheessa sisällön oikeellisuudelle vahvistukset haastateltavilta, jotta aineistotriangulaation avulla tehdyt tulkinnat saavat vahvistuksen, koska tällä parannettaisiin laadullisen tutkimusosan luotettavuutta (Kananen, 133–134). Tämä vaihe oli hiukan kesken työn loppuvaiheessa ja ei ehtinyt täysin toteutua.

Kaikkien vastauksien luotettavuus pyrittiin varmistamaan kirjallisuuslähteiden, omien havaintojen, yrityksen intranetin ja viikoittain pidetyn seurantapalaverin kautta. Tulosten ristiin tarkistus toteutui melko hyvin, mutta tikettien käsittelyn osalta siihen ei saatu varmistusta, mutta saman suuntaisia vastauksia löytyi kuitenkin haastatteluissa. Jos vähintään kaksi haastateltavaa esittää samankaltaiset vastaukset samasta asiasta, niin tulosta voidaan pitää reliaabelina ja tämä toteutui pääosin tutkimuskysymysten osalta (Hirsjärvi ym. 2017, 226). Tuomi (2018) ja Eskola ym. (2014, 62–63) tuovat myös esille aineiston saturaation eli kylläänytymisen merkityksen tulosten luotettavuudessa teemahaastatteluissa ja aineiston keruussa. Aineiston kylläänytyminen osoittaa aineiston kattavuuden olevan myös riittävä (Eskola ym., 2014, 216). Tutkija itse pyrki olemaan vastauksien valinnoissa myös objektiivinen ja toi esille kaiken oleellisen tiedon ja tulkinnat läpinäkyvästi.

Haastattelun epäselvät ja epävarmat vastaukset jätettiin huomioimatta, koska tulosten validiteetti olisi kärsinyt niistä. Teemahaastatteluista litteroitu aineisto löytyy luvusta aineiston keruu. Haavoittuvuuden hallintaprosessin toimintaan ja tutkimuskysymyksien selvittämiseen löytyi tutkimus- ja kirjallisuuslähteistä kohtuullisen paljon tietoa, joiden avulla pyrittiin vahvistamaan tulosten luotettavuutta. Prosessia on muokattu yrityksen toimintaan sopivaksi, mutta se noudattaa yleisesti tunnettujen PwC, ITIL:n ja OWASP:n ohjeistuksia hyvin paljon, joten se vahvistaa prosessin toimivuuden luotettavuutta. Tutkimuksen validiutta on pyritty osoittamaan raportoimalla aineiston keruun ja menetelmien lisäksi aineiston ja tulosten analysointi sekä johtopäätökset, jolloin tutkimuksen lukija voi itse tulkita tutkimuksen luotettavuutta (Valli ym. 2015).

Haavoittuvuuksien seurantaan tarkoitetun KPI-mittarin reliabiliteetti ja validiteetti ovat hyviä. Validiteetti tulee esille siinä, että mittarin avulla mitataan juuri sitä, mitä on tarkoituskin mitata eli haavoittuvuusmäärien muutosta sovittuna

aikana (Kananen 2014, 126). KPI-mittarin aineiston eli skannaustulokset tuottaa haavoittuvuusskanneri. Nämä skannaukset ovat toistettavissa niin, että tulokset pysyvät samoina, kunnes laitteisiin ilmaantuu uusia haavoittuvuuksia ja tämä osoittaa hyvää reliabiliteettia (Kananen 2014, 126). Skannausten konfigurointi on vakioitu ja vain järjestelmänomistaja tai ylläpitäjät voivat tehdä siihen muutoksia. Seurattava haavoittuvuuksien kehityskäyrä muuttuisi vain, jos skannausasetuksiin tai raportointisuodatuksiin tehtäisiin muutoksia

Tutkimuksessa kuvattuja toimintatapoja ja KPI-mittaria voisi hyödyntää vastaavanlaisissa yrityksissä, ja myös esitetty haavoittuvuuksien hallintaprosessin vuokaavio voisi olla toimiva muissakin yrityksissä mahdollisesti pienin muutoksin. Tutkimuksen aikana todettiin, että vastaavia esimerkkiprosessikaavioita ei löydy kovin helposti. Tutkimuksessa esitetyt tiedot haavoittuvuusskannereista voisivat auttaa skannerin valinnassa sekä yrityskäyttöön kuin myös kotikäyttöön. Myös jotkut tutkimuskysymyksistä ovat voineet olla jonkun muunkin ongelmana. Kananen (2014) kuitenkin toteaa, ettei toimintatutkimus tuota yleistettävää tietoa, koska ulkoinen validiteetti ei toteudu. Tällä tarkoitetaan tulkintojen, johtopäätösten ja aineiston välistä pätevyyttä (Eskola ym. 2014). Tutkimuksen tulosten siirrettävyys ei kaikilta osin toimi toimintatutkimuksessa, koska tulokset pätevät täysin vain kohdeorganisaatioon.

10.2 Jatkotutkimusmahdollisuudet

Tässä työssäkin mainittiin väärien haavoittuvuuksien käsittelyn kohdassa SOAR- tai SIEM-järjestelmän hyödyntäminen haavoittuvuusskannerin yhteydessä. Tätä mahdollisuus tullaan ottamaan huomioon todennäköisesti kohdeorganisaatiossakin myöhemmin. Organisaation tämänhetkisen valmistajan järjestelmät eivät kuitenkaan tukeneet toisiaan, joten tarkempaa tutkimusta ei voinut nyt tehdäkään. Tämä voisi olla myös sopiva jatkotutkimusaihe jollekin.

Ohjelmistokomponenttien haavoittuvuuksien ennustamistekniikoista on tehty jo jonkinlaista kehitystyötä ja tutkimuksia (Gelenbe 2021). Voisi olla mielenkiintoista selvittää näiden tekniikoiden soveltuvuus ja käytettävyys yritysten haavoittuvuuksien hallinnassa. Nämä tekniikat voisivat sopia erityisen hyvin omia sovellutuksia tekevien ohjelmistotalojen käyttöön.

IoT-laitteiden ja kulkuneuvojen verkkoihin kytkemisen myötä myös erikoisempien laitteistoajureiden, -ohjelmistojen ja rajapintojen tietoturvariskitkin kasvavat (Gelenbe 2021). Onko tätä varten jo tehty yleiskäyttöisiä haavoittuvuusskannereita tai miten hyvin valmistajat tutkivat näitä asioita? Todennäköisesti erilaiset käyttöliittymät, väylät (kuten CAN, Bluetooth) ja tarkemmin rajoitettu sisäänpääsy itse laitteisiin tekee skannerin kehittämisestä hankalampaa, mutta tämä olisi hieman erilaisempi tutkimusalue haavoittuvuuksien kannalta.

Pilvipalveluiden haavoittuvuuksien valvonta vaatii siihen tarkoitukseen kehitetyt järjestelmät ja ominaisuudet. Suurimmilla ja uusimmilla haavoittuvuusskannerivalmistajilla on omat versionsa pilvipalveluiden seurantaa ja skannausta varten. Pilviratkaisujen haavoittuvuuksien riskialueet ovat jo yleisesti melko hyvin tiedostettu (Purplesec 2023). Pilvipalvelut yleistyvät nopeaa vauhtia, mutta niiden haavoittuvuuksien seurannasta ei vielä löydy kovin paljon opinnäytetöitä. Onko pilvipalveluiden toiminta käytännössä luotettavaa vai johtuvat ongelmat lähinnä käyttäjien vääristä konfiguroinneista, erehdyksistä ja kirjautumisongelmista? Entä miten yritysten haavoittuvuuden hallintaprosessi muuttuu siirryttäessä käyttämään täysin pilvipohjaisia tuotteita tai muuttuko se? Näiden asioiden empiirinen tutkiminen voisi olla hyödyllistä ja kiinnostavaa.

