Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2019

Tuomas Jauhiainen

PALVELUNA TOIMITETTAVAN SIEM-JÄRJESTELMÄN VALVONTA YRITYSVERKOSSA

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikka

2019 | 25 sivua

Tuomas Jauhiainen

PALVELUNA TOIMITETTAVAN SIEM-JÄRJESTELMÄN VALVONTA YRITYSVERKOSSA

Opinnäytetyön tarkoituksena oli suunnitella ja toteuttaa palveluna toimitettavan SIEM-järjestelmän valvonta käyttöjärjestelmä- ja käyttöliittymätasolla. Työn lähtökohdaksi asetettiin täysin erillisen verkkolaitteiden toiminnan valvontaan erikoistuneen järjestelmän asennus. Ennen työn toteuttamista SIEM-järjestelmä oli täysin omavaraisten hälytysten varassa. Tätä ei yrityksessä koettu riittävän kattavaksi valvonnaksi. Tässä työssä käytettäväksi valvontaohjelmistoksi valittiin OP5 Monitor. Käytettävä tuote valittiin lisensointiin liittyvistä syistä. Tämä työ ei käsittele vertailua muiden markkinoilla olevien tuotteiden kanssa.

Työn toteuttamista varten oli ensin tutustuttava toteutuksessa käytettäviin verkkoprotokolliin sekä asennusympäristön tietoturvavaatimuksiin. Valvonnassa käytettäviksi protokolliksi valittiin SNMP ja HTTPS. Näillä kahdella protokollalla oli mahdollista valvoa sekä järjestelmän alla olevaa Linux-käyttöjärjestelmää, että selaimessa toimivaa käyttöliittymää. Verkkoliikenne palvelimien välillä minimoitiin vain vaadittaviin protokolliin. Tällä tavalla oli mahdollista rajata mahdollisia tietoturvauhkia. Asennusympäristö oli yrityksen oma sisäinen tietoverkko.

Ulkoisen valvontajärjestelmän asennus oli helppo ja nopea toimenpide. Järjestelmä asennettiin valmiin Linux-palvelimen päälle. Lisenssin lisäämisen jälkeen OP5 Monitor oli käytännössä täysin käyttövalmis. SIEM-järjestelmä lisättiin valvottavaksi kohteeksi automaattisen asennusvelhon avulla. SIEM erosi rakenteeltaan normaalista Linux-palvelimesta, joten esimerkiksi muutamia levyosioita oli lisättävä jälkikäteen valvottaviksi kohteiksi. Käyttöliittymän valvonta oli myös määriteltävä erikseen. Valvonnassa käytettyjen lisäosien asetuksia muokattiin SIEM-järjestelmän valvontaan sopiviksi. Hälytysrajoja nostettiin normaalia korkeammaksi, jotta vääriä hälytyksiä ei olisi tullut käsiteltäväksi.

Työ saatiin valmiiksi ja tavoiteltu valvonnan taso saavutettiin. Työn tuloksista saatiin myös paljon ideoita valvonnan jatkokehittämiselle. Alkuperäinen valmistajan tarjoama dokumentaatio oli huonoa. Työn ohessa kirjoitettu ohjeistus mallikuvineen loi hyvät edellytykset valvonnan käyttöönottoon muissakin ympäristöissä.

ASIASANAT:

käyttöliittymä, Linux, protokolla, SNMP

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information and Communications Technology

2019 | 25 pages

Tuomas Jauhiainen

MONITORING A SIEM SYSTEM IN A CORPORAL NETWORK

The goal of this thesis was to design and implement a simple network monitoring system and procedure. Targeted host for monitoring was a SIEM system which was delivered as a service to customers. Both the web-based interface and the underlying Linux operating system were monitored. Before this thesis started, the company did not have any kind of external monitoring. All monitoring was done on the SIEM system itself. This was not seen as sufficient solution. The chosen network monitoring system was OP5 Monitor. It was chosen due to licensing reasons. This thesis does not include any comparison between other systems or providers in the market today.

Before installing the system, there was a need to research the protocols used in monitoring. The basic guidelines for secure network infrastructure were also studied. The chosen protocols for monitoring were SNMP and HTTPS. These protocols enabled the monitoring for the underlying Linux system and for the user interface. Network traffic between these servers was limited to absolute minimum. This was to ensure a more secure network. The implementation environment was one of many internal networks in this company.

The installation of the external monitoring system was simple and fast procedure. The system was installed on top of Linux server that was prepared in advance. After a license was applied, the OP5 Monitor was basically ready to be used. The SIEM was added as monitored host using the automated host installation wizard. The SIEM was a bit different than a normal Linux system so there were some monitored services to add afterwards. Those were for example various disk partitions. The monitoring of user interface also had to be added separately. The plugins used in this thesis were modified to better suit the SIEM system. The limits for alerts were tuned a bit higher in order to prevent unnecessary alarms.

Thesis was finished and the objective was achieved. The results also gave many ideas for further development. The original documentation provided by the OP5 was quite limited and poor. The documentation written during the thesis made the implementation of monitoring easier in other environments.

KEYWORDS:

interface, Linux, protocol, SNMP

SISÄLTÖ

KUVAT

KÄYTETYT LYHENTEET

BASH	Bourne again shell, Linuxin oletuskomentotulkki
HTTP	Hypertext transfer protocol, tiedonsiirtoprotokolla
HTTPS	Hypertext transfer protocol secure, salausta hyödyntävä tiedonsiirtoprotokolla
ICMP	Internet control message protocol, kontrolliprotokolla
MIB	Management information base, määrittelytiedosto
OID	Object identifier, hallittavien kohteiden tunnistus
RPM	Red Hat package manager, paketinhallintaohjelma ja tiedostomuoto
SIEM	Security information and event management, lokienhallinta ja tapahtumakorrelointi
SNMP	Simple network monitoring protocol, verkonhallintaprotokolla
SSH	Secure shell, salatun liikenteen yhteysprotokolla
TCP	Transmission control protocol, verkkoliikenteen yhteysprotokolla
TLS	Transport layer security, salausprotokolla
URI	Uniform resource identifier, määrittelyyn käytettävä merkkijono
URL	Uniform resource locator, verkkosivujen osoitetunniste
UDP	User datagram protocol, prosessien välinen viestiprotokolla
YUM	Yellow dog updater modified, paketinhallintaohjelma

1 JOHDANTO

Tämän opinnäytetyön aiheena oli suunnitella ja toteuttaa kyberturvapalveluna toimitettavan järjestelmäkokonaisuuden (SIEM) toiminnan valvonta yrityksen omassa sisäverkossa. SIEM on suuri ohjelmisto- ja komponenttikokonaisuus, jolla kerätään tietoa verkkolaitteilta ja verkossa tapahtuvasta tietoliikenteestä. SIEM-järjestelmän toiminnan valvonta oli ennen työn toteuttamista omien ilmoitustensa varassa. Tätä ei koettu riittäväksi tavaksi valvoa tätä järjestelmää. Tavoitteena oli saavuttaa kokoonpano, jonka avulla olisi mahdollista valvoa sekä omaa tuotantoympäristöä että yhdistää sama valvontatuote myös asiakkaiden ulkopuolisiin verkkoympäristöihin. Yrityksen nimi, palveluna toimitettavat tuotteet ja asiakaskunta pidettiin salassa yrityksen antamien ehtojen mukaisesti.

Yrityksen käyttämä SIEM-järjestelmä on varsin kyvykäs huolehtimaan itsestään ja ilmoittamaan poikkeavista järjestelmätapahtumista. On kuitenkin monia erilaisia tapahtumia ja ongelmakohtia, joista järjestelmä ei ilmoita riittävän nopeasti, tai se ei ilmoita niistä ollenkaan. Näiden poikkeustapahtumien varalta ulkoinen valvontajärjestelmä on pakollinen, kun tarkoituksena on toimittaa vuorokauden ympäri käytössä olevaa palvelua. Tässä työssä käytettäväksi valvontajärjestelmäksi valittiin OP5 Monitor. Päällimmäiset syyt valintaan olivat hyvin vastaavanlaiset ominaisuudet kilpailijoiden tuotteisiin verrattaessa, mahdollisuus lähitukeen- ja konsultaatioon, sekä lisensointikulujen edullisuus näihin kilpailijoihin nähden. Tuotetta verrattiin esimerkiksi Pandora FMS -järjestelmään. Tämä opinnäytetyö ei käsittele vertailua muihin vastaaviin tuotteisiin.

Ennen käytännön toteutusta työssäni käsitellään eri verkkoprotokollia, joita OP5 Monitor hyödynsi valvonnassaan. Käytännön toteutuksen ensimmäinen vaihe sisälsi asennusympäristön kartoittamisen ja sen asettamien ehtojen määrittelyn, sekä valvontajärjestelmän asentamisen. Toisessa vaiheessa asennetulle OP5 Monitorille määriteltiin valvontaan vaadittavat perusasetukset. SIEM-järjestelmän alustana toimivan Linux-jakelun valvontamenetelmäksi valikoitui SNMP-protokolla. Työssä on hyödynnetty protokollan viimeisintä julkaisuversiota, joka on SNMPv3. SIEM-järjestelmän käyttöliittymän valvonta sen sijaan toteutettiin tekemällä HTTPS-lisäosalla tarkistuksia suoraan järjestelmän www-pohjaiseen käyttöliittymään.

