Tampereen ammattikorkeakoulu

# Kotiympäristön tietoturvan parantaminen SIEM-ohjelmistolla

Miika Airaksinen

OPINNÄYTETYÖ
Maaliskuu 2024

Tietotekniikan tutkinto-ohjelma
Tietoliikennetekniikka ja tietoverkot

**TIIVISTELMÄ**

Tampereen ammattikorkeakoulu
Tietotekniikan tutkinto-ohjelma
Tietoliikennetekniikka ja tietoverkot

AIRAKSINEN, MIIKA:
Kotiympäristön tietoturvan parantaminen SIEM-ohjelmistolla

Opinnäytetyö 28 sivua, joista liitteitä 0 sivua
Maaliskuu 2024

---

Teknologian kehittyessä uusia hyökkäyskanavia ihmisten tietoihin aukeaa jatkuvasti. Yritykset ovat tietoturvassa edelläkävijöitä, mutta miksei samanlaisia suojauskeinoja voisi käyttää myös kuluttajien arjessa. Opinnäytetyössä kokeiltiin ideaa, jossa normaalisti yrityksissä käytettävä SIEM-tarkkailuohjelmisto asetettaisiin toimintaan kotiverkkoon. Esimerkkinä oleva Wazuh-ohjelma tarkkailisi tietokoneiden sekä verkon liikennettä. Työn tavoitteena oli saada selville, miten toteuttamiskelpoinen ja hyödyllinen ratkaisu on.

Tarkkailun koeympäristönä toimi virtuaalikoneilla rakennettu verkko, jossa Wazuh toimi Linux-serverillä, ja siinä oli kiinni kaksi Windows-tietokonetta. Lisäksi erillinen Kali Linux -tietokone edustaa pahantahtoista hyökkääjää. Asennusprosessi ja ohjelman käyttö oli suhteellisen helppoa. Ongelmia kuitenkin ilmeni oleellisten suojausmekanismien ja toiminnallisuuksien puuttumisessa. Kuten moni muukin toiminto tässä hyvin muokattavassa ohjelmistossa, olisi ne pitänyt erikseen ottaa käyttöön.

Työn tulosten perusteella voidaan todeta, että Wazuh on helppokäyttöinen henkilölle, joka ymmärtää tietoturvatermistöä sekä osaa käyttää Linuxia ja Windowsia yksinkertaisten konfiguraatiomuutosten tekemiseen. Tämä on kuitenkin tällä hetkellä paljon vaadittu jokaiselta nykypäivän tietokoneen käyttäjiltä. Lisäksi muokkauksen tarve heti ohjelmiston käyttöönotossa ei ole toivottua. Täten SIEM-ohjelmisto voisi olla tietoturvatyökalu koteihin tulevaisuudessa, mutta tällä hetkellä se vaativat lisää käyttäjäystävällisyyttä.

---

Asiasanat: tietoturva, SIEM, kotiympäristö

## ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in ICT Engineering
Telecommunication and Networks

AIRAKSINEN, MIIKA:
The Improvement of a Home Environment's Information Security Using SIEM Software

Bachelor's thesis 28 pages, appendices 0 pages
March 2024

---

With the advancement of technology, new avenues for attacking people's personal information are opening constantly. Companies are forerunners in information security, but why couldn't similar defence mechanisms be used in the everyday life of consumers. In this thesis, the idea of using a normally enterprise level program SIEM for home environments, was put to the test. As a practical example, a program named Wazuh would be monitoring the traffic of computers and the network. The wanted conclusion for the thesis was an assessment of feasibility and usefulness of the solution.

The test environment of the surveillance was a virtual computer network containing a Linux server and two Windows computers. In addition, a Kali Linux computer represented a malicious attacker. The installation process and the usage of the program were relatively easy, but problems appeared in the lack of essential defence mechanisms and functionalities. As many other options in the highly customizable program, they had to be switched on separately.

In conclusion, Wazuh was thought to be easy to use for people who knew information security vocabulary and had simple skills in Linux and Windows configuration commands, though that is currently a tall ask for every computer user in the current society. Also, the need for modification right away after installation is not wanted. Therefore, a SIEM program could be an information security tool for homes in the future, but currently they need more user friendliness.

---

Key words: information security, SIEM, home environment

**SISÄLLYS**

## LYHENTEET JA TERMIT

| | |
|---|---|
| Agentti | Käyttäjän tietokone, joka on osa agenttipohjaista hierarkiaa |
| Black Hat | Ilkeämielinen hakkeri |
| EICAR | European Institute for Computer Antivirus Research |
| HIDS | Host Intrusion Detection System, eli tietyn tietokoneen suojaamiseen keskittynyt ohjelma |
| Kojelauta | Graafinen käyttöliittymä, joka visualisoi ohjelman data yhteen paikkaan |
| Palvelin | Tietokone, joka tarjoaa erilaisia palveluita tietokoneverkkoon palvelinohjelmistolla |
| RAM | Random Access Memory, eli tietokoneen väliaikainen muisti |
| RDP | Remote Desktop Protocol, eli työpöydän etähallintaprotokolla |
| SEM | Security Event Management, eli turvallisuustapahtumien hallinta |
| SIEM | Security Information and Event Management, eli turvallisuustiedon ja -tapahtumien hallinta |
| SIM | Security Information Management, eli turvallisuustiedon hallinta |
| Tietokoneverkko | Tietokoneiden ja niitä yhdistävien laitteiden kokonaisuus |
| Tietoturva | Varmistaa tiedon saatavuuden, luottamuksellisuuden ja eheyden |
| Uhkapankki | Tietokanta tunnetuista tietoturvauhista |
| White Hat | Eettinen hakkeri |

