



# Järjestelmävalvojan työkalupakki

Lari Hokkanen

Opinnäytetyö, AMK

Toukokuu 2024

Tieto- ja viestintätekniikan tutkinto-ohjelma

**Hokkanen, Lari**

## **Järjestelmävalvojan työkalupakki**

Jyväskylä: Jyväskylän ammattikorkeakoulu. **Toukokuu 2024**, 36 sivua

Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

## **Tiivistelmä**

Opinnäytetyön tehtävänä oli luoda työkalupakki järjestelmävalvojille sopivista työkaluista, joita voisi käyttää parantamaan yritysten kyberturvallisuutta. Työllä ei ollut erillistä toimeksiantajaa.

Opinnäytetyön tavoitteena oli verrata saatavilla olevia työkaluja käyttämällä arvosteluja ja suosituksia alan asiantuntijoilta. Lisäksi kerättiin tietoa järjestelmävalvojien työtehtävistä ja tietoturvakeskusten rakenteesta ja toiminnasta. Kahta työkalua, ELK Stackia ja Zabbixia, verrattiin tarkemmin asentamalla työkalu ja testaamalla niiden toimintakykyä hälytyksen aiheuttavissa tilanteissa. Tavoitteisiin myös sisältyi korostaa apuohjelmia, jotka voivat auttaa järjestelmävalvojia ongelmatilanteissa tai vaarojen vahvistamisessa.

Opinnäytetyön tuloksina syntyi esimerkkirakenteita tietoturvakeskuksille ja kokoelma järjestelmävalvojien työtehtävistä ja näiden tehtävien suorittamisesta. Lisäksi työssä koottiin listaus hyödyllisistä työkaluista, jotka voi valita yrityksen tarpeiden mukaan. Työssä havaittiin työkalujen ominaisuuksien suuri päällekkäisyys, joka vaikeutti konkreettisten suositusten luontia. Työssä myös arvosteltiin ELK Stackin ja Zabbixin käyttöliittymä, ominaisuudet, hinta ja dokumentaation laatu.

## **Avainsanat (asiasanat)**

Järjestelmävalvoja, järjestelmien valvonta, kyberturvallisuus, työkalu, poikkeamien hallinta, kyberturvallisuuskeskus

## **Muut tiedot (salassa pidettävät liitteet)**

**Hokkanen, Lari**

**System administrator's toolbox**

Jyväskylä: JAMK University of Applied Sciences, May 2024, 36 pages

Degree Programme in Information and Communications Technology. Bachelor's thesis.

Permission for open access publication: Yes

Language of publication: Finnish

**Abstract**

The goal of the thesis was to create a toolkit of suitable tools for system administrators, which could be used to improve companies' cyber security. There was no separate client for the thesis.

The aim of the thesis was to compare the available tools using reviews and recommendations from experts in the field. In addition, information was collected on the work tasks of system administrators and the structure and operation of security operations centers. The two tools, ELK Stack and Zabbix, were compared in more detail by installing the tool and testing their capabilities in alarming situations. The goals of the thesis also included highlighting utilities that can help system administrators in problem situations or in confirming hazards.

The thesis resulted in example structures for information security centers and a collection of system administrators' work tasks and how these tasks are performed. In addition, the thesis compiled a list of useful tools that can be chosen according to the company's needs. In the thesis, a large overlap of the features of the tools was observed, which made it difficult to create concrete recommendations. The user interface, features, price, and documentation quality of ELK Stack and Zabbix were also evaluated.

**Keywords/tags (subjects)**

System administrator, system monitoring, cybersecurity, tool, incident response, security operations center

**Miscellaneous (Confidential information)**

## Sisältö

<b>1</b>	<b>Johdanto .....</b>	<b>6</b>
<b>2</b>	<b>Järjestelmien valvonta .....</b>	<b>7</b>
2.1	Järjestelmävalvonnan tärkeys .....	7
2.2	Torjunta ja suunnitelmat .....	7
2.3	Valvojien työtehtävät .....	8
2.4	Valvontatyökalujen valinta .....	9
<b>3</b>	<b>Järjestelmävalvojien työtehtävät .....</b>	<b>10</b>
3.1	Työtehtävien tärkeys .....	10
3.2	Pienet yritykset .....	11
3.3	Keskikokoiset yritykset .....	12
3.4	Suuret yritykset .....	14
<b>4</b>	<b>Työtehtäviin käytettävät työkalut .....</b>	<b>15</b>
4.1	Avoimen lähdekoodin valvontatyökalut .....	15
4.2	ELK Stack vs Zabbix .....	18
4.2.1	ELK Stack .....	18
4.2.2	Zabbix .....	25
4.3	Kaupalliset yritystason valvontatyökalut .....	27
4.4	Muut aputyökalut .....	30
<b>5</b>	<b>Tulokset .....</b>	<b>32</b>
<b>6</b>	<b>Yhteenveto ja pohdinta .....</b>	<b>35</b>
	<b>Lähteet .....</b>	<b>38</b>

## Kuviot

Kuvio 1.	Prometheusin työpöytä. ....	16
Kuvio 2.	Grafanalla luotu työpöytä. ....	17
Kuvio 3.	ELK Stackin Kibana-pohjainen työpöytä .....	19
Kuvio 4.	Kibanan hakutoiminnon automaattinen täyttö. ....	21
Kuvio 5.	Suurin osa Kibanan visualisointityypeistä. ....	22
Kuvio 6.	Pieni osa ELK Stackillä tarjolla olevia valmiita integraatiomoduuleja .....	23
Kuvio 7.	Osa ELK Stackin dokumentaationsivuista .....	24
Kuvio 8.	Zabbixin oletustyöpöytä .....	26
Kuvio 9.	Zabbixin järjestelmätietoraportti .....	27
Kuvio 10.	Splunkin työpöytä. ....	29

Kuvio 11. LogRhythm-työkalun työpöytä.....	30
Kuvio 12. Virustotal-työkalun etusivu .....	32

## **Taulukot**

Taulukko 1. Tiivistelmä käsiteltyjen avoimen lähdekoodin työkalujen ominaisuuksista. ....	33
Taulukko 2. Arvioitujen työkalujen numeroarvosanat .....	34

# 1 Johdanto

Nykyisin kyberturvallisuuden tärkeys on kasvamassa entistä suuremmaksi. Yritykset suojautuvat joka päivä monilta turvallisuushkilta ja uusia turvallisuusaukkoja löytyy ohjelmista säännöllisellä tahdilla. Täydellinen suojautuminen näiltä riskeiltä on mahdotonta, joten järjestelmänvalvonta on erittäin tärkeässä asemassa kaikissa yrityksissä tietomurtojen havaintoa ja vahinkojen estoa varten. Valvontaan käytettäviä työkaluja on kuitenkin suuri määrä ja niiden luotettavuudesta ja toimintakyvystä ei ole paljoa helposti saatavilla olevaa tietoa.

Opinnäytetyön tarkoituksena oli kerätä kokoelma järjestelmänvalvontatyökaluja ja selvittää niiden toimivuutta ja soveltuvuutta jokapäiväiseen järjestelmänvalvontaan. Työn aikana kerättiin suosituksia toimivista työkaluista ja usein käytetyistä konsolikomennoista. Nämä tiedot kerättiin luotettavista lähteistä ammattilaisjärjestelmänvalvojilta sekä teorianlähteistä. Lisäksi kahta työkalua testattiin itse asentamalla ne ja testaamalla luomalla hälytyksiä käynnistäviä tapahtumia. Opinnäytetyöllä ei ollut erillistä toimeksiantajaa.

Opinnäytetyön tavoitteena oli luoda kerättyjen tietojen, suositusten ja arvostelujen avulla työkalupakki sopivia työkaluja ja skriptejä työssä käsiteltäviin työtehtäviin. Työn käsiteltävänä olevat työtehtävät rajattiin kyberturvallisuuteen liittyviin työtehtäviin ja työkaluihin. Käsittelyn alla oli Windows-käyttöjärjestelmän työkalut, joita käytetään kyberturvallisuuden ylläpitämiseen ja valvontaan yritysten ja muiden järjestöjen laitteistoverkoissa. Tavoitteena oli muodostaa kokoelma työkaluja, joita voi käyttää koventamaan kyberturvallisuutta yrityksissä, joissa tämä voi olla heikommalla kannalla.

Opinnäytetyö on tutkimuksellinen kehitystyö järjestelmänvalvonnan työkaluihin. Kehitystyössä kootaan kokoelma valvontaan käytettyjä työkaluja ja tutkitaan, miten niillä voi parantaa työelämää. Opinnäytetyössä tutkitaan käyttämällä kerättyjä materiaaleja, mitkä työkalut ja skriptit sopivat parhaiten käsittelyn alla oleviin työtehtäviin. Tutkimuksessa selvitetään vastaukset tutkimuskysymykseen: Millä työkaluilla järjestelmänvalvojat voivat parantaa järjestön kyberturvallisuutta ja miten sitä voi ylläpitää ja valvoa?

## 2 Järjestelmien valvonta

### 2.1 Järjestelmävalvonnan tärkeys

Järjestelmän valvonta on tärkeä osa nykypäivän tietoturvallisuutta vaativia tietoverkkoja. Tietoturvatapahtumien tapahtuminen on vain ajan kysymys ja organisaation tietoturvaa tullaan rikkomaan tai murtamaan. Tietoturvan parantamista varten on tärkeää ylläpitää ajan tasalla oleva ylläpitosuunnitelma, aktiivisesti havaita ja tunnistaa poikkeamia normaalista tilasta, minimoida tapahtuman aiheuttamaa vahinkoa, poistaa poikkeama järjestelmästä, ja palauttaa järjestelmä mahdollisimman hyvin normaalitilaan. (Kral 2012)

Järjestelmän valvonnan tärkein osa on luoda laaja ja yksityiskohtainen valmistelusuunnitelma tapahtumia varten. Suunnitelma määrittelee esimerkiksi toimenpiteet tapahtumien aikana, mahdollisia kovennostoimenpiteitä murtoriskien vähentämiseksi, yhteyshenkilöt, joilla on omat vastuut verkon eri alueilla ja muut vastaavanlaiset valmistautumismenetelmät. Parhain tapa ylläpitää tietoturvaa on välttää tietoturvaongelmien ilmestyminen niin usein kuin mahdollista.

### 2.2 Torjunta ja suunnitelmat

Tietomurtojen torjunnan voi jakaa kolmeen tärkeään vaiheeseen: tietomurron estämiseen, havaitsemiseen ja tutkintaan. Tietomurtojen estäminen on parhain tapa välttyä ongelmilta, mutta täydellinen esto on lähes mahdotonta. Murtoriskejä voi minimoida esimerkiksi hallitsemalla käyttöoikeuksia ja palvelimia, poistamalla peruskäyttäjiltä ylimääräiset oikeudet ja asentamalla ainoastaan työtehtäviin liittyvät ohjelmistot. Tietomurtojen havaitsemisessa on tärkeää onnistua mahdollisimman nopeasti, vahingon minimoimista varten. Havaitsemista voi tehostaa esimerkiksi hyvillä lokitiedoilla. Tietomurron tutkinta havainnon jälkeen on tärkeää, jotta tapaus ei toistu tulevaisuudessa. Tutkinnan aikana ilmoitetaan murrosta viranomaisille, eristetään ja karkotetaan tunkeutuja ja varmistetaan että sama murtautumistapa ei toimi tulevaisuudessa. (Opas tietomurtojen havaitsemiseen 2020)

Tutkinnon jälkeen järjestelmänvalvojien tehtävänä on myös koventaa järjestelmää murtoriskin minimoimiseksi. Murtoon johtaneen vahingoittuvaisuuden paikkaamisen lisäksi on tärkeää suojau-

tua muilla tavoilla, kuten esimerkiksi ylläpitämällä automaattisia päivityksiä ohjelmistojen turvallisuuden ylläpitoa varten, varmuuskopioida tärkeät tiedostot ja käyttämällä monivaiheista tunnistautumista. Hyökkäykset järjestelmään vaativat usein käyttökelpoiset tunnukset, jotka hyökkääjä on hankkinut esimerkiksi kalastuksella, joten monivaiheinen tunnistautuminen voi olla tehokas estokeino välttämään murtautumisia. Varmuuskopiointi estää lähes kaiken vahingon, jota voi aiheutua kiristysohjelmista. (Opas tietomurtojen havaitsemiseen 2020; Pienyritysten kyberturvallisuusopas 2020)

Minkään järjestelmän valvontasuunnitelma ei ole kuitenkaan täydellinen. Kuten Kral (2012) mainitsee, järjestelmätapahtumat voivat olla laajuudeltaan monenlaisia, pienistä sähkökatkoksista tai komponenttivioista, vakaviin hakkereiden tai vanhojen työntekijöiden suorittamiin tietoturvarikkomuksiin. Tämän laajan vakavuustasojen vaihtelevuuden takia, tapahtumien tunnistaminen ja oikea kategorisointi on järjestelmävalvojien yleisimpiä vastuita. Lisäksi samaa mieltä on myös Tietoturvakeskus, joka kannustaa tunnistamisen tehostamista varten keräämään runsaasti lokitietoja järjestelmän tapahtumista. (Kral 2012; Opas tietomurtojen havaitsemiseen 2020)

## 2.3 Valvojien työtehtävät

Tapahtumia voidaan havaita monin eri tavoin. Havaintojärjestelmiä voi olla esimerkiksi automaattiset järjestelmätilanteen kirjausjärjestelmät, jotka voivat ilmoittaa ja kirjata epäilyttäviä kirjautumisyhteyksiä tai palvelimen kaatumisia. Havaintoja varten voi myös olla hyödyksi neuvoa ja kouluttaa käyttäjiä rohkeasti ilmoittamaan palvelun epätavallisesta käyttäytymisestä järjestelmävalvojille. Näissä tapauksissa on myös hyvä ilmoittaa käyttäjien käyttökokemuksiin tai turvallisuuteen vaikuttavista tapauksista kaikille käyttäjille esimerkiksi sähköpostilla turhien ilmoitusten vähentämiseksi ja turvallisuuden lisäämiseksi.