2 VERKKOPROTOKOLLAT

Tässä luvussa käsitellään opinnäytetyössä käytettyjä SNMP-, HTTP/HTTPS-, SSH-, UDP- ja ICMP-protokollia. Ensiksi tutustutaan lyhyesti HTTP- ja HTTPS-protokolliin. Tämän jälkeen käydään läpi SNMPv3-protokolla ja viimeiseksi ICMP-, UDP- sekä SSH-protokolla.

2.1 HTTP ja HTTPS

Opinnäytetyön näkökulmasta katsottuna käyttöliittymän toiminnan kannalta olennaisia tekijöitä ovat palvelimen vastausaika ja käyttöliittymän luotettavuuden takaaminen. Web-pohjaisen käyttöliittymän toiminta vaatii protokollan, jota selaimet ja palvelimet käyttävät tiedonsiirtoon. Tämä protokolla on joko HTTP- tai HTTPS-protokolla. Opinnäytetyössä käytetty protokolla oli HTTPS, mutta tässä luvussa käsitellään myös HTTP, sillä HTTPS käyttää sitä toimintansa perustana.

2.1.1 HTTP

Hypertext transfer protocol on sovellustason protokolla, jota käytetään tiedon siirtoon internetissä. HTTP toimii pyyntö- ja vastausperiaatteella. Tämä tarkoittaa sitä, että asiakassovellus (esimerkiksi käyttäjän verkkoselain) tekee kohdepalvelimelle pyynnön, joka sisältää uniform resource identifier–merkkijonon ja protokollan versiotiedot. URI on esimerkiksi uniform resource locator-merkkijono (eli URL), jolla tarkoitetaan tässä tapauksessa verkkosivun osoitetta, jonka käyttäjä kirjoittaa verkkoselaimen osoiteriville. Esimerkki tällaisesta osoitteesta on http://www.google.com. Heti tämän perään sovellus lähettää viestin, joka sisältää pyyntömääritelmiä ja asiakassovelluksen tietoja. Kohdepalvelin vastaa asiakassovelluksen pyyntöön lähettämällä tietoja viestiprotokollan versiosta, viestin kyselyn onnistumisesta (tai epäonnistumisesta), sekä myös tarkempia palvelintietoja ja kohdeolion tavoitetietoja. Todellisuudessa tämä sovelluksen ja palvelimen välinen keskustelu on vielä monimutkaisempaa, mutta tämän opinnäytetyön kannalta sen käsitteleminen ei ole tarpeellista. (Berners-Lee ym. 1999, 12.)

2.1.2 HTTPS

Toimintaperiaatteeltaan Hypertext transfer protocol secured on hyvin samanlainen kuin aiemmin esitelty HTTP. Näiden erottava tekijä on protokollan verkkoliikenteen salaus. HTTPS käyttää porttia 443 liikenteen vastaanottamiseen, kun taas HTTP käyttää porttia 80. Porttien numerointi ja valinta perustuu muistettavuuteen ja vakiointiin, eikä niinkään portin varsinaiseen kyvykkyyteen. HTTPS käyttää TLS-salausmenetelmää verkkoliikenteen salauksen ja luotettavuuden varmistamiseen. Asiakassovellus ja kohdepalvelin käyttävät yhteisiä salausavaimia, joiden oikeellisuus todennetaan ennen yhteyden lopullista luomista. HTTPS-protokollan URL-merkkijono on tunnistettavissa HTTP:n perään lisätystä s-kirjaimesta. Merkkijono voi olla esimerkiksi https://www.google.com. (Rescorla 2000, 2–4.)

TLS on itsenäinen protokolla suhteessa sovellustason protokolliin. Se ei itsessään määritä kuinka sitä hyödynnetään salauksen saavuttamiseksi. Yksi tavallisimmista tavoista käyttää TLS-protokollaa on tiedonsiirto HTTPS-protokollalla. Tässä työssä asiakassovellus on verkkoselain. Tämä tarkoittaa sitä, että salauksen saavuttamiseksi on käytettävä symmetristä salausta. Symmetrinen salaus toteutetaan PKI-menetelmällä. Tässä menetelmässä on kaksi avainta, joista toinen on julkinen avain ja toinen salainen avain. Jos verkkoliikenteessä käytettävä viesti salataan julkisella avaimella, on se avattava salaisella avaimella. Tämän voi toteuttaa myös toisinpäin. Tämän opinnäytetyön tapauksessa palvelimelle on asennettu salainen avain ja allekirjoitettu TLS-varmenne. Selain muodostaa istunnon ajaksi symmetrisen avaimen, jonka se lähettää palvelimelle. Istunnon viesti salataan palvelimen julkisella avaimella. Tämän viestin voi purkaa ainoastaan palvelimen salaisella avaimella. Tällä tapaa saavutetaan yhteys, jossa vain näillä kahdella osapuolella on näkyvyys keskustelun sisältöön. (Rescorla 2018,10–13; Wesentra Oy 2019.)

2.2 SNMP

Simple network management protocol on jo pitkään käytetty verkonhallintaprotokolla. Tässä työssä sitä hyödynnettiin kohdepalvelimen Linux-käyttöjärjestelmän valvontaan. Protokollan versioksi valittiin SNMPv3 sen salausominaisuuksien takia. SNMP koostuu kahdesta eri komponentista: hallinta- ja agenttikomponentista. Tässä opinnäytetyössä käytetyssä tavassa hallintakomponentti tekee aktiivisia kyselyitä agenttikomponentilta,

joka on asennettu ja konfiguroitu kohdepalvelimelle. Agenttikomponentti kerää isäntäpalvelimen tietoja ja kääntää niitä yhteensopivaksi SNMP-formaatiksi MIB-määritelmien mukaisesti. (Froom ym. 2015, 337–339.)

2.2.1 SNMPV3 ja sen toiminta

SNMPv3 eroaa aikaisemmista versioista sillä, että siihen on lisätty tietoturvaominaisuuksia kuten käyttäjätili, tunnistautuminen ja tietopakettien sisältämän tiedon salaus. Tämä tuo toki mukanaan ongelmakohtia, kuten asetusten monimutkaisuuden ja protokollan aiheuttaman raskaamman kuorman. Muun muassa tietopakettien salaus ja salauksen purkaminen kuormittavat verkkoa ja palvelinlaitteistoa hieman enemmän. Tässä työssä käytetty turvallisuustaso on nimeltään AuthPriv. Se tulee sanoista Authentication and Privacy. Käytännössä tämä tarkoittaa sitä, että viestin lähettäjä on tunnistettava ja viesti on salattava. Tunnistamalla oikea käyttäjä, voidaan estää mahdollisen ulkopuolisen käyttäjän (hakkerin) toimittamat Get- tai Set-komennot. Näillä komennoilla voidaan joko hakea tietoa (Get) kohdelaitteelta tai suorittaa käskyjä (Set) kohdelaitteella. Salaus mahdollistaa sen, ettei tämä ulkopuolinen tekijä voi lukea verkossa välitettyä viestiä. (Paessler 2019.)

2.2.2 MIB ja OID

Object identifier on tunnistearvo, jonka avulla erotellaan hallittavia tai kyseltäviä kohteita halutulla laitteella. Nämä kohteet on erikseen määritelty management information base-tiedostoissa, joka käytännössä sisältää laitteen kaikki tarvittavat OID-tiedot. Esimerkkinä OID:sta toimii hyvin tässäkin työssä käytetty palvelimen suorittimen kuorma yhden minuutin aikana, joka on OID:na ilmaistuna muodossa 1.3.6.1.4.1.2021.10.1.3.1. Tästä numerosarjasta alkuosa 1.3.6.1.4 on standardin mukainen ja ilmenee jokaisessa OID-numerossa. Sarjan loppuosa on yleensä valmistajan määrittämä. Näitä OID-tunnisteita käytetään kyselyissä, jotta oikea tieto saadaan noudettua kohdelaitteelta. (Paessler 2019.)

2.3 ICMP

Internet control message protocol on protokolla, joka teoriassa toimii Internet protokollan päällä, mutta käytännössä se on integroitu osa sen toimintaa. IP-protokollan tehtävänä on välittää datapaketteja tietoverkon eri kohteiden välillä. Se osioi paketit, reitittää liikenteen IP-osoitteen perusteella, sekä määrittelee muun muassa pakettien koon ja muut mahdolliset käytettävät argumentit tiedonsiirron yhteydessä. ICMP-viestejä siirtyy laitteelta laitteelle esimerkiksi silloin, kun kohdelaite ei ole saavutettavissa verkossa. ICMP ei itsessään ole täysin luotettava, mutta sen tavanomainen tarkoitus on tuottaa mahdollisesti hyödyllistä tietoa verkossa olevien laitteiden vikatiloista. Tavanomaisin käyttötapa ICMP-protokollalle on olemassa tässäkin työssä hyödynnetty ping-työkalu, jolla tiedustellaan kohdepalvelimen tavoitettavuutta verkossa. (Postel 1981,1.)

2.4 SSH

SSH eli Secure Shell on protokolla, jota hyödynnetään etäkirjautumiseen halutulle kohdekoneelle. Se tarjoaa tietoturvallisia ominaisuuksia koneiden väliseen kommunikointiin. Se hyödyntää samalla tapaa autentikointia ja salausta kuin esimerkiksi SNMPv3. SSH yhteys muodostetaan päätelaitteelta (esimerkiksi käyttäjän oma työasema) kohdekoneelle. Päälaite avaa yhteyden ja pyytää palvelimen julkista salausavainta varmistaakseen, että palvelin on se kohde, jolle halutaan kirjautua. Tämän jälkeen päätelaite neuvottelee tarvittavat parametrit, kuten esimerkiksi symmetrisen salauksen. Tässä työssä hyödynnettiin julkista avainta ja palvelimelle luotua käyttäjää, jolla on oikeus SSH yhteyteen. (Ylonen 1996, 37–42.)