# 1 JOHDANTO

Internet ja eri sovellukset jatkavat yhdistäytymistä meidän jokapäiväiseen elämäämme. Palveluita siirretään verkkoon ja arkipäivää pyritään helpottamaan uusilla tavoilla. Kaiken tämän takana jatkuu myös ainainen kamppailu tämän muutoksen hyväksikäyttäjien ja suojelijoiden välillä. Toisella puolella hyökkääjät (sanotaan myös Black Hat-hakkereiksi) pyrkivät pääsemään käsiksi tietoihin yksityisiltä ja julkisilta henkilöiltä, kun taas kääntöpuolella asiantuntijat (White Hat-hakkerit) kehittävät tapoja estää tämän tapahtumista. Hyppönen (2022) vastakkain asettelee tietotekniikan kukoistamisvaihetta 80-luvulta alkaen ja vertaa sitä nykypäivään. Hyökkääjillä on samoja taktiikoita vieläkin, mutta tulevaisuus tuo uusia mahdollisuuksia uusien keksintöjen myötä. (Hyppönen 2022). Tämä niin sanottu asekisa jää monelta kuluttajalta näkymättömäksi ja luotetaan käytössä olevan laitteen tai virustorjuntaohjelman tekevän tehtävänsä. Valitettavasti tietoturvan maailma on arvaamatonta ja ennennäkemättömiä hyökkäyksiä tapahtuu, vaikka niiltä yritetään suojautua.

Tämä herättää kysymyksen: voisiko kuluttaja tehdä enemmän suojellakseen omaa liikkumistaan elektronisessa maailmassa? Yritykset ovat kysymyksessä edelläkävijöitä, sillä liiketoimintaa kannattaa ja täytyy suojella kaikista näkökulmista. Ne ovatkin ottaneet erilaisia varoratkaisuja käyttöön. Yksi näistä on SIEM-ohjelmistot (Security Information and Event Management). Ne antavat tietoa yhdistettyjen laitteiden toiminnasta virustorjuntaohjelmien tavoin, mutta menevät vielä askeleen pitemmälle. Ohjelmistot keräävät tietoa tietokoneverkosta kattavammin ja tekevät johtopäätöksiä kerätystä kokonaisuudesta. Tämän työn tavoitteena on tutkia SIEM-ratkaisun toteutettavuutta kotiverkossa ja katsoa sen parantavaa vaikutusta tietoturvaan. Keskipisteenä on Wazuh-ohjelmisto, josta tehdään testiverkko kotiolosuhteita vastaavassa ympäristössä ja lisäksi sitä verrataan muihin markkinoilla oleviin vaihtoehtoihin.

# 2 SIEM-ohjelmistot

SIEM on ohjelmisto, joka tarkkailee tietoverkon ja sen laitteiden liikennettä. Tarkkailun tarkoituksena on kyber- ja tietoturvan ylläpito. SIEM-ohjelmistot yhdistävät turvallisuustiedon- ja turvallisuustapahtumien hallinnoinnin yhdelle alustalle, jota seurataan esimerkiksi verkkoselainpohjaisella kojelaudalla. SIEM käsittelee erittäin paljon tietoa, mutta se kerätään käsiteltävään ja visuaaliseen muotoon käyttäjälle kojelaudalle. Asettamalla monilähteistä tietoa reaaliaikaisen analyysiin, ohjelmisto pystyy reagoimaan monimuotoisiin uhkiin, johon esimerkiksi perinteiset virustorjuntaohjelmistot eivät pysty. Aikaiset kustomoitavat hälytykset takaavat nopean reagoinnin ja vahinkojen minimoimisen. Myös muokkausmahdollisuuksia on paljon, mikä mahdollistaa tiettyihin verkon tapahtumiin ja ongelmiin kohdentamisen. SIEM:in historiaa ei ole tarkoin määritelty, sillä se muodostui kehittyvän teknologian tarpeeseen eri muodoissa eri valmistajilta. Tämän takia myös toteutuksia on erilaisia, mutta kaikilla niillä on yhteneviä piirteitä.

Yleisiin SIEM-ohjelmistojen piirteisiin ja tarkoituksiin kuuluvat

- tietojen kerääminen yhteen paikkaan
- tapahtumien tarkastelu, korrelointi, analyysi ja hälytys
- datan säilytys pitkäaikaista käyttöä varten
- kojelaudat tiedon sisäistämisen helpottamiseksi visuaalisilla keinoilla
- määräystenmukaisuuden hallinta ja raportointi.

SIEM-ohjelmiston käyttöönotossa on tärkeä huomioida käytettävän ympäristön tarpeet. Huomioitavana asiana esille nousee vertailu agenttipohjaisesta ohjelmasta verrattuna agentittomaan. Agenttipohjaisessa ympäristössä seurattaville laitteille asennetaan automaattisesti toimiva ohjelmisto, joka lähettää tietoja palvelimelle. Laitteisiin voidaan myös viitata suoraan termillä agentti. Agentittomassa ympäristössä palvelin pyytää tietoja suoraan laitteelta. Asennetun ohjelmiston avulla on mahdollista saada yksityiskohtaisempaa tietoa laitteen toiminnasta. Toisaalta agenttien asentaminen ja ylläpitäminen on ylimääräistä työtä.