Suuret yritykset saattavat käsitellä niin paljon dataa, että normaalit valvontamenetelmät eivät ole riittäviä. Yritykset, joilla on valvontaa varten keskitetty tietoturvallisuuskeskus (Security Operations Center eli SOC) voivat käyttää datavirran valvontaa varten turvallisuustiedon ja -tapahtumien käsittelytyökaluja (Security Information and Event Management eli SIEM). SIEM-työkalut toimivat parhaissa olosuhteissa keinona antaa suhteellisen pienelle valvontatiimille mahdollisuus suodattaa ja analysoida massiivisia määriä verkkoliikennettä, jota suuren yrityksen ylläpito tuottaa. Sen li-

säksi, SIEM-työkalut auttavat myös varmistamaan varoitusten todenmukaisuuden, sekä valitsemaan sopivan vastauksen mahdollisiin tapauksiin. (Knerler, Parker & Zimmerman 2022, s. 243–245)

Päätelaitteet ovat usein verkoston heikoin lenkki. Järjestelmänvalvojien vastuulla on usein myös valvoa päätelaitteita ja niiden turvallisuutta. Jos yrityksen työntekijät käyttävät omia laitteita työympäristössä, turvallisuusprotokollat ja ohjeistukset ovat tärkeitä sujuvan kyberturvallisuusympäristön ylläpitämiseksi. Mahdollisten kolmannen osapuolten, kuten esimerkiksi tavarantoimittajien laitteiden turvallisuuden ylläpito on hankalampaa. He voivat mahdollisesti käyttää vanhentuneita ohjelmistoja tai laitteita, joita järjestelmänvalvojat eivät voi ylläpitää. Jos haavoittuvainen laite ottaa yhteyden suoraan työverkkoon, se voi mahdollisesti tartuttaa haittaohjelmia muihin verkon turvallisiin laitteisiin. (Alcon 2017)

Itse päätelaitteiden turvallisuuden lisäksi järjestelmävalvojat kouluttavat ja tarkkailevat päätelaitteiden käyttäjiä. Erityisen vaarallista pienenkokoisille yrityksille voi olla tietojenkalastelu, aidolta vaikuttavat viestit, joiden tarkoituksena on saada käyttäjä syöttämään tärkeitä tietoja hyökkääjän verkkosivulle, joka on naamioitu jonkin oikean organisaation sivuksi (Pienyritysten kyberturvallisuusopas 2020). Kyberturvallisuuskeskus suositteleeikin suojautumaan kalastelulta esimerkiksi sähköpostisuodatuksella ja kouluttamalla työntekijöitä tunnistamaan epäilyttävät viestit.

## **2.4 Valvontatyökalujen valinta**

Työkalujen valinta on myös tärkeätä. Turvallisuuden vahvistamista varten käytetään usein työkaluja, joiden vakuutetaan olevan turvallisia. Kuitenkin työkalut, joita kehuttiin tutkimuksilla, jotka väittivät todistavan käytetyn suojausteorian turvallisuuden, pystyttiin murtamaan jopa seitsemän minuutin sisällä (Wilson & Kiy 2014). Kaupalliset työkalut usein liioittelevat turvallisuusominaisuuksiaan ja suojauskeinojaan. Lisäksi turvallisten työkalujen väärinkäyttö voi luoda uusia vaaroja, vaikka työkalu itse olisi turvallinen. Tämän takia työn tavoitteena on suositella hyödyllisiä työkaluja, jotka vastaavat turvallisuusodotuksia ja käyttötarkoituksia.

Sekä Wilson ja Kiy (2014) että Knerler, Parker ja Zimmerman (2022) suosittelevatkin tutkimaan yrityksen kyberturvallisuustarpeita ja käyttämään ainoastaan yrityksen käyttötarkoituksiin soveltuvia työkaluja. Pienten yritysten ei tarvitse käyttää suuria tietoturvallisuuskeskustyökaluja ja kuten

Knerler ja muut varoittavatkin, ylimitoitettut työkalut pahimmassa tapauksessa heikentävät turvallisuutta hidastamalla pienen turvallisuustiimin työskentelynopeutta nostamalla työmäärää. Wilson ja Kiy puolestaan suosittelevat tutkimaan tarkasti käytettyjen työkalujen ja suojauskeinojen synergiaa. Heidän mukaansa järjestelmän turvallisuus voi heikentyä, jos huonon puolustuskeinon murtuminen auttaa hyökkääjiä kiertämään muut työkalut ja puolustukset. (Knerler, Parker & Zimmerman 2022; Wilson & Kiy 2014)

### 3 Järjestelmävalvojen työtehtävät

#### 3.1 Työtehtävien tärkeys

Järjestelmävalvojat ovat tärkeässä roolissa kyberturvallisuuden kannalta kaikissa yrityksissä. Nykypäiväisin internetin kautta voi kohdistua kaikkiin yrityksiin monenlaisia haittaongelmia ja tunkeutumisyrittäjiä. Vaikka kyberturvallisuusinsinöörit ylläpitäisivätkin tehokkaita ja ajantasaisia torjuntakeinoja yrityksen verkoissa, mikään järjestelmä ei ole murtovarma. Mistä tahansa järjestelmästä voi löytyä niin kutsuttu nollapäivähaavoittuvuus (zero-day-vulnerability), mikä tarkoittaa haavoittuvuutta, jota ei ole havaittu ja johon ei ole kehitetty puolustuskeinoja.

Nollapäivähaavoittuvuuksia vastaan on mahdoton puolustautua täydellisesti, joten järjestelmävalvojat ovat tärkeä osa yritysten kyberturvallisuustiimiä minimisoimaan haavoittuvuuden aiheuttamaa vahinkoa tarkkailemalla mahdollisia tunkeutumisen merkkejä. Esimerkkinä voisi käyttää 2024 maaliskuussa löydettyä *xz utils* pakkauskirjastossa ollutta takaporttia. Hyökkääjä oli saanut kirjaston koodaajien luottamuksen lähettämällä monien vuosien aikana normaaleja ja hyödyllisiä koodimuutosehdotuksia, kunnes hän piilotti takaportin avaavan koodin yhteen muutokseensa (Pyyny 2024). Tämän nollapäivähaavoittuvuuden mahdollisilta vahingoilta pystyi ainoastaan suojautumaan valvomalla haavoittuneita järjestelmiä aktiivisesti. Takaportti havaittiin onneksi sattumalta nopeasti, mutta jos hyökkääjät olisivat voineet käyttää takaporttia, ainoa tapa suojautua vahingoilta olisi ollut aktiivinen järjestelmän valvonta.

Järjestelmävalvojen organisaatio vaihtelee heidän työtehtävien ja lukumäärän mukaan. Pienet yritykset eivät usein palkkaa suuria määriä tietotekniikkatyöntekijöitä, joten järjestelmävalvojat usein hoitavat muita työtehtäviä samanaikaisesti. Suuret yritykset voivat organisoida järjestelmän

valvojat keskitettyihin kyberturvallisuuskeskuksiin, joiden kautta he voivat organisoida suuria data-virtoja käyttäen organisaatioille tarkoitettuja SIEM- ja SOAR-työkaluja. Näiden kahden koon ja ratkaisun välissä keskikokoiset valvontaryhmät, joissa työskentelee yhteensä noin 10 järjestelmävalvojaa, yleensä järjestäytyvät yksinkertaistettuihin ja tiivistettyihin pienryhmiin heidän työtehtävien ja työkalujen mukaan.

### **3.2 Pienet yritykset**

Järjestelmävalvojien työtehtävät voivat vaihdella huomattavasti yrityksen koon perusteella. Pienillä yrityksillä ei usein ole tarvetta kokonaiselle tietoturvaluustimille, joten järjestelmävalvojat joutuvat usein työskentelemään pienessä ryhmässä tai jopa yksin. Pienen käyttäjämäärän hallintaan ei kuitenkaan ole tarve kovin isoille tai monimutkaisille työkaluille, joten pienetkin järjestelmävalvontaryhmät ja pelkät avoimen lähteen työkalut voivat riittää.

Kaiken kokoiset yritykset tarvitsevat kyberturvallisuutta ja järjestelmävalvontaa, jos heillä on käytössä pienikin internetiin yhdistetty tietokonejärjestelmä. Pienet yritykset voivat tietomurron aiheuttamien menetysten jälkeen pahimmassa tapauksessa joutua konkurssiin resurssien puutteen takia. Järjestelmän valvonnalla voi välttyä järjestelmään suorasta tunkeutumisesta.

Pienten yritysten suurin uhka on yleensä kuitenkin tietojenkalastelu. Järjestelmävalvojien työtehtävänä on suojella yritystä valvomalla sähköpostiliikennettä ja suodattamalla suurin osa kalastelusta hyvin määritetyllä roskapostisuodattimella. Lisäksi henkilökunnan kouluttaminen havaitsemaan tietojenkalastelun tunnusmerkit voi estää roskapostisuodatuksen ohittaneen kalastelun onnistumisen. Tämä myös kuuluu usein järjestelmävalvojien työtehtäviin, etenkin pienissä yrityksissä, joissa ei ole varaa kokonaiselle itsenäiselle järjestelmävalvontayksikölle.

Sähköpostin valvontaan voi käyttää sähköpostisovellusten omien toimintojen lisäksi erillistä sähköpostipalvelinta. Omalla palvelimella voi hyödyntää tehokkaampia palvelinpuolisia työkaluja ja halutessaan kirjoittaa omia roskapostinsuodatussääntöjä. Lisäksi kouluttamista varten voi hyödyntää oman palvelimen avulla lähetettyjä testiviestejä, joilla voidaan testata kuinka hyvin työntekijät ovat sisäistäneet kalastelunestokoulutuksen. Testiviesti voi olla esimerkiksi järjestelmävalvojan

itse tekemä kalasteluviesti, joka vie käyttäjän hyökkäyssivun sijasta sivulle, joka varoittaa käyttäjää, että he olivat langenneet kalastelun uhriksi. Viestin linkin klikanneet käyttäjät voidaan tarvittaessa kutsua lisäkoulutukseen.

Pienillä yrityksillä on harvoin tarvetta täydelle tietokoneverkostolle keskitetyn toimialueen hallintakoneen (Domain Controller) kera. Tämän takia järjestelmänvalvojat ovat pienissä yrityksissä usein vastuussa laitteiston asennuksesta tai palomuurin ylläpidosta. Tämä voi usein tuoda ylimääräistä kuormitusta heidän työpäiviinsä, mutta verkoston yksinkertaisuus voi myös helpottaa järjestelmänvalvontaa. Pienten yritysten valvontaan voi riittää ainoastaan kevyiden avoimen lähdekoodin valvontalaitteiden käyttö ja valvonnan voi monissa tapauksessa suorittaa suoraan IT-vastaavan omalta tietokoneelta.

Lisäksi järjestelmänvalvojilla voi usein olla vastuulla palomuurin ylläpito. Palomuurin asettaminen, valvominen, ja ylläpito ovat tärkeitä osia kyberturvallisuuden ylläpidosta. Pienillä yrityksillä ei ole välttämättä resursseja kovin yksityiskohtaiseen palomuurijärjestelmään, mutta heillä ei usein ole tälle tarvettakaan. Yrityksen pienestä koosta voi myös olla hyötyä palomuurin asetusten tehostamisesta. Palomuurin voi esimerkiksi asettaa estämään kaikki yhteydet ulkomailta, koska pienillä yrityksillä ei ole usein ulkomaalaisia kumppaneita, joiden tarvitsisi yhdistyä järjestelmään.