2.5 UDP

User Datagram Protocol on viestiprotokolla, joka toimii tämän työn tapauksessa kahden eri palvelimen prosessien välillä. Se tarvitsee saman prosessin molemmilla palvelimilla. OP5 Monitorin tapauksessa kohteen prosesseja jäljittelevät SNMP-lisäosat, eli pluginit. UDP hakee IP-protokollan avustuksella kohteen prosessin kehystietoja. Se käärii tiedon UDP-paketiksi ja lisää siihen omat tunnistetietonsa. UDP ei ole täysin toimintavarma protokolla. Se ei muodosta jatkuvaa yhteyttä palvelinten välille. Sen sijaan se toimittaa yk-

sittäisiä tietopaketteja. Tätä voidaan pitää protokollan heikkoutena, sillä tämä toimitustapa sisältää riskin tiedon katoamiselle. Vertauskuvana voidaan käyttää kirjeen katoamista postissa. Kadonnutta pakettia ei voi lähettää samalla tiedolla uudelleen. Monissa tapauksissa tätä UDP:n heikkoutta voidaan välttää käyttämällä Transmission Control-protokollaa, joka muodostuu jatkuvan yhteyden kohteiden välille. Tämä tapa varmistaa tiedon uudelleenlähetyksen, jos verkossa esiintyy häiriöitä. TCP:n avulla tietoa voidaan luoda puskuriin, josta se voidaan sitten lähettää eteenpäin, kun yhteys on todettu toimivaksi (Freesoft 2019). Valitettavasti SNMPv3 ei kuitenkaan toimi TCP:n välityksellä, vaan työssä oli käytettävä UDP-protokollaa. Protokollan hyviksi puoliksi voidaan sanoa sen kevyempi kuorma verkkoinfrastruktuurille ja pienempi mahdollisuus aikakatkaisuille. (Rouse 2019.)

3 VALVONNAN SUUNNITTELU JA OHJELMISTON ASENNUS

Tämä luku käsittelee tuotantoympäristön kartoittamisen, asennukseen liittyvän suunnittelun ja valvontatuotteen asennuksen.

3.1 Valvonnan toteutussuunnitelma

Yrityksen käyttämän SIEM-järjestelmän valvonnassa haluttiin kiinnittää huomiota eri prosesseihin, levyosioiden tilankäyttöön, suorittimen ja RAM-muistin kuormaan, sekä mahdollisesti myös verkkoliikenteen kokoon. Käyttöliittymän vastausaikaan tai ylipäätään toimintaan haluttiin myös toimiva valvontatapa. SNMP valittiin käyttöjärjestelmätason valvontaan, sillä se kykenee havainnoimaan muutoksia sen tilassa ja raportoimaan niistä nopeasti. Ennen tämän työn toteutusta käytössä ei ollut minkäänlaista valvontaa esimerkiksi levyosioiden suhteen. Tämä on erittäin kriittinen seikka, sillä SIEM on asetettu pysäyttämään prosesseja, kun tiettyjen levyosioiden tila lähenee maksimiksi asetettua rajaa. Käyttöliittymä on oleellinen osa analyytikkojen työssä ja sen on oltava saavutettavissa kaikkina ajankohtina sovittujen huoltokatkojen ulkopuolella. Tämän palvelun valvontaan nopeat HTTPS-kyselyt soveltuvat hyvin. Samalla kyselyllä on mahdollista toteuttaa myös käyttöliittymän sertifikaatin voimassaolon tarkistus.

3.2 Verkkoliikenne

Asennusympäristö on yksi monista tämän yrityksen erilaisista verkkoympäristöistä. Sen suunnittelussa on otettu huomioon monia tietoturvaa lisääviä ominaisuuksia. Näistä ensimmäinen asennuksessa huomioitava ominaisuus oli verkon segmentointi. Vaikka verkon jaottelu pienempiin osioihin ei vielä yksinään lisää tietoturvaa, voidaan sillä silti välttää turhaa liikennettä ei-haluttuihin kohteisiin luomalla erilaisia palomuurisääntöjä osioiden välille.

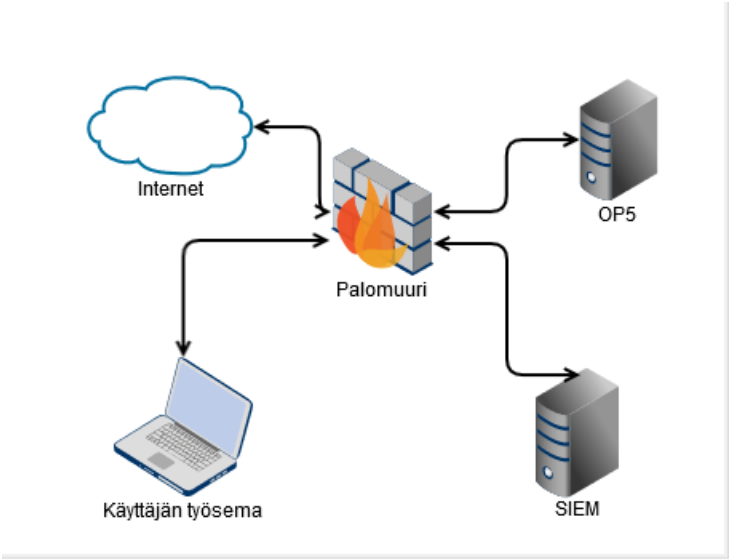
Tässä työssä valvontajärjestelmä asennettiin eri verkkosegmenttiin kuin missä valvottava kohde sijaitsi. Ratkaisuun vaikuttivat nämä tärkeäksi koetut tekijät:

- OP5 tulisi olemaan suorassa kontaktissa myös ulkopuolisiin asiakasverkkoihin. Valvottava SIEM-järjestelmä on tarkoitettu vain yrityksen oman sisäverkon tapahtumien havainnointiin ja sitä haluttiin suojella mahdolliselta ulkopuolelta tulevalta vihamieliseltä liikenteeltä.
- SNMP- ja HTTPS-kyselyitä on helpompi jäljittää kohteiden välillä, kun liikenne kulkee palomuurin läpi. Palomuurin tapahtumista siirretään reaaliaikaista lokitietoa SIEM-järjestelmään.
- Segmentti voidaan tarvittaessa eristää täysin muusta verkossa tapahtuvasta liikenteestä. Esimerkiksi mahdollisen haittaohjelmatartunnan seurauksena.

Verkon segmentointi ei vielä yksinään riitä takaamaan riittävää tietoturvan tasoa. Tästä syystä palomuurisäännöstöön oli kiinnitettävä huomiota ja verkkoliikenteen oli oltava salattua:

- Palvelimien välillä ei saanut olla muuta liikennettä kuin vaadittavat HTTPS-, ICMP- ja SNMP-yhteydet.
- Pääsy OP5 valvontapalvelimen käyttöliittymään ja käyttöjärjestelmään tuli olla rajattu vain valvontaa suorittavalle yksikölle. Liikenteen oli oltava myös salattua. Salatun ja tunnistetun liikenteen takaamiseksi yhteysprotokollaksi valittiin SSH.

Yrityksessä tietoverkkojen asetuksien hallinta on toisen osaston vastuulla, joten tarvittavista avauksista palomuurisäännöstöön tehtiin erillinen työpyyntö käyttäen ICT-palveluiden tarjoamaa tukipyyntöjärjestelmää. Kuvassa 1 on yksinkertaistettu hahmotelma siitä, kuinka jokaisen osaaottavan laitteen liikenne kulkee palomuurin lävitse. Yksikään työn laitteista ei sijainnut samassa verkkosegmentissä.



Kuva 1. Hahmotelma verkkoliikenteestä laitteiden välillä.

Työasemalta on pääsy kaikkiin opinnäytetyössä tarvittaviin verkkosegmentteihin. OP5 palvelin on yhteydessä myös internetin suuntaan. Palvelin hakee kerran kuukaudessa päivitykset sille määritellystä sovelluskirjastosta, joka sijaitsee järjestelmää kehittävän yrityksen omilla palvelimilla.

3.3 OP5:n asennus ja palvelimen peruskonfiguraatio

OP5 Monitor asennettiin Red Hat Linux 7.5 käyttöjärjestelmän päälle. Kyseisen Linux käyttöjärjestelmän asennusta, asetuksia tai teoriaa ei tässä työssä käsitelty.

3.3.1 Asentaminen asennuspaketista

OP5 Monitorin asennus aloitettiin suorittamalla komento, johon sisällytettiin palvelimelle viety asennustiedosto. Tämä tiedosto sisälsi asennusskriptejä, sekä määritelmät järjestelmän tarvitsemille sovelluskirjastoille. Ennen komennon suorittamista palvelimelle oli kirjauduttava omalta työkoneelta SSH:ta käyttämällä. Kirjauduttaessa ensimmäistä kertaa palvelin tarjoaa julkisen avaimensa. Tämän jälkeen palvelin kysyy käyttäjätunnusta ja salasanaa. Salasana ja käyttäjätunnus olivat valmiiksi asetettuina ICT-yksikön toi-

mesta. Tämä toiminto sisältyy yksikön käyttämään asennusskriptiin, jonka avulla palvelimien asennuksia automatisoidaan. Tietoturvan lisäämiseksi jokainen käyttäjä on pakotettu vaihtamaan salasanansa ensimmäisellä kirjautumiskerralla.