Tässä työssä keskitytään tapahtumien tarkasteluun tarjolla olevien työkalujen ja hälytysten avulla. On kuitenkin hyvä huomata, että yrityksille ohjelmasta on olemassa paljon ylimääräistä hyötyä. Esimerkiksi tietoturva-asetusten täyttämistä voi olla vaikea seurata, mutta SIEM-ohjelman raporttien avulla saa nopeasti tietoa verkon tilanteesta lain vaatimuksiin verrattuna.

## 2.1 SIEM:in historia ja nykytilanne

Tietoturvan ja teknologian kehittyessä palomuurit ja säännöt eivät riittäneet enää työkaluiksi uusille tilanteille. Manuaalisen työn määrä oli liian suuri ja käytössä ei ollut tarpeeksi skaalattavia vaihtoehtoja. Gartnerin raportissa esitettiin ensimmäistä kertaa termi SIEM, joka yhdistää käsitteet security event management (SEM) ja security information management (SIM) (Williams & Nicolett 2005). Termien yhdistäminen kuvaa kokoavaa ratkaisua, joka keräisi lisääntyneet lokitiedot ja muun verkon datan yhteen paikkaan. Kaiken kerätyn datan läpi lukeminen manuaalisesti olisi vienyt lukemattomia työtunteja. Tämän jälkeen saadut tulokset olisivat myös suurella todennäköisyydellä vanhentuneita, koska tilanne on jo kehittynyt seuraavaan vaiheeseen. Olisi siis tarvittu tehokas ohjelmisto ja laitteistoyhdistelmä, joka olisi voinut hoitaa läpikäymisen. Gailey (2020) arvioi 2000-luvun alussa saatavilla olevaa teknologiaa ja sen vaikutusta kehitykseen. Aikaiset järjestelmät kohtasivat ongelmia skaalautuvuuden kanssa, sillä monet kohdat, kuten hälytysten tarkastelu, vaativat manuaalista käyttäjän puuttumista toimintaan. Lisäksi ohjelmistojen vaativia järjestelmävaatimuksia oli vaikea täyttää sen aikaisella teknologialla. (Gailey 2020).

Nykytilanteessa pilvipalveluja ja koneoppimista hyödyntämällä SIEM-ohjelmistoista on tullut tehokkaita tiedon analysaattoreita, sekä poikkeuksien löytäjiä. Velásquez, Monterrubio ja Crespo (2023) tarkastelevat SIEM-teknologioiden tilannetta vertailemalla eri tahojen julkaisemia artikkeleita ja tutkimuksia. Uudet tietotekniikan ratkaisut ovat kehittäneet SIEM:ien toimintamahdollisuuksia ja tulevaisuus näyttää olevan juuri näiden paremmassa integraatiossa. (Velásquez, Monterrubio ja Crespo 2023). Tietotekniikan kehittymisen takia ohjelmistoihin on pystytty liittämään lisäominaisuuksia. Yksi esimerkki niistä on jatkuvasti päivittyvät niin sanotut uhkapankit, joista saadaan ajankohtaista tietoa uusista uhista tietoturvalle maailmalla. Käyttämällä verkon toiminnasta saatua informaatiota, ohjelma pystyy muodostamaan ympäristölle normaalin vertailukohdan. Sen jälkeen poikkeustilanteita pystytään vertaamaan siihen. Esimerkiksi yhdessä yrityksessä tapahtuva tietoliikenne voi olla hälyttävää, kun taas toisessa yrityksessä se on normaalia. Tämän ja muiden tekniikoiden avulla jokainen SIEM-ratkaisu on erilainen, mutta tarpeisiin kohdistettu. Tulevaisuudessa teknologian analysointiteho ja kykenevyys tulevat todennäköisesti jälleen kasvamaan, jolloin SIEM:in merkittävyys työkaluna tulee nousemaan entisestään. Velásquez, Monterrubio ja Crespo (2023) huomasivat lähes kaikkien ehdotettujen ideoiden SIEM:in kyvykkyydestä tulleen toteen epäilyistä huolimatta viimeisen 12 vuoden aikana. (Velásquez, Monterrubio ja Crespo 2023).

## 2.2 Virustorjuntaohjelmistot ja SIEM

Oletuksena kaikilta nykyisiltä tietokoneilta löytyy virustorjuntaohjelmisto valmiiksi asennettuna ja toiminnassa. Lisäksi markkinoilta löytyy laajasti käytettyjä ilmaisia ja maksullisia ohjelmistoja. Yksinkertaisesti mietittynä SIEM voi kuulostaa vain erilaiselta virusten löytämisen ratkaisulta, mutta todellisuudessa näiden toiminnassa on eroa. On hyvä lähteä oletuksesta, että mikään ei turvaa kaikelta, mutta erityisesti virustorjuntaohjelmat on tehty tarkasti yhteen tehtävään, eli suojelemaan päätelaitetta. Tämä lähtökohta on rajallinen nykymaailmassa, jossa rikolliset tietävät minkälaisiin ympäristöihin he pyrkivät pääsemään sisälle, jolloin tunkeutumiskanavat voivat olla missä tahansa verkon sisällä. SIEM tarkkailee koko verkon liikennettä päätelaitteen lisäksi ja tekee päätelmiä yhteyksistä ja poikkeavuuksista. Virustorjuntaohjelma tarkastelee paikallisia tapahtumia ja vertaa niitä tunnettuihin uhkiin. Se ei osaa vastata tuntemattomiin tapahtumiin, paitsi parhaassa tilanteessa varoittamalla vieraasta käyttäytymisestä. Kyseinen tietämättömyys voi myös johtaa usein niin sanottuun false positive-tilanteeseen, jossa havaittu uhka ei olekaan vaarallinen.

