Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2019

Jarkko Ojanperä

CISCO STEALTHWATCH - KÄYTTÖÖNOTTO

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikka

2019 | 34 sivua

Jarkko Ojanperä

CISCO STEALTHWATCH -KÄYTTÖÖNOTTO

Stealthwatch on Cisco Systemsin tuottama työkalu, jolla yrityksessä pystytään seuraamaan tietoliikennettä ja tarkemmin tutkimaan dataa, joka verkossa liikkuu. Opinnäytetyön taustalla oli tarve ottaa palvelu käyttöön yrityksen sisällä ja opetella palvelun käyttöä. Käyttöönotto dokumentoitiin sillä ajatuksella, että mahdolliset uudet työntekijät voivat dokumentaation perusteella opetella Stealthwatchin käyttöä.

Toimeksiantajayrityksellä oli tavoitteena syventää ymmärrystä Stealthwatchin kokonaisuudesta sekä opetella Stealthwatchin käyttö, jotta palvelua voidaan myydä edelleen asiakasyrityksille. Palvelu tuli uutena yrityksen testattavaksi.

Opinnäytetyössä keskitytään teorian osuudessa selvittämään, mitä on yrityksen tietoturva ja mitä osa-alueita se pitää sisällään. Teoriaosuudessa käydään myös läpi Stealthwatchin moninaiset ominaisuudet ja kuinka ne parantavat yrityksen tietoturvaa ja tietoliikenteen läpinäkyvyyttä IT-hallinnon kannalta. Käytännön osuudessa keskitytään sovelluksien asentamiseen ja kuinka palvelua voidaan hyödyntää testaamalla sovelluksia toimeksiantajayrityksen omassa verkossa.

Opinnäytetyössä käydään läpi jokainen Stealthwatchin sovellus, mutta opinnäytetyön käytännön osuudessa käydään tarkemmin läpi Stealthwatchin pakolliset osat, System Management Console sekä Flow Collector. Tärkeänä osana käyttöönottoa on raja-arvojen määritys eri hälytyksille ja kuinka voidaan toimia, jos väärä hälytys tulee ja raja-arvoja tarvitsee muokata. Käytännön osuudessa selvitetään, kuinka hälytykset saadaan lähetettyä asiantuntijoiden tietoisuuteen Stealthwatchin Management Consolen avulla, jos yrityksellä on käytössä tikettijärjestelmä

Johtopäätöksenä opinnäytetyöstä voidaan todeta, että ohjelmistojen perusosien asennus on helposti toteutettavissa virtuaaliympäristöön ja käyttöönotto voidaan suorittaa nopealla aikataululla, mutta sovelluksien konfigurointi yritystarpeisiin sopivaksi vaatii paljon aikaa käyttöönoton jälkeen.

ASIASANAT:

Cisco Stealthwatch, yrityksen tietoturva, hallinnointi, tietoliikenne, NetFlow

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information Technology

2019 | 34 pages

Jarkko Ojanperä

CISCO STEALTHWATCH DEPLOYMENT

Click here to enter text.

Stealthwatch is a tool produced by Cisco Systems, which allows monitoring and deep inspection of the network. Stealthwatch is a set which includes 5 different applications. All the applications are mentioned in this thesis, but the practical part of the thesis is focused on the System Management console and the Flow Collector. The previously mentioned applications are mandatory for Stealthwatch to be functional. The Flow Collector collects all the network data and forwards it to The System Management console for inspection.

The thesis was based on the need to introduce the service within the commissioning company and to learn how to use the service. The deployment was documented having in mind that potential new employees can learn how to use Stealthwatch from the documentation.

The bachelor's thesis focused on the theory as to what is enterprise security and what it contains. The theoretical section also explores the many features of Stealthwatch and how they improve corporate security and transparency in IT administration. The practical section focused on installing applications and how the service can be leveraged by testing applications on the client company’s own network. An important part of the implementation was the setting of limit values for different alarms, and the thesis examines one example of how to act if an alarm comes in and the limit values need to be modified. The practical section also shows how alerts can be sent to experts if the company has a ticket system.

In conclusion it is easy to install the basic software components in a virtual environment and the deployment can be implemented quickly, but it takes a great amount of time after the implementation to configure the applications to suit the business needs.

KEYWORDS:

Cisco Stealthwatch, enterprise information security, data communications, NetFlow

SISÄLTÖ

1 JOHDANTO **1**

1.1 Opinnäytetyön tausta ja tavoitteet 1

1.2 Käytännön osuus 1

2 YRITYKSIEN TIETOTURVA **2**

2.1 Tietoturvan määritys 2

2.2 Riskien hallinta 3

2.3 Palomuuri ja aliverkot 4

2.4 Ohjelmisto 5

2.5 Virustorjuntaohjelmisto 5

2.6 Fyysiset laitteet 5

2.7 Käyttäjäturvallisuus 6

2.8 Hallinnollinen tietoturva 7

2.9 Kolmannen osapuolen palvelut 7

3 CISCO STEALTHWATCH **9**

3.1 Tarkoitus ja käyttö 9

3.2 Stealthwatch ja hallintaratkaisut 10

3.3 Stealthwatch Management Console (SMC) 11

3.4 NetFlow 12

3.5 Stealthwatch Flow Collector (FC) 13

3.6 Flow Sensor (FS) 13

3.7 Packet Analyser (PA) 14

3.8 UDP Director 14

4 KÄYTTÖÖNOTTO **15**

4.1 Laitevaatimukset 15

4.2 Verkkoliikenteen määritykset 16

4.3 Asennus 16

4.4 Keskeisiä kysymyksiä käyttöönoton jälkeen 18

4.5 Itseoppiva tekoäly 20

5 ESIMERKKITAPAUS KÄYTTÖÖNOTON JÄLKEEN **22**

5.1 Hälytyksen muokkaus 23

5.2 Aiheellisista hälytyksistä tiedottaminen 25
5.3 Jatkotoimenpiteet 26
5.4 Indeksien muokkaaminen käyttötarkoituksiin sopiviksi 27

6 FLOW COLLECTOR 29

7 PÄÄTELMÄT 32
7.1 Opinnäytetyön tavoitteet ja onnistumiset 32
7.2 Stealthwathin management consolen ja Flow collectorin käyttö 33

LÄHTEET 34

KUVAT

Kuva 1. Riskien arviointiprosessi [3]. 3
Kuva 2. PDCA-malli [5]. 7
Kuva 3. Stealthwatchin logo [11]. 9
Kuva 4. Stealthwatch tuotekaavio [11]. 11
Kuva 5. Paketin tarkasteltavat osat [12]. 12
Kuva 6. Koneoppivan tekoälyn rakenne [16]. 20
Kuva 7. SMC Etusivu. 22
Kuva 8. Tiedot concern indexin aiheuttaneesta hälytyksestä. 23
Kuva 9. Esimerkki räätälöityjen hälytyksien luonnista. 24
Kuva 10. Hälytyksien prioriteettimääritykset. 25
Kuva 11. Hälytykseen reagointi. 26
Kuva 12. Indeksien muokkaus policy managerilla. 27
Kuva 13. Raja-arvojen muokkaus. 28
Kuva 14. Cisco Flow collectorin toimintakaavio. 29
Kuva 15. Flow Collector etusivu. 30
Kuva 16. Flow Collectorin tallennus statistiikkaa. 31

TAULUKOT

Taulukko 1. Stealthwatch laitevaatimukset. 15
Taulukko 2. Verkkoliikennemääritykset [11]. 16

1 JOHDANTO

1.1 Opinnäytetyön tausta ja tavoitteet

Valitsin opinnäytetyöni aiheeksi projektin, jossa otetaan käyttöön Cisco Stealthwatch yrityksen sisällä testikäyttöön. Projektin tarkoituksena on tutustua Stealthwatch kokonaisuuteen sekä yrityksien tietoturvaan ja käydä läpi eri Stealthwatchin erilaisia ominaisuuksia ja dokumentoida palvelun käyttöönotto sekä peruskäyttö. Opinnäytetyön toimeksiantajana toimii Wisdomic Solutions Oy. Opinnäytetyön tehtävä on kertoa yleiskatsausta tietoturvasta yritysmaailmassa ja siitä, kuinka Cisco Stealthwatch helpottaa IT-asiantuntijan reagointikykyä ja ennaltaehkäisykykyä tietoturvaa uhkaavissa tilanteissa.

Opinnäytetyön tavoitteena on muodostaa käsitys yrityksien tietoturvasta ja siitä, kuinka tärkeä osa se on nykypäivän yritysmaailmassa sekä kuinka Cisco Stealthwatch parantaa tietoturvaa ja uhkien ennaltaehkäisyä.

1.2 Käytännön osuus

Asennus ja käyttöönottovaiheessa on käytössä kaksi VMware-ympäristössä toimivaa virtuaalipalvelinta, joihin asennetaan ainoastaan Stealthwatchin pakolliset osuudet Stealthwatch Management Console sekä Flow Collector.

Stealthwatchin käyttöönotossa otetaan palvelu käyttöön yrityksen sisäisesti testaukseen, jotta saadaan parempi käsitys itse palvelusta ja sen määrityksistä, ennen kuin palvelua tarjotaan asiakkaille.

Lähdemateriaalina on käytetty suurimmilta osin Ciscon omia esittelyitä sekä Ciscon ylläpitämää resurssipankkia. Näiden lisäksi yleisen yritystietoturvan osuudessa on käytetty materiaaleina verkkojulkaisuja ja verkossa julkaistuihin tutkielmia, koska kirjallinen materiaali on vaikeasti saatavilla kyseisistä aiheista.

Opinnäytetyöstä on rajattu pois kaikki valinnaiset Stealthwatch -palvelut, koska näitä ei tulla yrityksen sisäisesti ottamaan käyttöön. Jokainen osa on kuitenkin teoreettisessa osassa mainittuna.

2 YRITYKSIEN TIETOTURVA

Tietoturvan merkitys digitalisoituneessa maailmassa on kasvanut viime vuosien ajan. Nykypäivän tietoturva on jatkuvaa kilpailua uusia uhkia vastaan. Sitä mukaan, kun tietoturva-aukkoja paikataan, ovat tietoturvaa uhkaavat tahot etsimässä jo uusia mahdollisia aukkoja. Yrityksien tietoturva ei ole pelkästään virustorjunta ja palomuuri, vaan tietoturva koostuu monista eri osa-alueista, joka yhdessä muodostaa kattavan kokonaisuuden. Tässä luvussa käydään läpi yleisesti tietoturvaa ja sen määrityksiä sekä perinteisiä tietoturvalaitteita yritysympäristössä ja niiden käytäntöjä.

2.1 Tietoturvan määritys

Tietoturvan tarkoituksena on varmistaa, että yrityksen kaikki verkossa olevat laitteet ja niihin kuuluvat ohjelmat tekevät aina sen, mihin ne on tarkoitettu. Tietoturva on onnistunut siinä tapauksessa, jos järjestelmät voidaan suojata mahdollisimman monelta odotetulta ja odottamattomalta riskiltä sekä varmistaa, että suojatut tiedostot ovat vain niiden henkilöiden käytössä, joille käyttöoikeus kuuluu [1, s. 15].

Tietoturvan tavoitteet ovat jaettu viiteen eri kategoriaan: luottamuksellisuuteen, autenttisuuteen, kiistämättömyyteen, käytettävyyteen ja eheyteen.

Luottamuksellisuuden tavoitteena on varmistaa, että järjestelmien tietoja pystyvät käyttämään vain siihen oikeutetut käyttäjät. Jos ulkopuolinen taho on päässyt käyttämään sellaista tietoa, jonka käyttöön hänelle ei ole oikeutta, on luottamuksellisuus menetetty.

Autenttisuus varmistaa, että kaikki järjestelmän osat voidaan tunnistaa luotettavasti. Osiksi voidaan luokitella käyttäjät, tiedostot ja verkon tapahtumat.

Kiistämättömyydellä varmistetaan, että kaikki järjestelmissä tapahtuneet asiat voidaan todistaa myöhemmin luotettavasti. Verkossa tapahtuvat asiat voidaan esimerkiksi tallentaa lokitietoihin, joista voidaan todentaa mahdollisesti haitalliset aktiviteetit.