Kirjautumisen jälkeen käytettäväksi avautui Linuxin Bash-ympäristö. Asennus voitiin aloittaa ja sen toteutus oli nopeaa ja yksinkertaista muutamalla Bash-komennolla. Asennuspaketti oli pakatussa muodossa, joten sen sisältö oli ensin purettava haluttuun tiedostopolkuun (kirjautuessa palvelimelle oletuspolkuna on käyttäjän oma kotikansio) komennolla

```
sudo tar -zxf op5-monitor*.tar.gz .
```

Koska käyttäjätunnukseni ei ole oletusarvoisesti korkeimman luokan käyttäjä (root), oli komentojen eteen muistettava lisätä komento sudo, joka korotti käyttäjäoikeuteni komennon suorittamisen ajaksi riittävälle tasolle (sudo 2019). Purkamisen yhteydessä syntyneeseen kansioon siirryttiin ja sen sisältö tuotiin näkyville komennolla

```
cd op5-monitor* && ls -lah .
```

Kansion sisältä löytyi asennukseen vaadittava install.sh-asennusskripti. Ennen sen ajamista oli kuitenkin lisättävä vielä yksi ylimääräinen sovelluskirjasto, jotta yksikään tarvittavista komponenteista ei jäisi puuttumaan. Tämä oli poikkeustapaus nimenomaan käytetyn Red Hat 7 Linuxin kohdalla (Hansen 2019). Sovelluskirjasto otettiin käyttöön komennolla

```
sudo subscription-manager repos --enable=rhel-7-server-optional-rpms .
```

Tämän jälkeen asennusskripti oli valmis ajettavaksi. Koska olin jo samassa kansiossa kuin suoritettava asennusskripti, ajoin sen komennolla

```
sudo ./install.sh .
```

Skripti haki määritellyistä sovelluskirjastoista tarvittavat tiedostot, tarkisti niiden oikeellisuuden ja tämän jälkeen asensi ne. Skripti määritteli myös oletusasetukset, jotka on valmistajan toimesta koettu tarpeellisiksi, jotta järjestelmän käytön aloittaminen olisi helppoa ja välitöntä. Asennuksen jälkeen järjestelmä olisi ollut suoraan käytettävissä, mutta vielä oli tehtävä muutama asetus, jotta valvonnan määrityksen aloittaminen oli mahdollista.

3.3.2 Lisenssin asentaminen

OP5 Monitor vaatii toimiakseen kaupallisen lisenssin, jotta sen käyttö olisi laillista yritysympäristössä. Palveluun soveltuvan lisenssin lisääminen avaa myös tarvittavat ominaisuudet käytettävästä järjestelmästä.

Op5 Monitor loi asennuksen yhteydessä oman kansionsa lisensseille, jonka sisältä järjestelmä kykenee niitä lukemaan. Lisenssi kopioitiin tähän kansioon komennolla

```
sudo op5license2018 /opt/op5license/op5license.lic ,
```

joka samalla nimesi lisenssitiedoston oikeaan muotoonsa. Lisenssin oikeuksia oli vielä muutettava niin, että järjestelmän käyttöliittymästä vastaava palvelinosa kykenisi sitä lukemaan (itrsgroup 2019). Lukuoikeudet ja omistus siirrettiin tälle palvelinosalle komennolla

```
sudo chmod 640 /etc/op5license/op5license.lic && sudo chown apache:apache /etc/op5license/op5license.lic .
```

3.3.3 Palvelimen palomuuriasetukset

Yrityksen palvelimilla on käytössä omat palomuurinsa tietyillä määrityksillä. Oletuksena tällä palvelimella liikenne oli hyvinkin rajattua. Valvonnan ja käyttöliittymän käytön mahdollistamiseksi oli palvelimen omalta muurilta avattava HTTPS- ja SNMP-liikenne. Red Hat 7 hyödyntää palomuurinsa hallinnassa komentorivipohjaista firewalld-työkalua. Haluttu liikenne on mahdollista lisätä joko käyttämällä porttinumeroita, tai nimeämällä palvelu (firewalld 2019). Tässä työssä lisäsin halutun liikenteen palveluiden nimillä. Tarvittavat avaukset ja sääntöjen aktivointi suoritettiin komennoilla

```
sudo firewall-cmd --permanent --add-service=https && sudo firewall-cmd --permanent --add-service=snmp && sudo firewall-cmd –-reload .
```

Komennot oli mahdollista suorittaa erillisinä, mutta pidän tavasta ketjuttaa komentoja huomattavasti nopeampana ja käytännöllisempänä. Lisäysten jälkeen palvelin oli täysin käyttövalmis.

4 VALVONNAN TOTEUTTAMINEN

Tässä luvussa toteutettiin valvonnan vaatimat asetukset SIEM-palvelimella ja OP5 Monitorilla. Asetusten määrittämisen jälkeen valvonta oli käyttövalmis.

4.1 SNMP:n asetusten määrittely SIEM-palvelimella

Linux palvelimille on saatavissa net-snmp-paketti, joka sisältää kaiken SNMPv3:en asetusten määrittämiseen tarvittavan. Tässä työssä asennusta ei tarvinnut erikseen suorittaa. Vaadittava paketti, sekä asetustiedostot olivat SIEM-palvelimella esiasennettuna.

Ensiksi palvelimelle luotiin SNMPv3-käyttäjä. Käyttäjä hyödyntää snmp-palvelua kyselyiden vastaanottamisessa ja niihin vastaamisessa (Semenescu 2019). Käyttäjän turvallisuustasoksi valittiin authPriv (luku 2.2.1). Tietojen syöttämisen mahdollistamiseksi snmp-palvelu oli pysäytettävä komennolla

```
systemctl stop snmpd ,
```

jonka jälkeen haluttua tiedostoa oli mahdollista muokata. Käyttäjä ja salasanat syötettiin tiedostoon `/var/lib/net-snmp/snmpd.conf.` Tiedostoon syötettiin rivi

```
createUser            op5kayttaja SHA salasana1 AES salasana2 ,
```

joka asetti käyttäjän, autentikoinnin ja salauksen. Esimerkin käyttäjä ja salasanat ovat keksittyjä. Käyttäjälle oli vielä annettava oikeudet lukea kaikkia SNMP:llä saatavia tietoja (Semenescu 2019). Tiedostoon `/etc/snmp/snmpd.conf` syötettiin rivi

```
rouser                op5kayttaja priv .1 ,
```

jonka jälkeen asetuksien määrittely oli valmis (Semenescu 2019). Tämän jälkeen SNMP-palvelu käynnistettiin komennolla

```
systemctl start snmpd .
```

4.2 Palomuurisääntö ICMP-kyselyille SIEM-palvelimella

Yrityksen käyttämä SIEM ei normaalisti hyväksy siihen kohdistuvaa ICMP-liikennettä. Se on erikseen määriteltävä palvelimen palomuurisäännöstöön sallituksi liikenteeksi. Liikenteen kieltäminen on helposti perusteltavissa tietoturvallisuudella, sillä ICMP mahdollistaa palvelimien löytämisen verkosta. Se mahdollistaa myös ICMP-tulvituksen, jolla voidaan rampauttaa palvelimen toiminta ylikuormittamalla sen kyky käsitellä verkkoliikennettä. (Thomas 2005, 42.)

Poikkeussääntöjen lisääminen palomuuriin oli varsin yksinkertaista. Käytin mallina jo muualla tuotannossa käytettyä asetusta. Sääntöihin muutin ainoastaan OP5 Monitorin IP-osoitteen. Säännöt lisättiin tiedostoon `/opt/qradar/conf/iptables.pre`. Lisätyt säännöt olivat:

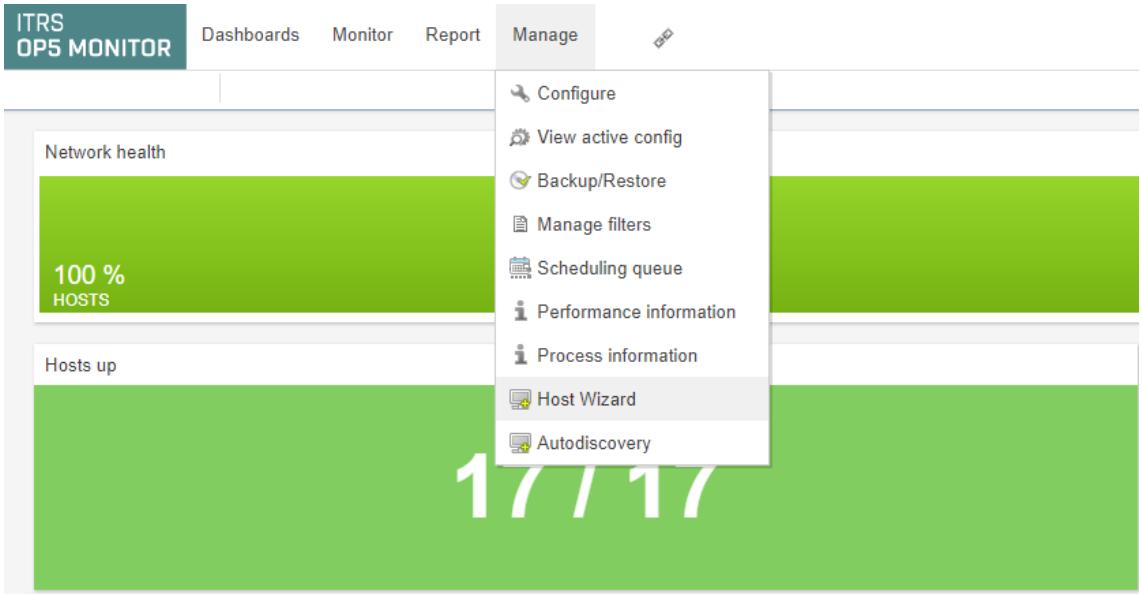
```
-A INPUT -i ens192 -p icmp --icmp-type 8 -s 10.10.100.2/32 -j ACCEPT

-A INPUT -i ens192 -p icmp --icmp-type 0 -s 10.10.100.2/32 -j ACCEPT .
```

Nämä kaksi sääntöä mahdollistivat ICMP-liikenteen vastaanottamisen ja siihen vastaamisen. Säännöt ladattiin käyttöön bin-kansiosta löytyvällä `iptables_update.pl`-skriptillä.