Yrityksissä hyvä käytäntö on kerrostettu puolustus, jossa turvallisuuden parantamiseksi käytetään monta palvelua. Tällöin käytössä voisivat esimerkiksi olla molemmat SIEM ja virustorjuntaohjelmat päätelaitteilla. Kuitenkin nousee kysymys tämän tarpeellisuudesta kotiverkossa ja tähän mietintään palataan tämän työn lopussa. Kuitenkin tällä katsonnalla SIEM tarjoaa paljon tietoa ja kustomoitavuutta, jota ei perinteisellä ratkaisulla saa.

# 3 Wazuh

Wazuh on 2015 vuotena alkunsa saanut turvallisuusalusta, joka tarkkailee ja analysoi verkon sekä laitteiden tietoturvaa. SIEM-ratkaisuna Wazuh keskittyy laitteiden liikenteeseen ja turvaamiseen. Avoimen lähdekoodin kautta käyttäjät voivat vaikuttaa ohjelmiston kehittymiseen ja halutessaan käyttää sekä muokata koodia, miten sitä itse haluaa. Wazuh on kerennyt saamaan laajan käyttäjäkunnan, mutta markkinoilla on myös muita kilpailevia vaihtoehtoja.

## 3.1 Yleiskuva Wazuhista

Wazuh on ilmainen turvallisuusratkaisu ja se sopii pienistä keskikokoisiin verkkoihin. Sen toimintamalli SIEM:inä on kuitenkin sama riippumatta ympäristöstä. Palvelin kerää tietoja laitteille asennetuilta agenteilta. Tieto asetetaan reaaliaikaiseen analyysiin, jonka tulokset näkyvät verkkoselainpohjaisella kojelaudalla. Palvelin pitää verkkosivua toiminnassa siinä verkossa mihin se on yhdistetty. Palvelinta on tarkoitus pitää toiminnassa vuorokauden ympäri, jotta tietoa kerätään kaikista tapahtumista. Täten tietokoneen kojelaudalle voi kirjautua koska tahansa tarkastelemaan turvallisuustapahtumia. Tarkastelua ei kuitenkaan ole mahdollista tehdä koko aikaa arkielämässä, minkä takia ohjelmassa on mahdollista asettaa sähköpostiin lähetettävät hälytykset. Hälytyksien sääntöjä voi muokata haluamikseen, jotta vain oleellisista tapahtumista tulee sähköposti.

Wazuh ei vaadi paljon resursseja, joten se ei ole vaativa tietokoneen suorituskyvyn kannalta. Tämä kuitenkin muuttuu, jos ympäristöön lisätään useampia palvelimia ja agenttien määrä kasvaa merkittävästi. Alkuun pääsee kuitenkin seuraavilla vaatimuksilla palvelimelle:

- 64-bittinen Linux-käyttöjärjestelmä (Amazon Linux 2, CentOS 7, 8, Red Hat Enterprise Linux 7, 8, 9 tai Ubuntu 16.04, 18.04, 20.04, 22.04)
- 2 GB RAM-muistia kahdella prosessoriytimellä (suositeltu 4 GB RAM-muistia 8 prosessoriytimellä).

Edellä mainitun lisäksi tietokoneelle, jolla tarkastellaan kojelautaa, suositellaan 8 GB RAM-muistia neljällä prosessoriytimellä. Tuettuja verkkoselaimia ovat Chrome, Firefox ja Safari. On kannattavaa myös varata levytilaa ohjelman lokitietoja varten, jotta vanhoja tietoja voidaan säilyttää pitempään.

### 3.2 Wazuhin vahvuudet ja heikkoudet

Wazuhin vahvuutena näkyy sen yksinkertaisuus ja maksuttomuus. Tämä ilmenee Suskalon, Moricin, Redzepagicin ja Regvartin (2023) vertailussa, jossa Wazuhia verrataan IBM QRadar ohjelmaan. Wazuh tarjoaa paljon ominaisuuksia, joita SIEM-ohjelmasta voisi toivoa. Lisäksi Wazuh on helppokäyttöinen ja se sopii hyvin pienempiin ympäristöihin, koska sen käyttöönotossa ei ole lisenssikustannuksia. Lisäksi avoin lähdekoodi tuo ihmisiä yhteen ratkaisemaan ohjelmassa piileviä ongelmia. Käyttämällä avoimia keskustelupalstoja, pystyy löytämään tukea yllättäviinkin kysymyksiin ohjelman käytöstä. Suskalo, Moric, Redzepagic ja Regvart (2023).

Vaikka Wazuh on helppokäyttöinen, se silti voi vaatia konfiguraatiota alkuvaiheessa tiettyjen haluttujen ominaisuuksien toteuttamiseksi. (Packetlabs 2023). Toteuttaminen vaatii perehtymistä ohjelman toimintaan, mikä vaikeuttaa käyttöä alkuvaiheessa. On myös kannattavaa huomioida ilmaisen ohjelmiston kääntöpuoli. Vakavassa ongelmatilanteessa varmaa apua ei ole saatavilla. Tämän voi halutessaan välttää hankkimalla maksullisia Wazuhin virallisia tukipalveluita.