LÄHTEET

Aalto University. 2023. Aalto Handbook: Annual Clock. WWW-dokumentti. Saatavissa: https://www.aalto.fi/en/aalto-handbook/annual-clock [viitattu 26.3.2023].

Andreasson, A & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Helsinki: Tietosanoma.

Astra. 2023. Nivedita James: 17 Best Vulnerability Scanners: Features, Steps, And Limitations. WWW-dokumentti. Saatavissa: https://www.getastra.com/blog/security-audit/best-vulnerability-scanners/ [viitattu 4.2.2023].

Baran, G. 2020. GBHackers On Security. Top 7 Vulnerability Database Sources to Trace New Vulnerabilities. WWW-dokumentti. Saatavissa: https://gbhackers.com/sources-trace-new-vulnerabilities/ [viitattu 29.01.2023].

Bitdefender. 2023. Bitdefender Home Scanner. WWW-dokumentti. Saatavilla: https://www.bitdefender.com/solutions/home-scanner.html [viitattu 1.2.2023].

Buildahelpdesk. 2022. ITIL Incident Management Priority Matrix. WWW-dokumentti. Saatavilla: https://buildahelpdesk.com/itil-incident-management-priority-matrix/ [viitattu 25.2.2023].

Businessbeam. s.a. DIFFERENCE BETWEEN IT GOVERNANCE AND IT SERVICE MANAGEMENT. WWW-dokumentti. https://www.businessbeam.com/blog/it-service-management/difference-between-it-governance-and-it-service-management/ [viitattu 1.2.2023].

Calder, A. 2020. Cyber Security: Essential principles to secure your organization. WWW-dokumentti. Saatavilla: https://ebookcentral.proquest.com/lib/xamk-ebooks/detail.action?docID=6176700 [viitattu 22.12.2022].

Castsoftware. 2017. Reduce False Positives in Application Security Testing. WWW-dokumentti. Saatavilla: https://www.castsoftware.com/blog/reduce-false-positives-in-application-security-testing [viitattu 26.02.2023].

Cavelty, M.C. & Wenger, A. 2022. Cyber Security Politics. Socio-tehnological transformations and political fragmentation. PDF-dokumentti. Saatavissa: https://library.oapen.org/handle/20.500.12657/52574 [viitattu 22.12.2022].

CIO. 2022. What is ITIL? Your guide to the IT Infrastructure Library. WWW-dokumentti. Saatavissa: https://www.cio.com/article/272361/infrastructure-it-infrastructure-library-itil-definition-and-solutions.html [viitattu 22.12.2022].

CIS. 2021. CIS Controls Version 8. PDF-dokumentti. Saatavissa: https://paper.bobylive.com/Security/CIS/CIS_Controls_v8_Guide.pdf [viitattu 22.01.2023].

ControlCase. 2021. What is PCI-DSS? WWW-dokumentti. Saatavissa: https://www.controlcase.com/what-are-the-6-major-principles-of-pci-dss/ [viitattu 22.01.2023].

CVE. 2023a. Frequently Asked Questions (FAQs). WWW-dokumentti. Saatavissa: https://www.cve.org/ResourcesSupport/FAQs [viitattu 29.01.2023].

CVE. 2023b. About CVE Records. WWW-dokumentti. Saatavissa: https://cve.mitre.org/cve/identifiers/ [viitattu 29.01.2023].

CWE. 2023. Common Weakness Enumeration. WWW-dokumentti. Saatavissa: https://cwe.mitre.org/ [viitattu 29.01.2023].

Datamation. 2022. Emma Crockett - External vs. Internal Vulnerability Scans: What's the Difference? Blogi. WWW-dokumentti. Saatavissa: https://www.datamation.com/security/external-vs-internal-vulnerability-scans-whats-the-difference/ [viitattu 25.02.2023].

ENISA. 2016. Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations. WWW-dokumentti. Saatavissa: https://www.enisa.europa.eu/publications/vulnerability-disclosure [viitattu 8.10.2022].

ENISA. 2019. State of Vulnerabilities 2018-2019 - Analysis of Events in the life of Vulnerabilities. WWW-dokumentti. Saatavissa: https://www.enisa.europa.eu/publications/technical-reports-on-cybersecurity-situation-the-state-of-cyber-security-vulnerabilities/download/fullReport [viitattu 8.10.2022].

ERA. 2018. Opas: Johtamisen ja hallinnan kypsyysmalli. PDF-dokumentti. Saatavissa: https://www.era.europa.eu/system/files/2022-11/ERA%20management%20maturity%20model%20-%20FI.pdf [viitattu 26.3.2023].

Eskola, J. & Suoranta, J. 2014. Johdatus laadulliseen tutkimukseen. 10. painos. Tampere. Vastapaino.

First. 2022. Common Vulnerability Scoring System v3.1: Specification Document. WWW-dokumentti. Saatavissa: https://www.first.org/cvss/v3.1/specification-document [viitattu 29.01.2023].

Forrester. 2022. The Total Economic Impact™ Of ScienceLogic SL1 For Capgemini. PDF-dokumentti. Saatavissa: https://sciencelogic.com/wp-content/uploads/2022/01/Forrester-TEI_ScienceLogic_Capgemini_FINAL.pdf [viitattu 22.02.2023].

Frwiki. s.a. Haavoittuvuuksien skanneri. WWW-dokumentti. Saatavissa: https://fi.frwiki.wiki/wiki/Scanner_de_vuln%C3%A9rabilit%C3%A9 [viitattu 25.9.2022].

G2. 2023a. Where you go for software. WWW-dokumentti. Saatavissa: https://www.g2.com/ [viitattu 3.2.2023].

G2. 2023b. Best Vulnerability Scanner Software. WWW-dokumentti. Saatavissa: https://www.g2.com/categories/vulnerability-scanner [viitattu 3.2.2023].

Gartner. 2023a. Vulnerability Assessment Solutions Reviews and Ratings. WWW-dokumentti. Saatavissa: https://www.gartner.com/reviews/market/vulnerability-assessment [viitattu 3.2.2023].

Gartner. 2023b. About Gartner. WWW-dokumentti. Saatavissa: https://www.gartner.com/en/about [viitattu 3.2.2023].

Gelenbe, Erol & Jankovic, Marija & Kehagias, Dionysios & Marton, Anna & Vilmos, Andras. 2021. Security in Computer and Information Sciences. WWW-dokumentti. Saatavissa: https://library.oapen.org/handle/20.500.12657/57380 [viitattu 3.2.2023].

Grönfors, M. 2011. Laadullisen tutkimuksen kenttätyömenetelmät. PDF-dokumentti. Saatavissa: http://vilkka.fi/books/Laadullisen_tutkimuksen.pdf [viitattu 18.2.2023].

Harkamp, Wim. 2006. IT Security Vulnerability and Incident Response Management. PDF-dokumentti. Saatavissa: https://ris.utwente.nl/ws/portalfiles/portal/5387035/ISSE2006-Paper_Wim_Hafkamp_03_July_2006_final.pdf [viitattu 18.2.2023].