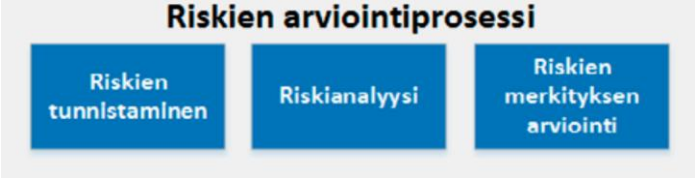
Käytettävyyden tavoite on, että järjestelmien tiedot ovat aina käytettävissä. Yritysverkossa käytettävyys on käyttäjän näkökulmasta tärkein ja näkyvin palvelu. Järjestelmien hallitsijoiden suurimpiin haasteisiin sisältyy tietojen käytettävyyden varmistaminen.

Eheys tarkoittaa Tietoturvassa tietojen tarkkuuden ja täydellisyyden ylläpitämistä ja varmistamista koko elinkaarensa ajan. Tämä tarkoittaa, että käyttäjä ei voi muokata tietoja luvattomasti tai havaitsematta. Eheydessä on myös huomioitava tietokoneen tai sen ohjelmien mahdolliset virheet [1, s. 17].

Nykypäivänä voidaan myös määritellä tietoturvan osa-alueeksi anonymiteetti. Anonymiteetillä tarkoitetaan sitä, että käytössä olevaan dataan ei käytetä henkilökohtaisten tietojen keräämiseen ja niiden hyödyntämiseen [2, s. 5].

2.2 Riskien hallinta

Riskien hallinta on yrityksen tietoturvan kannalta elintärkeä prosessi. Alla olevassa kuvassa havainnoidaan arviointiprosessin kolmea eri kohtaa.



Kuva 1. Riskien arviointiprosessi [3].

Riskien tunnistamisen tavoite on havaita ja kuvata kaikki merkittävät riskit ja mahdollisuudet, riskien lähteet, vaikutusalueet, tapahtumat, mukaan lukien olosuhteiden muutokset ja niiden syyt sekä mahdolliset seuraukset. Riskien tunnistukseen osallistuvilla asiantuntijoilla on oltava tarkasteltavan toiminnan riittävä ymmärrys. Tunnistamisessa on huomioitava organisaatioon vaikuttavat tekijät riippumatta siitä, onko riskien lähde yrityksen hallinnassa [3, s. 21].

Riskien tunnistamisessa on neljä vaihetta:

- estävien, tai haittaavien tekijöiden tunnistus
- menetyksen sekä hyödyntämättä jättämisen aiheuttamat riskit
- luodaan luettelo riskeistä, jotka mahdollistavat, tai estävät tavoitteiden saavuttamisen
- luodaan luettelo yrityksen hallitsemattomista riskeistä

Analyysin perusteella luodaan pohja päätöksille siitä, mitä ja miten riskejä käsitellään. Analyysissä arviot todennäköisyydestä ja vaikutuksista perustuvat subjektiivisiin näkemyksiin, jolloin voi olla vaikea muodostaa yhteistä käsitystä riskin vakavuudesta. Siksi on tärkeää kirjata mahdolliset mielipiteisiin tai muihin epävarmuustekijöihin perustuvat seikat riittävän selkeästi myöhemmin tapahtuvaa päätöksentekoa varten [3, s. 22].

Merkityksen arvioinnin tavoitteena on auttaa tekemään päätöksiä, mitä riskejä on tarpeen käsitellä ja mikä on käsittelyn tärkeysjärjestys. Arvioinnin yhteydessä voi käydä ilmi, että jotkut riskit täytyy arvioida uudelleen tai että tarvitaan muu täydentävä analyysi. Merkityksen arvioinnin yhteydessä voidaan päättää, että joitakin havaittuja riskejä ei käsitellä [3, s. 15].

2.3 Palomuuri ja aliverkot

Palomuurin tarkoituksena on hallinnoida ja tarvittaessa estää liikennettä ulkoverkosta. Kaikki data, mitä saapuu yrityksen sisäverkkoon ulkopuolelta, kulkee palomuurin kautta ja liikenne tarkistetaan, ennen kuin se pääsee käyttäjälle. Tietoturvavastaavan on tärkeää olla perillä, mitä portteja palomuureissa on sovelluksia varten auki ja mitä tietoturvauhkia nämä voi pitää sisällään.

Aliverkkojen luonti on erityisen tärkeää, jos yrityksellä on käytössä palveluita, jotka ovat sisä- ja ulkoverkon rajapinnoissa. Tällaisia palveluita ovat verkkopalvelimet, sähköpostipalvelimet, DNS-palvelimet sekä muut palvelimet, joihin viestit tulevat sisäverkkoon, ulkoverkon kautta.

Edellä mainitut palvelimet laitetaan Demilitarisoituun alueeseen (engl. Demilitarized zone) eli DMZ-aliverkkoon, joka yhdistää turvattomat palvelimet yrityksen sisäverkkoon. DMZ-verkossa olevat laitteet eivät voi muodostaa suoraa yhteyttä lähiverkon laitteisiin, ainoastaan muihin aliverkossa oleviin laitteisiin sekä verkon ulkopuolisiin laitteisiin. Jos hyökkäys tämän aliverkon laitteisiin onnistuu, on silloin muu yrityksen verkko suojassa.

2.4 Ohjelmisto

Päivittämättömät ohjelmistot ovat varsinkin isoissa yrityksissä monesti ongelmakohtia. Suuria määriä uusia versioita on työlästä hankkia ja useimmiten yritykset päivittävät sovelluksia vain tietyin väliajoin. Päivittämättömät sovellukset saattavat sisältää tietoturva-aukkoja, jotka voivat pahimmillaan altistaa koko yritysverkon uhan alle. Myös ohjelmistojen lisensseistä on pidettävä tarkkaa huolta, jos lisenssi umpeutuu voi sovellus lopettaa toiminnan kokonaan.

Tietotekniikasta vastuussa olevien henkilöiden tehtävänä on huolehtia, että sovelluksiin asennetaan tärkeimmät päivitykset mahdollisimman nopeasti ja tarvittaessa hankkia ohjelmistoista uudemmat versiot, jos vanhojen tuki on lopetettu sovellustoimittajan toimesta. Vastuuhenkilön täytyy myös olla hyvin perillä siitä, mitä lisenssejä yrityksellä on ja kauan ne ovat voimassa.

2.5 Virustorjuntaohjelmisto

Viimeisimpänä suojana tietoturvauhalle toimii virustorjuntaohjelmistot. Suurissa yrityksissä on käytännössä katsoen mahdotonta suojata kaikki verkossa kulkevat datat ja nettisivustot. Jos käyttäjä pääsee omalla koneellaan palomuurimääritysten ohi lataamaan saastuneen tiedoston, tai päätyy nettisivulle, josta koneeseen hyökätään, niin ainoa mahdollinen keino estää saastuminen tässä vaiheessa on virustorjunta.

Yritykset, jotka myyvät virustorjuntaohjelmia palveluina kehittävät jatkuvasti tietokantojaan ja suojauksia, jotka siirtyvät automaattisesti päivityksinä käyttäjien koneelle.

2.6 Fyysiset laitteet

Fyysisellä tietoturvalla ennaltaehkäistään kaikki uhkatekijät, jotka kohdistuvat itse laitteisiin. Jos esimerkiksi yrityksen tärkeiden tietojen palvelin ei ole turvattu fyysisesti, niin palvelimen luottamuksellisuutta ja saatavuutta ei voida varmistaa. Palo-, vesi- tai sähkövahingoilta suojautuminen on tärkeässä osassa kokonaisvaltaisen tietoturvan hallintaa. Myös inhimilliset uhat, kuten varkaudet ja ilkivalta, tulee ottaa huomioon.

Fyysisiin laitteisiin voidaan myös luokitella massamuistit sekä muistitikut. Ulkoset tallennuslaitteet ovat helposti altistuvia varkauksille. Varkauden sattuessa on tärkeää, että tallennuslaitteet ovat salasanasuojattuja, etteivät laitteeseen tallennetut tiedostot pääse vääriin käsiin.

Vasta kun laitteiden toimintaympäristö on saatu suojattua, voidaan alkaa suunnittelemaan ja kehittämään tietoturvan muita osa-alueita laitteille.

2.7 Käyttäjäturvallisuus

Yksi suurimmista haasteista tietoturvassa on loppukäyttäjän käyttäytyminen. Tietoturvan kehittyessä, myös uusia uhkia syntyy jatkuvasti ja niiden perässä on liki mahdotonta pysyä. Tässä kohtaa loppukäyttäjällä on suuri vastuu siitä, kuinka käyttäytyy internetissä ja palveluissa [4].

Erilaisilla tietoturvamäärityksillä voidaan pakottaa käyttäjä luomaan salasana, joka on nykyisten tietoturvastandardien mukainen, tai voidaan rajoittaa palveluita, jotka eivät ole tietoturvastandardien mukaisia. Rajoitetut käyttöoikeudet voivat estää ylimääräisten sovelluksien latauksen ja asennuksen koneelle, mutta kuormittavat IT-tukihenkilöitä, jos sovellus on luvallinen ja sen asennukseen tarvitaan ylennetyt käyttöoikeudet.

Määrityksien lisäksi tietoturvasta vastaavien henkilöiden vastuulla on tiedottaa, kouluttaa ja luoda ohjeistuksia, kuinka toimia turvallisesti. Mikään suojaus ei auta silloin, jos käyttäjä jättää esimerkiksi salasanansa post-it -lapulle näyttöön, tai kirjaa salasanan omaan muistioonsa. Jos käyttäjä ei huomaa menneensä väärälle sivulle kirjoitusvirheen johdosta, tai jos käyttäjä ei huomaa tarkistaa saadun sähköpostin lähettäjätietoja, voi olla koko yrityksen tietoverkko uhattuna.

2.8 Hallinnollinen tietoturva

Hallinnollisen tietoturvan vastuulla on varmistaa, että kaikki tämän luvun aikaisemmin mainitut tietoturvan osat sekä kriteerit toteutuvat.

Hallinnollisen tietoturvan apuna voidaan käyttää PDCA-mallia (Kuva 2), joka tulee englanninkielen sanoista Plan-Do-Check-Act., joka Suomennettuna tarkoittaa Suunnittele-Tee-Tarkasta-Toimi.

Kuva 2. PDCA-malli [5].

Suunnittelussa määritellään tietoturvan tarpeet. Tee-vaiheessa toimeenpannaan käytännössä määritelty tietoturva. Tietoturvaongelmat voivat johtua myös väärästä tietoturvaratkaisusta, jolloin yrityksellä ei ole ollut tarvittavaa asiantuntemusta määritellä oikeanlaista tietoturvaratkaisua. Hallinnollinen tietoturva määrittelee myös linjaukset henkilöstölle sekä vastaa koulutuksesta tietoturva-asioissa [6].

2.9 Kolmannen osapuolen palvelut

Kolmannen osapuolen tietoturvaratkaisut ovat yrityksille hyvä vaihtoehto, kun yrityksellä ei ole omia resursseja suunnitella ja toteuttaa kokonaisvaltaista tietoturvaratkaisua. Ciscon lisäksi maailmalla on muita palveluntarjoajia, jotka pystyvät huolehtimaan tietyistä tietoturvan osa-alueista. Seuraavaksi listattu muutamia erilaisia tietoturvaratkaisuja yrityskäyttöön.

F-secure on tunnettu päätelaitteiden tietoturvasuojistaan. F-secure tarjoaa Protection Service for Business (PSB) ratkaisulla virustorjunnan yrityksen kaikkiin päätelaitteisiin ja se ei vaadi ylimääräisiä hallintatoimia. Yrityksen tietoturvapäivitykset laitteisiin tapahtuvat kootusti palvelun kautta. PSB pystytään liittämään yrityksen SIEM-ratkaisuun, jolloin mahdolliset tietoturvariskit tulevat asiantuntijoiden tietoisuuteen mahdollisimman nopeasti [7].