### 3.3 Wazuh verrattuna kilpailijoihin

Wazuhun verrattuna markkinoilta löytyy vastaavaa tarjontaa, usein ilmaisten versioiden kautta. Pienessä kotiverkossa ei ole samankaltaisia tarpeita verrattuna yritykseen, minkä pohjalta on valittu vertailtavat tuotteet taulukkoon 1. Samalla tarkastellaan kuitenkin myös laajennusmahdollisuuksia ja potentiaalia toimia suuremmassa kokonaisuudessa.

TAULUKKO 1. Wazuhin ja muiden valikoitujen SIEM-kilpailijoiden pääpiirteet taulukoituna.

| Tuote | Julkaisuvuosi | Maksullinen | Kohdeympäristö |
|---|---|---|---|
| **Wazuh** | 2015 | Ei | Pieni-keskikokoinen |
| **Security Onion** | 2009 | Ei | Pieni-keskikokoinen |
| **Elastic** | 2010 | Kyllä (ilmais-versio ole-massa) | Pieni-Suuri |
| **Splunk** | 2004 | Kyllä (laajasti rajattu ilmais-versio ole-massa) | Suuri |

Security Onion on vanhempi ohjelma verrattuna Wazuhun, kuten muutkin kilpailijat listassa. Ajan myötä ohjelman kehityksellä on ollut enemmän aikaa. Kiinnostavasti Wazuh oli ennen osa Security Onionia, ennen kuin se siirtyi itsenäiseksi ohjelmaksi, minkä takia näissä kahdessa on paljon samoja asioita. Kuitenkin Wazuhin toiminnallisuudet ovat enemmän HIDS (Host Intrusion Detection System) -puoleen asettuvia verrattuna Security Onionin perinteiseen SIEM:in kaltaiseen toimintaan. Wazuh perustaa toimintansa suureksi osaksi päätelaitteiden liikenteen dataan, kun taas Security Onion tarkkailee paljon verkon liikennettäkin. Molemmat ovat avoimen lähdekoodin ohjelmia ja ilmaisia. Kuitenkin maksullista virallista tukea ja koulutusta on saatavilla, mikä antaa edun maksullisiin vastakappaleisiin siinä, että alkuun pääsee kustannuksitta ja osaamista voi lisätä pienissä määrin aina tarpeen mukaan. Yksinkertaisuudellaan molemmat sopivat pienistä verkoista keskikokoisiin, mutta ilman kertynyttä kokemusta ja maksullista tukea täytyisi ensin harkita tarkasti ennen ohjelmien asettamista suureen verkkoon. Näiden ominaisuuksien perusteella myös Security Onion voisi sopeutua työn tutkimuskohteeksi.

Elastic ja tarkemmin sen alatuote Elasticsearch antaa tietoja liikenteestä samaan tapaan kuin Wazuh. Ilmaisversio on rajattu, mutta tarjoaa paljon vaihtoehtoja. Verrattuna Wazuhun, Elasticsearch ei ole niin valmis paketti heti käytettäväksi. Muokattavuuspaketit, kuten visualisointikojelauta Kibana, ovat tarjolla ilmaiseksi ladattavina. Teoriassa niistä kokoamalla pystyisi tekemään tarpeen mukaisen erinomaisen ympäristön. Kuitenkin kotiympäristössä enemmän valmiiksi rakennettu ratkaisu on eduksi, sillä se vähentää opiskeluun käytettävää aikaa. Elasticsearchista saisi maksullisilla ominaisuuksilla voimakkaan työkalun ja niillä se voisi soveltua jo isommallekin yritykselle. Elasticin tuotteisiin on saatavilla paljon materiaalia ja mahdollisia koulutuksia. Työn skaalalle kuitenkin Wazuh soveltuu paremmin.

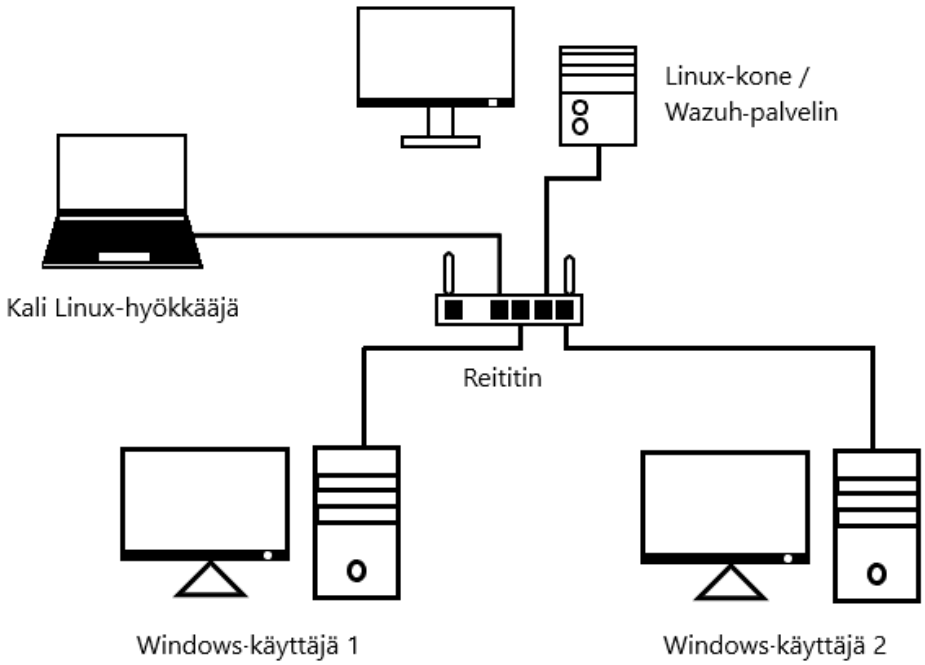
Splunk on pitkään markkinoilla ollut ohjelmistokehittäjä ja heidän tuotteensa Splunk Enterprise on monen tarpeen kattava. Nimestäkin päätellen ohjelmisto on suunniteltu suuriin ympäristöihin. Ilmainen versio on olemassa, mutta sen rajaukset tekevät siitä enemmän kokeiluversion. Liikkuvan datan määrä on rajattu ja turvallisuusominaisuuksia, kuten kirjautuminen, ei ole käytössä. Splunkin hinnoittelu ei myöskään ole suunnattu yksityisille henkilöille. Näin ollen Splunk on vaihtoehto suuriin tarpeisiin, mutta tälle työlle se ei ole varteenotettava vaihtoehto.