### **3.3 Keskikokoiset yritykset**

Keskikokoisten yritysten työtehtävät ovat laajalti samanlaiset verrattuna pieniin yrityksiin. Suurempi käyttäjämäärä vaatii kuitenkin keskitetyn järjestelmänvalvontaorganisaation. Kun käyttäjien luoma liikenne verkostossa on liian monimutkaista yhden järjestelmävalvojan käsiteltäväksi, organisaatiot perustavat tietoturvakeskuksen, jonka vastuulla on hoitaa järjestelmien valvonta. Tietoturvakeskus koordinoi ja keskittää useiden valvojien työtehtävät ja ilmoittavat tapahtumista käyttäjille ja johtoportaalle.

Tietoturvakeskuksen koko voi vaihdella työntekijöiden lukumäärän perusteella. Keskikokoiset organisaatiot eivät yleensä tarvitse monimutkaista työnjakoa. Alle kahdenkymmenen työntekijän kokoinen tietoturvakeskus voi toimia sujuvammin, jos sen jakaa yksinkertaisesti johtoon, valvontaan ja verkoston rakenteeseen vastuussa oleviin osastoihin (Knerler, Parker & Zimmerman 2022, s. 61–62). Nämä osastot eivät välttämättä ole tiukkoja rajauksia, etenkin pienemmillä valvojamäärillä,

mutta ne antavat rakennetta tietoturvakeskukselle ja auttavat valvojia priorisoimaan omia työtehtäviään.

Keskuksen johtoportaahan työtehtävänä on valvoa ja koordinoida muita järjestelmänvalvojia. He tekevät strategisia päätöksiä työtehtävien ja tapausten tärkeysasteista ja järjestävät muiden osastojen työntekijät työmäärän mukaan. Heidän vastuullansa on kommunikoida yrityksen johtajien kanssa ja tiedottaa heille tietoturvakeskuksen toiminnasta ja sen tärkeydestä. Lisäksi vastuuksiin voi kuulua ilmoittaa yrityksen työntekijöille häiriöistä tai turvatapahtumista, sekä niiden ratkaisusta.

Valvontaosion vastuulla on suurin osa itse järjestelmävalvonnan työtehtävistä. Tämän vuoksi, se on lähes aina suurin osasto tietoturvakeskuksesta. Heidän tehtävänä on valvoa verkkoliikennettä ja tietokoneiden tapahtumia, käyttäen keskuksen SIEM- ja SOAR-työkaluja. Jos järjestelmässä on havaittu mahdollinen tunkeutuminen, haittaohjelma tai muu tietoturvamurros, heidän vastuullansa on koordinoida tehtävät uhkan eristämistä ja poistamista varten, sekä järjestelmän normaali-tilaan palautuminen.

Uhkien eristäminen on tärkeä tehtävä vahingon minimisointia varten. Kun uhka on havaittu ja vahvistettu, sen leviäminen tai vahingon aiheuttaminen täytyy pysäyttää mahdollisimman nopeasti. Esimerkiksi, jos verkostossa on havaittu haittaongelmia, niiden leviämisen muihin verkoston laitteisiin voi estää katkaisemalla vaikutettujen laitteiden yhteyden internettiin. Tämän jälkeen uhkan poistamisen voi aloittaa turvallisesti.

Uhkatapahtuman jälkeen valvontaosion täytyy palauttaa järjestelmä normaalitilaan. Heidän tehtäviinsä kuuluu verkoston tarkkailu uhkan täydellisen poiston vahvistamiseksi. He voivat aloittaa uhkan käyttämän haavoittuvuuden etsimisen ja haavoittuvuuden korjaussuunnitelman laatimisen. Haavoittuvuuden korjaaminen on myös heidän vastuullansa, mutta jos verkoston rakennetta tai työkaluja tarvitsee muokata, he voivat lähettää suunnitelmat verkoston rakenne -osastolle.

Rakenneosaston tarkoituksena on olla vastuussa tietoturvakeskuksen työkaluista ja verkoston rakenteesta. He varmistavat, että työkalut ovat ajan tasalla, asentavat tarvittavat ohjelmistot käyttäjille ja ylläpitävät valvontaohjelmistojen valvoja-agentteja. Agentit ovat ohjelmia, jotka toimivat

SOAR- ja SIEM-työkalujen valvojina käyttäjien päätelaitteilla, tallentaen verkkoliikennettä ja tietokoneiden turvallisuustapahtumia. Jos ohjelmistoa tarvitsee muuttaa turvallisuusongelman korjaamiseksi, se on myös heidän vastuullansa.

### 3.4 Suuret yritykset

Suurten yritysten liikennemäärä on niin laaja, että tietoturvakeskus voi kasvaa työntekijämäärältään pienen yrityksen kokoiseksi. Tämä vaatii koordinoinnin korostamista ja tehokkaampien laitteiden käyttöä. Suuret yritykset jakavat usein tietoturvakeskukset pienempiin osioihin, jotka ovat tiukemmin eritelty toisistaan keskikokoisiin yrityksiin verrattuna. Suuren työmäärän takia turvakeskusten jäsenet erikoistuvat omien työtehtävien suorittamiseen ja heillä ei ole hätätilanteiden ulkopuolella aikaa avustaa muita osioita.

Työntekijöiden erikoistuminen johtaa laajempaan rakenteeseen verrattuna keskikokoiseen yrityksen tiiviimpään turvakeskusten rakenteeseen. Jokainen työntekijä suorittaa omaa työtehtäväänsä omassa osiossa, jotka ovat jaettu omiin kategorioihin osion työntekijöiden tehtävien mukaan. Osioiden tarkka jakaminen voi vaihdella yrityksen tarpeiden mukaan, mutta esimerkkinä turvakeskusten voi jakaa johto- ja hallintaosioon, tapahtumien analyysi- ja ratkaisuosioon, järjestelmien valvontaosioon, turvallisuus- ja järjestelmärakennearkenteeseen ja tilannevalvonta- ja kommunikaatioosioon. (Knerler, Parker & Zimmerman 2022, s. 56–60)

Johto- ja tilannevalvontaosasto toimivat samoin tavoin kuin keskikokoisissa yrityksissä, mutta osa heidän työtehtävistään on siirretty tilannevalvontaosiolle. Johtoporras työskentelee tilannevalvonta- ja kommunikaatio-osion kanssa, jotka valvovat käynnissä olevia tilanteita ja tapauksia ja kommunikoivat yrityksen työntekijöiden ja turvakeskusten jäsenten kanssa. He antavat keskitettyjä viestejä ja tilannepäivityksiä tietoturvatapahtumien vaikutuksista järjestelmiin ja niiden ratkaisuista. Lisäksi heidän vastuullansa on valvoa yrityksen työntekijöiden tietoturvakoulutusta.

Järjestelmien valvontaosio keskittyy itse järjestelmän valvontatyöhön. He etsivät järjestelmästä tunkeutumisen merkkejä, tarkastavat valvoja-agenttien luomia varoituksia ja lähettävät todennetut vaarat analyysi- ja ratkaisuosiolle. Valvontaosion tehtävänä on pysyä ajan tasalla uusista varoituksista ja kerätä ja organisoida mahdolliset merkit tunkeutumisesta, keskittyen näiden merkkien lopputulokseen. Kuten Knerler ja muut (2022) mainitsevatkin, tunkeutumismerkkejä ei pidä kerätä

pelkän keräämisen vuoksi, vaan ne täytyy ymmärtää kokonaisuutena ja lähettää muille osastoille omassa kontekstissaan.

Analyysi- ja ratkaisuosio keskittyy toteuttamaan tietoturvakeskuksen tärkeimmät toiminnot. Heidän tehtävinään on tehdä alustava analyysi järjestelmien valvontaosion lähettämiin tapauksiin ja selvittää mahdolliset ratkaisukeinot. Suurella yrityksellä voi olla monia tapauksia ja tutkimuksia käynnissä samaan aikaan, joten analyysi- ja ratkaisuosio voi olla suhteelliselta kooltaan muita osioita huomattavasti suurempi keskikokoisten yritysten osioihin verrattuna.

Turvallisuus- ja järjestelmärakenneosio on vastuussa työkalujen valvoja-agenteista, verkoston turvallisuudesta ja työkaluista. Jos tietoturvakeskus on vastuussa omista työkaluistaan ja muista kalusteresursseistaan, ne voi keskittää itse keskuksen tarpeisiin. Tarvittavat muutokset järjestelmän rakenteeseen tai turvallisuuspäivitykset voi suorittaa mahdollisimman nopeasti. Muiden turvakeskuksen jäsenten ei myös tarvitse työskennellä mahdollisten tarpeettomien työkalujen tai ominaisuuksien ympäri, jos keskus on vastuussa ainoastaan keskuksen tarpeiden mukaisten työkalujen asennuksesta.

Suurimmalta osin suurten yritysten työtehtävät eivät eroa laajalti keskikokoisesta yrityksestä. Suuri tietomäärä korostaa kuitenkin koordinaatiota, organisaatiota ja etenkin sujuvaa kommunikointia eri osastojen välillä. Järjestelmän valvojien täytyy olla myös valmiina käsittelemään useita tapauksia yhtäaikaaisesti ja pystyä jakautumaan näiden tapausten ratkaisua varten omiin ryhmiin. Jotkut järjestelmän valvojat jokaisesta turvakeskuksen osiosta voivat olla vastuussa tilannekuvan lähettämisestä johtoportaalille tai tilannevalvontaan. Suuressa yrityksessä on erityisen tärkeitä pitää kaikki työntekijät ajan tasalla.

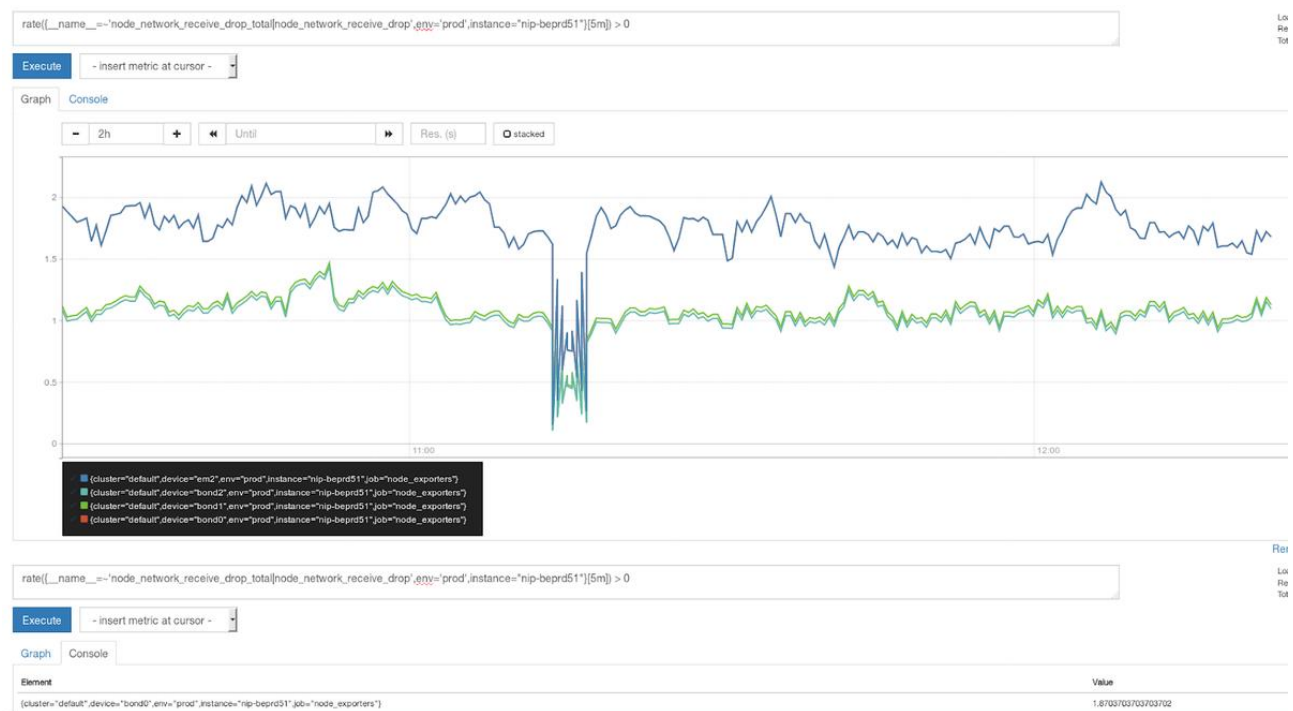
## **4 Työtehtäviin käytettävät työkalut**

### **4.1 Avoimen lähdekoodin valvontatyökalut**

Avoimen lähdekoodin työkalut ovat usein sopivia pienten ja keskikokoisten yritysten käyttötarkoituksiin. Nämä työkalut ovat ilmaisia ja monipuolisia ja niiden avoin lähdekoodi parantaa luotettavuutta ja läpinäkyvyyttä. Monilla työkaluilla on myös saatavilla maksullinen yritysversio, joka voi

helpottaa laajentamista, mikäli alkuperäisen työkalun ominaisuudet eivät riitä työtehtävien suorittamiseen yrityksen laajenemisen takia.