Perinteisen virustorjunnan lisäksi F-secure tarjoaa Radar palvelun, joka vastaa toiminnallisuudeltaan hyvin paljon Ciscon Stealthwatchia. Radar tutkii ja tarkkailee yrityksen verkkoa ja havaitsee järjestelmien, tai sovelluksien puutokset sekä haavoittuvuudet. Lisäksi Radar tunnistaa ja havaitsee tapahtuvat tietoverkkohyökkäykset ja tunnistaa haittaohjelmasivustot [8].

Palo Alto tarjoaa yrityksille fyysisiä ja virtuaalisia palomuureja. Palomuurien teknologia keskittyy perinteisten porttien sijaan sovelluksien tunnistamiseen (App-ID) sekä käyttäjien tunnistamiseen. Identiteettien kautta verkkoliikenteen hallinta ei ole paikka, tai IP-osoitteesta riippuvaista. Virtuaalisella palomuurilla voidaan suojata mahdolliset sivukonttorit yrityksen yhdestä datakeskuksesta ilman paikallista fyysistä palomuuria [9].

Proofpoint on sähköpostisuojausjärjestelmä, joka tunnistaa ja estää haitallisten sähköpostien ja liitetiedostojen pääsyn sähköpostiin. Haitallisten tiedostojen lisäksi, sovellus tarkistaa automaattisesti verkko-osoitteet ennen niiden aukaisua ja osaa varoittaa käyttäjää, jos linkki on haitallinen. Proofpoint ei yksinomaan ole tarpeeksi laaja palvelu suojaamaan yrityksen verkkoa, mutta palvelu pystyy estämään yksittäisiä uhkia liittyen käyttäjäturvallisuuteen [10].

3 CISCO STEALTHWATCH

Nykypäivänä yritykset joutuvat panostamaan enemmän tietoturvaan jatkuvasti lisääntyvien verkkoon kytkettävien laitteiden myötä. IoT sekä liikuteltavat laitteet, kuten puhelimet ja kannettavat tietokoneet ovat suuri haaste yrityksen tietoturvalle. Tietoturvalle on tärkeää seurata tilannetta ja laitteiden käyttäytymistä reaaliajassa ja reagoida poikkeamiin mahdollisimman nopeasti, että pystytään selvittämään, onko aihetta toimenpiteille.

Cisco Stealthwatch (kuva 3) on yritystason tietoturvaratkaisu, joka tarjoaa reaaliaikaisten uhkien havaitsemiseen ja hallitsemiseen tarkoitetut työkalut. Stealthwatch ei korvaa nykyisiä olemassa olevia tietoturva palveluita, vaan sen on tarkoitus toimia niiden lisäksi, paikkaamassa tietoturva-aukkoja sieltä mihin perinteiset palomuurit ja virustorjunnat eivät kykene. Stealthwatch lukee laitteiden välisiä keskusteluita, havaitsee näistä poikkeamat ja ilmoittaa niistä suoraan verkkohallinnalle, joka voi tutkia tarkemmin ilmoitukset ja ryhtyä tarvittaviin toimenpiteisiin.

Kuva 3. Stealthwatchin logo [11].

Stealthwatch hyödyntää tietoturvauhkien torjunnassa yhdistetysti käyttäjien käyttäytymismallinnusta, itseoppivaa teknologiaa sekä Ciscon ylläpitämää maailmanlaajuista verkkouhka tietokantaa, jota päivitetään jatkuvasti.

3.1 Tarkoitus ja käyttö

Yrityksien verkot ja niitä käyttävien laitteiden ja palveluiden määrä kasvaa jatkuvasti. Perinteiset tietoturvaratkaisut kuten palomuurit ja virustorjunnat on suunniteltu tiettyihin käyttötarkoituksiin ja ne vaativat jatkuvaa ylläpitoa ja konfigurointia. Stealthwatchin

avulla voi nähdä kaikki laitteiden väliset keskustelut ja asettaa järjestelmät tietyt kriteerit, joiden avulla se oppii havaitsemaan riskit ja epäilyttävät käytökset. Palvelu on jaettu kolmeen eri osaan: näkyvyys, havaitseminen sekä toimenpide

Stealthwatchin näkyvyys perustuu Ciscon kehittämään NetFlow-protokollaan, jonka avulla voidaan yhdistää koko yrityksen verkko, niin fyysiset laitteet, kuin pilvipalvelutkin, ilman ylimääräisiä antureita, tai sensoreita.

Havaitsemisella tarkoitetaan sovellusta, joka yhdistää verkkohallintatiimin sekä tietoturvatiimin. Tietoturvan osalta se havaitsee edistyneemmät jatkuvat uhat, Bottiverkot (Botnet), virukset, palvelunestohyökkäykset (DDoS) hyökkäykset, tiedostohaavoittuvuudet sekä Nollapäivähaavoittuvuudet (Day 0 hyökkäykset). Näiden lisäksi Stealthwatch seuraa yleisimpiä päätelaitteita, sovelluksia, verkon latenssia ja suorituskykyä.

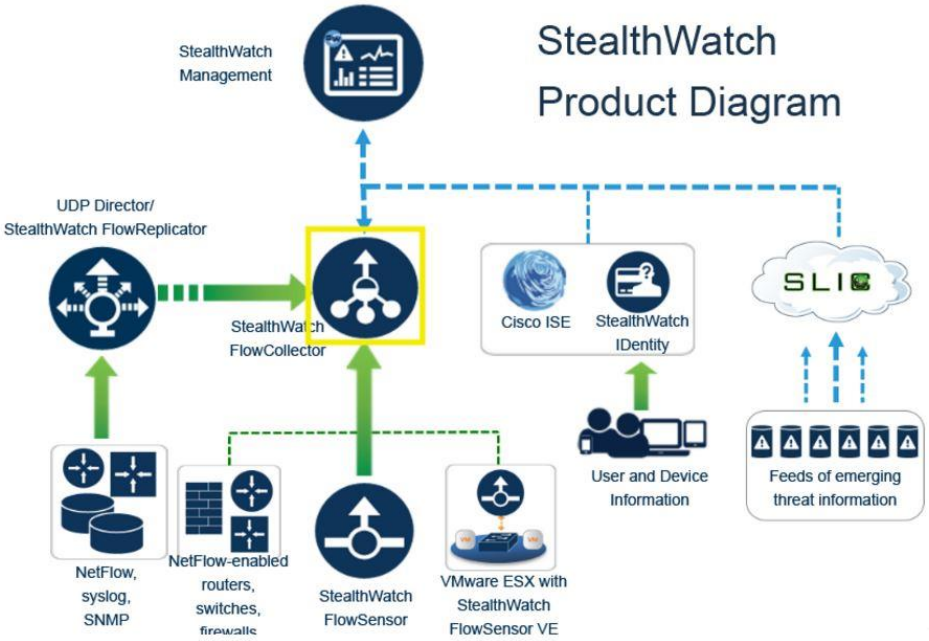
Toimenpiteen osan tarkoitus on tallentaa kaikki lokitiedot ja havainnot palvelimelle myöhempää tarkastelua varten, jolloin järjestelmävalvoja voi todeta uhan aiheelliseksi, tai aiheettomaksi ja tehdä tarvittavat toimenpiteet.

3.2 Stealthwatch ja hallintaratkaisut

Stealthwatch toimii yhteen ja täydentää yrityksen turvatietojen ja -tapahtumien hallintapalveluita (engl. Security information and event management), eli SIEM-ratkaisuja. Siinä missä SIEM tarkastelee lokitiedostoja verkkolaitteista ja luo siitä hälytykset perustuen standardien määrittelemiin työkaluihin, niin Stealthwatch tutkii pakettien metatietoja, kuten NetFlowta ja IPFIX-tietoja kokonaiskuvan muodostamiseksi ja tunnistaa käyttäytymismalliin perustuvat poikkeumat. Stealthwatch kerää kaiken datan NetFlow’sta ja ilmoittaa kriittiset viat suoraan tietoturvavastaaville, jolloin heidän ei tarvitse itse käydä läpi kaikkea tietoa itse.

SIEM-palvelut veloittavat yrityksiltä datamäärien mukaan ja suurissa yritysverkoissa tulee paljon duplikaattidataa, kun yksi paketti on saattanut kiertää useamman laitteen kautta. Stealthwatch kerää tiedot laitteista ja osaa poistaa duplikaattitiedot, jotta kaikki liikenne, joka saattaa kulkea useamman laitteen kautta luetaan vain yhtenä tietona.

Stealthwatch koostuu eri sovelluksista ja palveluista, jotka luovat yhtenäisen kokonaisuuden. Palvelun käyttöönottoon vaaditaan vähintäänkin System Management Console ja Flow Collector. Kuvassa 4 esitellään Stealthwatchin tuotekaaviota ja nuolilla havainnoidaan eri palveluiden tiedon kulkusuunta.



Kuva 4. Stealthwatch tuotekaavio [11].

3.3 Stealthwatch Management Console (SMC)

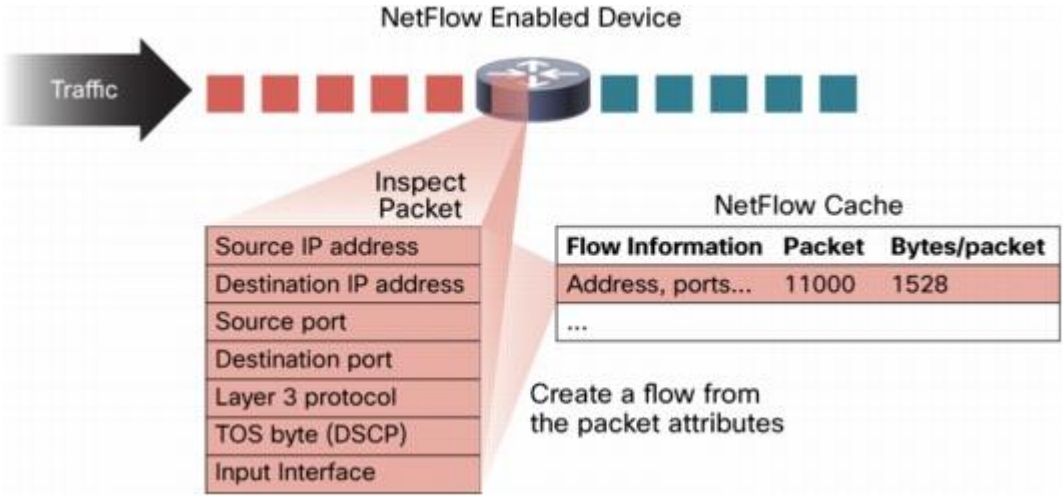
SMC toimii käyttöliittymänä kokonaisuudelle. Se ohjaa, määrittelee ja organisoi datan muilta Stealthwatch-laitteilta ja -palveluilta, sekä tutkii epäilyttävän käytöksen niiden tallentamasta datasta. Konsolin kautta pystytään hallitsemaan muita Stealthwatch laitteita ja se toimii käyttöliittymänä järjestelmänvalvojalle. Kaikki Stealthwatchin tutkima data on nähtävissä SMC-käyttöliittymässä.

SMC seuraa verkon kaikkia laitteita ja niiden välisiä keskusteluita. Verkkoliikenne visualisoidaan helposti ymmärrettäväksi ja luettavaksi. Kerätyn datan perusteella luodaan syväluotaavia analyysejä verkon tilasta ja jaotellaan mahdolliset uhkatilanteet eri kategorioihin. Verkkoliikenteestä luodaan automaattisesti visuaalisia kaavioita, joista voidaan nähdä esimerkiksi mihin maahan kulkee eniten dataa, tai mikä laite kuormittaa verkkoa eniten.

3.4 NetFlow

NetFlow on Ciscon kehittämä ominaisuus, joka on sulautettu Ciscon IOS-ohjelmistoihin verkon toiminnan helpompaa ymmärtämistä varten. NetFlow eroaa perinteisestä SNMP:stä siten, että NetFlow'lla voidaan tarkastella IP-liikennettä ja saada parempi käsitys siitä, mihin liikenne virtaa, jotta voidaan varautua saatavuuden, suorituskyvyn sekä vian etsinnän tarjoamiseen juuri sinne mihin tarvitaan, kun taas perinteinen SNMP kertoo vain pelkän kaistanleveyden.