# 4 Wazuh kokeilu kotiverkossa

Tutkimukseen lähdettiin lähtökohdasta, jossa tietokonetta usein käyttävä henkilö pyrkii parantamaan tietoturvaa kodissaan Wazuhin avulla ja mitä tämä vaatisi. Vertailukohdan tilanteessa tietoturvan suojana on vain palomuuri ja virustorjuntaohjelma. Alusta tiesin asennuksen vaativan ainakin jonkin verran tietämystä erilaisista valikoista ja komennoista, joten ihan aloittavan tietokoneen käyttäjän näkökulmasta en kokeilua tarkastele. Tärkeitä tekijöitä kannattavuudelle ovat testiympäristön asennuksen ja ylläpidon helppous, ymmärrettävyys ja konkreettisen hyödyn saaminen.

## 4.1 Testiympäristö ja sen asennus

Testiympäristöksi valitsin Linux-koneen, joka toimii Wazuh-palvelimena ja kaksi Windows konetta, jotka simuloivat kahta muuta käyttäjää kodissa esimerkiksi perheenjäseniä. Linux-kone on kodissa jossakin pääkäyttäjän saatavilla ja suojattu salasanalla. Windows-koneet voivat olla kodissa missä tahansa, kunhan ne ovat yhdistetty reitittimen kautta samaan verkkoon. Viimeisenä kokoonpanoon on yhdistetty Kali Linux-käyttöjärjestelmäinen tietokone, joka edustaa pahantahtoista hyökkääjää. Tämä tietokoneverkko on havainnollistettu kuviossa 1. Kaiken tämän simuloimiseksi käytin VMware-ohjelmistoa, mikä vastaa reaalitilannetta fyysisillä laitteilla käyttämällä virtuaalikoneita.




KUVIO 1. Työssä käytetty tietokoneverkko havainnollistettuna.

Palvelimen asennus onnistui vaivattomasti yhden komennon avulla komentorivillä, joka kutsui asennusassistenttia Wazuhin nettisivuilta. Asennuksen jälkeen näytölle tulostui ylläpitäjän tunnukset ja Wazuh oli käyttövalmis menemällä kojelaudalle, jonka saa näkyviin kirjoittamalla verkkoselaimen hakupalkkiin asetetun IP-osoitteen. Osoite oli sama kuin tietokoneelle asetettu staattinen, eli muuttumaton IP-osoite reitittimessä. Kojelauta antoi valmiin komennon agenttien asentamista varten muille koneille. Komento on yleinen, mutta hieman riippuvainen kohdekäyttöjärjestelmästä, Wazuh-serverin IP-osoitteesta ja agentin haluamisesta nimeämisestä. Täysin valmiin komennon saaminen kojelaudan kautta oli kätevä tapa. Komennon asettaminen Windowsin Powershell-komento-ohjelmaan vaati ylläpitäjäoikeuksia, jonka jälkeen agentit olivat asennettuja ja yhteys palvelimeen muodostettu. Oletuksena palvelin ja agentit käynnistyvät automaattisesti tietokoneiden kanssa, joten Wazuh oli käyttövalmis.