Jos yritys käyttää konttiorjestelmistöjä, kuten Dockeria tai Kubernetesia, hyvä työkalu konttien valvontaa varten on Prometheus. Tämä Soundcloudin alun perin kehittämä työkalu voi valvoa verkon käyttötilastoja, konttiympäristön tapahtumia ja kokoaa tämän datan helposti haettaviin tilastoihin. Tätä dataa voi tarkkailla ja hakea käyttämällä joko Prometheusin omaa PromQL hakukieltä tai käyttämällä työpöytäkoorisohjelmaa, kuten Grafanaa, jonka kanssa Prometheusilla on hyvät integraatiomahdollisuudet. Kuten kuviossa 1 näkyy, työpöytä ilman erillistä työpöytäohjelmaa on hyvin yksinkertainen ja kaaviointimahdollisuuksia ei ole paljoa. Prometheusin mahdollisia haittapuolia voi olla lyhyt 14 päivän datansäilytys ja moniprosessisten ohjelmien monitoroinnin vaikeus. (Top 5 Open Source Server Monitoring Tools 2023; Wilson & Gupta 2023.)



Kuvio 1. Prometheusin työpöytä. (Top 5 Open Source Server Monitoring Tools 2023)

Grafana on vaihtoehtoinen työpöytätyökalu, jota voi käyttää Prometheusin kaltaisten työkalujen, joilla ei ole omia hyviä työpöytäominaisuuksia. Sitä voi myös halutessaan käyttää korvaamaan muidenkin työkalujen työpöydän, jos ne jostain syystä eivät sovi käyttötarkoitukseen tai Grafanan työ-

pöytä vaikuttaa muuten paremmalta. Grafana mahdollistaa täysin muokattavan työpöydän rakentamisen, johon voi asettaa paneeleja, jotka sisältävät käyttäjän haluavan kaavion, jolla voi visualisoida dataa. Paneeleja on tarjolla runsaasti eri vaihtoehtoja ja työkalu tukee lähes kaikkia dataformaatteja käsittelyä varten. Grafanalla voi myös yhdistää tietoja useasta lähteestä, jos yritys käyttää useampaa valvontatyökalua eri käyttötarkoituksia varten. Esimerkki Grafanalla luodusta työpöydästä näkyy kuviossa 2. Grafanalla voi luoda hälytyksiä, kuten muilla valvontatyökaluilla, mutta se ei kerää itse ollenkaan dataa, joten se täytyy yhdistää muiden valvontatyökalujen kanssa.



Kuvio 2. Grafanalla luotu työpöytä. (Top 5 Open Source Server Monitoring Tools 2023)

ELK Stack (Elasticsearch, Logstash, Kibana) on kokoelma luotettavia ja pitkään aktiivisesti kehitettyjä avoimen lähdekoodin työkaluja, jotka työskentelevät keskenään luodakseen kattavan valvontatyökalun. Elasticsearch toimii työkalun datasäiliönä, jota voi hakea monipuolisesti halutulla tavalla, kuten pelkällä tekstillä tai JSON-pyyynnöillä. Lisäksi se tarjoaa ELK Stackin valvonta- ja turvallisuusominaisuudet, sekä hälytystoiminnot. Logstash kerää ja järjestee verkoston datan Elasticsearchiin lähettämistä varten ja Kibana toimii pääosin kerätyn datan visualisointityökaluna. ELK Stack voi kuitenkin olla hankala ja aikaa kuluttava asentaa järjestelmään.

Verrattuna Prometheusiin, ELK Stack toimii paremmin datan säilyttämistä varten pitkällä kannalla. ELK Stack voi myös prosessoida suuria datamääriä paremmin ja luotettavammin kuin Prometheus. Molemmilla työkaluilla on kuitenkin omat tarkoituksensa ja yritykset käyttävät tarvittaessa kumpaakin työkalua riippuen työtehtävästä. ELK Stack soveltuu paremmin tallentamaan tapahtumalokkeja ja tarkkailemaan syvästi yksittäisiä järjestelmätapahtumia. Prometheus on yksinkertaisempi käyttää ja asentaa ja soveltuu parhaiten luomaan tapahtumatilastoja kerätystä datasta. (Prometheus vs. ELK 2023.)

Zabbix on monipuolinen vaihtoehto valvontaa varten. Sillä voi suorittaa monipuolisesti verkoston, palvelimien, sovellusten ja palveluiden sekä pilviympäristön valvontaa. Zabbix on myös nopea asentaa ja tukee yritystason laajentamista ja datan keräystä käyttämällä Zabbix-välittäjiä. Nämä ominaisuudet antavat Zabbixille uniikin edun aloittaville yrityksille. Työkalun käytön voi aloittaa ilmaiseksi pienellä pinta-alalla, jota voi laajentaa yrityksen kasvun rinnalla luomalla lisää Zabbix-välittäjiä keräämään tietoja uusista osastoista tai työntekijöiltä. Työkalun asiakastuki on kuitenkin suurimmalta osin maksullinen. (Explore Zabbix features n.d; Wilson & Gupta 2023.)

## **4.2 ELK Stack vs Zabbix**

### **4.2.1 ELK Stack**

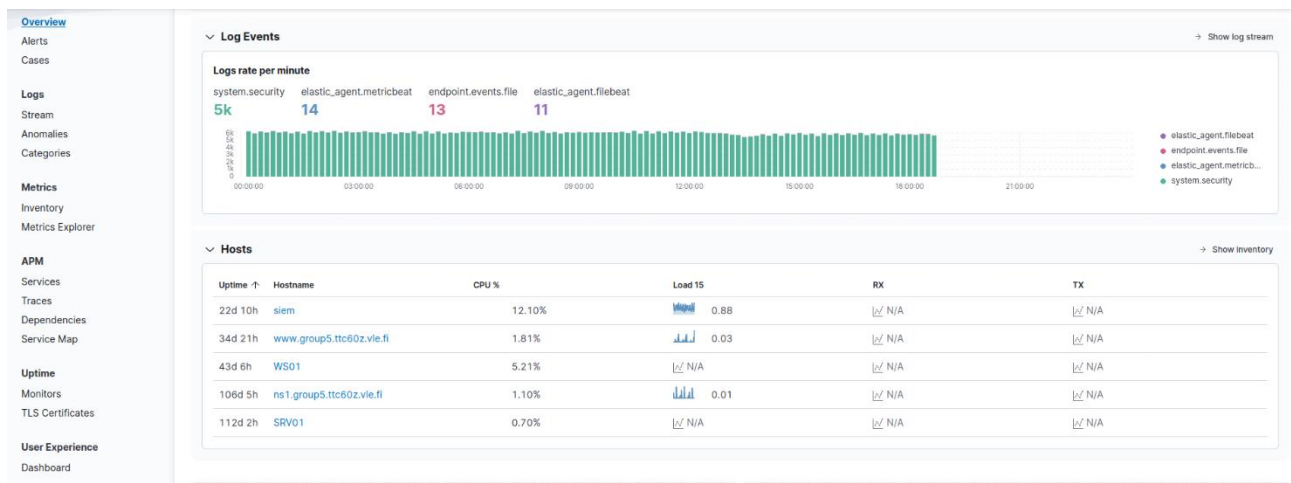
Työssä vertaillaan tarkemmin Zabbixin ja ELK Stackin ominaisuuksia. Molemmat työkalut ovat SIEM-työkaluja, joita käytetään valvomaan verkostojen laitteita epäilyttäviä toimenpiteitä ja liikennettä varten. Työkalut käyttävät samanlaisia menetelmiä valvontaan ja toimivat samanlaisissa ympäristöissä samantapaisesti. Tavoitteena on arvioida, kumpaa työkalua on parempi käyttää tietyissä tilanteissa. Työkalut valittiin vertailuun suositusten ja käyttötarkoitusten samantapaisuuden takia.

Työkalut arvioidaan perustuen, kuinka hyvin seuraavat arviointikriteerit toteutuivat niiden käytön aikana. Työkalun tehokkuus valvonnassa ja tehtävien suorittamisessa on todennäköisesti tärkein kriteeri. Jos työkalu ei voi suorittaa työtehtäviä sujuvasti, sen muista hyvistä ominaisuuksista ei ole paljoa hyötyä. Lisäksi työkalun käyttöliittymä ja helppokäyttöisyys on tärkeä osa työkalun laadusta. Jos tehtävien suoritus hidastuu huomattavasti huonon käyttöliittymän takia, se voi häiritä ongel-

matilanteen ratkomista kriittisillä hetkillä tietoturvatapahtumien aikana. Lisäksi arviointiin vaikuttaa dokumentaation laatu ja työkalun hinta, jotka ovat tärkeitä toissijaisia kriteereitä yritysten päätösten teossa.

ELK Stack ja Zabbix ovat molemmat valvontatyökaluja, joiden avulla voi tarkkailla verkoston laitteita asentamalla niille valvoja-agentin, joka lähettää kerätyn datan keskeiselle palvelimelle. ELK Stackin voi asentaa itsenäisesti ja ilmaiseksi omille palvelimille käytettäväksi. Tämä asennus- ja konfiguraatioprosessi on kuitenkin monimutkaista ja vaikeata, koska ELK Stack koostuu monesta erillisistä työkaluista, jotka tekevät yhteistyötä toimivana SIEM-kokonaisuutena. Vaihtoehtona on myös vuokrata työkalun valmistajalta Elasticilta pilvipalvelun, joka hoitaa työkalun asentamisen, isännöinnin ja ylläpidon. Tämä pilvipalvelu maksaa palvelutason mukaan 95 \$ - 175 \$ kuukaudessa.

ELK Stackin käyttöliittymä, josta näkyy esimerkki alla olevassa kuviossa 3, on monipuolinen datan kokoamistyökalu Kibana. ELK Stack käyttää Elasticsearch-työkalua tallentamaan ja kokoamaan kerättyä dataa tietokantaan. Nimensä mukaisesti Elasticsearch myös suorittaa tietohakuja tästä tietokannasta, mutta itse tietojen keräys agenteilta on Stackin viimeisen työkalun, Logstashin vastuulla.



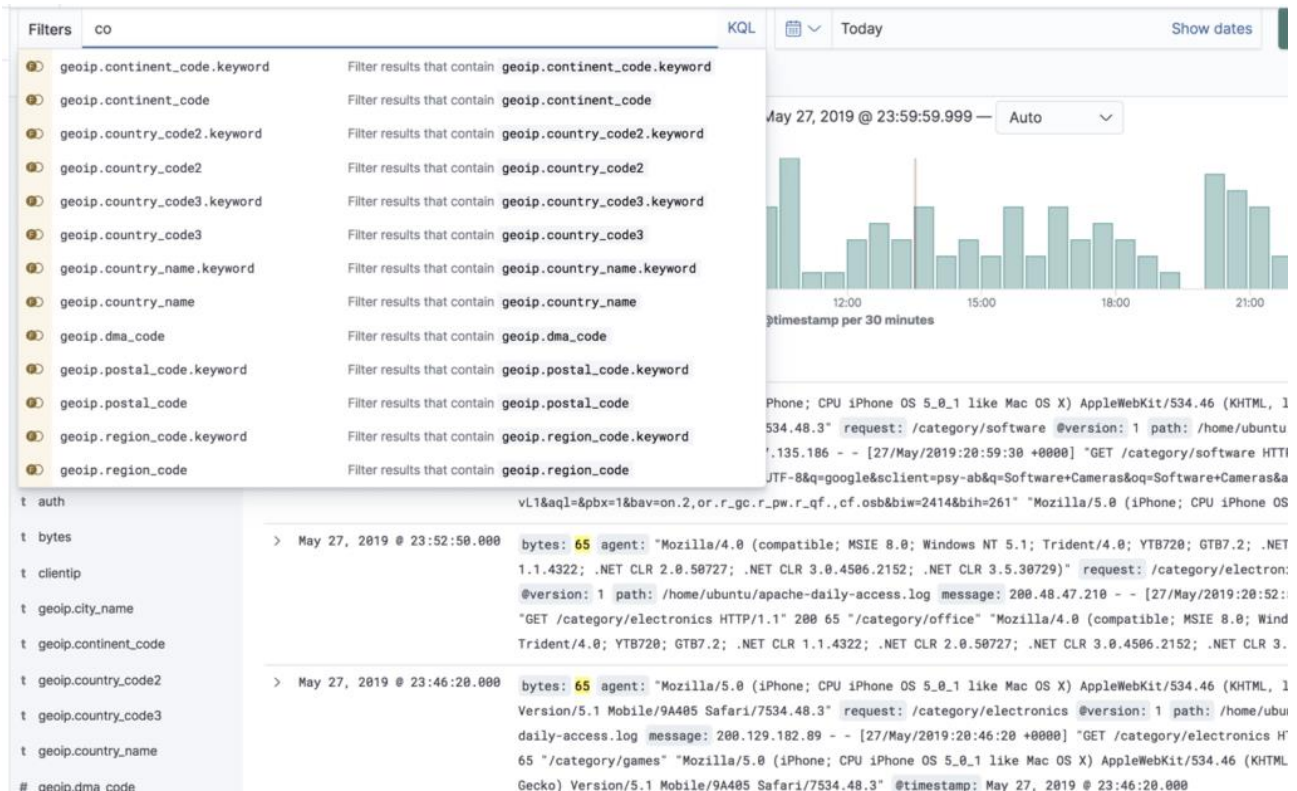
Kuvio 3. ELK Stackin Kibana-pohjainen työpöytä

Nämä työkalut toimivat yllättäen hyvin teknisellä tasolla valvontaa varten, mutta Kibanan käyttöjärjestelmä voi olla monimutkainen käyttää ja sisältää paljon erilaisia ominaisuuksia, joita ELK Stack on kerännyt kehityksen aikana. Laaja määrä ominaisuuksia on hyvä puoli monissa tapuksissa,

mutta Kibanan käyttöliittymä ei ole kehittynyt samaa tahtia. Suuri osa ominaisuuksista on piilossa epämääräisten alivalikkojen ja välilehtien takana. Kun ominaisuudet löytyvät, ne toimivat hyvin, mutta Kibana ei myöskään erottele ollenkaan käytössä olevien, konfiguroimattomien ja rahamuurin taakse lukittujen ominaisuuksien välillä.