Jokainen paketti, joka lähetetään, tai vastaanotetaan NetFlowlla varustetun kytkimen kautta tutkitaan IP-pakettimääritteiden suhteen (Kuva 5). Nämä määreet ovat paketin IP-identiteetti ja ne määrittävät onko paketti uniikki, vai samankaltainen aikaisempien pakettien kanssa.



Kuva 5. Paketin tarkasteltavat osat [12].

Kaikki paketit, joilla on samat lähde-, tai kohdetiedot, protokollat ja palveluluokat on ryhmitelty virtaan, jonka jälkeen paketit kootaan yhdeksi kokonaisuudeksi. Näillä tiedoilla pystytään ymmärtämään helpommin verkon käyttäytymistä ja näkemään mistä data on lähtenyt ulkoverkossa liikkeelle ja mikä laite vastaanottaa sen. Porttitiedot luonnehtivat sovellusta, joka käyttää liikennettä ja palveluluokka tutkii prioriteettia. TOS byte eli laiterajapinta kertoo, miten verkkolaite käyttää liikennettä. Lopuksi tallennetut paketit kertovat liikenteen määrän [12].

Näiden tietojen avulla pystytään luomaan kokonaisuuksia jokaisesta laitteesta ja havaitsemaan nopeasti poikkeamat ja reagoimaan poikkeamiin tarvittavilla toimenpiteillä. NetFlow'n avulla pystytään vähentämään vianetsintäaikaa, koska poikkeamat on helpompi huomata reaaliajassa päivittyvässä virrassa, sekä luo helpommin ymmärrettäviä raportteja verkon käytöstä. Raporteista voi nähdä kuka käyttää verkkoa ja minkä tyyppiset sovellukset kuormittavat verkkoa.

3.5 Stealthwatch Flow Collector (FC)

Flow Collector vastaanottaa kaiken yrityksen sisäverkossa liikkuvan NetFlown, jonka se säilyttää paikallisessa tietokannassa raportointia ja tietoturva-analyysia varten. Kaikki tallennetut tiedot muutetaan helposti luettavaksi raportiksi, jotka voidaan lukea SMC:n kautta. FC pystyy myös vastaanottamaan ja tallentamaan dataa välityspalvelimien lähteistä ja analysoimaan saadun datan pilvipohjaisen ja monitasoisen itseoppivan tietokannan kautta, saavuttaakseen syvällisen sekä tarkan kuvan yrityksen verkosta ja sen liikenteestä [13].

3.6 Flow Sensor (FS)

Flow Sensor ei ole pakollinen osa Stealthwatchin kokonaisuutta. Flow Sensorin tehtävänä on tuottaa reititin- sekä kytkentäinfrastruktuuriin Netflow'ta laitteisiin, joissa se ei normaalisti ole mahdollista. NetFlown luonnin lisäksi FS tekee syväluotaavaa pakettitutkintaa (DPI) sovelluskerroksen tiedoista ja ottaa paketeista näkyvää dataa, jolla mahdollistetaan verkon käytön ja nopeuden seuranta. Uudempi 7.1 käyttöjärjestelmäversio mahdollistaa myös salatun liikenteen analytiikan, eli ETA:n (engl. encrypted traffic analytics), jolla voidaan tutkia esimerkiksi salattujen https-protokollia hyväksikäyttävien pakettitietojen tutkinta, mahdollisten vaarallisten tiedostojen varalta.

Sensorit voidaan asentaa joko virtuaalisina, tai fyysisinä laitteina ja ne asetetaan peilaamaan portteja, joiden dataa halutaan tarkemmin tutkia. Sensoreita voi asentaa myös useampia käyttöön, mahdollistaakseen laajemman ja nopeamman tutkinnan yrityksen verkossa [14].

3.7 Packet Analyser (PA)

Cisco Packet Analyzer on erillinen fyysinen laite, joka tutkii Stealthwatchin NetFlow:ta ja tallentaa jokaisen paketin, toisin kuten tavalliset verkkokortit. Mahdollisessa tietoturvaa uhkaavassa tilanteessa voidaan Packet Analyserista ottaa saastuneet paketit tarkempaan tutkintaan, selvittää paketin alkuperä ja hakea saastuneen paketin tiedoilla mahdolliset muut saastuneiden tiedostojen olinpaikat ja estää laajempi vahinko sattumasta. Pakettien alkuperän selvittämisessä on myös suuri etu mahdollisten uusien samantyylisien uhkien estämisessä.

3.8 UDP Director

Kytkimillä ja reitittimillä on käytössä rajallinen määrä istuntoja NetFlown luontia varten. Jos yrityksellä on käytössä useita laitteita, jotka keräävät NetFlow'ta, pystytään data lähettämään UDP Directorille, joka kopioi NetFlown datat ja uudelleen lähettää ne tarvittaville laitteille, joka vähentää verkon kuormitusta. UDP Directorin ominaisuuksiin kuuluu myös muiden eri NetFlow standardien replikoiminen ja muuntaminen yhteneväiseksi NetFlowksi, jolloin ei tarvitse useampaa laitetta lukemaan eri NetFlow -standardeja. UDP Directorin voi asentaa fyysisenä tai virtuaalisena laitteena verkkoon.

4 KÄYTTÖÖNOTTO

Stealthwatchin käyttöönotossa on huomioitava sovelluksien laitevaatimukset ja vähimmäisuositukset. Tässä luvussa käydään läpi palvelimien vaatimukset sovelluksien osalta, sekä asennuksen eri vaiheet.

Ennen varsinaista käyttöönottoa on huomioitava, että Stealthwatchin, kuten muidenkin tietoliikennettä seuraavien palveluiden käyttöönotossa on noudatettava lakia yksityisyyden suojasta työelämässä. Laki yksityisyyden suojasta työelämässä määrittelee tietoliikennettä seuraavien palveluiden käytöstä seuraavasti:

”Yhteistoiminta- tai kuulemismenettelyn jälkeen työnantajan on määriteltävä työntekijöihin kohdistuvan teknisin menetelmin toteutuvan valvonnan käyttötarkoitus ja siinä käytettävät menetelmät sekä tiedotettava työntekijöille valvonnan tarkoituksesta, käyttöönotosta ja siinä käytettävistä menetelmistä sekä sähköpostin ja tietoverkon käytöstä” [15].

4.1 Laitevaatimukset

Jotta Stealthwatch ja sen oheislaitteet toimivat luotettavasti ja tasaisesti, on niille varattava taulukon mukaiset vähimmäislaitevaatimukset palvelimelta. Palvelimille on hyvä varata levytilaa enemmän, mitä vaaditaan, jotta lokitiedostoja pystytään säilömään pidemmältä aikaväliltä.

Taulukko 1. Stealthwatch laitevaatimukset.

Laite	**Muisti**	**Levytila**	**CPU**
SMC	16GB	50GB	4 CPUs
FC	16GB	500GB	4 CPUs
FS	4GB	8GB	2 CPUs
UPD Director	4GB	50GB	2 CPUs

4.2 Verkkoliikenteen määritykset

Verkkomäärityksillä varmistetaan, että Stealthwatchin kaikki palvelut voivat keskustella keskenään esteettömästi. Verkkoasetuksista ja palomuurista on määriteltävä palvelimien ohjelmistoportit seuraavasti:

Taulukko 2. Verkkoliikennemääritykset [11].

From (Client)	To (Server)	Port	Protocol
Admin User PC	All appliances	TCP/443	HTTPS
All appliances	Network time source	UDP/123	NTP
FlowCollector	SMC	TCP/443	HTTPS
SMC (SLIC Feed)	Internet	TCP/443	HTTPS
UDP Director	FlowCollector - sFlow	UDP/6343	sFlow
UDP Director	FlowCollector - NetFlow	UDP/2055	NetFlow
FlowSensor	SMC	TCP/443	HTTPS
FlowSensor	FlowCollector - NetFlow	UDP/2055	NetFlow
NetFlow Exporters	UDP Director - NetFlow	UDP/2055	NetFlow
All appliances	DNS	UDP/53	DNS
SMC	FlowCollector	TCP/443	HTTPS
SMC	FlowSensor	TCP/443	HTTPS
SMC	Flow Exporters	UDP/161	SNMP
User PC	SMC	TCP/443	HTTPS

4.3 Asennus

Stealthwatchin asennus ja käyttöönotto koostuu kolmesta eri vaiheesta. Suunnittelu verkon osalta, jotta voidaan sisällyttää tarvittavat laitteet palvelun alle. Ympäristön valmistelu, kuten laitteiden päivittäminen ja tarvittavien resurssien varaaminen. Kun verkon suunnittelu ja ympäristön valmistelu on valmiina, voidaan aloittaa itse alustan asennus ja käyttöönotto

Cisco Stealthwatchin voi asentaa fyysisille, tai virtuaalisille palvelimille. Tämän opinnäytetyön puitteissa Stealthwatchin tarvittavat osat, FC ja SMC asennetaan virtuaalisille palvelimille. Tässä projektissa käytetään palvelinalustana VMwaren vCenteriä.

Stealthwatch käyttö voidaan aloittaa kahdella eri palvelimella, joihin asennetaan, Stealthwatch Management Console (SMC), sekä Flow Collector (FC). Muita osia, kuten Flow Sensor (FS), sekä UDP Directoria ei asenneta tämän opinnäytetyön puitteissa. Ennen asennusta on kannattavaa kartoittaa myös muiden tarvittavien palvelinten ja palveluiden resurssit, kuten Active Directoryn käyttöönotto, lokitiedosto palvelin, Identity Service Engine (ISE), sekä SIEM. Palvelinten alustoina toimii VMware virtuaalipalvelinkoneet, joihin on ennalta määritelty tarvittavat resurssit tasaista toimintaa varten.

Suunnitteluvaiheessa on oltava tiedossa yrityksen verkot ja niiden aliverkot, sekä lista reitittimistä, kytkimistä, palomuureista ja muista laitteista, jotka tuottavat NetFlowta. Näistä laitteista on tiedettävä niiden IP-osoitteet, laitetyyppi ja malli, jotta Stealthwatch pystyy näkemään datan kaikista verkon laitteista. Stealthwatch laitteille täytyy olla myös varattuna IP-osoitteet, jotka ovat kaikki samassa aliverkossa.

Jotta Stealthwatch pystyy tuottamaan merkityksellistä dataa, on tietyt isäntäpalvelimet (hostit) määritettävä omiin ryhmiinsä Stealthwatchin sisällä. Seuraavat laitteet tarvitsevat olla tunnistettavissa IP-osoitteilla, jotta ne voidaan lisätä host ryhmiin Stealthwatchin sisällä:

- DNS -palvelimet
- Proxyjen osoitteet
- NAT yhdyskäytävä
- sähköpostipalvelimet, jotka sisältävät sähköposti ja SMTP liikenteen
- toimialueen ohjauskoneet
- tietoverkon Skannerit, jotka seuraavat verkon tilaa, tai heikkouksia
- suojattujen omaisuuksien seuranta, palvelimet, jotka sisältävät arkaluontoisen materiaalin

Kun Service Management console -palvelimelle on määritelty resurssit virtuaalipalvelimelta, voidaan palvelin asentaa. Asennuksen jälkeen ensimmäisenä määritetään palvelimelle IP-osoite, verkkomaski, sekä oletus yhdyskäytävä. Osoitteiden määrityksien jälkeen palvelin käynnistyy uudelleen, jonka jälkeen on syytä määrittää ennalta-asennetut salasanat uudelleen.

Selainpohjaiseen hallintapaneeliin pääsee osoitteella https:// ja palvelimen määritetty IP-osoite. Selainsovelluksen kautta tarvitsee viimeistellä vielä seuraavat asetukset: Host name, network domain, DNS-asetukset, NTP-palvelimen osoite, jonka jälkeen palvelin käynnistetään uudelleen.

Palvelin on nyt asennettu valmiiksi ja seuraavalla kirjautumisella viimeistellään suunnitteluvaiheessa kerätyt tiedot palvelimista ja osoitteista.

4.4 Keskeisiä kysymyksiä käyttöönoton jälkeen

Käyttöönoton jälkeen on käytävä läpi eri hälytyksiä aiheuttavat tekijät ja suorittaa näiden määrittely. Erilaiset uhat ja varoitukset vaativat jokainen omanlaisensa konfiguraation ja niiden määrittely vaihtelee yrityksittäin. Jokaiseen määriteltävään tilanteeseen on ehdotetut reunaehdot, joita voi muokata omaan käyttöön sopivaksi.