Heikkinen, H. & Jyrkämä, J. 1999. Mitä on toimintatutkimus. Teoksessa Hannu Heikkinen & Rauno Huttunen & Pentti Moilanen (toim.) Siinä tutkija missä tekijä: toimintatutkimuksen perusteita ja näköaloja. Jyväskylä: Atena Kustannus.

Hirsjärvi, S. & Remes, P & Sajavaara, P. 2007. Tutki ja kirjoita. 13. osin uudistettu painos. Keuruu: Otavan Kirjapaino Oy.

Hirsjärvi, S. & Remes, P. 2009. Tutki ja kirjoita. 15. uudistettu painos. Helsinki: Tammi.

HolmSecurity. 2022. Erik Torlén - How do I scan for backported patches? WWW-dokumentti. Saatavissa: https://support.holmsecurity.com/hc/en-us/articles/360014479679-How-do-I-scan-for-backported-patches- [viitattu 11.3.2023].

Hyvärinen, T. 2013. Haavoittuvuusskannausten ja IDS-hälytyksien ristiinkorrelointi AlienVault OSSIM SIEM -järjestelmässä. PDF-dokumentti. Saatavissa: https://www.theseus.fi/handle/10024/64116 [viitattu 26.2.2023].

IBM. 2021. Enabling RSA key-based authentication on UNIX and Linux® operating systems. WWW-dokumentti. Saatavissa: https://www.ibm.com/docs/en/sia?topic=kbaula-enabling-rsa-key-based-authentication-unix-linux-operating-systems-3 [viitattu 26.4.2023].

IBM. 2022a. False positives management. WWW-dokumentti. Saatavissa: https://www.ibm.com/docs/en/qsip/7.4?topic=manager-management-false-positives [viitattu 26.2.2023].

IBM. 2022b. Scanning on Windows-based assets. WWW-dokumentti. Saatavissa: https://www.ibm.com/docs/en/qsip/7.4?topic=manager-scanning-windows-based-assets [viitattu 26.2.2023].

INfosec. 2023. Core Security Principles. WWW-dokumentti. Saatavissa: https://www.infosec.gov.hk/en/knowledge-centre/core-security-principles [viitattu 25.4.2023].

Intel. s.a.a. What Is Patch Management? WWW-dokumentti. Saatavissa: https://www.intel.com/content/www/us/en/business/enterprise-computers/resources/patch-management.html [viitattu 26.2.2023].

Intel. s.a.b. What Is a Zero-Day Exploit? WWW-dokumentti. Saatavissa: https://www.intel.com/content/www/us/en/business/enterprise-computers/resources/what-is-a-zero-day-exploit.html [viitattu 26.2.2023].

Iplocation. 2018. What are different File Sharing protocols? WWW-dokumentti. Saatavissa: https://www.iplocation.net/file-sharing-protocols [viitattu 8.1.2023].

ISO. 2022. ISO/IEC 27001 Information security management systems. WWW-dokumentti. Saatavissa: https://www.iso.org/standard/27001 [viitattu 25.4.2023].

ITIL. 2011a. ITIL Service Design. 2011 Edition. Norwich: Crown.

ITIL. 2011b. ITIL Service Strategy. 2011 Edition. Norwich: Crown.

ITIL4. 2020a. ITIL4: Digital and IT Strategy. First Edition. London: Axelos.

ITIL4. 2020b. ITIL4: Direct, Plan and Improve. First Edition. London: Axelos.

Juhila, K. s.a. Laadullinen tutkimus ja teoria. WWW-dokumentti. Saatavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/mita-on-laadullinen-tutkimus/laadullinen-tutkimus-ja-teoria/ [viitattu 18.12.2022].

Jyrkämä, J. s.a. Laadullisen tutkimuksen verkkokäsikirja. Toimintatutkimus. Tampere: Yhteiskuntatieteellinen tietoarkisto. WWW-dokumentti. Saatavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/tutkimusasetelma/toimintatutkimus/ [viitattu 10.12.2022].

Kabelova, A & Dostalek, L. 2006. Understanding TCP/IP : A Clear and Comprehensive Guide to TCP/IP Protocols. E-kirja. Saatavissa: https://kaakkuri.finna.fi/Record/nelli29_mamk.1000000000750326 [viitattu 22.12.2022].

Kallinen, T. & Kinnunen, T. s.a. Etnografia. Teoksessa Jaana Vuori (toim.) Laadullisen tutkimuksen verkkokäsikirja. WWW-dokumentti. Saatavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/laadullisen-tutkimuksen-aineistot/etnografinen-havainnointiaineisto/ [viitattu 18.01.2023].

Kananen, J. 2014. Toimintatutkimus kehittämistutkimuksen muotona. Tampere: Suomen Yliopistopaino Oy – Juvenes Print.

Kananen, J. 2015. Opinnäytetyön kirjoittajan opas – Näin kirjoitan opinnäytetyön tai pro gradun alusta loppuun. Tampere: Suomen Yliopistopaino Oy – Juvenes Print.

Katakri 2020. Ulkoministeriö. Tietoturvallisuuden auditointityökalu viranomaisille. PDF-dokumentti. Saatavissa: https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246 [viitattu 21.11.2022].

Kerzner, H. 2017. Project Management Metrics, KPIs, and Dashboards: A Guide to Measuring and Monitoring Project Performance. 3. edition. E-kirja. Hoboken: John Wiley & Sons. Saatavissa: https://kaakkuri.finna.fi/Record/nelli29_mamk.4100000000641142 [viitattu 03.01.2022].

Keskuskauppakamari. 2020. Tietoturvaopas yrityksille. PDF-dokumentti. Saatavissa: https://kauppakamari.fi/wp-content/uploads/2020/06/tietoturvaopas-yrityksille.pdf [viitattu 10.12.2022].

Kiviniemi, K. 1999. Toimintatutkimus yhteisöllisenä prosessina. Teoksessa Kuusela, P. 2005. Realistinen toimintatutkimus? Toimintatutkimus, työorganisaatiot ja realismi. Helsinki: Työturvallisuuskeskus.

Knowledgehut. 2023. ITIL KPI - An Ultimate Guide to Understand Concept of ITIL KPIs. WWW-dokumentti. Saatavissa: https://www.knowledgehut.com/blog/it-service-management/itil-kpi [viitattu 1.4.2023].

Kohdeyritys. 2022. Tuotannon järjestelmien hallinta. WWW-dokumentti. Saatavissa: https://kohdeyritys.sharepoint.com/sites/ProductionGovernance/ [viitattu 11.3.2023].

Kohdeyritys. 2023. Tietoturvahäiriöiden hallinta. WWW-dokumentti. Saatavissa: https://confluence.kohdeyritys.fi/pages/viewpage.action?pageId=75203429 [viitattu 11.3.2023].

Kokonat. 2022. Tilanneanalyysi. WWW-dokumentti. Saatavissa: https://www.kokonat.fi/tilanneanalyysi/ [viitattu 18.12.2022].

Koski, P. & Kelo, M. 2019. Toimintatutkimus menetelmänä. Metropolia. Blogi. Saatavissa: https://blogit.metropolia.fi/masterminds/2019/09/30/toimintatutkimus-menetelmana/ [viitattu 15.12.2022].

Kuula, A. 2006. Toimintatutkimus. Luku 5.4. kokonaisuudesta Saaranen-Kauppinen A. & Puusniekka A. 2006. KvaliMOTV – Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. WWW-dokumentti. Saatavissa: https://www.fsd.tuni.fi/menetelmaopetus/kvali/L5_4.html [viitattu 15.12.2022].