Logstash voi kerätä dataa ilman erillistä järjestelyä helposti kaikista verkoston laitteista ja agenteista. Nämä järjestelmälokit, palvelinlokit, verkkosivulokit ja muut vastaavat tiedot voi käsitellä käyttäen Kibanaa visualisoiduiksi kuvioiksi. Datan voi järjestellä trendeiksi, interaktiivisiksi taulukoiksi tai automaattisiksi työpöydiksi. Kibana jopa tukee datan sijoittamiseksi sijainnin mukaan kartalle, jota voi käyttää esimerkiksi IP-blokkien luomiseksi, jos yhdestä sijainnista saapuu huomattavasti roskapostia tai hyökkäyksiä.

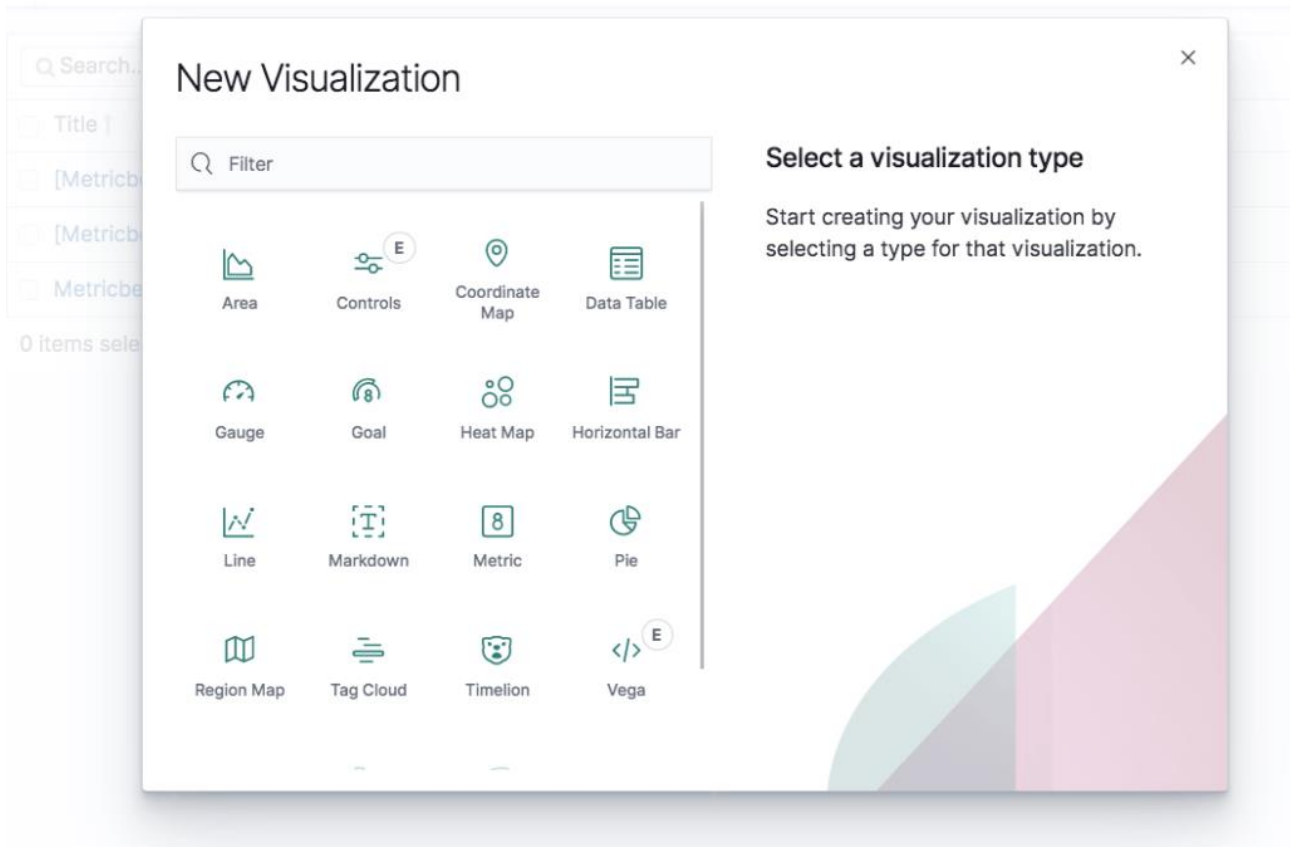
Tapahtumista ja hälytyksistä voi luoda tapauksia, joiden avulla voi koordinoida helpommin ryhmän jäsenten kanssa ja lajitella toisiinsa liittyvät hälytykset keskenään. ELK Stackin haku- ja suodatusominaisuudet ovat tehokkaat ja mahdollistavat helpon datan suodatuksen. Hakuja voi suorittaa pelkällä tekstillä, ilman erillisiä tietokannan hakukomentoja ja haku tukee monia ylimääräisiä operaattoreita, kuten AND, OR ja TO, joilla voi esimerkiksi yhdistää monia hakuja tai hakea numerosarjoja. Lisäksi hakemisessa voi käyttää jokerioperaattoria, läheisyyshakuja (haku onnistuu, jos tulos vastaa hakusanaa, kun halutun määrän kirjaimia muuttaa) ja hakuruutu antaa automaattisia tähtöehdotuksia, jotka näkyvät alla olevassa kuviossa 4.



Kuvio 4. Kibanan hakutoiminnon automaattinen täyttö. (Horovits, n.d)

ELK Stack sisältää tehokkaita suodatusmahdollisuuksia, jotka tukevat normaaleja hakutoimintoja. Datan keräystä voi suodattaa Logstashin valmiiksi luotujen datan keräyssuodattimien avulla, jotka voivat helposti muuntaa tarvittaessa yleisiä datatyypppejä Elasticsearchin tietokantaa varten. Tätä tietokantaa voi tiedon hakemisen aikana suodattaa Kibanan vapaasti muokattavilla suodatuskriteereillä, käsiteltävän tiedon rajaamiseksi.

Suodatetun datan voi visualisoida, käyttämällä Kibanan hyvin tunnettuja datan visualisointiominaisuuksia. Kun data on suodatettu ja sopiva datahaku on annettu Elasticsearchille, haun palauttaman datan voi kerätä kaavion, joka auttaa datan analysoinnissa. Käyttäen sopivaa kaaviotyyppiä, jotka ovat näkyvissä kuviossa 5, datan trendit voi osoittaa ja havaita helpommin. Nämä visualisoinnit voi yhdistää vapaasti muokattavaksi työpöydäksi, joka voisi toimia esimerkiksi kyberturvallisuuskeskuksen työntekijöiden etusivuna.



Kuvio 5. Suurin osa Kibanan visualisointityypeistä. (Horovits, n.d)

ELK Stack tukee myös monia integraatiomodduuleja yleisiä pilvipalvelun tarjoajia, työkaluja ja verkosovelluksia varten, joista osa on esillä kuviossa 6. Näiden moduulien avulla voi kerätä dataa esimerkiksi yrityksen pilvipalveluista tai tuetuista konttiratkaisuista. Lisäksi tarjolla on valmiiden moduulien lisäksi Elastic Agent- tai Beats-keräysjärjestelmiä, sekä perinteisempi indeksointibotti, joita voi käyttää datankeruuseen, jos valmista integraatiota ei ole olemassa.

**All categories** 324

- Advanced Analytics (UEBA) 2
- Analytics Engine 1
- AuditD 1
- AWS 30
- Azure 23
- Big Data 1
- Content Delivery Network 3
- Cloud 43
- Communications 3
- Config management 1
- Containers 19
- Credential Management 2

If an integration is available for [Elastic Agent and Beats](#), show:

- ☒ Recommended
- ☐ Elastic Agent only
- ☐ Beats only

**1Password**  
 Collect logs from 1Password with Elastic Agent.

**AbuseCH**  
 Ingest threat intelligence indicators from URL Haus, Malware Bazaar, and Threat Fox feeds with Elastic Agent.

**ActiveMQ Logs**  
 Collect and parse logs from ActiveMQ instances with Filebeat.

**ActiveMQ Metrics**  
 Collect metrics from ActiveMQ instances with Metricbeat.

**Aerospike Metrics**  
 Collect metrics from Aerospike servers with Metricbeat.

**Akamai**  
 Collect logs from Akamai with Elastic Agent.

**AlienVault OTX**  
 Ingest threat intelligence indicators from AlienVault Open Threat Exchange (OTX) with Elastic Agent.

**Amazon CloudFront**  
 Collect Amazon CloudFront logs with Elastic Agent

**Amazon DynamoDB**  
 Collect Amazon DynamoDB metrics with Elastic Agent

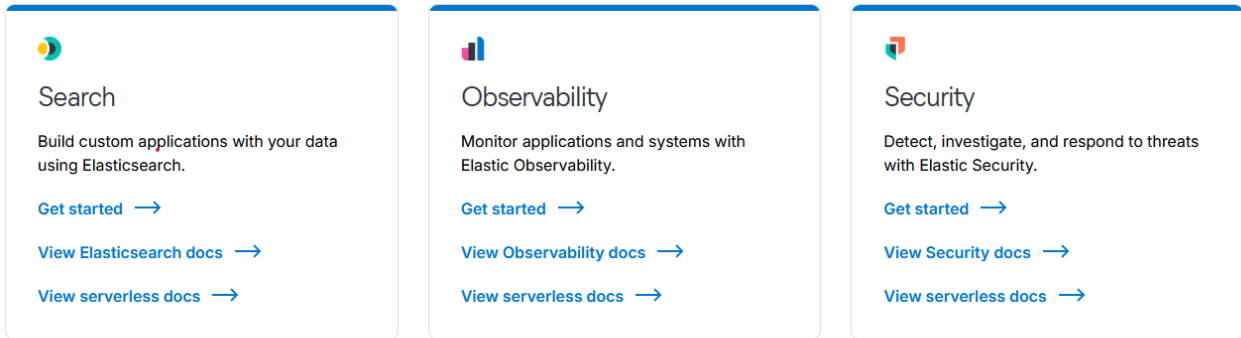
**Amazon EBS**  
 Collect Amazon Elastic Block Storage metrics with Elastic Agent

**Amazon EC2**  
 Collect logs and metrics for Amazon Elastic Compute Cloud service with Elastic Agent

**Amazon ECS**  
 Collect metrics for Amazon Elastic Container Service with Elastic Agent

Kuvio 6. Pieni osa ELK Stackillä tarjolla olevia valmiita integraatiomoduuleja

ELK Stackin dokumentaatio on erittäin laaja ja jaettu moniin osioihin, joista näkyy osa kuviossa 7. Jokaisella ominaisuudella ja toiminnolla on oma sivunsa, mikä on tyypillistä pitkään kehitetylle avoimen lähdekoodin projektille. Lisäksi dokumentaatiossa on huomattava määrä hyödyllisiä asennusohjeita ja vaiheittain selostettuja ohjeita, jotka auttavat huomattavasti välttämään monimutkaisen asennuksen ja konfiguraation ongelmia. Lisäksi vanhan version dokumentaatiot ovat saatavilla versiotukea varten, jos yritys ei voi jostain syystä päivittää uusimpaan versioon.