Stealthwatch käyttää pisteytysjärjestelmää, jolla voidaan konfiguroida rajat eri ilmoituksille ja hälytyksille. Kaikki verkossa tapahtuvat asiat pisteytetään ja näitä voidaan mukauttaa SMC:n kautta. Itseoppivan järjestelmän ansiosta rajat voivat joustaa käyttäjäkohtaisesti opitun käyttäytymisen perusteella. Kaikille pisteytettäville kategorioille on asetettu valmiiksi pisteytykset Ciscon toimesta etukäteen, joita voidaan muokata käyttötarpeen mukaan tarvittaessa. Osa hälytyksiä aiheuttavista kategorioista, kuten data hoarding, on dynaaminen ja muokkautuu käyttäjäkohtaisesti.

Concern Index seuraa lähteen käyttäytymistä verkossa. Concern index seuraa kaikkea dataa, joka liikkuu lähteestä kohteeseen ja tekee ilmoituksen, jos käyttäjä ylittää ennalta määritetyn pisteytyksen.

Target Index toimii samalla periaatteella ja samoilla kategorioilla, kuin Concern Index, mutta seuraa dataa, joka liikkuu kohteesta lähteeseen. Esimerkkinä, jos uhkaava taho skannaa avonaisia portteja verkosta, niin tästä tulee ilmoitus.

Recon seuraa luvatonta ja potentiaalisesti vaarallista UDP, sekä TCP porttien skannausta. Nämä saattavat olla alustavia merkkejä hyökkäyksestä yrityksen verkkoon ja ne voi tulla niin sisä-, kuin ulkoverkosta.

Command & Control ilmoittaa jo saastuneista laitteista ja palvelimista, jotka ottavat kontaktia hakkerin määräämään osoitteeseen. C&C hyökkäykset ovat kriittisyydeltään suurimmat, koska ilmoituksen tullessa on murtautuja päässyt jo järjestelmään.

Exploitation seuraa suoria tietomurtoyrityksiä, kuten raakahyökkäyksiä tai madon leviämistä sisäverkossa. Pisteytykset näille ovat ennalta määritettyjä ja niitä voi muokata oman yrityksen tarpeen mukaan.

DdoS Source seuraa sisäverkon laitteita ja tunnistaa onko sisäverkossa laite, josta lähtee DdoS hyökkäys. Osa hälytyskategorioista on pisteytetty ja osa toimii vain muuttujina ja ilmoittaa heti, jos rike on tapahtunut.

DdoS Target sama kuin DdoS Source, mutta seuraa laitteita, jotka kohdistuvat DdoS hyökkäykselle.

Data Hoarding seuraa**,** jos lähde, tai käyttäjä on ladannut suuren määrän dataa yhdestä, tai useammasta sisäverkon laitteesta. Stealthwatch seuraa liikennettä ja ilmoittaa poikkeamista. Itseoppivan järjestelmän ansiosta, Stealthwatch oppii tunnistamaan eron normaalin käyttäjän ja esimerkiksi järjestelmävalvojan välillä, koska näiden välillä liikkuvan datan määrän ero voi olla huomattava.

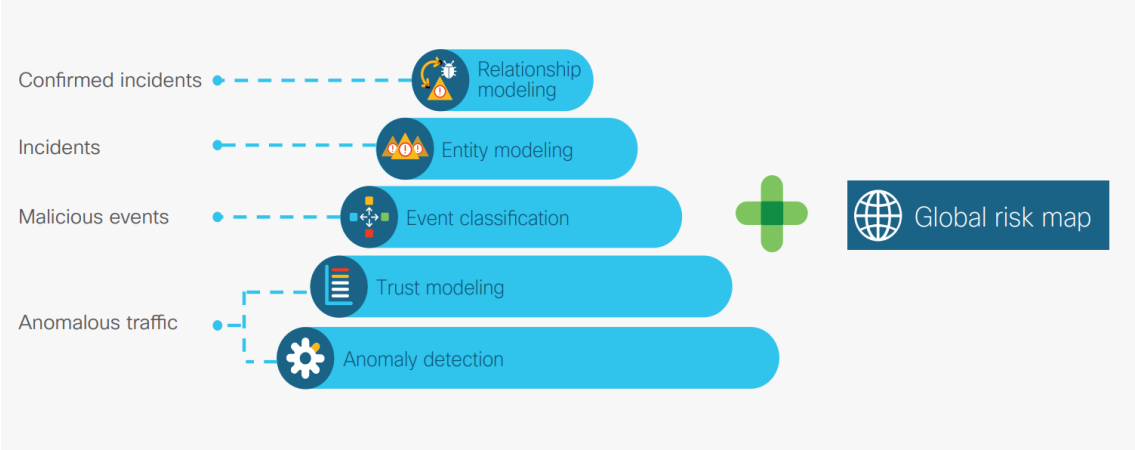
Exfiltration seuraa sisä- ja ulkoverkon laitteita, joilla on poikkeavan suuri määrä dataliikennettä. Jos käyttäjä(host) ylittää ennalta määritetyn datasiirtorajan, niin Stealthwatch aiheuttaa hälytyksen.

Policy Violation valvoo verkon ennalta määritettyjen policyjen noudattamista. Kaikki hälytykset eivät välttämättä ole toimenpiteiden tarpeessa. Järjestelmänvalvojan täytyy tarkistaa ja päättää onko hälytys aiheellinen, vai aiheeton

Anomaly tutkii tapahtumia, jotka poikkeavat normaalista, mutta eivät täytä muiden hälytyksien kriteereitä.

4.5 Itseoppiva tekoäly

Stealthwatchin toiminta perustuu konfiguraatioiden lisäksi monikerroksiseen koneoppimiseen. Kerrokset voidaan jakaa kolmeen erilaiseen osaan. (Kuva 6)



Kuva 6. Koneoppivan tekoälyn rakenne [16].

Ensimmäinen osa koostuu poikkeuksien havaitsemisesta (Anomaly Detection), sekä käyttäjäluottamuksen mallintamisesta (Trust Modeling). Stealthwatch kerää statistiikkaa käyttäjien poikkeuksellisesta käyttäytymisestä ja osaa oppia erottamaan niitä käyttäjien laitteiden IP-osoitteen perusteella. Kaikki poikkeama ei aina ole vaarallista, esimerkiksi järjestelmävalvojalla voi olla enemmän liikennettä kuin normaalilla käyttäjällä. Alimmalla portaalla poikkeumat käydään läpi statistiikkaan perustuvalla koneoppimisella, joka erottaa poikkeumat normaalista käyttäytymisestä. Stealthwatch hyödyntää yli 70 eri ilmaisinta, joista jokainen käyttää erilaista statistiikkaan perustuvaa algoritmia ja luovat pisteytyksen poikkeamille. Näiden ilmaisimien pisteytykset yhdistetään, jonka perusteella osataan erottaa normaali liikenne haitallisesta [16].

Käyttäjäluottamuksen mallintamisessa samantyyliset pyynnöt ryhmitetään yhteen ja näiden poikkeumien pisteytykset on yhdistetty pitkän aikavälin keskiarvoksi. Tällä voidaan luoda käyttäjille eriarvoiset pisteytykset, joiden mukaan Stealthwatch osaa antaa hälytyksen käyttäjäkohtaisesti.

Toisessa osassa kaikki ensimmäisen tason poikkeamat luokitellaan omiin kategorioihin (Event Classification), joita luodaan erilaisin perustein, kuten jokaisen käyttäjän yksilölliseen käyttäytymiseen, laitteiden ryhmäsuhteisiin, tai käyttäytymiseen maailmanlaajuisella, sekä paikallisella tasolla. Kategoriat voivat havaita esimerkiksi C&C liikennettä, luvattomia ohjelmapäivityksiä, tai lisäosia

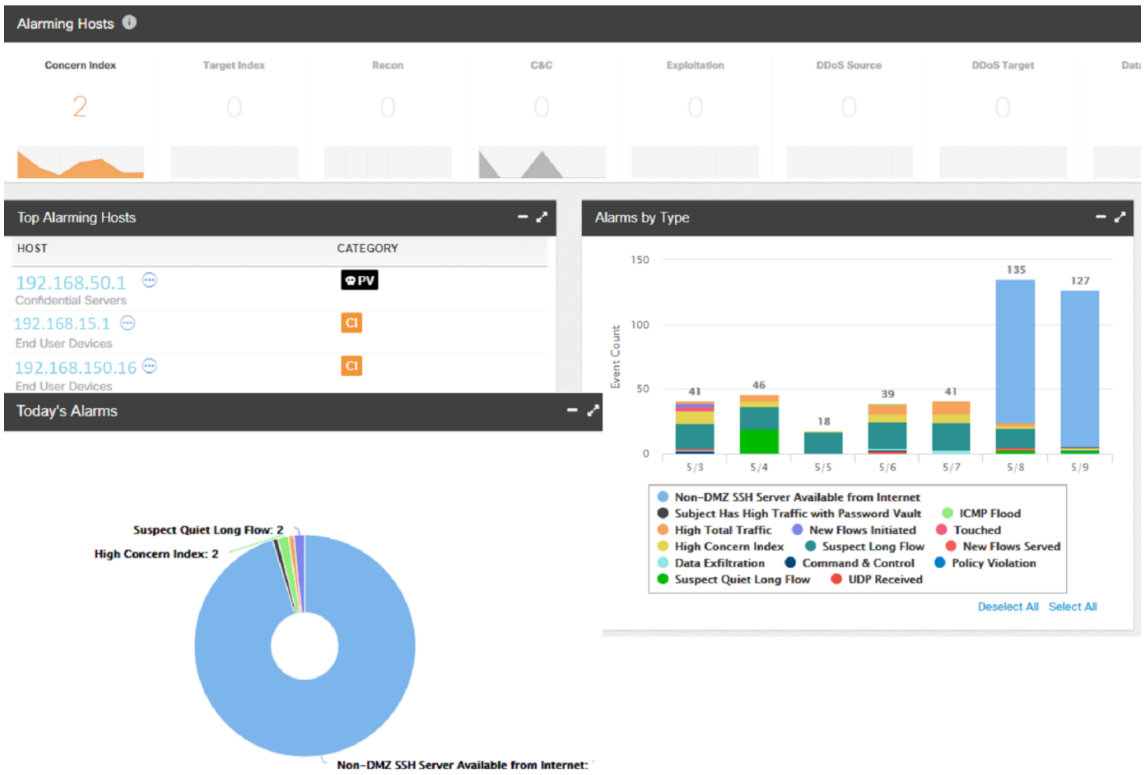
Kokonaisuuden mallintaminen (entity modeling) huomaa, jos haittaohjelmaa tukevan todisteiden määrä ylittää hälytyskynnyksen. Kaikki tapahtumat mitkä verkossa ovat vaikuttaneet uhan luomiseen liitetään yhteen ja niistä tulee uusi erillinen pitkän aikavälin seurantakategoria, jonka varalta Stealthwatch tutkii liikennettä. Taso on dynaaminen ja sopeutua luokittelemaan osia turvalliseksi, jos näistä ei ole tullut enää uusia hälytyksiä.

Kolmas osa keskittyy olemassa olevien suhteiden mallintamiseen (Relationship modeling). Yrityksen aikaisempien kerroksien havaintoja verrataan maailmanlaajuiseen tietokantaan, josta nähdään, onko hyökkäys tapahtunut vain kyseiseen yritykseen, vai onko kyseessä maailmanlaajuinen hyökkäys. Kaikki havaitut tapahtumat joko vahvistetaan tai havaitaan. Vahvistetut tapahtumat ovat niitä, jotka ovat maailmanlaajuisesti tunnettuja ja havaitut tapahtumat ovat yksilöityjä uusia tapahtumia, joita on havaittu vain kyseisessä verkossa. Vahvistettuihin tapahtumiin pystytään tekemään tarvittavat toimenpiteet nopeasti ennakkotapauksien tietojen perusteella, kun taas havaitut tapahtumat tarvitsee ratkaista yhteistyössä tietoturva-asiantuntijoiden kanssa [16].