Laurio, J-M. 2014. Haavoittuvuuden vakavuuden luokittelu lähtee CVSS-arvosta. Saatavissa: https://www.nixu.com/fi/blog/haavoittuvuuden-vakavuuden-luokittelu-lahtee-cvss-arvosta [viitattu 08.10.2022].

Liaison. 2017. Patch Management Policy and Procedure. Saatavissa: https://help.liaisonedu.com/Documentation/Repository/Patch_Management_Policy_and_Procedure [viitattu 5.3.2023].

Maglaras, L. & Janicke, H. & Ferrag, M.A. 2022. Cyber Security and Critical Infrastructures. PDF-dokumentti. Saatavissa: https://www.mdpi.com/books/pdfdownload/topic/5920 [viitattu 22.12.2022].

Manzuik, S., Pfeil, K., & Gold, A. 2006. Network Security Assessment: from Vulnerability to Patch. Rockland: Elsevier Science & Technology Books. E-kirja. Saatavissa: https://ebookcentral.proquest.com/lib/xamk-ebooks/reader.action?docID=280219 [viitattu 08.12.2022].

Microsoft. 2022. Mitä haavoittuvuuksien hallinta on? WWW-dokumentti. Saatavissa: https://www.microsoft.com/fi-fi/security/business/security-101/what-is-vulnerability-management [viitattu 15.12.2022].

Mikrobitti. 2019. Vertailussa tietoturvaskannerit - mitä kotiverkossani luuraa? WWW-dokumentti. Saatavissa: https://www.mikrobitti.fi/testit/vertailussa-tietoturvaskannerit-mita-kotiverkossani-luuraa/b354d965-e10c-4251-b7bd-3e9a6cf2aa44?_gl=1*1qlem2p*_ga*OTUwNjQ4MjI0LjE2NzUyNzE3MTU.*_ga_3L539PMN3X*MTY3NTI3MTcxNC4xLjAuMTY3NTI3MTcxNC4wLjAuMA [viitattu 2.02.2023].

MintSecurity. 2019. Mitä tarkoittaa tietoturvaskannaus – 5 näkökulmaa. WWW-dokumentti. Saatavissa: https://www.mintsecurity.fi/mita-tarkoittaa-tietoturvaskannaus-5-nakokulmaa/ [viitattu 15.12.2022].

Motadata. 2023. Mikä on CMDB ja miten se liittyy IT-omaisuuden hallintaan. Blogi. WWW-dokumentti. Saatavissa: https://www.motadata.com/fi/blog/what-is-cmdb/ [viitattu 19.2.2023].

Muotio, L. 2022. Teemahaastattelu tutkimusmenetelmänä. WWW-dokumentti. Saatavissa: http://www.muotoilu.info/index.php/tutkiva-muotoilu/menetelmat/teemahaastattelu-tutkimusmenetelmana/ [viitattu 25.03.2023].

NIST. 2020. NIST Special Publication 800-53 Revision 5. PDF-dokumentti. Saatavissa: https://doi.org/10.6028/NIST.SP.800-53r5 [viitattu 29.01.2023].

NIST. 2018. The Technical Specification for the Security Content Automation Protocol (SCAP). PDF-dokumentti. Saatavissa: https://doi.org/10.6028/NIST.SP.800-126r3 [viitattu 29.01.2023].

NIST. 2022a. National vulnerability database. WWW-dokumentti. Saatavissa: https://nvd.nist.gov [viitattu 22.12.2022].

NIST. 2022b. National Vulnerability Database. Vulnerability Metrics. WWW-dokumentti. Saatavissa: https://nvd.nist.gov/vuln-metrics/cvss [viitattu 15.12.2022].

NIST. 2022c. National Vulnerability Database. NVD CWE Slice. WWW-dokumentti. Saatavissa: https://nvd.nist.gov/vuln/categories [viitattu 29.01.2023].

NIST. 2022d. Technical Guide to Information Security Testing and Assessment. Special Publication 800-115. PDF-dokumentti. Saatavissa: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf [viitattu 29.01.2023].

Nmap. s.a. Nmap: Discover your network. WWW-dokumentti. Saatavissa: https://nmap.org/ [viitattu 07.01.2023].

NordicDefender. 2022. How to Handle Zero-day Vulnerability? Methods and Strategies. WWW-dokumentti. Saatavissa: https://nordicdefender.com/blog/how-to-handle-zero-day-vulnerability-methods-and-strategies [viitattu 26.02.2023].

Nummenmaa, L. 2009. Käyttäytymistieteiden tilastolliset menetelmät. 5. painos. Helsinki: Tammi.

Nuojua, P. 2021. Vierasnurkka: Turha sitä on kiistää, etätyö ja pilvipalvelut kasvattavat tietoturvariskiä – F-Securen Petri Nuojua. Tietokeskus. Blogi. Saatavissa: https://www.tietokeskus.fi/blogi/tietoturvariskit-vierasnurkka-f-secure-petri-nuojua/ [viitattu 15.12.2022].

Outpost24. 2023a. Knowledge Base. WWW-dokumentti. Saatavissa: https://kb.outpost24.com/kb [viitattu 07.01.2023].

Outpost24. 2023b. HIAB Deployment Guide. WWW-dokumentti. Saatavissa: https://kb.outpost24.com/kb/vulnerability-management-netsec/outscan-hiab/netsec-getting-started/hiab-deployment-guide [viitattu 07.01.2023].

Outpost24. 2023c. HIAB Backup. WWW-dokumentti. Saatavissa: https://kb.outpost24.com/kb/vulnerability-management-netsec/outscan-hiab/netsec-maintenance/hiab-backup [viitattu 07.01.2023].

Outpost24. 2023d. HIAB Restore. WWW-dokumentti. Saatavissa: https://kb.outpost24.com/kb/vulnerability-management-netsec/outscan-hiab/netsec-maintenance/hiab-restore [viitattu 07.01.2023].

Outpost24. 2023e. HIAB Internal Network Security. PDF-dokumentti. Saatavissa: https://outpost24.com/sites/default/files/2017-10/English_HIAB.pdf [viitattu 07.01.2023].

Outpost24. 2023f. Knowledge base. Scan Scheduling. WWW-dokumentti. Saatavissa: https://kb.outpost24.com/kb/vulnerability-management-netsec/outscan-hiab/netsec-scanning/scan-scheduling [viitattu 11.02.2023].

Outpost24. 2023g. Scan Stages. WWW-dokumentti. Saatavissa: https://kb.outpost24.com/kb/vulnerability-management-netsec/outscan-hiab/netsec-scanning/netsec-scan-stages [viitattu 11.02.2023].

Outpost24. 2023h. Manage Targets. WWW-dokumentti. Saatavissa: https://kb.outpost24.com/kb/vulnerability-management-netsec/outscan-hiab/netsec-target-management/manage-targets [viitattu 11.02.2023].

Outpost24. 2023i. Mark as False Positives. WWW-dokumentti. Saatavissa: https://kb.outpost24.com/kb/vulnerability-management-netsec/outscan-hiab/netsec-reporting/mark-as-false-positives [viitattu 25.03.2023].

OVAL. 2016. Open Vulnerability and Assessment Language. WWW-dokumentti. Saatavissa: https://oval.mitre.org/ [viitattu 11.02.2023].

OWASP. 2020. OWASP Vulnerability Management Guide (OVMG). PDF-dokumentti. Saatavissa: https://owasp.org/www-project-vulnerability-management-guide/OWASP-Vuln-Mgm-Guide-Jun05-2020.pdf [viitattu 4.3.2023].