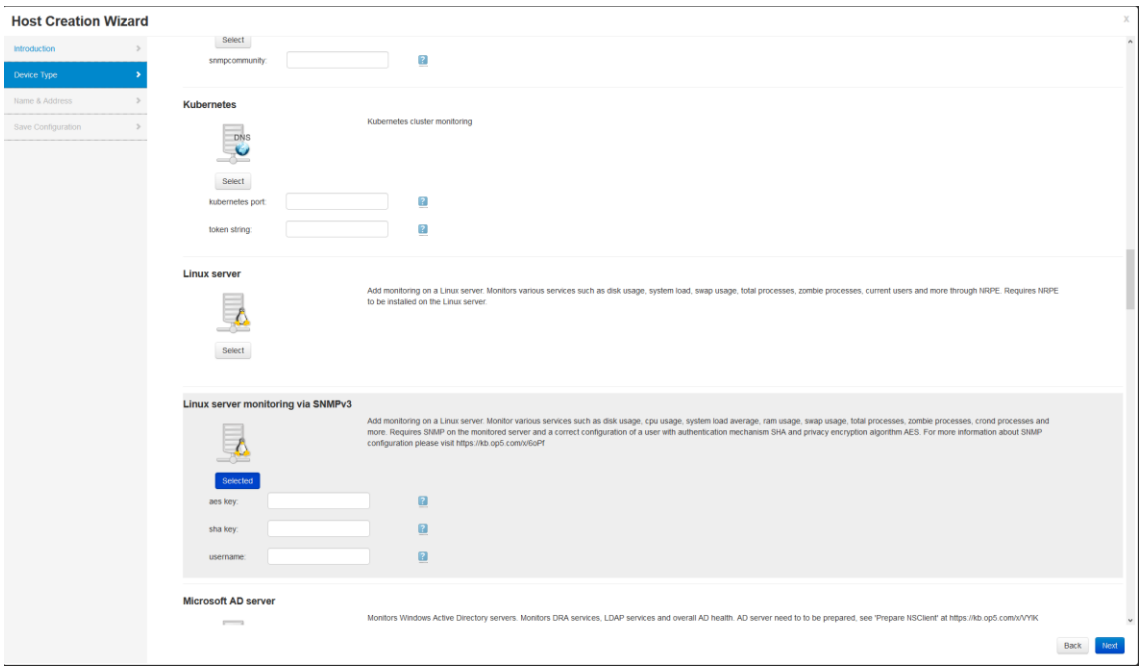
4.3 SIEM-palvelimen lisääminen OP5 Monitorin käyttöliittymässä

Järjestelmän käyttöliittymä ei tyydyttänyt käyttäjiä jokaisella osa-alueella, mutta kohdepalvelimien lisääminen oli tehty erittäin helpoksi. Järjestelmään kirjauduttuessa ensimmäisenä eteen avautui käyttöliittymän pääsivusto (dashboard), joka sisälsi useita erilaisia pikanäyttöjä valvottavien kohteiden eri toiminnoista. Kuvan 2 mukaisesta käyttöliittymän ylälaidasta valittiin Manage-tiputusvalikko, joka paljasti useita pikalinkkejä asetusten määrittämiselle. Pudotusvalikosta valittiin kohta Host Wizard.



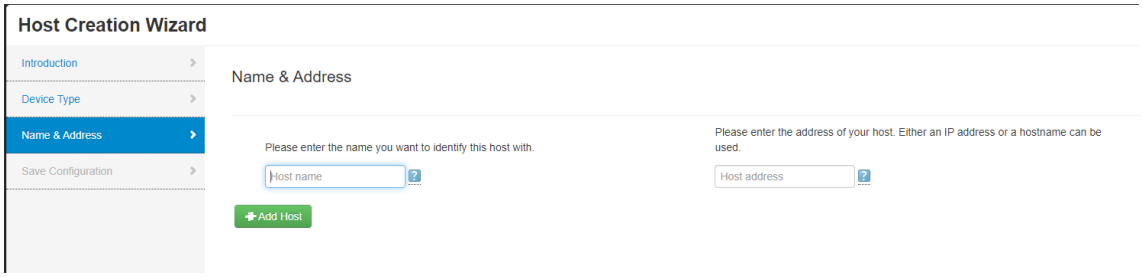
Kuva 2. Käyttöliittymän etusivu.

Host Wizard oli ulkoasultaan ja toiminnaltaan hyvin yksinkertainen. Ensimmäisenä valikkona avautui pitkä lista, joka sisälsi valmiita pohjia erilaisille palvelintyypeille. Kuvassa 3 on nähtävissä Linux palvelimille tarkoitettu SNMPv3-pohja. Vaaditut arvot ovat samoja, jotka määriteltiin SIEM-palvelimelle luvussa 4.1.



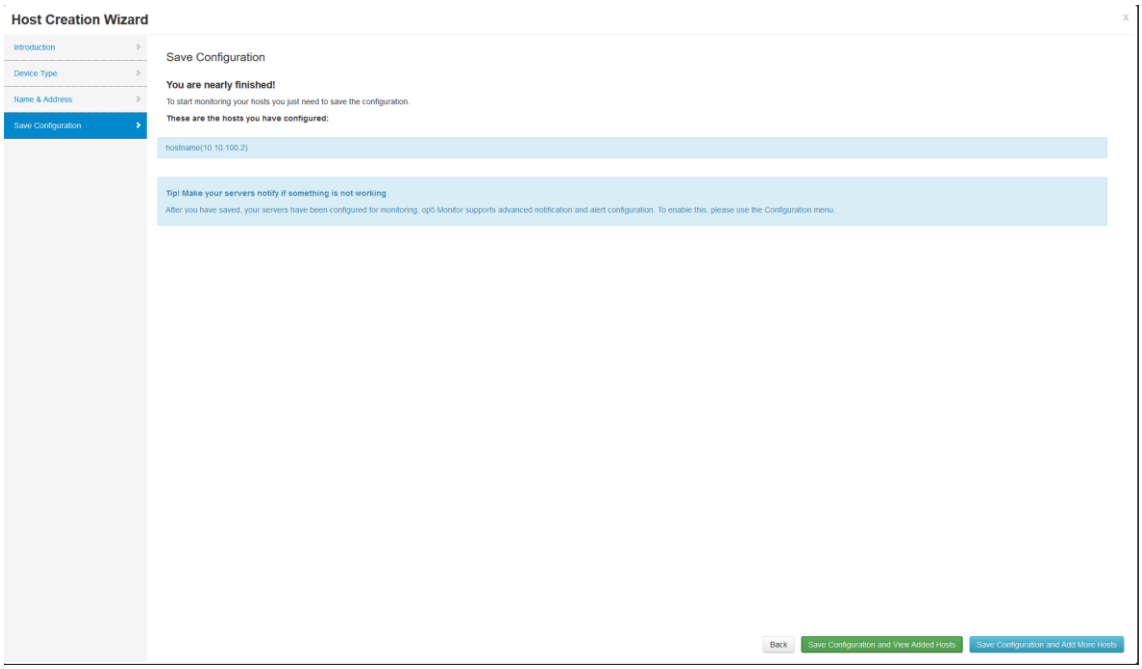
Kuva 3. SNMPv3:n tavan valitseminen.

Arvojen syöttämisen jälkeen sivun alalaidasta painettiin Next-painiketta, joka siirsi tilan Kuvan 4 mukaiseen valikkosivuun. Tällä sivulla Host Wizard pyysi kohdepalvelimen palvelinnimeä ja sen IP-osoitetta. Palvelimen nimeksi asetettiin yrityksen nimipalvelimelta löytyvä virallinen nimitys. Alalaidasta valittiin Next-painike, jolla päästiin Kuvan 5 mukaiseen viimeiseen näkymään.



Kuva 4. Palvelimen nimen ja IP-osoitteen määrittely.

Host Wizardin viimeisessä vaiheessa asetuksia ei enää määritelty. Tässä kohtaa Host Wizard tarkisti annetut parametrit ja käski käyttäjää tallentamaan tehdyn konfiguraation. Annetut parametrit, sekä tarvittavat salasanat olivat oikein, joten tässä vaiheessa palvelimen lisääminen valvottavaksi kohteeksi oli onnistunut. Tämän jälkeen oli tarkennettava ja muokattava palvelimeen kohdistettavia valvontasääntöjä.