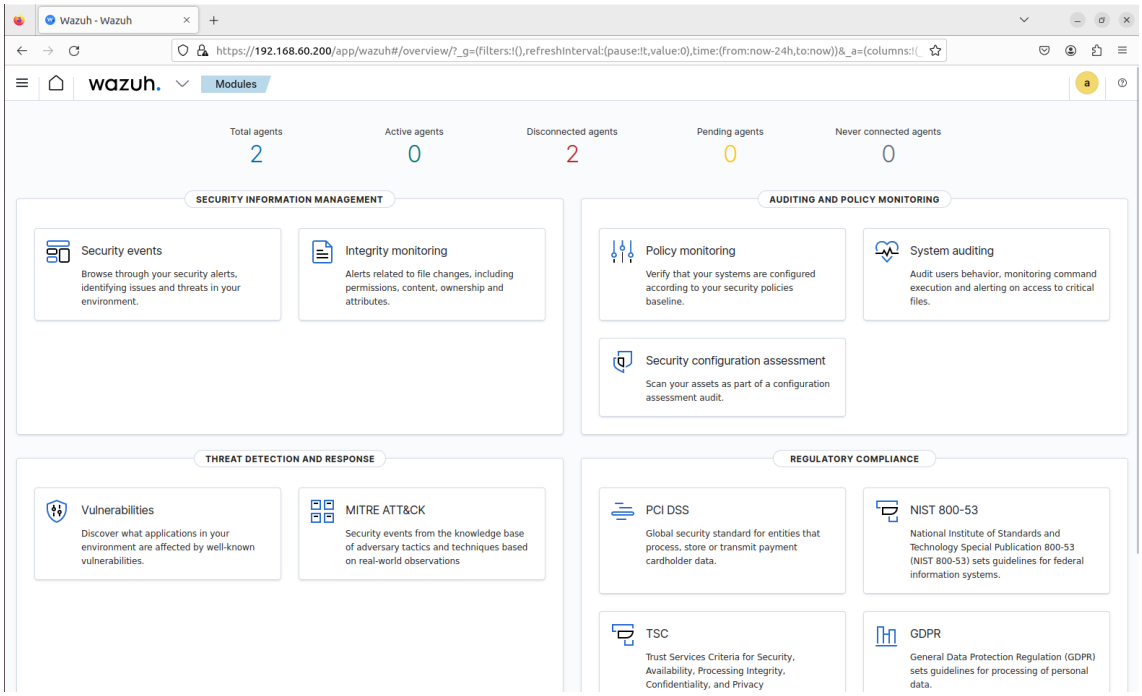
Ongelmia asennuksen kanssa tuli vain virtuaalikoneiden ja IP-osoitteiden kanssa, joita normaalikotiympäristössä ei tapahtuisi. Huomioitavana on kuitenkin, että Linux-koneelle täytyy asettaa muuttumaton IP-osoite sen asetuksissa, koska muuten agentit voivat yrittää yhdistää väärään osoitteeseen vaihdon jälkeen esimerkiksi DHCP:n (Dynamic Host Configuration Protocol) aiheuttamana. Agenttien tietokoneet voivat olla oletuksena muuttuvilla IP-osoitteilla, sillä Wazuh ei käytä niitä pääasiallisena tunnistuskeinona. Koko asennusprosessi on koottuna taulukkoon 2.

TAULUKKO 2. Wazuhin asennusprosessi. Prosessi kattaa itse palvelimen ja agenttien asennuksen.

| Asennusvaihe | Toimenpide | Selite |
|---|---|---|
| **Palvelimen asennus Linux-koneelle** | Staattisen IP-osoitteen asetus | Linux-koneelle täytyy asettaa muuttumaton IP-osoite reitittimessä, jotta agentit löytävät sen luotettavasti. |
| | Asennuskomennon syöttäminen | Linuxin terminaaliin syötettävän komennon saa Wazuhin nettisivuilta. Se hakee asennuspaketin Wazuhin nettisivuilta ja asentaa sen. Kirjautumistunnukset tulostuvat näytölle. |
| | Wazuhin kojelaudan testaus | Kojelauta on saatavilla kirjautumistunnuksilla verkkoselaimessa. Sitä pääsee käyttämään syöttämällä palvelintietokoneen IP-osoite selaimen hakupalkkiin. |
| **Agenttien asennus** | Asennuskomennon kopioiminen | Wazuhin kojelaudalta pääsee tekemään agenteille asennuskomennon. Ohjelma tarvii tiedoiksi käyttöjärjestelmän ja haluamansa nimen agentille. |
| | Agenttien asennuskomennon syöttäminen | Edellisessä askeleessa saatu komento syötetään Windows-koneiden Powershell-ohjelmaan. |
| **Asennuksen testaus** | Yhteyden varmistaminen | Nyt asennetut agentit näkyvät Wazuhin kojelaudalle kirjautuessa. |