Maailmanlaajuinen riskikartta (Global riskmap) on tulos kaikista koneiden oppimista algoritmeista. Se tarjoaa laajat käyttäytymistilastot internet-palvelimista. Nämä palvelimet liitetään usein hyökkäyksiin, niitä on pystytty käyttämään hyväksi, tai niitä voidaan käyttää osana hyökkäystä tulevaisuudessa [16].

5 ESIMERKKITAPAUS KÄYTTÖÖNOTON JÄLKEEN

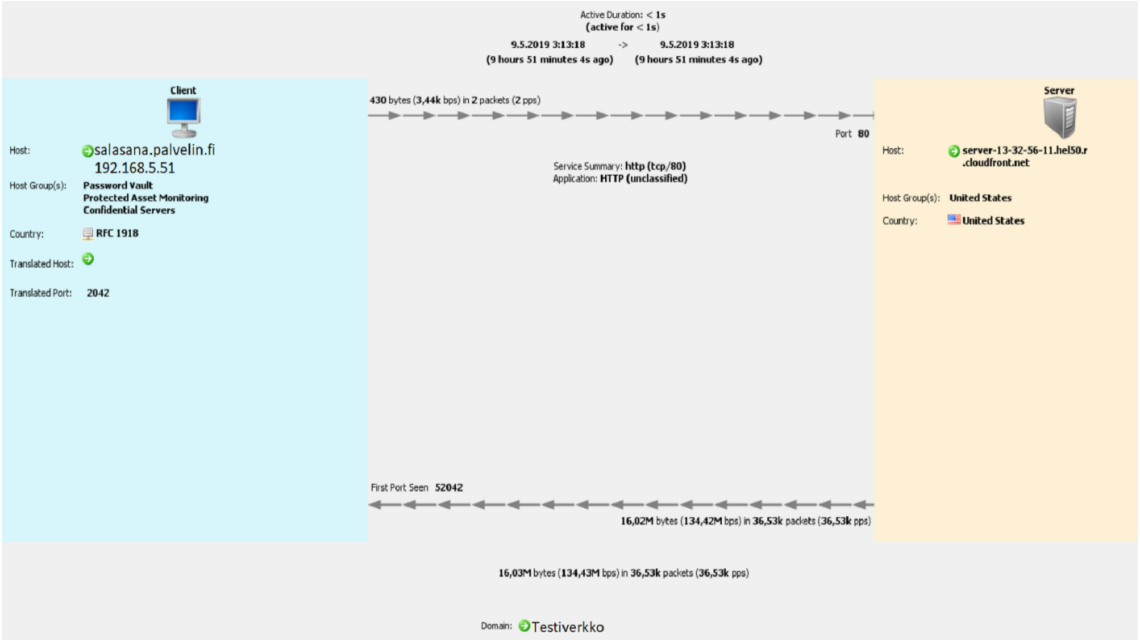
Avatessa selainkäyttöliittymän aukeaa etusivulle näkymä (Kuva 7), josta näkyvät kaikki aiheutuneet hälytykset ja aktiviteetit, jotka ovat herättäneet epäilyksen mahdollisesta haitallisesta käyttäytymisestä.



Kuva 7. SMC Etusivu.

Esimerkkinä kuvasta näkyy 2 Concern Index -hälytystä ja 1 policy violationia. Tarkastellessa Policy Violation hälytystä, voidaan huomata, että kyseisellä IP-osoitteella on Policyn mukaan enemmän liikkunutta dataa, kun on sallittu. Tarkasteluvaiheessa täytyy todeta, että onko hälytys aiheeton ja tarvitseeko hälytyksen aiheuttanutta sääntöä muokata, vai onko kyseessä oikea uhka. Testin aikana säännön maksimidata määrä on asetettu 5MB, joka tässä tapauksessa on vähän ja hälytys on aiheeton.

Työpöytäversiolla hälytyksestä saadaan tarkempaa tietoa avaamalla kyseisen hälytyksen kohdalta Flow Table ja avaamalla tallennetut tiedot. Kuvasta 8 näkyvällä informaatiolla voidaan todeta hälytys aiheettomaksi, kyseessä on päivityksen ajaminen palvelimelle.

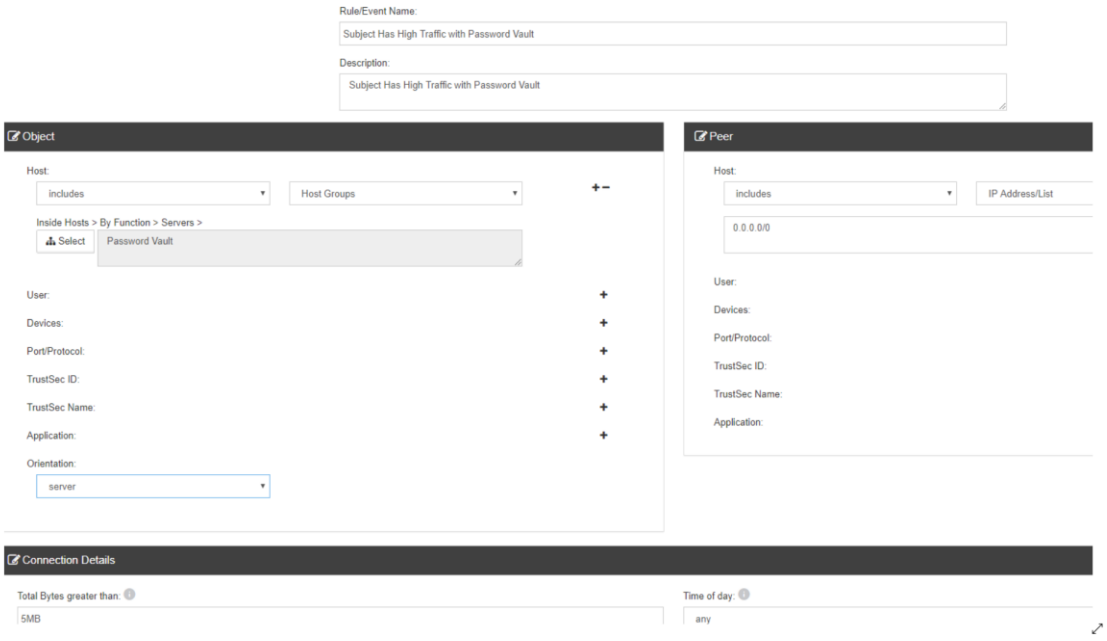


Kuva 8. Tiedot concern indexin aiheuttaneesta hälytyksestä.

5.1 Hälytyksen muokkaus

Jos hälytys todetaan aiheettomaksi ja hälytyksen aiheuttamia reunaehtoja on syytä muokata, voidaan palata takaisin selainpohjaiseen sovellukseen. Ylhäältä löytyvän configure-välilehden alta valitaan Custom Security Events. Kyseisen hälytyksen on aiheuttanut sääntö ”Subject has high traffic with password vault”, joten klikkaamalla kyseistä sääntöä aukeaa konfigurointi-ikkuna.

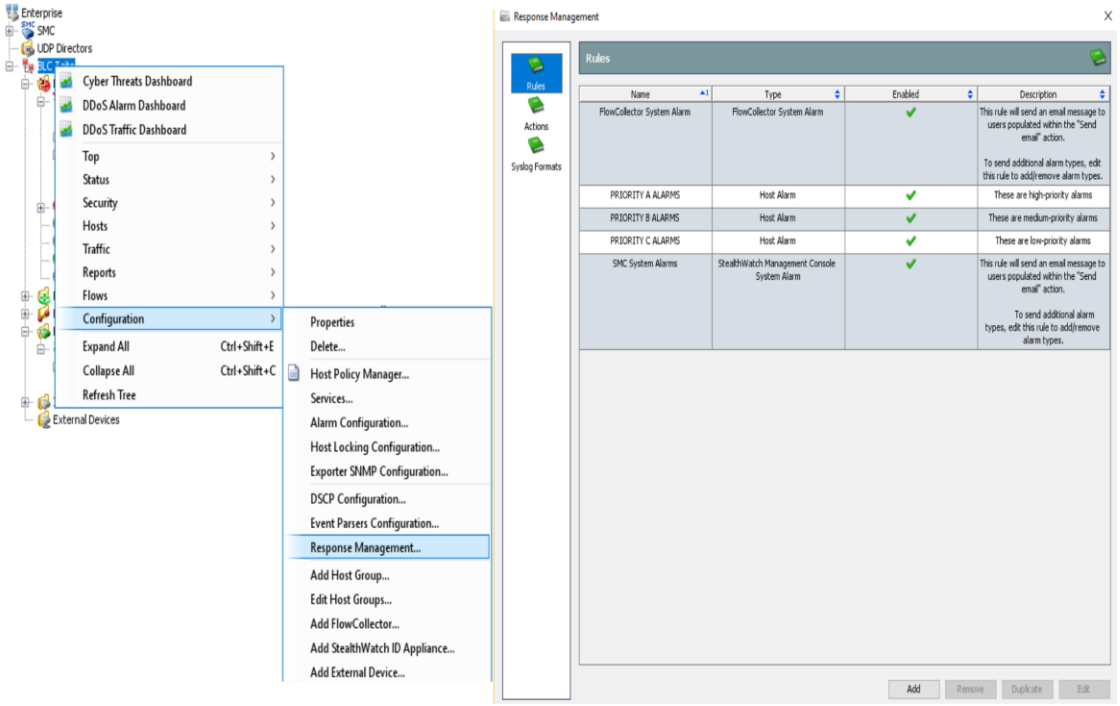
Alla olevasta kuvasta voidaan huomata seuraavat voimassa olevat säännöt. Vasemmalla määritellään hälytyksen piiriin kuuluvat osoitteet, tässä tapauksessa kyseessä on ennalta määritetty salasanapalvelin. Hälytys aiheutuu, kun palvelimelta ladataan dataa 5 MB:n verran. Oikealta puolelta määritellään osoitteet, jotka otetaan tarkasteluun, kun niistä yhdistetään palvelimelle. Tässä tapauksessa seurannassa ovat kaikki osoitteet, jotka yhdistävät palvelimelle. Yhdistäville osoitteille voidaan myös määritellä tarvittaessa maksimiaika, yksittäisen ladatun paketin maksimikoko, sekä kellonaika, joiden ylittyessä tulee ilmoitus.



Kuva 9. Esimerkki räätälöityjen hälytyksien luonnista.

5.2 Aiheellisista hälytyksistä tiedottaminen

Kun sääntö on saatu muokattua tarpeiden mukaiseksi, tarvitsee vielä määritellä, kuinka aiheelliset hälytykset saadaan tietoturvasta vastuussa olevien henkilöiden tietoisuuteen mahdollisimman nopeasti. Näiden määritys onnistuu helposti Hallintakonsolin työpöytäversiosta. Kuvan 10 osoittamalla tavalla, valitaan management consolesta ylläpidettävä yritysverkko ja avataan configuration välilehden alta Response Management.



Kuva 10. Hälytyksien prioriteettimääritykset.