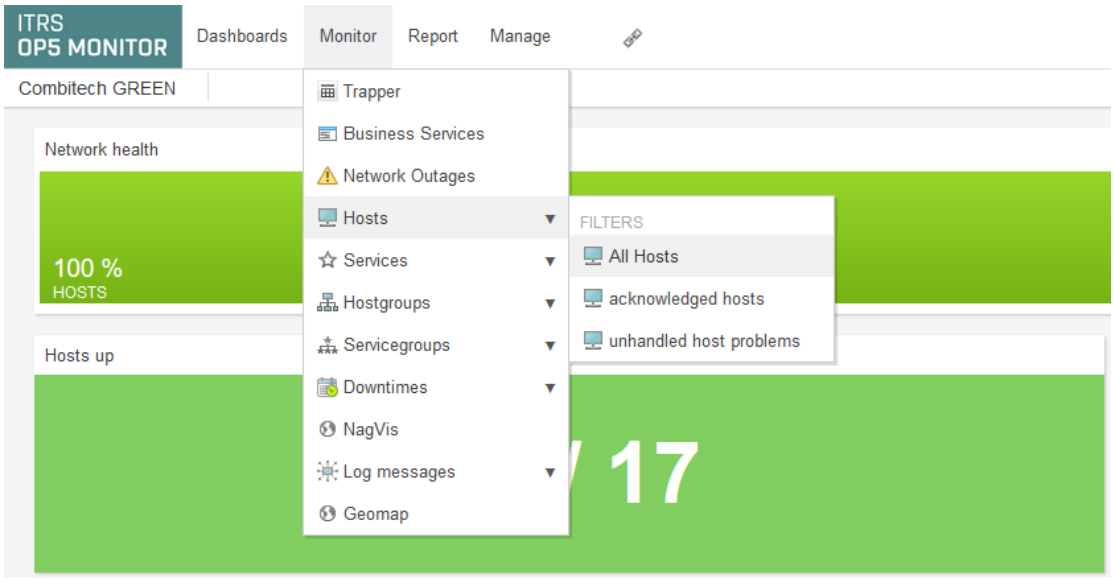
Kuva 5. Syötettyjen asetusten tallentaminen.

4.4 Kyselyiden muokkaaminen

Palvelimen lisääminen valvottavaksi kohteeksi perusasetuksilla ei riittänyt kattamaan haluttua valvonnan tasoa. Lisättäviksi kohteiksi haluttiin vielä käyttöliittymän valvonta (sivuston vastausaika ja sertifikaatin voimassaolo) sekä muutama erillinen levyosio. Palvelin lisättiin käyttämällä Linux palvelimille tarkoitettua SNMPv3-pohjaa, joten HTTPS-protokollaa hyödyntävät kyselyt eivät automaattisesti kuuluneet perusasetuksiin. ICMP sisältyi valvontaan automaattisesti, eikä sen asettamiseen kiinnitetty sen enempää huomiota. Sen ainut tehtävä oli tarkastaa, että kohdepalvelin oli vielä olemassa. Tässä luvussa käsitellään vain erikseen lisättävien valvontasääntöjen asettamista. Lopuksi näytetään yleiskatsaus valvonnan kokonaiskuvasta.

4.4.1 Käyttöliittymän toiminnan valvonta

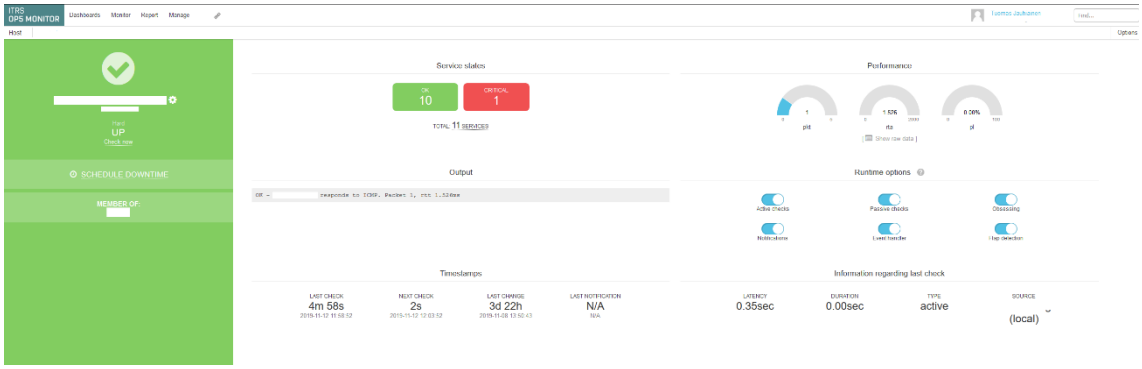
OP5 Monitorin etusivulta pääsee pudotusvalikosta haluttuun kohdepalvelimeen. Helpoin tapa navigoida kaikkiin valvottuihin kohteisiin oli valita Monitor-pudotusvalikosta Hosts ja sen alta All Hosts (Kuva 6).



Kuva 6. Navigointi valvottavien palvelimien listalle.

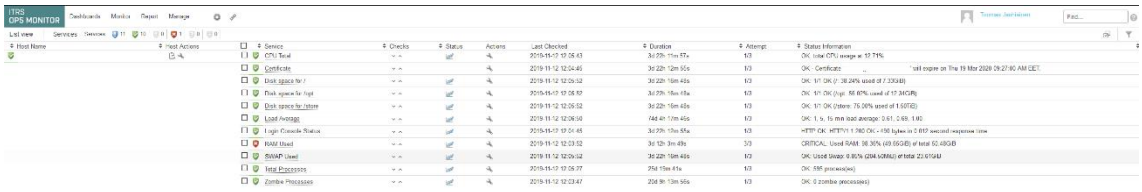
Tämä suodatin paljasti listan kaikista valvonnan alla olevista kohteista. Listalta valittiin aiemmin lisätty SIEM-järjestelmä. Tämä avasi valvottavan palvelimen etusivun. Tällä

etusivulla oli kootusti tietoja SIEM-palvelimen sen hetkisestä tilasta. Sivu on nähtävissä kuvassa 7.



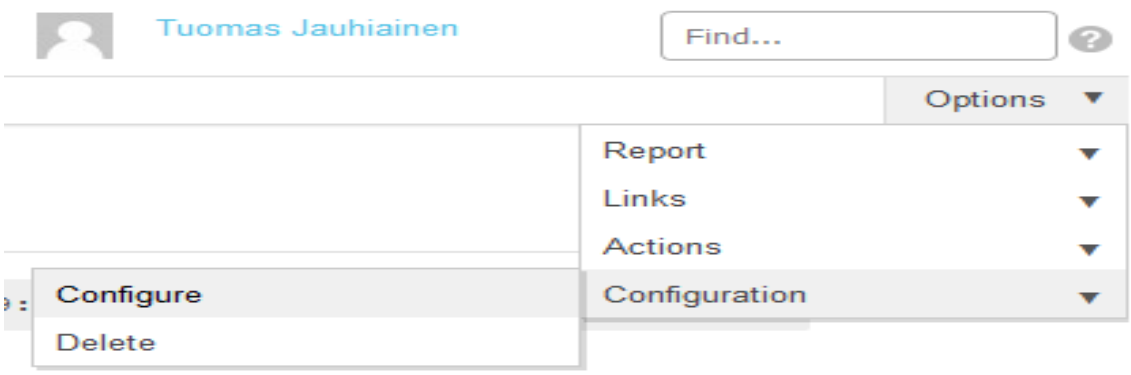
Kuva 7. Valvottavan kohteen yleisnäkymä.

Käyttöliittymän valvonnan lisäämiseksi oli avattava Services-näkymä. Tämä onnistui helpoiten painamalla yleisnäkymästä Services-tekstiä Service States-otsikon alta. Tämän kautta päästiin All Services-näkymään, joka on esiteltynä kuvassa 8. Tähän työhön liitetty kuva 8 on otettu kaikkien valvottavien kohteiden lisäämisen jälkeen, joten se sisältää jo valmiiksi halutut valvonnat.