OWASP. 2023a. Who is the OWASP Foundation? WWW-dokumentti. Saatavissa: https://owasp.org/ [viitattu 29.01.2023].

OWASP. 2023b. OWASP Zed Attack Proxy (ZAP). WWW-dokumentti. Saatavissa: https://owasp.org/www-project-zap/ [viitattu 29.01.2023].

Parmenter, D. 2015. Key Performance Indicators (KPI): Developing, Implementing, and Using Winning KPIs. E-kirja. Hoboken: John Wiley & Sons. Saatavissa: https://kaakkuri.finna.fi/Record/nelli29_mamk.3710000000391761 [viitattu 22.12.2022].

PCI DSS GUIDE. 2020. What is a PCI Approved Scanning Vendor (ASV)? WWW-dokumentti. Saatavissa: https://www.pcidssguide.com/what-is-a-pci-approved-scanning-vendor-asv/ [viitattu 22.12.2022].

Pedab. s.a. VULNERABILITY SCANNING. WWW-dokumentti. Saatavissa: https://www.pedab.fi/what-we-do-3/tietoturva/pedab-security-operation-centre-soc/vulnerability-scanning/ [viitattu 25.03.2023].

Peltonen, J. 2003. TUREAN tunkeutumisreittianalyysi. PDF-dokumentti. Saatavissa: http://yhteisturvallisuus.net/materiaali.html [viitattu 25.4.2023].

PhoenixNAP. 2020. Goran Jevtic. 17 Best Vulnerability Assessment Scanning Tools. WWW-dokumentti. Saatavissa: https://phoenixnap.com/blog/vulnerability-assessment-scanning-tools [viitattu 22.12.2022].

Pricop, E. & Stamatescu, G. & Fattahi, J. 2021. Advanced Topics in Systems Safety and Security. PDF-dokumentti. Saatavissa: https://www.mdpi.com/books/pdfdownload/book/3965 [viitattu 22.12.2022].

Purplesec. 2023. Best Practices For Cloud Vulnerability Management In 2023. WWW-dokumentti. Saatavissa: https://purplesec.us/learn/cloud-vulnerability-management/ [viitattu 26.3.2023].

PwC. 2022. Vulnerability management. PDF-dokumentti. Saatavissa: https://www.pwc.ch/en/publications/2022/ch-vulnerability-management-EN.pdf [viitattu 1.3.2023].

RedHat. 2023. Backporting Security Fixes. WWW-dokumentti. Saatavissa: https://access.redhat.com/security/updates/backporting [viitattu 11.3.2023].

Ronkainen, S. & Pehkonen L. & Lindblom-Ylänne S. 2011. Tutkimuksen voimasanat. Helsinki: Sanoma Pro.

Rousku, K. 2022. Hyviksiä vai pahiksia – hakkeroinnin lyhyt oppimäärä. Esitetty 14.12.2022. XAMK webinaari. [viitattu 15.12.2022].

Saaranen-Kauppinen, A & Puusniekka, A. 2006. KvaliMOTV – 6.3.2. Teemahaastattelu. Tampere: Yhteiskuntatieteellinen tietoarkisto. WWW-dokumentti. Saatavissa: https://www.fsd.tuni.fi/menetelmaopetus/kvali/L6_3_2.html [viitattu 17.12.2022].

Salmi, T. 2021. Haavoittuvuusskannaukset osana organisaation tietoturvallisuuden kehittämistä. Diplomityö. PDF-dokumentti. Saatavissa: https://trepo.tuni.fi/bitstream/handle/10024/132349/SalmiTomi.pdf?sequence=2 [viitattu 25.9.2022].

Salminen, J. 2020. Verkkosovelluksen haavoittuvuustestaus. Pro gradu -työ. WWW-dokumentti. Saatavissa: https://jyx.jyu.fi/handle/123456789/69031 [viitattu 08.10.2022].

Scott, J.S. 2022. Cyber Peace. Charting a path toward a sustainable, stable, and secure cyberspace. PDF-dokumentti. Saatavissa: https://www.cambridge.org/core/books/cyber-peace/8C458021C6FEC398064867A9B5EA938D [viitattu 22.12.2022].

Securitymetrics. 2015a. How to choose the best vulnerability scanner. WWW-dokumentti. Saatavissa: http://info.securitymetrics.com/how-to-choose-the-best-vulnerability-scanner [viitattu 3.2.2023].

Securitymetrics. 2015b. Picking Your Vulnerability Scanner: The Questions You Should Ask. WWW-dokumentti. Saatavissa: https://www.securitymetrics.com/blog/picking-your-vulnerability-scanner-questions-you-should-ask [viitattu 3.2.2023].

Securitymetrics. s.a. Vulnerability Scanning 101. WWW-dokumentti. Saatavissa: https://www.securitymetrics.com/learn/vulnerability-scanning-101 [viitattu 3.2.2023].

Securiwiser. 2021. Ryan Branagan. How Dangerous is a Rogue Device on a Network? WWW-dokumentti. Saatavissa: https://www.securiwiser.com/blog/how-dangerous-is-a-rogue-device-on-a-network/ [viitattu 3.2.2023].

SFS-ISO/IEC27000. 2020. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Yleiskatsaus ja sanasto. Helsinki: Suomen Standardoimisliitto SFS. SFS-online. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 08.10.2022].

SFS-ISO/IEC27001. 2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. PDF-dokumentti. Helsinki: Suomen Standardoimisliitto SFS. SFS-online. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 08.10.2022].

SFS-ISO/IEC27002. 2017. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet. PDF-dokumentti. Helsinki: Suomen Standardoimisliitto SFS. SFS-online. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 08.10.2022].

SFS-ISO/IEC27035-1:2016. 2016. Informaatioteknologia. Turvallisuustekniikat. Tietoturvahäiriöiden hallinta. Osa 1: Tietoturvahäiriöiden hallinnan periaatteet. Helsinki: Suomen Standardoimisliitto SFS. SFS-online. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 08.10.2022].

SFS-ISO/IEC27043:2016:en. 2016. Information technology. Security techniques. Incident investigation principles and processes (ISO/IEC 27043:2015). Helsinki: Suomen Standardoimisliitto SFS. SFS-online. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 02.01.2023].

SFS-ISO/IEC29147:2020:en. 2020. Information technology. Security techniques. Vulnerability disclosure (ISO/IEC 29147:2018). Helsinki: Suomen Standardoimisliitto SFS. SFS-online. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 02.01.2023].

SFS-ISO/IEC30111:2020:en. 2020. Information technology. Security techniques. Vulnerability handling processes (ISO/IEC 30111:2019). Helsinki: Suomen Standardoimisliitto SFS. SFS-online. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 02.01.2023].

SFS-opas 4:2022. 2022. Suomalaisen SFS-standardin laadinta ja rakenne. PDF-dokumentti. Helsinki: Suomen Standardoimisliitto SFS. SFS-online. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 03.01.2023].

Shetty, D. 2011. Penetration Testing with Metasploit Framework. PDF-dokumentti. Viitattu 25.3.2023. http://dl.packetstormsecurity.net/papers/general/pentesting-with-metasploit.pdf

SoftwareTestingHelp. 2023. Top 10 Vulnerability Scanners [Most Popular Scanners In 2023]. WWW-dokumentti. Saatavissa: https://www.softwaretestinghelp.com/top-vulnerability-scanners/ [viitattu 4.2.2023].