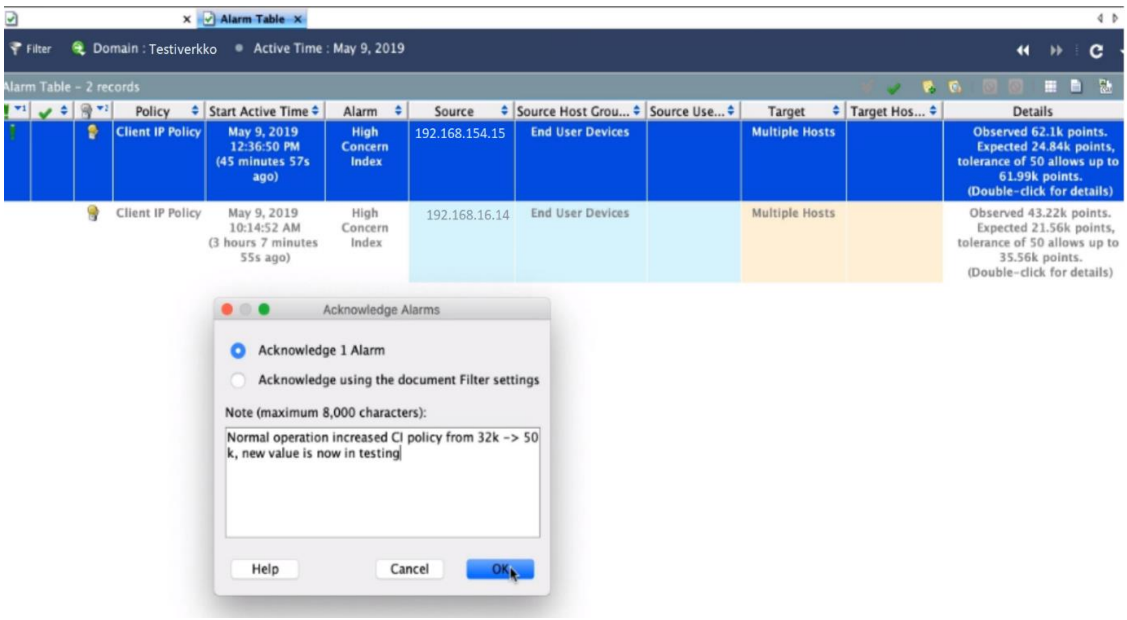
Esimerkkitapauksessa priority C ja B tyypin ilmoitukset ovat alhaisen ja keskitason prioriteettien hälytykset, joihin ei tarvitse reagoida nopealla vasteajalla. Niistä luodaan syslog viestit, jotka tietoturvavastaavat käyvät läpi. Priority A tyypin ilmoitukset ovat kriittisiä tietoturva uhkia, joista lähtee heti sähköpostiviesti ennalta määritettyihin sähköpostiosoitteisiin. Jos yrityksellä on käytössä tikettijärjestelmä, voidaan viesti lähettää tietoturvasta vastaavien lisäksi myös suoraan tikettijärjestelmään, josta asiantuntijat voivat reagoida ilmoitukseen esimerkiksi soittamalla vastaavalle henkilölle.

5.3 Jatkotoimenpiteet

Konfiguraatioiden jälkeen tietoturva-asiantuntijoille jää päivittäiset tehtävät, kuten lokitiedostojen läpikäynti ja hälytyksiin reagointi ja niiden kuittaus.

Stealthwatchin oma AI oppii tuntemaan IP-osoitteiden käyttäytymisen ja osaa asettaa automaattiset toleranssirajat, jolloin ilmoitus lähtee eteenpäin. Asiat, jotka aiheuttavat hälytyksen, kuten liiallinen datan liikkuvuus tietyn palvelimen sisällä pystytään jaottelemaan automaattisesti normaalin käyttäytymisen piiriin, jos kyseessä on järjestelmävalvoja, jolloin turhat ilmoitukset tietoturvauhista minimoidaan ja työmäärää vähennetään.

Kuvasta 11 voidaan nähdä esimerkkihälytys, josta selviää käyttäjän IP-osoite, policyyn määritetyn datan liikkuvuuden yläraja, havaittu liiallinen datan liikkuvuuden määrä sekä toleranssiraja, johon asti datan liikkumisen yläraja on määritetty IP-osoite kohtaisesti.

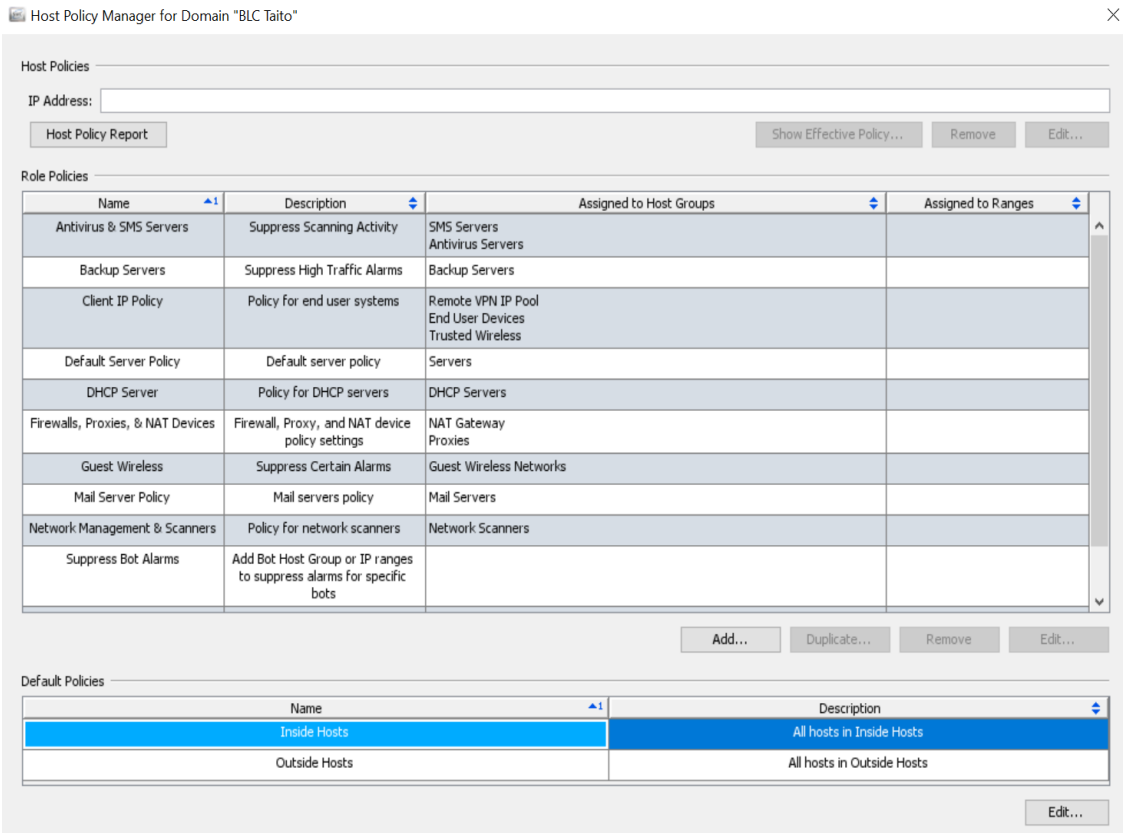


Kuva 11. Hälytykseen reagointi.

Kuvassa huomioidaan esimerkkitapauksen hälytys ja kirjataan järjestelmään toimenpide.

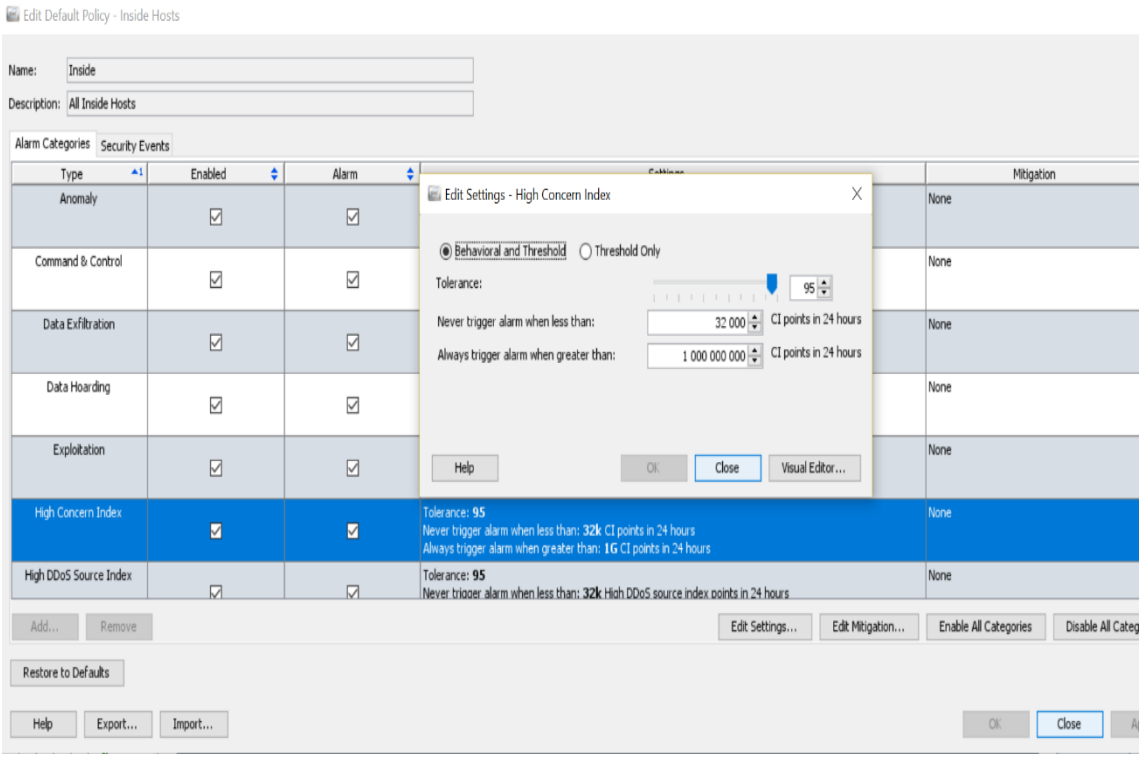
5.4 Indeksien muokkaaminen käyttötarkoituksiin sopiviksi

Turvallisuusilmoituksien rajojen muokkaus tapahtuu Management Consolen työpöytä versiosta. Konsolista valitaan ensimmäisenä configuration-välilehti ja sen alta host policy manager, jonka jälkeen aukeaa kuvan mukainen hallintaikkuna. Ruudun keskeltä löytyy policyt, joita voidaan halutessaan itse luoda ja määrittää ja näitä voi liittää haluttuihin verkon osa-alueisiin, tai laitteisiin. Kuvan 12 osoittamat Role Policyt ovat Stealthwatchin ennaltaluotuja ja niistä voidaan huomata, ettei ne ole käytössä puuttuven IP-osoite rajojen takia.



Kuva 12. Indeksien muokkaus policy managerilla.

Valikon alareunalta (Kuva 13) valitaan default policies otsikon alta inside hosts aktiiviseksi, jonka jälkeen voidaan editoida kaikkien sisäverkon laitteiden hälytyskriteereitä.

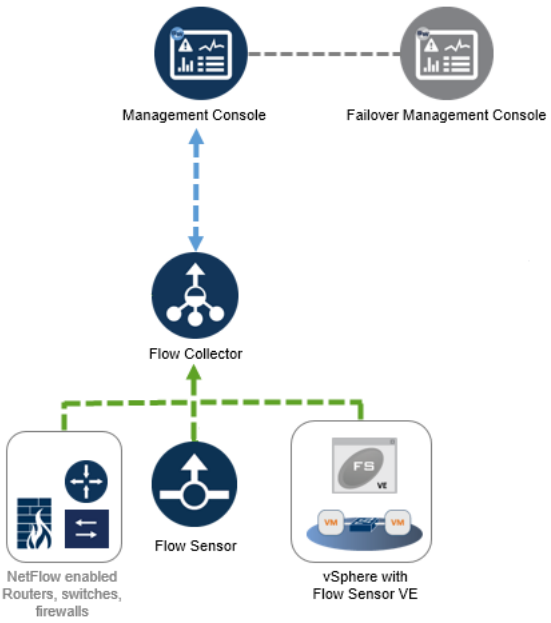


Kuva 13. Raja-arvojen muokkaus.

Listasta löytyy kaikki Stealthwatchin tarkastelemat osa-alueet ja jokaista voidaan muokata omien tarpeiden mukaan. Esimerkkitapauksessa valitaan High Concern Index, jonka jälkeen ruudulle tulee kuvan mukainen ikkuna, josta voidaan muokata kriteereitä, joka laukaisee hälytyksen. Jos valittuna on Behavioral and Threshhold, niin Stealthwatchin itseoppiva järjestelmä osaa määrittää laite- ja IP-osoite kohtaisia poikkeuksia, jotka saavat ylittää rajat ilman hälytystä. Jos taas valitaan pelkkä threshold, niin ilmoitus tulee heti, jos mikään laite menee yli annetun rajan.

6 FLOW COLLECTOR

Flow Collectorin pääasiallinen tehtävä on kerätä kaikki data NetFlowsta ja lähettää se eteenpäin management consoleen, jossa NetFlown tiedot puretaan helposti ymmärrettävään muotoon. Kuvassa 14 havainnoidaan toimintaperiaate, jonka mukaan Flow Collector toimii.