## Browse all docs

### SEARCH

- [Elasticsearch Guide \[8.13\] — other versions](#)
- [Enterprise Search Guide \[8.13\] — other versions](#)
- [Workplace Search Guide \[8.13\] — other versions](#)
- [App Search Guide \[8.13\] — other versions](#)
- [Enterprise Search Clients](#)

### OBSERVABILITY: APM, LOGS, METRICS, AND UPTIME

### INGEST: ADD YOUR DATA

- [Elastic Ingest Reference Architectures \[8.13\] — other versions](#)
- [Fleet and Elastic Agent Guide \[8.13\] — other versions](#)
- [Logstash Reference \[8.13\] — other versions](#)
- [Logstash Versioned Plugin Reference](#)
- [Elastic Logging Plugin for Docker \[8.13\] — other versions](#)
- [Elastic Serverless Forwarder Guide](#)
- [Integrations Developer Guide](#)
- [Auditbeat Reference \[8.13\] — other versions](#)

## Kuvio 7. Osa ELK Stackin dokumentaationsivuista

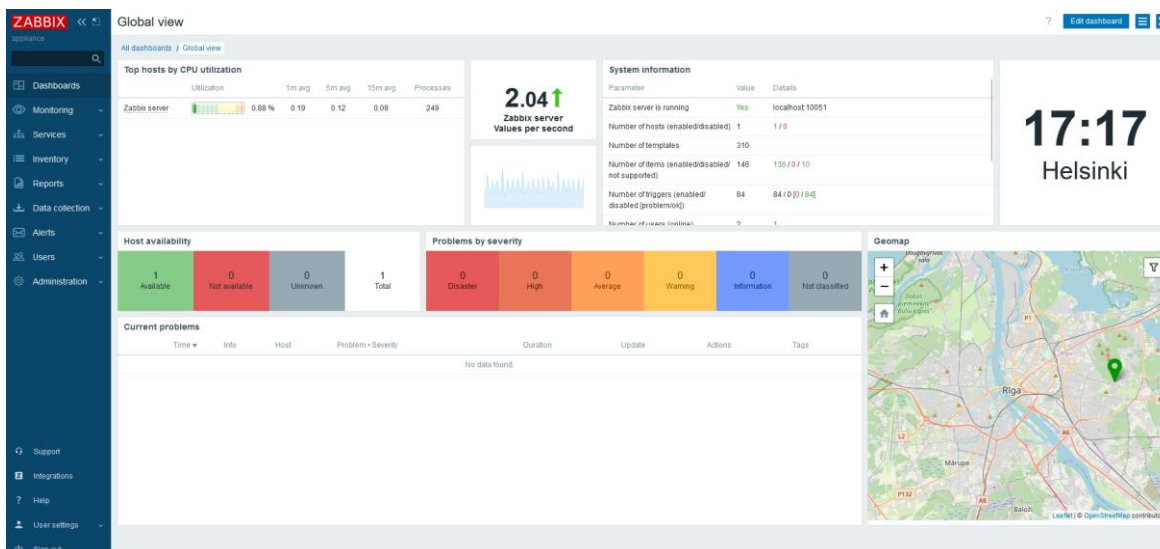
Kun käyttäjä pääsee ELK Stackin melko korkean oppimiskynnyksen yli, työkalun tehokkaat ominaisuudet mahdollistavat nopean ja selkeän työnteon. Kerätty data näkyy selkeästi hakutuloksissa ja vapaasti muokattavissa kuvioissa, joista muodostetut työpöydät paljastavat työtehtäville tarpeellisia datatrendejä. Ongelmatilanteissa voi käyttää laajaa dokumentaatiota, joka sisältää tietoja kaikista työkalun lukuisista ominaisuuksista. Tämä suuri ominaisuusmäärä, joka on kertynyt työkalun pitkän kehitysajan aikana, on kuitenkin yksi työkalun heikkouksista. Suuri määrä ominaisuuksia ja välilehtiä tekevät työkalun käytöstä aluksi kömpelöä ja vaikeuttavat käytön oppimista. Tämän tilanteen muuttaminen on kuitenkin epätodennäköistä, koska se vaatisi lähes täyden työkalun koodin uudelleenkirjoittamisen ja vähentäisi työkalun valmistajan tarjoaman itsenäisen pilvipalvelun houkuttelevuutta.

#### 4.2.2 Zabbix

Zabbix on saman tyyppinen SIEM-valvontatyökalu kuin ELK Stack. Sen monipuoliset datan keräämistyökalut mahdollistavat lokien ja analytiikan keräämisen lähes mistä tahansa lähteestä. Lataaminen ja asentaminen on täysin ilmaista ja mitkään työkalun ominaisuudet eivät ole lukittu rahamuurin taakse, tosin asiakastuki on ainoastaan saatavilla maksullisena.

Datan keräämisen voi suorittaa joko keräyskohteelle asennettavilla agenteilla tai käyttämällä esimerkiksi verkoston valvontaa seuraamaan verkkosovelluksia. Zabbix myös tukee itse muilla työkaluilla kerätyn datan lisäämistä tietokantaan erikoistapauksissa, jos yrityksellä on jokin erikoislaitte, jolle ei voi asentaa Zabbixin omia agentteja. Kerätyn datan voi järjestää kaavioiksi, tosin ELK Stackillä on hieman enemmän kaaviovaihtoehtoja. Vapaasti muokattavat työpöydät ovat myös saatavilla, jotka toimivat yhtä hyvin kuin ELK Stackin vastaavat ominaisuudet.

Työpöytä on vapaasti muokattava ja oletusnäkyminen, joka näkyy kuviossa 8, on tyydyttävä suurimpaan osaan käyttötarkoituksista. Muokkauksia voi tehdä helposti käyttäen kulmassa olevaa muokkausnappia, jolla voi muokata työpöydän osia helposti raahaamalla niitä tai valitsemalla uuden osan alavalikosta. Vaikka kaavio-osia on saatavilla vähemmän verrattuna ELK Stackiin, Zabbixin työpöydälle on saatavia hyviä oletusosia, jotka voivat esittää usein käytettyjä datatrendejä, kuten esimerkiksi varoitusten määrät ja kategoriat, ilman erillistä konfigurointia. Lisäksi saatavilla on osa, jolla voi kiinnittää työpöydälle minkä tahansa verkkosivun, jolla voi näyttää työpöydällä esimerkiksi yrityksen intranetin tai verkkoselaimella käytettävän työkalun.



Kuvio 8. Zabbixin oletustyöpöytä

Zabbixin käyttöliittymä on paljon selkeämpi ELK Stackiin verrattuna. Työkalun ominaisuudet ovat jaettu selkeisiin kategorioihin, jotka ovat lajiteltu yksinkertaisesti nimetyiksi kategorioiksi. Lisäksi mitkään ominaisuuksista ei ole lukittu maksullisen version taakse, joka myös selkeyttää ja yksinkertaistaa työkalun käytön oppimista.

Työkalun löytämistä epäilyttävistä tapahtumista voi luoda varoituksia, jotka voi lähettää haluamalaan viestintäkanavalla järjestelmänvalvojille. Tapahtumat, jotka luovat varoituksen, sekä varoitusten toimitustapaa voi muokata vapaasti selkeällä käyttöliittymällä. Nämä varoitukset täytyy laukaista luomalla niille ”laukaisin” (trigger), joka luo ongelmatapahtuman, kun jokin kerätty data ylittää määritetyn turvarajan. Oletuksena Zabbix vain kerää dataa ja sisältää valmiiksi tehtyjä laukaisimia työkalun ylläpitopalvelimen datasta, joten kaikille päätelaitteille tai muille yrityksen omille datalähteille täytyy luoda omat laukaisimet.

Laukaisimien luonti ja kiinnittäminen jokaiseen relevanttiin datalähteeseen ja datalajiin voi olla työlästä, etenkin suuremmissa verkostoissa, joissa voi olla tuhansia laitteita, joista kerätään dataa. Zabbixilla on tämän tehtävän automatisointia varten hyödyllinen ominaisuus, jolla voi luoda valmiita laukaisinryhmiä (templates), jotka voi yhdistää datalähteisiin tai ryhmiin datalähteitä. Läheteet perivät kaikki kiinnitetyn laukaisinryhmän laukaisimet ja niiden asetukset. Ryhmien käyttäminen nopeuttaa huomattavasti uusien datalähteiden lisäämistä työkalun valvontaan ja vähentää vahingossa jonkin laukaisimen unohtamisen riskiä.

Datan voi järjestellä työpöytien lisäksi tietyn aikavälein luoduiksi raporteiksi. Näitä raportteja voi käyttää näyttämään hyödyllistä dataa, kuten esimerkiksi verkkoliikenteen aiheuttamaa kuormitusta. Raporttien käyttötarkoitus on data, jota on tärkeätä tarkkailla, mutta ei saavuta hälytyksiä aiheuttavia tilanteita usein, sekä data, mitä voi käyttää esimerkiksi palvelun kehittämiseen. Zabbixilla on oletuksena tarjolla raportti työkalun järjestelmätiedoista, joka näkyy kuviossa 9. Samoin kuten kaaviot, raportteja voi kiinnittää työpöydille.

#### System information

Parameter	Value	Details
Zabbix server is running	Yes	localhost:10051
Number of hosts (enabled/disabled)	1	1 / 0
Number of templates	310	
Number of items (enabled/disabled/not supported)	146	136 / 0 / 10
Number of triggers (enabled/disabled [problem/ok])	84	84 / 0 [0 / 84]
Number of users (online)	2	1
Required server performance, new values per second	1.64	
Database history tables upgraded	No	Support for the old numeric type is deprecated. Please upgrade to numeric values of extended range.
High availability cluster	Disabled	

Kuvio 9. Zabbixin järjestelmätietoraportti

Zabbixin dokumentaatio on paremmin järjestelty ja lyhyempi kuin ELK Stackin dokumentaatio. Se on jaettu kolmeen pääosaan sivujen käyttötarkoituksen mukaan: Zabbix-käsikirja, joka sisältää käyttäjille suunnattuja ohjeita työkalun ominaisuuksista ja käytöstä, Kehittäjäkeskus, joka sisältää moduulien kehittäjille tarkoitettua teknistä tietoa ja Zabbix man-sivut, joka sisältää Zabbixin työkaluprosessien komentojen ohjesivut. Käsikirjaosion sivut ovat kirjoitettu selkeästi ja ovat helposti luettavissa. Lisäksi vanhojen versioiden sivut ovat saatavilla, jos yritys ei jostain syystä voi käyttää ajantasaista versiota työkalusta.

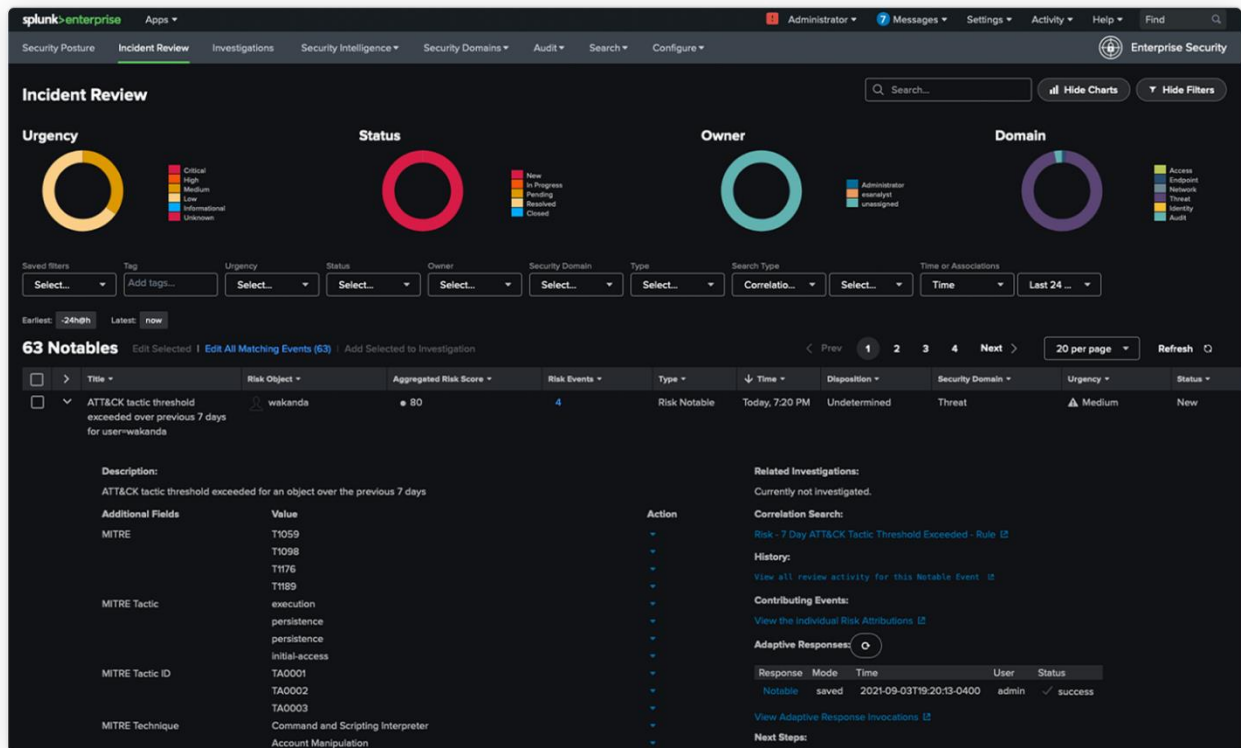
### 4.3 Kaupalliset yritystason valvontatyökalut

Avoimen lähdekoodin työkaluilla voi olla heikkouksia suurten yritysten käyttötarkoituksia varten. Näillä työkaluilla on usein heikommat tukimahdollisuudet ongelmia varten ja voivat olla hankalia asentaa järjestelmälle. Niissä voi olla kömpelömpi käyttöliittymä tai puuttuvia ominaisuuksia kaupallisiin työkaluihin verrattuna. Kaupallisilla työkaluilla on mahdollisuus ottaa ongelmatilanteissa yhteyttä suoraan asiantuntijoihin, jotka voivat auttaa ongelman ratkomisessa suoran yhteyden

välityksellä. Lisäksi, jos yrityksellä ei ole väestöä omaa tietoturvakeskusta varten, kaupallisia työkaluja voi olla saatavilla tietoturvakeskuspalveluista, jotka voivat hoitaa tietoturvakeskukseen työtehtävät yrityksen puolesta.