Sourceforge. 2023. Vulnerability Scanners. WWW-dokumentti. Saatavissa: https://sourceforge.net/software/vulnerability-scanners/ [viitattu 4.2.2023].

Spiceworks. 2022. Google Rolls Out Emergency Patch for Ninth Zero-Day Chrome Vulnerability of 2022. WWW-dokumentti. Saatavissa: https://www.spiceworks.com/it-security/vulnerability-management/news/google-chrome-ninth-zero-day-vulnerability/ [viitattu 15.12.2022].

StackExchange. 2021. How to restrict an SSH key to certain IP addresses? WWW-dokumentti. Saatavissa: https://unix.stackexchange.com/questions/353044/how-to-restrict-an-ssh-key-to-certain-ip-addresses [viitattu 26.4.2023].

Stewart, J. & Chapple M. & Gibson, D. 2012. CISSP: Certified Information Systems Security Professional Study Guide. E-kirja. Saatavissa: http://ebookcentral.proquest.com/lib/xamk-ebooks/detail.action?docID=875861 [viitattu 11.12.2022].

Suojanen, U. 2014. Toimintatutkimus ammatillisen kehittymisen välineenä. WWW-dokumentti. Saatavissa: https://metodix.fi/2014/05/19/suojanen-toimintatutkimus/ [viitattu 15.12.2022].

Taanila, A. 2019. Akin menetelmäblogi. Blogi. WWW-dokumentti. Saatavissa: https://tilastoapu.wordpress.com/2012/03/01/otoskoko/ [viitattu 4.2.2023].

Tanium. 2022. Tanium Patch User Guide. Version 3.8.196. PDF-dokumentti. Saatavissa: https://docs.tanium.com/pdf/patch/Tanium_Patch_3.8.196_ug.pdf [viitattu 28.2.2023].

TechTarget. 2021. Linda Rosencrance - Identity management (ID management). WWW-dokumentti. Saatavissa: https://www.techtarget.com/searchsecurity/definition/identity-management-ID-management [viitattu 19.2.2023].

TechTarget. s.a. Kati Terrell Hanna & Linda Rosencrance - Vulnerability disclosure. WWW-dokumentti. Saatavissa: https://www.techtarget.com/searchsecurity/definition/vulnerability-disclosure [viitattu 4.3.2023].

Tenable. 2019. Lindsay Van Gemert: Nessus Home Is Now Nessus Essentials. WWW-dokumentti. Saatavilla: https://www.tenable.com/blog/nessus-home-is-now-nessus-essentials [viitattu 02.02.2023].

TENK. 2023. Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa. Julkaisu 2/2023. PDF-dokumentti. Saatavilla: https://tenk.fi/sites/default/files/2023-03/HTK-ohje_2023.pdf [viitattu 25.4.2023].

Termipankki. s.a. TEPA-termipankki. WWW-dokumentti. Saatavilla: https://termipankki.fi/tepa/fi/haku/haavoittuvuus [viitattu 15.12.2022].

Tiketöinti. 2022. Mikä on tiketöinti? WWW -dokumentti. Saatavissa: https://tiketointi.fi/mika-on-tiketointi/ [viitattu 11.3.2023].

Torkkola, S. 2015. Lean asiantuntijatyön johtamisessa. Helsinki: Talentum pro.

Traficom. 2020. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). Versio 1.1. PDF-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf [viitattu 25.04.2023].

Traficom. 2022. Kybersää – marraskuu 2022. PDF-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4%2C%20marraskuu%202022_0.pdf [viitattu 15.12.2022].

Tuomi, J. & Sarajärvi A. 2018. Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Tammi.

Valtiovarainministeriö. 2017. Tietoturvapoikkeamatilanteiden hallinta. Valtiovarainministeriön julkaisuja 8/2017. VAHTI. PDF-dokumentti. Saatavissa: https://www.suomidigi.fi/sites/default/files/2020-06/VM_8_2017.pdf [viitattu 20.12.2022].

Valli, R & Aaltola, J. 2015. Ikkunoita tutkimusmetodeihin 2. 4. painos. Juva: Bookwell Oy.

Vehkalahti, K. 2014. Kyselytutkimuksen mittarit ja menetelmät. Helsinki: Finn Lectura Ab.

Viinamäki, L. 2007. Polkuja soveltavaan yhteiskuntatieteelliseen tutkimukseen. Helsinki: Tammi.

Viinikainen, M. 2014. Tietoturvatapahtumien hallinta. Opinnäyte. PDF-dokumentti: Saatavissa: https://www.theseus.fi/bitstream/handle/10024/78265/Viinikainen_Miika.pdf;jsessionid=C51219D2A82D8190BBE6617E310AFD67?sequence=1 [viitattu 08.10.2022].

Vilka, H. 2015. Tutki ja kehitä. 4. uudistettu painos. Juva: PS-kustannus.

Vulnerability Metrics s.a. NIST. National Institute of Standards and Technology. WWW-dokumentti. Saatavissa: https://nvd.nist.gov/vuln-metrics/cvss [viitattu 11.12.2022].

Vuori, J. 2021. Laadullisen tutkimuksen verkkokäsikirja. Tutkimusasetelman rakentaminen. Tampere: Yhteiskuntatieteellinen tietoarkisto. WWW-dokumentti. Saatavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/tutkimusasetelma/tutkimusasetelman-rakentaminen/ [viitattu 10.12.2022].

Vuori, J. s.a. Laadullinen sisällönanalyysi. Tampere: Yhteiskuntatieteellinen tietoarkisto. WWW-dokumentti. Saatavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/analyysitavan-valinta-ja-yleiset-analyysitavat/laadullinen-sisallonanalyysi/ [viitattu 10.12.2022].

Wei, L. & Yuqing, Z. & Weiping, W. & Hanbing, Y. & Chao, L. 2021. Cyber Security. 18th China Annual Conference, CNCERT 2021. PDF-dokumentti. Saatavissa: https://library.oapen.org/bitstream/20.500.12657/52870/1/978-981-16-9229-1.pdf [viitattu 22.12.2022].

VMware. 2021. Best practices for using VMware snapshots in the vSphere environment (1025279). WWW-dokumentti. Saatavissa: https://kb.vmware.com/s/article/1025279 [viitattu 12.3.2023].

Ylätalo, A. DEVELOPMENT OF PROCESS AND TOOLS FOR VULNERABILITY MANAGEMENT. WWW-dokumentti. Saatavissa: https://www.theseus.fi/handle/10024/160876/browse?type=author&value=Yl%C3%A4talo%2C+Anssi [viitattu 25.4.2023].

ZAP. 2023. Getting Started. WWW-dokumentti. Saatavissa: https://www.zaproxy.org/getting-started/ [viitattu 1.2.2023].