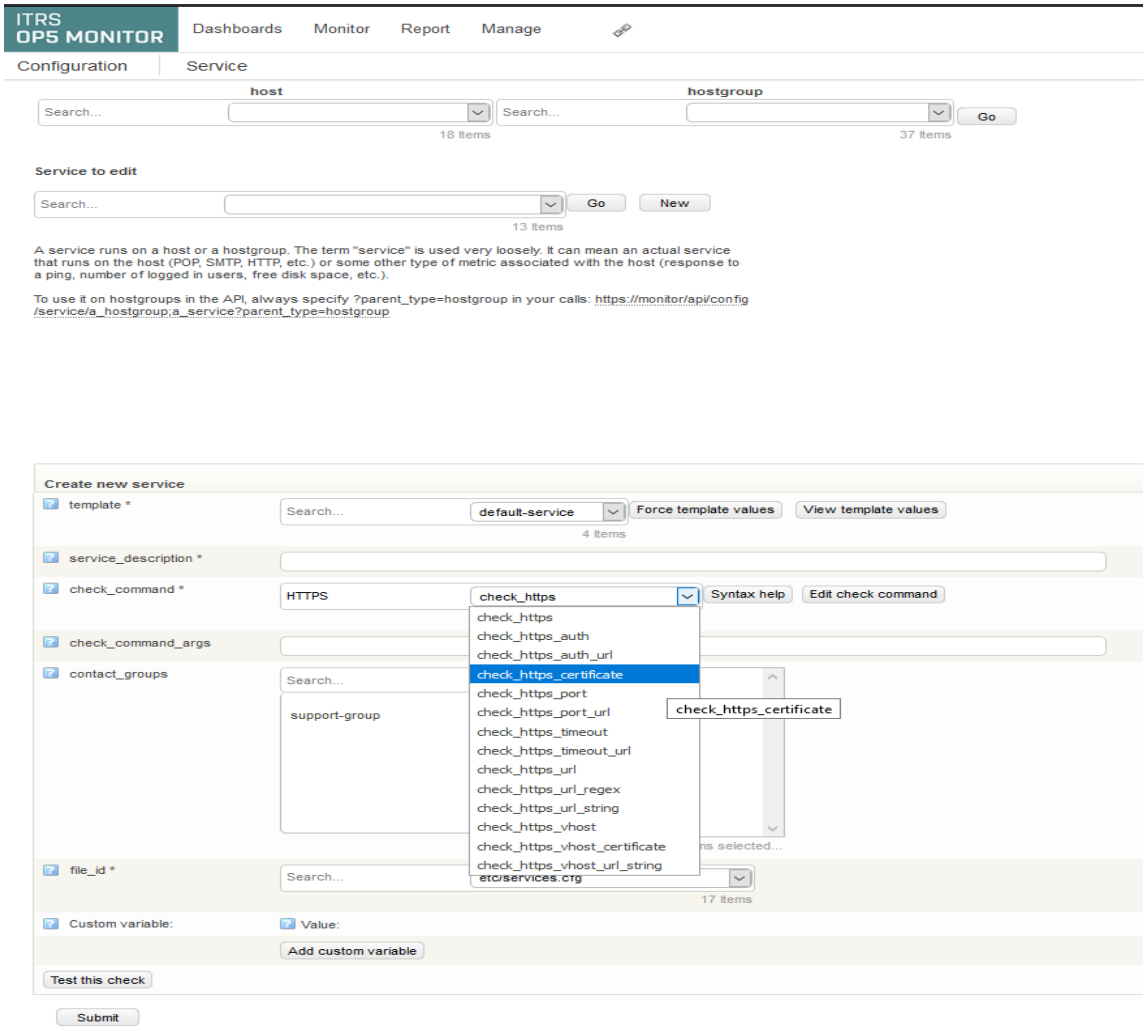
Kuva 8. Kaikki SIEM-järjestelmän valvottavat kohteet.

Uusi kysely lisättiin valitsemalla oikean ylälaidan Options-pudotusvalikosta Configuration, jonka alta valittiin vielä Configure (Kuva 9).



Kuva 9. Kyselyiden asettamiseen navigoiminen.

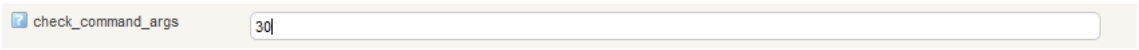
Configure-sivulla Service to edit-kohdasta valittiin New. Check_command*-osion pudotusvalikosta etsittiin komento nimeltään `check_https_certificate`. Tämä vaihe on esiteltynä kuvassa 10.



Kuva 10. Sertifikaatti-komennon valinta.

Komennon valinnan jälkeen komennolle oli mahdollista määrittää tarvittavat argumentit. Komento oli perusmuodossaan seuraavanlainen: `$USER1$/check_http -H $HOSTADDRESS$ -S -C $ARG1$`. Dollarimerkkien sisälle merkityt muuttujat oli määritelty jo palvelimen lisäämisvaiheessa. Kohtaan $USER1$ määrittyi SIEM-palvelimelle asetettu SNMPv3-käyttäjä. HOSTADDRESS määriteltiin Host Wizardin IP-kentässä (Kuva 4). Argumentti -S tarkoitti sitä, että komento käytti HTTPS-protokollaa ja sille vakioitua porttia 443. Ainoa manuaalisesti lisätty argumentti oli -C, jolla määritettiin varoitusaika sertifikaatin vanhenemiselle. Arvoksi asetettiin 30 päivää. OP5 Monitorin komentojen muokkaaminen oli helppoa, ja järjestelmä osasi hyvin tunnistaa asetetut arvot. Esimerkki arvon lisäämisestä Kuvassa 11. Jos komentoon oli asetettava useampia argumentteja, ne eroteltiin käyttämällä huutomerkkiä arvojen välissä. Järjestelmä osasi automaattisesti tunnistaa mikä argumentti oli kyseessä ja asetti arvon oikeaan paikkaan. Argumenteille

oli helppo etsiä selityksiä, sillä komentosivulla oli valmiina ohjeet jokaiselle mahdolliselle argumentille. Arvojen asettaminen jälkeen komento voitiin tallentaa sivun oikean yläreunan Save-painikkeella.



Kuva 11. Komennon argumenttien arvojen asettaminen.

Komennon toiminta voitiin tarkastaa Services-sivulta, josta voitiin nähdä, että käyttöliittymän sertifikaatti oli voimassa (Kuva 8). Käyttöliittymän vastausaikaa voitiin valvoa komennolla `$USER1$/check_http -H $HOSTADDRESS$ -S`. Käytännössä tämä komento oli hyvin samanlainen kuin sertifikaatin valvontaan käytetty komento. Tämä komento ei vaatinut erikseen määriteltäviä argumentteja. Se lisättiin samalla tapaa kuin edellinenkin komento ja tallentamisen jälkeen se oli käyttövalmis. Käyttöliittymän vastausajan se ilmoitti muodossa b/s (bittiä sekunnissa). Tämä kertoi siirretyn tiedon määrän tietyssä ajassa.

4.4.2 Levyjakojen ja muiden komentojen lisääminen

Loputkin valvontakomennot lisättiin täysin samalla tavalla kuin käyttöliittymän valvontaan käytetyt komennot. Kun palvelin lisättiin valvottavaksi kohteeksi, oli monissa komennoissa hyvät perusasetukset. Komennoissa käytettiinkin hälytysrajoja, jotka järjestelmä oli automaattisesti määritellyt. Järjestelmä ilmoitti varoituksella, kun levyjaon täyttötaso ylitti 85 prosenttia sen kokonaistilavuudesta. Järjestelmä antoi kriittisen ilmoituksen, kun levyjaon täyttöaste ylitti 95 prosenttia kokonaistilavuudesta. Valvottaviksi levyjaoiksi lisättiin `/`, `/store`, `/var/log` sekä `/opt`. Nämä koettiin SIEM-palvelimen toiminnan kannalta kriittisimmiksi. Esimerkiksi `/store` sisältää kaiken SIEM-järjestelmän keräämän lokitiedon. Muitakin levyjakoja oli mahdollista lisätä, mutta työn aikana niihin ei paneuduttu.

Levyjakojen lisäksi SNMP-protokollalla valvottavia kohteita olivat suorittimen kokonaiskuorma (CPU), keskimääräinen kuorma palvelimella (Load Average), SWAP- ja RAM-muistit, sekä niin kutsutut jäännösprosessit (Zombie Process). Näiden kohteiden raja-arvot olivat asennusvelhon määrittelyjen mukaiset, eikä niitä tämän työn aikana muokattu. Raja-arvot noudattivat samoja tasoja kuin levyjakojenkin kohdalla. Ainoana poik-

keuksena jäännösprosessit, joita valvottiin lukumäärällisesti. Liian suuri jäännösprosessien määrä voi mahdollisesti viitata ongelmiin prosessien automaattisessa sammutuksessa.

4.5 Muut asetukset

Kaikkia OP5 Monitorilla tehtyjä lisäasetuksia ei tarkoituksen mukaisesti sisällytetty tähän työhön. OP5 Monitorin tuottamista hälytyksistä haluttiin ilmoitus valvomon sähköpostiin. Tarkoituksena ei kuitenkaan ollut sisällyttää tätä kaikkiin valvottaviin kohteisiin. Syitä tähän olivat esimerkiksi ajoittaiset, mutta hyväksyttävät raja-arvojen ylitykset suorittimen kokonaiskuormassa. SIEM-palvelin voi olla tiettyinä aikoina (varmuuskopiot) tai tietyissä tehtävissä hyvinkin raskaan kuorman alla. Tämä on kuitenkin täysin tiedostettua ja normaalia. Pitkäaikaisesta kuormasta olisi toki voinut lähettää sähköpostin, mutta sen asetusten säätäminen onnistuneesti olisi vaatinut pidempiaikaisia testejä.

Rajasin sähköpostien lähetykset levyjakojen raja-arvojen ylityksistä muodostuviin hälytyksiin. Tämä asetus lisättiin kuvan 10 mukaisella asetussivulla. SNMP-kyselyn asetusten määrittelyjen jälkeen sivun alalaidasta valittiin kohta ”Contact Group”. Tähän kenttään syötettiin valvomon käyttämä sähköpostiosoite. Asetus tallentui samalla, kun SNMP-asetus tallennettiin.