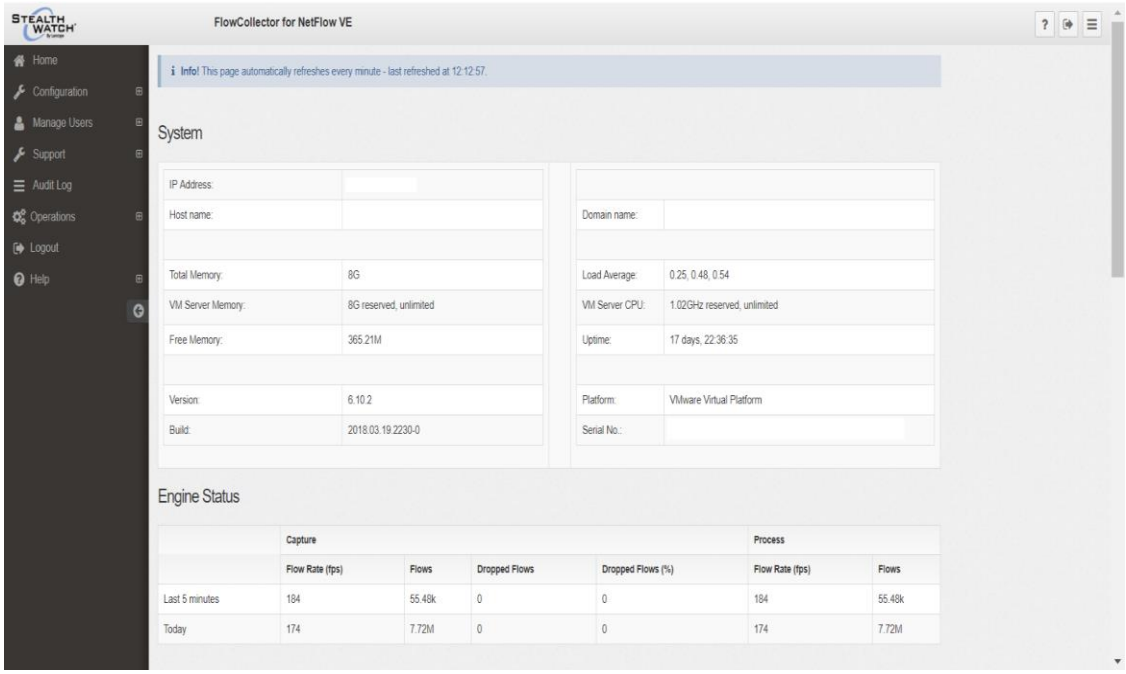


Kuva 14. Cisco Flow collectorin toimintakaavio.

Flow Collector kerää kaiken datan kytkimistä, reitittimistä ja palomuureista, joissa NetFlow on otettu käyttöön. NetFlow ei kerää tiettyjä toiminnallisuuteen liittyviä statistiikkoja, kuten viivettä ja vasteaikaa. Tarvittaessa em. tietoja verkosta, voidaan ottaa käyttöön Flow Sensor, joka lisää tiedot NetFlowiin Internet Protocol Flow Information Export (IPFIX) -paketteina. Jos sama tietopaketti kulkee useamman kuin yhden reitittimen kautta tehdään paketeista yksi yhtenäinen kokonaisuus ja näin ollen poistetaan ylimääräiset duplikaattipaketit tarkastelusta.

Flow Collectorin hallintasivuilta ei voi itsessään tarkastella verkon tapahtumia, tai tehdä toimenpiteitä mahdollisten tietoturvauhkien sattuessa. Hallintasivuilla voi tarkastella palvelimen ja palveluiden tilat, sekä seurata päivittäisen Flow:n määrän lukuina (fps), sekä Flow:n koon tavuissa.

Hallintasivuilta (Kuva 15) voidaan tarkastella ja tarvittaessa muokata asennusvaiheessa määriteltyjä asetuksia, luoda käyttäjätunnuksia palveluun hallintahenkilöille, sekä tarvittaessa sammuttaa ja uudelleen käynnistää palvelu.



Kuva 15. Flow Collector etusivu.

Audit logista voidaan tarkistaa kaikki Flow Collectorin asetuksiin tehdyt muutokset ja päivitykset, tai nähdä kuka Flow Collectoriin on kirjautunut.

Support -välilehden alta voidaan päivittää sovellus uudempaan versioon, tehdä sovelluksen asetuksista varmistukset tai palautukset sekä nähdä Tietokannan tallennus statistiikat. Statistiikoista nähdään päivissä, kuinka pitkään voidaan tallentaa tietokantaan lokitiedostoja, ennen kuin palvelimen tallennustila on täynnä. Kuvan 16 mukaisella palvelimella tallennustilaa on jäljellä vielä keskimääräisesti laskettuna 2884 päivää. Kapasiteetti lasketaan myös keskiarvon lisäksi pahimman tapauksen mukaan, joka on laskettu korkeimman datasiirtomäärän piikin mukaan.

Database Storage Statistics

Capacity

	Average	Worst Case
Capacity in Days	3242	338
Remaining Days	2884	297
Bytes Per Day	319.9M	498.39M

Flow Data Summary

			Rows			Bytes		
Data	Days	Containers	Total	Average Per Day	Largest Day	Total	Average Per Day	Largest Day
Flow Details	358	389	1.19G	3.32M	6.09M	18.39G	51.38M	100.23M
Flow Interface Details	8	37	81.18M	10.15M	13.14M	2.02G	252.34M	326.61M
Total	358	426	1.27G	13.47M	19.23M	20.41G	303.72M	426.83M

Kuva 16. Flow Collectorin tallennus statistiikkaa.

7 PÄÄTELMÄT

7.1 Opinnäytetyön tavoitteet ja onnistumiset

Opinnäytetyön tavoitteena oli luoda toimeksiantajayritykselle dokumentaatio, kuinka Stealthwatchin käyttö voidaan aloittaa, sekä luoda dokumentaatio, josta asiakasyritys saa käsityksen, mitä Stealthwatch tekee ja kuinka sitä voidaan käyttää. Käyttöönoton lisäksi tavoitteena oli luoda käsitys siitä, mitä yrityksien tietoturva pitää sisällään, ja tutustua hieman tarkemmin siihen, mitä erilaisia osa-alueita tarvitsee ottaa huomioon yrityksen tietoturvassa. Onnistuneen tietoturvan kannalta on tärkeää pitää huoli siitä, että jokainen osa-alue on oltava huomioituna. Yksikin aukko tietoturvassa voi vaarantaa yrityksen arkaluontoisten materiaalien vuotamisen väärille henkilöille tai mahdollistaa hyökkäyksen verkkoon ja palvelimiin pysäyttääkseen koko verkon liikenteen.

Opinnäytetyön perusteella voidaan nähdä, mitä eri osa-alueita kuuluu yrityksen kokonaisvaltaiseen tietoturvaan. Itse Stealthwatchin käyttöönotto oli hyvin onnistunut, ja palvelun ollessa oikeassa yritysverkossa käytössä saatettiin nähdä käytännössä Stealthwatchin vaikutus. Palvelua testattaessa suurin haaste oli selvittää kaikista alussa tulleista hälytyksistä, mitkä ovat aiheellisia ja mitkä eivät. Moni täysin turvalliseksi todettu sovellus saattoi aiheuttaa hälytyksen, kun sovellus käynnistettiin koneella. Stealthwatch tarjoaa yrityksen tietoliikenteelle läpinäkyvyyttä, jonka avulla verkkoasiantuntijat voivat havainnoida epätoivotun verkkoliikenteen, ja sen perusteella voivat muokata verkkoliikennemäärityksiä.

Opinnäytetyötä tarkastellen aihepiiri oli kiinnostava ja antaa käsityksen siitä, minkälaista yrityksen tietoturva voi olla. Tietoturvan merkityksen ymmärtäminen ja yrityksen tietojen suojauksen tärkeys on kriittinen osa onnistunutta yrityksen IT:tä.

7.2 Stealthwathin management consolen ja Flow collectorin käyttö

Opinnäytetyössä käytiin läpi esimerkkitapaus, jonka avulla luotiin kuva Stealthwatchin yleisestä käytöstä. Opinnäytetyön käytännön osuudessa käytettiin esimerkkinä vain yhtä tapausta siitä syystä, että raja-arvojen muokkaus on hyvin samankaltaista muidenkin hälytyksiä aiheuttavien uhkien kohdalla ja jokainen tapaus tarvitsee käydä yksilöllisesti läpi.

Stealthwatch on suunniteltu käytettäväksi suurille yrityksille, joissa IT-laitteiden tietoliikennettä on hankalaa seurata. Pk-yrityksetkin hyötyvät palvelusta, mutta helpompi ratkaisu tällaisille yrityksille on turvautua kolmannen osapuolen hallinnoimaan palveluun.

Tulevaisuudessa käyttöönotto osuuden ohjeilla pystyvät uudet käyttäjät saamaan hyvän peruskäsityksen siitä, miten hallintakonsolin työpöytäversiota käytetään. Vaikka hallintakonsolin käytön osaaminen on suuri osa Stealthwatchin kokonaisuutta, on silti loppukäyttäjän hyvä ymmärtää raja-arvojen yksilöllisyyden merkitys. Niitä muokattaessa olisi tärkeää keskustella muokkaamisesta mahdollisien muiden IT-osaston henkilöstön kanssa tai tarvittaessa konsultoida kolmatta osapuolta.

LÄHTEET

[1] Ruohonen, M. Peruskirjat. Tietoturva. Jyväskylä: Docendo, 2002.

[2] Karvi, T. Tietoturvan perusteet, 2017. https://www.cs.helsinki.fi/u/karvi/perusteet-luku1-bea_12.pdf. Viitattu 29.3.2019

[3] Rousku, K. Ohje riskienhallintaan. Helsinki: Valtiovarainministeriö, 2017. http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf. Viitattu 5.9.2019

[4] Hakala, M. & Wuorinen, O. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo, 2006. Viitattu 10.9.2019

[5] What is pdca cycle, 2019 https://kanbanize.com/wp-content/uploads/website-images/kanban-resources/pdca.png. Viitattu 5.9.2019

[6] Opetushallitus. Tietoturvan peruskäsitteitä, 2010. Luettavissa: http://www.oph.fi/opetustoimen_turvallisuusopas/turvallisuuden_osa-alueita/tietoturva/tietoturvan_peruskasitteita. Viitattu: 29.5.2019.

[7] F-Secure: Protection service for business. Esite https://www.f-secure.com/documents/10192/2179617/fsecure-protection-services-for-business-technical-brochure-en.pdf Viitattu 7.10.2019

[8] F-secure Radar. Esite, 2019 https://www.f-secure.com/fi/business/products/vulnerability-management/radar Viitattu 7.10.2019

[9] Palo Alto: Reducing business risks of cyberthreats. White paper, 2017 https://www.paloaltonetworks.com/resources/whitepapers/reducing-business-risks-cyberthreats Viitattu 15.9.2019

[10] Proofpoint: Stopping Email Fraud. White paper, 2018 https://www.infosecurity-magazine.com/white-papers/stopping-email-fraud/ Viitattu 18.9.2019

[11] Stealthwatch Management Console. User's guide for Stealthwatch https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/smc_users_guide/SW_6_9_0_SMC_Users_Guide_DV_1_2.pdf. Viitattu 30.5.2019

[12] Introduction to Cisco IOS NetFlow - A Technical Overview https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html. Viitattu 30.5.2019

[13] Stealthwatch Enterprise. White paper, 2019 https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch/datasheet-c78-739398.html. Viitattu 10.7.2019

[14] Cisco Encrypted Traffic Analytics. White paper, 2019 https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf. Viitattu 10.7.2019

[15] Direktiivi 13.8.2004/759: Finlexin laki yksityisyyden suojasta työelämässä. 15.08.2018 https://www.finlex.fi/fi/laki/ajantasa/2004/20040759 viitattu 20.4.2019

[16] Cisco security analytics. White paper, 2018 https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/white-paper-c11-740605.pdf Viitattu 15.9.2019