KUVALUETTELO

Kuva 1. Valitun tutkimusotteen kautta siirrytään tutkimismenetelmien ja aineiston tutkimisen kautta ratkaisuun (Kananen 2014, 30) 15
Kuva 2. Toimintatutkimuksen perusmalli (Heikkinen ym. 1999) 16
Kuva 3.Toimintatutkimuksen vaiheet (Kananen 2014, 34) 17
Kuva 4. Plan-Do-Check-Act -syklin kuvaus (ITIL 2011a, 27)..... 18
Kuva 5. Tutkimuksen triangulaation tarkastelunäkökulmat..... 19
Kuva 6. Opinnäytetyön prosessikuvaus 20
Kuva 7. Standardien ISO/IEC 29147 ja ISO/IEC 30111 välinen suhde (SFS-ISO/IEC29147 2020) haavoittuvuuksien käsittelyprosessissa..... 34
Kuva 8. Tiedonkulku haavoittuvuuden paljastumisprosessissa (SFS-ISO/IEC29147 2020) 35
Kuva 9. Yhteenveto ohjelmistovalmistajien haavoittuvuuksien hallintaprosessista (SFS-ISO/IEC30111 2020) 36
Kuva 10. Esimerkki Outpost24-ohjelman CVE-linkistä ODBC Driver Remote Code Execution-haavoittuvuudelle 41
Kuva 11. Haavoittuvuuksien tasot ja pistemäärät CVSS-järjestelmässä 43
Kuva 12. CVSS-järjestelmän pisteytykseen vaikuttavat tekijät (FIRST 2022) 43
Kuva 13. Suuryritysten käyttöön soveltuvien haavoittuvuusskannereiden markkinaosuudet G2:n tutkimuksen mukaan (G2 2023) 52
Kuva 14. Gartnerin tutkimuksesta kerätyt arvostelupistemäärät eri haavoittuvuusskannereille (Gartner 2023)..... 53
Kuva 15. Outpost24 asennuksen arkkitehtuurikuva toimeksiantajalla 55
Kuva 16. Väärien positiivisten haavoittuvuuksien suodatus Outpost24:ssa ... 64
Kuva 17. Esimerkkinä toimineen Windows-palvelimen haavoittuvuuksien historianäkymä 65
Kuva 18. Outpost24:n False Positive -sarake..... 65
Kuva 19. PwC:n esittämä haavoittuvuuksien hallintaprosessi (PwC 2022) 69
Kuva 20. Taniumin standardi korjausprosessi (Tanium 2022, 29)..... 70
Kuva 21. Taniumin korjausprosessikuvaus nollapäivän haavoittuvuudelle (Tanium 2022, 29) 71
Kuva 22. Taniumin korjausprosessikuvaus haavoittuvuusskannerin avulla löydetylle haavoittuvuudelle (Tanium 2022, 30) 72

Kuva 23. Haavoittuvuuksien liittyminen IT-palveluiden hallintaprosesseihin (Hafkamp 2006).....73
Kuva 24. Haavoittuvuuden elinkaari (Hafkamp 2006, 8) 74
Kuva 25. Liaisonin tietoturvapäivitysprosessi (Liaison 2017).....75
Kuva 26. Haavoittuvuuksien hallinnan prosessikuva SOC:n ja SL:n osalta ...79
Kuva 27. Korkean riskin haavojen käsittely haavoittuvuuksien hallintaprosessissa 80
Kuva 28. Esimerkki verkkoalueen keskitason ja korkean riskien haavoittuvuusmäärien kehityksestä Outpost24:n trend-toiminnon kautta.....84
Kuva 29. Esimerkkikuva haavoittuvuuksien seurannan KPI-mittarista 85
Kuva 30. HIAB:n ajastetun varmuuskopioinnin määritys (Outpost24 2023c) .91
Kuva 31. Varmuuskopioinnin FTP-asetukset (Outpost24 2023c).....92

Liite 1

KYSELYN JA TEEMAHAASTATTELUN ALUSTUS

Taustaa

Teen YAMK-opinnäytetyötä, johon kuuluu yrityksen sisäisen haavoittuvuuksien hallintaprosessin ja Outpost24-haavoittuvuusskannerin käytön kehittäminen. Opinnäytetyöhön on sopimus kohdeyrityksen kanssa. Opinnäytetyön ohjaajina toimivat XAMK:n vanhempi lehtori Vesa Kankare ja kohdeorganisaation IT-osaston johtaja.

Tässä teemahaastattelussa on tarkoitus käydä läpi työn alkuvaiheessa esille tulleita tutkimuskysymyksiä, joihin kerään teiltä mielipiteitä ja kommentteja. Jos ongelmaan liittyvä selvitys on jo työn alla, josta on jo esimerkiksi olemassa JIRA-tiketti, niin se kannattaa tuoda esille.

Jotkut kysymykset voivat olla melko laajoja, eikä ne kohdistu kaikille suoraan, mutta pienistäkin tiedoista voi olla hyötyä. Nämä tiedot ovat tärkeitä prosessin kehittämisen ja selvitykseni kannalta. Haastattelu tehdään vain niiden kesken, joilla on jonkinlainen yhteys haavoittuvuusprosessiin. Haastattelun lopuksi voi tuoda esille myös muita aiheeseen liittyviä asioita, jotka eivät tällä hetkellä tunnu toimivan tarpeeksi hyvin, niin ne pyritään myös huomiomaan tutkimuksessa.

Toimintaohje haastattelua ja kysymysten läpikäyntiä varten

Kysely lähetetään jonkin verran ennakkoon kyselyyn osallistujalle, niin että ehdit perehtyä kysymyksiin paremmin ja voit kirjoittaa vastaukset valmiiksi. Haastattelussa voidaan käydä selvyyden vuoksi kysymykset ja vastaukset läpi ja siinä vaiheessa asioista voi keskustella lisää, jos tulee mieleen jotain lisättävää. Käytännössä varmaan melko lyhyt palaveri. Olisi hyvä, jos lähettäisit tämän dokumentin vastauksineen takaisin sähköpostiini ennen sovittua haastatteluaikaa, niin ehtisin vilkaista myös vastaukset ennakkoon läpi.

Liite 2

Teemahaastattelun kyselypohja

Ajankohta:

Haastateltava:

Asema/titteli:

Teema-aiheet:

Yrityksen sisäisen haavoittuvuuksien hallintaprosessin toimivuus. Linkki nykyiseen prosessikuvaan: xxxx
Haavoittuvuuksien hallintaprosessin selkeimmät heikkoudet tai puutteet?
Haavoittuvuustikettien käsittely, haavoittuvuustikettien tekeminen, eskalointi ja seuranta.
Kuinka täytyisi reagoida nollapäivähaavoittuvuuksiin?
Kuinka voisi saada pienennettyä haavoittuvuusskannerin löytämien väärien positiivisten (false positive) haavoittuvuuksien määrää?
Hyväksytty haavoittuvuustaso organisaatiossa (esim. CVSS-luokittelun 0–10) mukaan pidemmällä aikajaksolla?

Liite 3

Lähetettävä kyselypohja

Ajankohta:

Vastaaja:

Asema/titteli:

Kysymykset:

Yrityksen sisäinen haavoittuvuuksien hallintaprosessi. Millä tavalla sitä kannattaisi kehittää paremmaksi? Linkki nykyiseen prosessikuvaan: xxxx
Nykyisen haavoittuvuuksien hallintaprosessin selkeimmät heikkoudet tai puutteet?
Onko haavoittuvuustikettien tekeminen, eskalointi ja seuranta toimivalla tasolla tällä hetkellä tai kuinka niitä voisi parantaa?
Kuinka täytyisi reagoida nollapäivähaavoittuvuuksiin (ilmoitustapa, minne ilmoitetaan, nopeus)?
Kuinka voisi saada pienennettyä haavoittuvuusskannerin löytämien väärien positiivisten (false positive) haavoittuvuuksien määrää?
Mikä voisi olla hyväksytty haavoittuvuustaso yleisellä tasolla organisaatiossa esim. CVSS-luokittelun (0–10) mukaan pidemmällä aikajaksolla?