Kaupalliset työkalut sisältävät laajalti samanlaisia toimintoja keskenään ja niiden eroavaisuudet eivät ole yhtä suuret kuin avoimen lähdekoodin työkaluissa. Yrityskoon työkalujen suuren hinnan takia, valmistajat houkuttelevat usein yrityksiä monipuolisuudella ja helppokäyttöisyydellä. Kaupallisilla työkaluilla on myös usein koulutuskursseja työkalun käyttöä varten saatavilla suoraan valmistajilta.

Splunk on työkalu, joka erikoistuu laajaan datan keräykseen ja suodatukseen. Kuva työkalun työpöydästä on kuviossa 10. Työkalun valmistaja Cisco kehuu Splunkin tehokkaita hakutyökaluja ja datan suodatusta, jotka voivat vähentää hälytysten määrää jopa 80 prosenttia suodattamalla turhat hälytykset. Työkalua käyttäneet yritykset ovat laajalti samaa mieltä, mutta huomioivat työkalun monimutkaisen asennuksen ja käyttöönoton. Lisäksi monien käyttäjien mielestä työkalu voi vaatia hyvin yksityiskohtaista konfigurointia ideaalista toimintaa varten ja lisenssin hinnoitusmalli, joka perustuu käsitellyn datan määrään voi osoittua kalliiksi isoissa verkostoissa. (Splunk Enterprise Reviews n.d; Splunk products n.d)



Kuvio 10. Splunkin työpöytä. (Splunk products n.d)

LogRhythm on SIEM-työkalu, joka keskittyy datan sujuvaan visualisointiin ja nopeisiin hälytyksiin ja niiden ratkaisemiseen. Työkalun valmistaja, sekä arvostelun jättäneet yritykset kehuvat selkeätä käyttöjärjestelmää, joka on näkyvissä kuviossa 11, sekä automaattisia turvallisuustoimenpiteitä, joita voi ohjelmoida valitsemilleen hälytyksille. Lisäksi työkalun hyviä puolia on helppo integraatio verkoston laitteiden tarkkailua varten, sekä tehokas ja nopea lokien keräys ja haku. Arvosteluissa on mainittu heikkouksina työkalun mahdolliset väärät positiiviset hälytykset ja keskivertoa kalliimpi hinta. (LogRhythm Enterprise Reviews n.d; LogRhythm SIEM: Learn about our self-hosted SIEM platform n.d)



Kuvio 11. LogRhythm-työkalun työpöytä. (LogRhythm SIEM: Learn about our self-hosted SIEM platform n.d)

Näiden työkalujen lisäksi suuremmilla avoimen lähdekoodin projekteilla, kuten ELK Stackillä ja Zabbixillä, on saatavilla suurille yrityksille suunnattu Enterprise-versio. Nämä versiot antavat kalliimmalla kuukausihinnalla suurille yrityksille suunnattuja ylimääräisiä ominaisuuksia. Lisäksi nopea ja vuorokauden ympäri toimiva asiakastuki voi olla priorisoituna yritysversioneille.

## 4.4 Muut aputyökalut

SOAR- ja SIEM-valvontatyökalujen lisäksi järjestelmänvalvojat käyttävät monia aputyökaluja tutkimaan verkoston rakennetta ja toimivuutta. Jos järjestelmävalvojat ovat havainneet häiriön verkostossa tai saaneet hälytyksen epäilyttävistä tiedostoista tai tapahtumista, näiden tutkimista varten tarvitsee usein käyttää erikoistuneita työkaluja. Joidenkin tietoturvakeskusten vastuulla voi myös olla testata verkoston turvallisuutta ja suorituskykyä.

Jos järjestelmävalvoja on pienen yrityksen jäsen, hän voi joutua suorittamaan monia työtehtäviä, jotka perinteisesti kuuluvat muille tieto- ja viestintätekniikkainsinööreille. Jos järjestelmävalvoja joutuu asentamaan tai ylläpitämään palomuuria, hyvä vaihtoehto voisi olla OPNsense. OPNsense

on avoimen lähdekoodin työkalu, joka soveltuu palomuurin ylläpitoon ja verkkoliikenteen reitittämiseen ja on täysin ilmainen. Työkalu saa viikoittaisia turvallisuuspäivityksiä ja keskittyy turvallisuuteen.

Famatech Advanced IP Scanner on ilmainen työkalu, jota käytetään skannaamaan ja listaamaan kaikki verkostoon yhdistetyt laitteet. Työkalulla voi tarkistaa kaikki yhteydet yrityksen verkostoon ja skannata niiden IP- ja MAC-osoitteet, jos niitä tarvitaan ongelman korjaamiseen. Lisäksi työkalulla voi sammuttaa esimerkiksi viruksen saastuttaman tietokoneen etäyhteyden yli, mikä voi olla tärkeitä leviämisen välttämiseksi, jos kone sijaitsee esimerkiksi toisella toimistolla. Työkalu on myös hyvin kevyt ja se ei vaadi asentamista, joten sitä voi käyttää helposti kannettavilla tietokoneilla tarvittaessa. (Wilson & Gupta 2023.)

AppNeta PathTest on työkalu, jolla voi varmistaa verkoston toimivuuden rasituksen alla ja etsiä mahdollisia pullonkauloja. Työkalu lähettää muutaman sekunnin ajan verkostoon erittäin suuren määrän liikennettä, täysin rasittaen verkoston täyteen verkkoviestintää. Kerätyllä datalla voi havaita heikkouksia verkoston toiminnassa ja parantaa kestävyyttä esimerkiksi DDoS-hyökkäyksiä vastaan. (Wilson & Gupta 2023.)

Virustotal on verkkoselaimessa toimiva haittaohjelmaskanneri. Skannauksen voi tehdä tiedostoille, URL-osoitteille, domaineille ja IP-osoitteille käyttämällä työkalun etusivulla olevaa tiedoston latausnappia, joka näkyy kuviossa 12. Virustotal käyttää yli 70 haittaohjelmaskanneria ja osoitteenestolistapalvelua tarkistamaan annettua tiedostoa tai osoitetta epäilyttävää sisältöä tai toimintaa varten (How it works n. d). Virustotal toimii itsenäisesti ja ei toimi suorassa yhteistyössä minkään selaimen tai hakukoneen kanssa, parantaen yksityisyyttä ja objektiivisuutta. Tietoturvapäivitykset ja uudet hälytykset uusista uhkaavista haittaohjelmista päivittyvät tietopohjaan nopeasti. Työkalu on myös nopea käyttää ja koska sen voi ajaa suoraan verkkoselaimesta, se soveltuu täydellisesti ensimmäiseksi korjaustoimenpiteeksi, kun valvontalaitteisto on havainnut epäilyttävän tiedoston tai osoitteen.



Kuvio 12. Virustotal-työkalun etusivu

## 5 Tulokset

Järjestelmän valvontaa varten on saatavilla laajasti työkaluja jokaiseen eri työtehtävään. Työtehtävät ovat myös tilanteen mukaan laajoja tai suppeita, riippuen yrityksen koosta ja turvakeskuksen olemassaolosta. Näiden vaihtelevuuksien takia, kaikkiin tilanteisiin soveltuva suositus käytettävistä työkaluista ei ole mahdollista. Esiin tuodut työkalut ovat monipuolisia ja laajasti sopivia, mutta silti käyttöön otettava työkalu täytyy valita harkitsemalla yrityksen työtehtäviä ja niiden vaativia työkaluominaisuuksia.

Avoimen lähdekoodin työkalut, joista on työssä käsitellyistä työkaluista tiivistelmä taulukossa 1, riittävät suurimmalle osalle yrityksistä. Niiden käyttövaikeudet voivat hankaloittaa käyttöönottoa ilman työkalua tuntevaa asiantuntijaa tai aktiivista käyttäjäpohjaa ja dokumentaatiota. Näiden työkalujen käyttö hinnat ovat myös huomattavasti halvempia vastaaviin yritystason työkaluihin verrattuna, mutta niiden tehokkuus ei usein ole kaukana yritystason tuotteista. Jos avoimen lähdekoodin työkalun ominaisuudet riittävät työtehtäviin, niillä voi olla parempi hinta/laatu -suhde.

Järjestelmävalvojan laaja rooli ja suuri määrä työtehtäviä pienissä yrityksissä ilman tietoturvakeskusta korostaa sujuvan ja monipuolisen työkalun valitsemista. Työkalussa on suositeltavaa olla esimerkiksi sähköpostihälytykset ominaisuutena, joita voisi käyttää hälyttämään pientä järjestelmävalvojaryhmää hätätilanteista. Automaattiset valvontatoimenpiteet yksinkertaisia ja usein toistuvia tilanteita varten auttaisivat keventämään työkuormitusta.

Taulukko 1. Tiivistelmä käsiteltyjen avoimen lähdekoodin työkalujen ominaisuuksista.

Avoimen lähdekoodin työkalu	Hyviä puolia	Heikkouksia	Huomioitavaa
Prometheus	Tehokas valvonta, organisoitu data ja tehokkaat hakutyökalut	Lyhyt säilytysaika	Tarkoitettu konttiympäristöille (Docker yms.)
ELK Stack	Itsenäinen kokoelma, tehokas datan prosessointi ja säilytysaika	Hankala asennus ja käyttöliittymä	Stackin työkaluissa on ominaisuudet kaikkiin valvojan työtehtäviin
Zabbix	Tehokas ja monipuolinen valvonta, erinomainen laajennettavuus	Vain maksullinen asiakastuki	Täysin ilmainen ohjelmisto

Tietoturvakeskus on hyvä rakenne organisoida kasvavan yrityksen järjestelmävalvonnan tarpeita. Kun yritys kasvaa kooltaan, työntekijöiden tarvitsee erikoistua hoitamaan omaa osiotaan suuresta dataliikennemäärästä. Avoimen lähdekoodin työkalut ovat viime vuosina kehittyneet huomattavasti ja niiden nykyajan toimikyvyt ovat riittäviä näihin tarkoituksiin. Erittäin suurille yrityksille voi kuitenkin aiheutua enemmän kuluja näiden työkalujen ylläpidosta, kuin säästyy välttämällä yritystason työkalujen kalliimmista lisenssihinnoista.

Kun yritys kasvaa tarpeeksi suureksi, kalliit yritystason työkalut muuttuvat rahanarvoisiksi. Ne ovat suunniteltu alusta asti käsittelemään suuria määriä verkkoliikennettä ja siitä aiheutuvaa rasitusta. Lisäksi niille saatavilla oleva 24/7 ammattilaistuki voi auttaa paremmin hätätilanteissa ja työkalujen ylläpidossa verrattuna avoimen lähdekoodin työkaluihin, joilla on yleensä vähemmän resursseja ylläpitää aktiivista asiakastukea.

Työkalujen monimuotoisuuden takia on mahdotonta luoda täydellinen suositus työkalua varten. Työkalun valinnassa täytyy harkita työtehtävät, yrityksen rakenne, työkalun hinta, järjestelmäympäristön arkkitehtuuri, saatavilla oleva dokumentaatio ja asiakastuki ja paljon muuta. Työssä esitetyt työkalut ovat hyviä lähtökohtia harkintaa varten, mutta suuri määrä sopivista työkaluista jäivät käsittelyn ulkopuolelle työn laajuuden rajaamiseksi.