4.6 Testaus ja tulokset

Ensimmäinen testauksen aikana tehty muutos oli hälytysrajojen muokkaaminen levyjakojen osalta. Useiden levyjakojen kohdalla kriittiseksi rajaksi asetettu 95 % olisi ollut riittävä, mutta esimerkiksi `/store` ja `/opt` osoittautuivat poikkeuksiksi. SIEM-järjestelmän tietyt toiminnot pysähtyvät, kun näiden levyjakojen täyttöaste ylittää 95 %:ia. Tästä syystä kriittisen tason hälytysrajaa laskettiin 90 %:iin. Tämä antoi riittävän toimintavaran järjestelmän ylläpitäjille.

SNMP-kyselyiden ongelmaksi osoittautui niiden oikeanlainen ajoittaminen. Oli mahdollista, että tiettyjä tapahtumia jäi huomaamatta, jos kyselyiden välinen aika oli liian suuri. Liian tiheä kyselyväli saattoi sen sijaan aiheuttaa turhia hälytyksiä. Tietyt toiminnot Linux-palvelimilla käynnistyivät uudelleen omia aikojaan ilman, että siitä oli mitään konkreet-

tista haittaa itse järjestelmän toiminnalle. Sopiva kyselyväli ei tämän työn aikana selvinnyt. Turhien hälytysten määrä ei kuitenkaan osoittautunut liian suureksi, eivätkä merkittävät tapahtumat palvelimilla jääneet huomaamatta testijakson aikana.

SIEM-järjestelmän käyttöliittymän valvonta toimi odotetulla tavalla. Kyselyiden tiheys asetettiin 30 sekuntiin. Tämä oli riittävä aikaväli valvonnan kannalta. Valvonnan tehostamisen vuoksi valvomon seinänäytöille luotiin erillinen valvontasivu, josta käyttöliittymän tilanteen kykeni tarkastamaan ilman, että oli tarvetta kirjautua itse OP5 Monitorin käyttöliittymään. Tämä toteutettiin siksi, että käyttöliittymä oli erittäin kriittinen työkalu analyytikkojen työtehtävissä.

5 TYÖN LOPPUTULOS

Työn tavoitteena oli suunnitella ja toteuttaa valvontajärjestelmä, jota hyödynnettäisiin yrityksen SIEM-järjestelmän toiminnan valvontaan. Valvontajärjestelmäksi valittiin OP5 Monitor. Valintaan vaikuttivat lisenssin hankintakustannukset ja paikallinen lähituki. Yrityksellä ei ole aikaisemmin ollut käytössä vastaavaa tuotetta. Tuotteen vertailua kilpailevien järjestelmien kanssa ei sisällytetty tähän opinnäytetyöhön.

OP5 Monitorin asentaminen oli nopeaa ja suoraviivaista. Aikaisempi kokemus Linuxin käytöstä ja ylläpidosta osoittautui tässä työssä erittäin hyödylliseksi. Useimmat komennot ja asetustiedostot olivat jo ennestään tuttuja. Tämä nopeutti varsinkin asennusvaihetta, koska aikaa ei tarvinnut käyttää kaiken opiskeluun dokumentaatiosta. Järjestelmän ylläpito oli myös helppoa, sillä päivittäminen hoitui aivan normaalisti Red Hat Linuxin yum-työkalulla, joka mahdollisti uusimpien päivitysten hakemisen yhdellä komennolla. Yum-työkalun käyttö mahdollisti myös hyvän ja helpon tavan ladata vain Red Hat-päivitykset ja jättää varsinainen OP5 Monitorin päivitys erilliseksi. Syy tähän ratkaisuun saattoi olla esimerkiksi tunnistettu virhe OP5 Monitorin seuraavassa versiossa, jota ei vielä oltu kehittäjän puolelta korjattu.

Asennuksen jälkeinen valvonnan aloittaminen oli myös hyvin suoraviivaista. Vaativin vaihe oli SIEM-palvelimelle tehty SNMP-agentin asetusten asettaminen. SIEM-palvelimen lisääminen OP5 Monitorin käyttöliittymässä oli helppoa, kun mahdollisuutena oli käyttää asennusvelhoa. Täysin kohdennettu asennus olisi vaatinut API-rajapinnan hyödyntämistä, mutta yhden palvelimen tapauksessa sitä ei haluttu tehdä. Asennusvelhon käytön jälkeen oli muutama valvottava kohde lisättävä manuaalisesti. Tämä ei kuitenkaan ollut ongelma, sillä valvonnan hienosäätöä työstettiin alkuvaiheessa hyvinkin paljon ja valvontakomentoja oli joka tapauksessa muokattava käsin.

Valvonnassa saavutettiin lopulta riittävä lopputulos. Yrityksen valvomon näytöille saatiin tuotua tietoa valvottavan järjestelmän käyttöliittymän tavoitettavuudesta, joka oli erittäin tärkeää, kun valvottavia kohteita oli useita, eikä jokaista järjestelmää ollut mahdollista valvoa manuaalisesti. Levytilan täyttymisestä ja esimerkiksi liiallisesta suorittimen kuormasta saatiin sähköpostiin ilmoitus siinä tapauksessa, jos asetetut hälytysrajat ylittyivät. Yrityksen päivystäjät seuraavat hälytyssähköpostien tilannetta aktiivisesti, joten mahdollisiin ongelmatilanteisiin on mahdollista puuttua hyvinkin nopeasti.

Valvonta vaatii tulevaisuudessa vielä paljon kehittämistä siitä huolimatta, että työssä saavutettiin riittävä lopputulos. Käyttöliittymän valvontaan on olemassa parempia ja kehittyneempiä tapoja kuin käytetty HTTPS-protokollaan pohjautuva testi. Järjestelmään olisi mahdollista liittää Selenium-viitekehys, jolla on voidaan toteuttaa automatisoituja ratkaisuja verkkosivuilla. Tällä tavoin käyttöliittymän sisällöstä olisi mahdollista saada paljon yksityiskohtaisempaa tietoa. SNMP jätti kehittämisen varaa, sillä aivan kaikkia haluttuja prosesseja ei lopulta saatu valvonnan piiriin. Tämä johtui pitkälti siitä, että saatavissa oleva dokumentaatio oli huonolaatuista eikä OP5 Monitorin käyttämien lisäosien luomiseen ollut riittävää ohjeistusta. Tulevaisuudessa valvontaa olisi hyvä siirtää esimerkiksi rajapintoja hyödyntäväksi menetelmäksi.

LÄHTEET

Baccala, B. 1997. Connected: An Internet Encyclopedia. Viitattu 22.11.2019 https://www.freesoft.org/CIE/Topics/83.htm.

Eastlake, D & Hansen, T. 2011.US Secure Hash Algorithms. Viitattu 5.6.2019 https://tools.ietf.org/html/rfc6234.

Fielding, R.; Gettys, J.; Mogul, J.; Frystyk, H.; Masinter, L.; Leach, P. & Berners-Lee, T. 1999. Hypertext Transfer Protocol – HTTP/1.1 https://tools.ietf.org/html/rfc2616.

Firewalld. 2019. Open a Port or Service. Viitattu 1.9.2019 https://firewalld.org/documentation/howto/open-a-port-or-service.html.

Frahim, E. & Froom R. 2015. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide. Indianapolis: Cisco Press.

Hansen, J. 2019. Missing dependencies when installing OP5 Monitor 8 on Red Hat Enterprice Linux 7. Viitattu 22.5.2019 https://support.itrsgroup.com/hc/en-us/articles/360002639158.

ITRS Group. 2019. Adding a .lic license file to OP5 Monitor. Viitattu 29.10.2019 https://support.itrsgroup.com/hc/en-us/articles/360020055714.

ITRS Group. 2019. Installing OP5 Monitor and Getting Started. Viitattu 20.5.2019 https://support.itrsgroup.com/hc/en-us/articles/360020054634-Installing-OP5-Monitor-and-Getting-Started.

Linode. 2018. Control Network Traffic with iptables. Viitattu 1.11.2019 https://www.linode.com/docs/security/firewalls/control-network-traffic-with-iptables/.

Miller, T. Sudo Manual. Viitattu 10.7.2019 https://www.sudo.ws/man/1.8.3/sudo.man.html.

Paessler. 2019. IT Explained: SNMP. Viitattu 7.7.2019 https://www.paessler.com/it-explained/snmp.

Postel, J. 1981. Internet Control Message Protocol https://tools.ietf.org/html/rfc792.

Rescola, E. 2018. The Transport Layer Security (TLS) Protocol Version 1.3. Viitattu 8.10.2019 https://tools.ietf.org/html/rfc8446.

Rescorla, E. 2000. HTTPS (HTTP over TLS). RTFM, INC https://tools.ietf.org/html/rfc2818.

Rouse, M. 2019. UDP (User Datagram Protocol). Viitattu 15.11.2019 https://searchnetworking.techtarget.com/definition/UDP-User-Datagram-Protocol.

Semenescu, A-R. 2019. Configure a Linux server for SNMP monitoring. Viitattu 5.5.2018 https://support.itrsgroup.com/hc/en-us/articles/360020056114-Configure-a-Linux-server-for-SNMP-monitoring.

Thomas, T. 2005. Verkkojen Tietoturva. Helsinki: Edita Prima Oy.

Wesentra Oy. 2019. Certificates, Sertifikaatit eli Varmenteet. Viitattu 9.10.2019 https://sslapua.fi/ssl.html.

Ylonen, T. 1996. SSH – Secure Login Connections over the Internet. Proceedings of the 6th USENIX Security Symposium USENIX.