Liite 4

TEEMAHAASTATTELUIHIN LIITTYVÄ KENTTÄPÄIVÄKIRJA

18.1.2023
Pidin ensimmäisen teemahaastattelun IT-puolen johtajalle, jolle IT-prosessien kuvaukset ovat tuttuja ja hän oli myös tehnyt ensimmäisen version haavoittuvuuden hallinnan prosessikuvauksesta. En muistanut lähettää kysymyslistaa tarpeeksi ajoissa hänelle, joten vastaamiseen ei ollut paljon mietintäaikaa, mutta meillä ei onneksi ollut tiukkaa aikarajaa haastatteluajalle. Tässä vaiheessa oli myös osittain tarkoitus miettiä hänen kanssaan, että ovatko kaikki kysymykset tarpeellisia ja oikealla tavalla muotoiltu. Muokkasinkin yhtä alakysymystä tämän haastattelun perusteella.

Tulimme siihen tulokseen, että kysymykset kannattaa laittaa hyvissä ajoin haastateltavalle ja pyytää ne vastauksineen myös takaisin ennen haastattelua, jolloin itsekin ehdin tutustua niihin. Sen jälkeen haastattelussa voidaan tehdä vain tarkennuksia ja syventyä epäselvempiin aiheisiin, jos on tarpeen. Totesimme myös, että osaan kysymyksistä ei pysty kunnolla vastaamaan kuin SOC-analyytikot tai heidän toimintansa hyvin tuntevat esimiehet ja ehkä myös kehityspäälliköt. Tässä haastattelussa sain heti tutkimuksen alkuun merkittäviä pohjatietoja, kuinka edetä.

20.1.2023
Lähetin teemahaastattelun kyselylomakkeen kahdelle seuraavalle ja tällä kertaa kokeneille SOC:n analyytikoille.

26.1.2023
Sain pari tarkentavaa kysymystä SOC:n analyytikolta Teams-kanavalla ja keskustelimme niistä jonkin aikaa. Sain häneltä sitten myöhemmin kyselylomakkeen takaisin kommentteineen.

27.1.2023
Kävimme SOC:n analyytikon kanssa 26.1. palautetun kyselylomakkeen läpi. Sain hyvää täydentävää tietoa muutamiin tutkimuskysymyskohtiin ja samalla

ajattelin hiukan muokata paria tutkimuskysymystä sopivammaksi. Samalla selvitin, että ketkä muut hänen ryhmässään olisivat sopivia haastateltavaksi ja sainkin kaksi uutta hyvää ehdokasta. Molemmat ovat kokeneita analyytikkoja ja heistä toinen on ollut myös esimiehenä samalla osastolla. Lähetin lopuksi kahdelle aiemmin päätetylle kyselykohteelle kyselylomakkeen täytettäväksi ja haastattelupyynnön.

28.1.2023
Lähetetty kyselylomake täytettäväksi ja haastattelupyyntö kahdelle seuraavalle SOC-analyytikolle. Yksi tärkeistä haastateltavista on osallisena uusissa organisaatiomuutoksissa, joka muuttaa hänen työnkuvaansa, joten häneltä voi olla vaikeampi saada vastauksia tässä vaiheessa. Muihinkin sidosryhmiin vaikuttaa hieman aiemmin aloitetut YT-neuvottelut.

6.2.2023
Laitettu taas pari kyselyä ja haastattelupyyntöä eteenpäin. Sain samana päivänä toiselta hyvät vastaukset kysymyksiini ja kävimme pari asiaa Teamsin kautta vielä läpi selvyyden vuoksi. Aloin tässä vaiheessa dokumentoida haastattelutietoja opinnäytetyöhöni.

7.2. – 12.2.2023
Haavoittuvuuden hallintaprosessin ja muiden rinnakkaisprosessien tietojen tutkimista organisaation intranet-sivuilta ja lähdemateriaaleista. Muiden organisaatioiden hallintaprosessien kuvauksia on todella vaikea löytää.

15.2.2023
Viikoittaisen opinnäytetyön ja siihen liittyvän haavoittuvuusskannerin statuspalaveri keskittyi tällä kertaa opinnäytetyön käsittelyyn, koska vain organisaation opinnäytetyöni valvoja pääsi paikalle. Sain lisää selvyyttä haavoittuvuuden hallintaprosessiin liittyviin kehitystarpeisiin ja samalla selvitettyä muutamia organisaation toimintatapoja.

20.2.2023
Lähetetty kysely vielä kahdelle henkilölle, jotka arvelin sopiviksi kyselykohteiksi aiemman taustatyön perusteella.

21.2.2023

Sain toimistolla käydessäni palautetta yhdeltä kyselyehdokkaalta, ettei hän osaa oikein kunnolla vastata kysymyksiin, mutta hän ehdotti toista SOC-analystiä haastateltavaksi, koska hän oli tutkinut jonkin verran aihetta sisäisesti tässä yrityksessä. Laitoin heti kyselyn tälle uudelle henkilölle. Samalla sain vinkin yhdestä hieman aiheeseen liittyvästä tutkimustyöstä, jonka kävin hakemassa aineistooni. Myöhemmin tapasin myös kaksi muuta henkilöä, joille laitoin kyselyn ja he valittelivat hiukan kiireitä ja sitä, etteivät olleet vielä miettineet tarpeeksi aiheeseen liittyviä kysymyksiä.

28.2.2022

Lisää vastauksia ei ole enää saapunut, joten tutkimusta koostetaan tähän asti saaduilla tiedoilla ja täydennetään myöhemmin tarvittaessa. Haastattelupyynnöt lähetettiin kolmelletoista henkilölle, joista seitsemän pääsi osallistumaan. Osallistumisprosessia alensivat todennäköisesti meneillään olevat YT-neuvottelut, suuret organisaatiomuutokset, jotka kohdistuivat kahteen haastateltavaan, ja myös työkiireet.

Liite 5

RACI-matriisiesimerkki rooleille ja vastuille (PwC 2022, 12)

		LOD 1					LOD 2			LOD 3
Process	Roles / Activities	Security Engineering	Service Owner	IT OPS Team	IT Management	CSIRT	Information Security	CISO	IT Risk	Internal Audit
Prework	Overall responsibility for compliance in terms of data protection and cybersecurity.	C	A	R			C	I	C	
	Overall responsibility for security requirements for IT infrastructure	C	I	I	I		R	A		C
	Maintaining IT Service and application inventory		A	R						
	Defining, planning and implementing measures to counter security vulnerabilities and risks	R	A				C			I
	Defining of Vulnerability KPIs	C			I		R	A	I	
Identify	Operating Vulnerability Scanner	R			A					
	Define / configurate scanning templates	C					R	A		
Evaluate	Analysis, assess vulnerabilities, applying environment rating and deciding on vulnerability rating	C	C	C			R	A	C	
	Analysing and proposing technology-specific remediation measures	R	A			I	C			
Remediate	Applying patches according to the applicable procedure within the defined patch cycle		A	R	I					
	Coordinating remediation action for critical and high vulnerabilities	C	A			R	C			
	Escalating incident if remediation cannot be applied within defined timeframe		A	R			I			
	Deciding how to proceed in the event of escalation	C			A	R	C	A		
	Raising exception if vulnerability is not mitigated within defined timeframe		A/R		A		I		I	
Verify	Track end-to-end Vulnerability Status		I	I	I		R	A	I	
Report	Providing reports (Ad hoc, regularly) including KPIs				I		R	A	I	I

A = Accountable R = Responsible C = Consulted I = Informed