Työssä tutkittiin myös tarkemmin käytännön testien avulla ELK Stackin ja Zabbixin ominaisuuksia ja arvosteltiin niiden tehokkuus. Alla olevassa taulukossa 2 on arvosanat asteikolla 1 (heikko) – 5 (erinomainen). Työkalujen arvioinnissa vertailtiin työkalujen ominaisuuksien tehokkuus, käyttöliittymän helppokäyttöisyys, työkalun hinta ja dokumentaation laatu.

Taulukko 2. Arvioitujen työkalujen numeroarvosanat

	Ominaisuudet	Käyttöliittymä	Hinta	Dokumentaatio	Yhteensä
ELK Stack	5	3	4.5	4	4.125
Zabbix	4.5	5	5	4.5	4.75

ELK Stack sisältää pitkän kehitystyön ansiosta runsaasti ominaisuuksia, jotka soveltuvat lähes jokaiseen tilanteeseen, mutta tämä johtaa myös työkalun suurimpaan heikkouteen. Suuri määrä ominaisuuksia johtaa heikkoon käyttöliittymäkokemukseen, koska työkalu on täynnä alivalikoita ja välilehtiä, jotka pysyvät näkyvissä, vaikka kyseinen ominaisuus ei olisi saatavilla. Työkalun voi ladata

ilmaiseksi, mutta pieni osa ei-kriittisistä ominaisuuksista on lukittu kuukausimaksullisen pilvipalveluversion taakse. Dokumentaatio on myös laaja ja hyvin kirjoitettu, mutta sisältää suuren ominaisuusmäärän takia niin paljon lukuja ja osioita, että halutun sivun löytäminen on haasteellista.

Zabbix sisältää lähes kaikki samat tärkeät ominaisuudet, kuin ELK Stack. Ainoita moitteita voisi olla hieman heikommät visualisointityökalut. Käyttöliittymä on Zabbixilla hallussa ja selkeästi helpompi käyttää verrattuna ELK Stackiin. Ominaisuudet ovat jaettu selkeisiin valikkoihin, jotka kaikki näkyvät yhtä aikaa ruudulla. Työkalu on myös täysin ilmainen ja ei lukitse mitään ominaisuuksia maksumuurin taakse. Dokumentaatio on yhtä laadukkaasti kirjoitettu kuin ELK Stackin sivut ja lajiteltu selkeämmin, joka tekee halutun sivun löytämisestä huomattavan helppoa.

## 6 Yhteenveto ja pohdinta

Opinnäytetyön tavoitteena oli löytää suosituksia järjestelmävalvojen työkaluista ja oppia niiden käyttö, sekä selvittää järjestelmävalvojen työtehtävät ja kyberturvallisuuskeskusten rakenne. Aluksi työtehtävien selvittämisen ja työkalusuositusten saamiseksi oli tarkoitus myös haastatella työtä tekeviä järjestelmävalvoja, mutta kaikki järjestelmävalvojat, joilta pystyi kysymään haastattelumahdollisuutta, kieltäytyivät tietoturvasyistä. Tavoitteeksi muuttui haastatteluiden epäonnistumisen jälkeen käyttää laajasti kirjallisia lähteitä tukemaan työkalujen arvosteluja, sekä testamaan ja vertaamaan itse muutamaa työkalua.

Työssä tutkittiin ulkoisilla arvosteluilla ja suosituksilla ELK Stack-, Zabbix-, Prometheus-, LogRhythm- ja Splunk-työkaluja. Yksityiskohtaisten arvostelujen ja suositusten löytäminen oli yllättävän haastavaa. Kaupallisille ja suurille yrityksille suunnatuille työkaluille löytyi huomattava määrä luotettavia arvosteluja ja suosituksia työkaluja käyttäneiltä ammattilaisilta. Avoimen lähteen työkaluille oli vaikeata löytää suoraan luotettavalta vaikuttavia lähteitä, jotka eivät yrittäneet markkinoida artikkelin kirjoittaneen yrityksen omaa työkaluvaihtoehtoa, joten mahdollisen puolueellisuuden vähentämistä varten, artikkeleiden väittämät vahvistettiin muiden lähteiden kanssa.

Lisäksi työssä tutustuttiin ja vertailtiin kahta työkalua tarkemmin: ELK Stack ja Zabbix. Työkalujen ominaisuudet ja käyttöliittymä vertailtiin ja huomioon otettiin myös työkalujen mahdolliset hintamuurit ja dokumentaation laatu. Työkalut asennettiin itse käyttäen ainoastaan dokumentaatiossa mainittuja ohjeita ja testattiin tutkimalla työkalun käyttöliittymää, sekä luomalla tapahtuman, joka

tekee hälytyksen työpöydälle. Työkalujen vertailu onnistui erinomaisesti ja sain kerättyä kokemusta valvontatyökalujen asentamisesta ja käytöstä.

Työn vertailuosioon valittiin kaksi avoimen lähdekoodin työkalua, joita käytetään samoihin työtehtäviin vertailun sopivuuden varmistamiseksi. Vertailun tulokset ovat tietenkin subjektiivisia, koska työkalut suorittivat työtehtävät tavoitteiden mukaisesti. Tämä tekee objektiivisesta vertailusta esimerkiksi havaintotarkkuudessa vaikeata tai lähes mahdotonta. Tulosten parantamista varten voisi vertailla lisää työkaluja, sekä vähentää subjektiivisuutta käyttämällä useampien arvostelijoiden mielipiteitä työkaluista ja arvostelutavoitteiden saavuttamisesta. Lisäksi arvosteluun voisi lisätä objektiivisia tavoitteita, kuten tietokoneen resurssien kulutuksen, toimivuuden verkostoruuhkan aikana tai valvonnan tarkkuuden, jos työkalut testattaisiin suurella kaavalla yritystä vastaavassa labraympäristössä.

Järjestelmävalvojan työtehtävät eivät olleet ennen työn alkua kovin tuttuja, joten työn tietopohjaa varten etsin erityisen luotettavia lähteitä ja osallistuin kursseille, jotka käsittelivät tietoturvakeskustoja. Työn aikana sain mielestäni sisäistettyä hyvin, miten tietoturvakeskukset toimivat ja mitä tehtäviä järjestelmävalvojat suorittavat rutiinityötehtävinä. Pienten yritysten järjestelmävalvojen tehtävät olivat vaikeata tiivistää työtä varten, koska heillä on usein monia rooleja pienikokoisen tietotekniikkaryhmän takia.

Tietoturvakeskustoista löytyi enemmän tietoa työtehtävistä ja keskusten rakenteesta. Rakenteita oli kuitenkin niin monia ja riippuivat huomattavasti yrityksen resursseista ja tarpeista, joten vain osa mahdollisista rakenteista on esillä opinnäytetyössä. Jatkokehitystä varten voisi mahdollisesti lisätä ylimääräisiä turvakeskusrakenteita ja tarkentaa milloin mikäkin rakenne sopii käytettäväksi.

Tutkimuksen tuloksia voi hyödyntää esimerkiksi sopivan valvontatyökalun löytämiseksi tai uuden tietoturvakeskustuksen rakenteen päättämiseksi. Lisäksi työ esittää muutaman valvonnan ulkopuolisen työkalun, joita voi hyödyntää valvontatöissä. Esimerkiksi Virustotal-työkalu on hyvä ja helppo keino diagnosoida epäilyttäviä tiedostoja ja linkkejä, jos valvontaohjelmat ovat havainneet epäilyttävää liikennettä.

Työtehtävän tietoperustalla ja työtehtäväosiolla voi myös käyttää neuvomaan uusia työntekijöitä tai työntekijöitä, joilla ei ole tietoturvakokemusta. Opinnäytetyössä sain mielestäni hyvin tiivistettyä järjestelmävalvojen yleisimmät työtehtävät ja uskoisin, että se olisi mahdollista lukea ilman erillistä tieto- ja viestintätekniikkakoulutusta. Opin myös itse opinnäytetyötä tehdessä lisää kyberturvallisuuden käytännön tehtävistä ja työstä.

Alun perin työn tavoitteena oli myös kirjoittaa lyhyt luku valvojan itse kirjoittamista skripteistä, joilla olisi voinut ajaa usein käytettyjä työkaluja ja komentoja ongelmien tutkimista varten. Tästä aiheesta en kuitenkaan löytänyt kirjallisia lähteitä. Leikkasin aiheen opinnäytetyöstä lähteiden puutteen ja haastattelujen epäonnistumisen takia. Yksi tärkeimmistä aiheista, joita olisin selvittänyt haastattelussa olisi ollut useitten käytetyt työkalut käytännön työtehtävissä, jotka olisivat olleet mahdollista automatisoida. Näiden haasteiden takia päätin leikata aiheen ja keskittyä suppilomallin mukaan tarkemmin itse työkaluihin.

Ylipäättään sain mielestäni suoritettua opinnäytetyön tavoitteeni ja työn laatu täyttää omat standardini. Mielestäni heikkouteni on yhä tekstin määrä ja kirjoittamieni tekstien lyhyys, mutta mielestäni itse kirjoitetun tekstin laatu on hyvä. Opin myös itse työn kirjoittamisen aikana paljon kyberturvallisuudesta ja järjestelmien valvonnasta.

## Lähteet

Alcon, J. 2017. What Is Endpoint Security & Why Is It Important? Artikkelit Bitsight-yrityksen sivuilla. Julkaistu 20.7.2017 Viitattu 12.3.2024. <https://www.bitsight.com/blog/what-is-endpoint-security>

Explore Zabbix features. N.d. Zabbix-työkalun kotisivuilla julkaistu lista työkalun ominaisuuksista. Viitattu 15.5.2024. <https://www.zabbix.com/features>

Horovits, D. N.d. The Complete Guide to the ELK Stack. Ohjeartikkeli ELK Stackin asentamisesta ja käytöstä. Viitattu 23.5.2024. <https://logz.io/learn/complete-guide-elk-stack/>

How it works. N.d. Virustotal-työkalun dokumentaationsivu työkalun toiminnasta ja ominaisuuksista. Viitattu 16.5.2024. <https://docs.virustotal.com/docs/how-it-works>

Knerler, K. Parker, I. & Zimmerman, C. 2022. 11 Strategies of a World-Class Cybersecurity Operations Center. 2. p. MITRE. Viitattu 29.3.2024. <https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf>

Kral, P. 2012. The Incident Handlers Handbook. Julkaisu SANS instituutin sivuilla. Julkaistu 21.2.2012. Viitattu 5.3.2024. <https://www.sans.org/white-papers/33901/>

LogRhythm SIEM: Learn about our self-hosted SIEM platform. N.d. LogRhythm-yrityksen kotisivu työkalustaan. Viitattu 17.5.2024. <https://logrhythm.com/products/logrhythm-siem/>

LogRhythm SIEM Reviews. N.d. Gartnerin keräämät arvostelut LogRhythm SIEM -työkalusta. Viitattu 17.5.2024. <https://www.gartner.com/reviews/market/security-information-event-management/vendor/logrhythm/product/logrhythm-siem>

Opas tietomurtojen havaitsemiseen. 2020. Kyberturvallisuuskeskuksen julkaisu. Julkaistu 22.12.2020. Viitattu 12.3.2024. <https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/opas-tietomurtojen-havaitsemiseen>

Pienyritysten kyberturvallisuusopas. 2020. Kyberturvallisuuskeskuksen julkaisu. Julkaistu 30.9.2020. Viitattu 13.3.2024. <https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pienyritysten-kyberturvallisuusopas>

Prometheus vs. ELK. 2023. MetricFire-yrityksen julkaisema artikkeli. Viitattu 14.5.2024. <https://www.metricfire.com/blog/prometheus-vs-elk/>

Pyyny, P. 2024. xz Utils - Kun koko netin turvallisuus oli uhattuna, tuuri pelasti. AfterDawn. 2.4.2024. Viitattu 18.4.2024. <https://dawn.fi/uutiset/2024/04/02/xz-utils-takaportti>

Splunk Enterprise Reviews. N.d. Gartnerin keräämät arvostelut Splunk-työkalusta. Viitattu 16.5.2024. <https://www.gartner.com/reviews/market/security-information-event-management/vendor/splunk/product/splunk-enterprise>

Splunk products. N.d. Splunk-yrityksen kotisivu työkalustaan. Viitattu 16.5.2024. [https://www.splunk.com/en\\_us/products.html](https://www.splunk.com/en_us/products.html)

Top 5 Open Source Server Monitoring Tools. 2023. MetricFire-yrityksen julkaisema artikkeli. Viitattu 14.5.2024. <https://www.metricfire.com/blog/top-5-open-source-server-monitoring-tools/>

Wilson, B. & Gupta, G. 2023. 13 Best Open Source & Free Monitoring Tools. Devopscube-sivuston julkaisema artikkeli. Viitattu 14.5.2024. <https://devopscube.com/best-opensource-monitoring-tools/>

Wilson, K. & Kiy, M. 2014. Some Fundamental Cybersecurity Concepts. IEEE:n julkaisema tutkimus. Viitattu 29.3.2024. <https://ieeexplore.ieee.org/abstract/document/6737236>