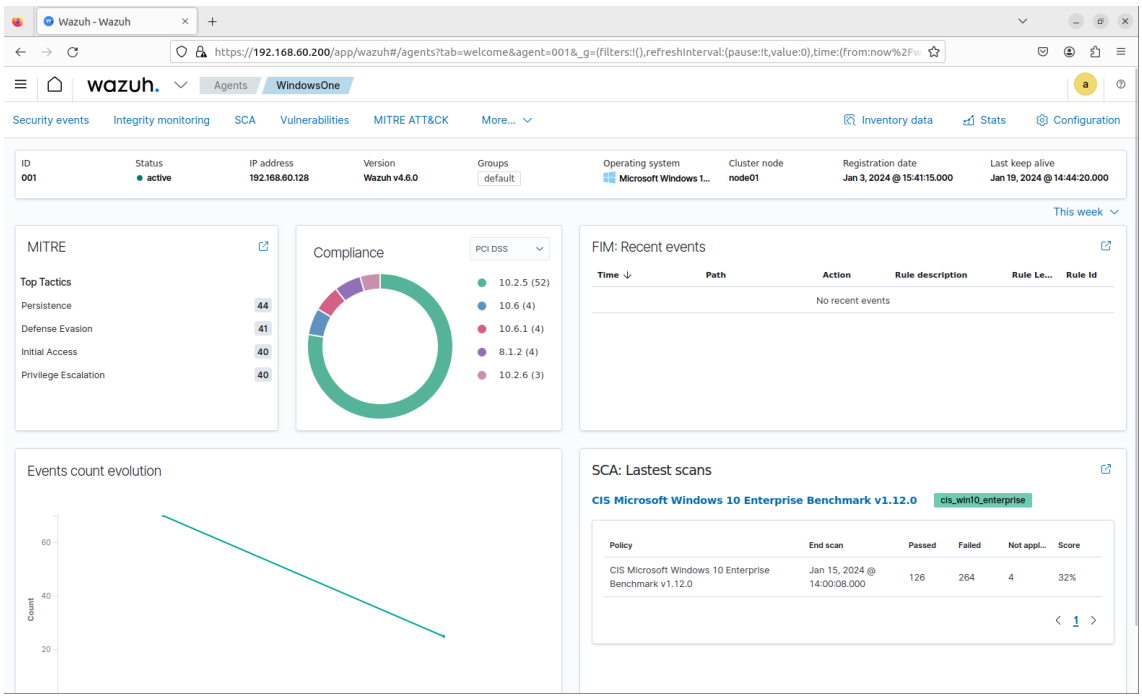
## 4.2 Wazuh-kojelauta

Wazuhin perusnäkymä aloitussivulla antaa ohjelman tarjonnan yksinkertaisella näkymällä, mikä näkyy kuvassa 1. Kerättyä tietoa voi tarkastella otsikoiden alta tai laite kerrallaan valitsemalla ensin laitteen eli agentin, minkä jälkeen data suodatetaan vain sitä koskevaksi.



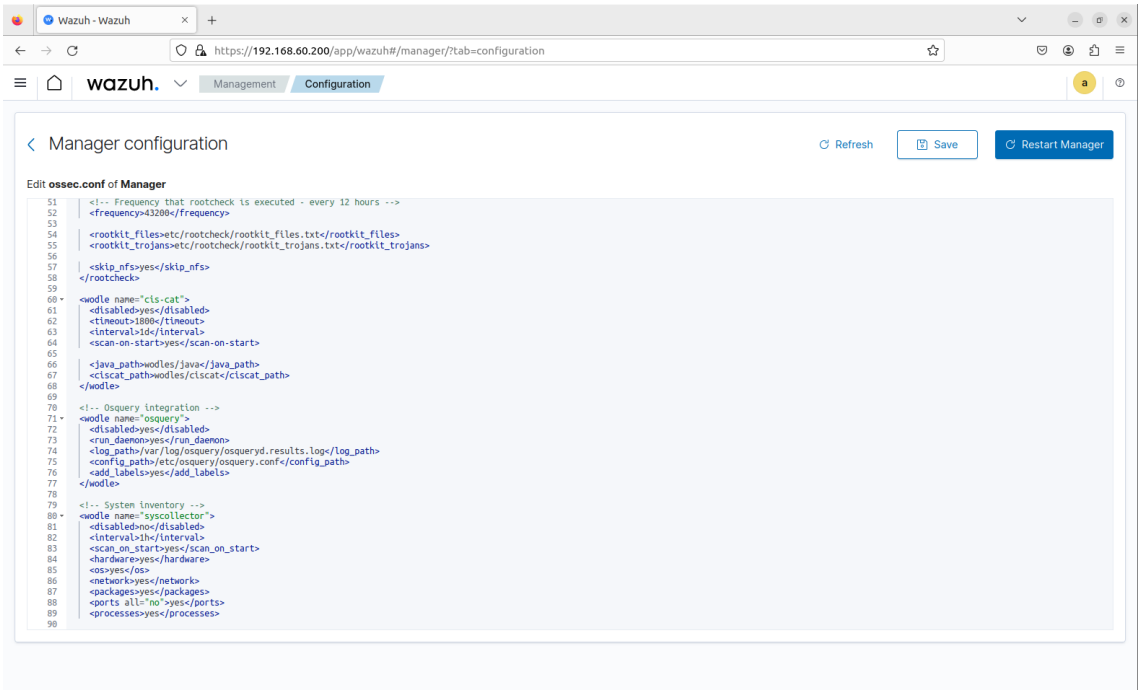

Kuva 1. Wazuh-kojelauta, jossa näkyvät ohjelman ominaisuudet.

Yksittäisen laitteen näkymä antaa nopean kuvauksen viimeaikaisista tapahtumista, mikä näkyy kuvassa 2. Wazuhin kaikkia näkymiä on täytetty taulukoilla ja kuvaajilla, jotka helpottavat tietojen sisäistämistä. Halutun tarkan tiedon löytäminen voi kuitenkin olla useiden valikoiden takana, jolloin täytyy tietää käytettyä termistöä ja osata käyttää suodatinasetuksia.




KUVA 2. Wazuhin yksittäisen laitteen kohdenettu näkymä.

Tärkeä osa ohjelmistoa on myös sen muokattavuus. Haettavia tietoja ja palveluita voi valita tarpeen mukaan. Lisäksi esimerkiksi aktiivisia toimenpiteitä tapahtumiin pystyy asettamaan ehtojen mukaan. Tällöin tapahtuman tiedon tallentamisen lisäksi ohjelma lähettää käskyn suorittaa toimenpide agentille. Näin pystyy käytännössä reagoimaan eri uhkiin, joita on huomannut kotiverkossa. Kaikki nämä ei kuitenkaan onnistu suoraan valikosta valitsemalla, vaan muutokset täytyy tehdä koodiin, jonka voi avata asetuksista. Koodi on kuvattu kuvassa 3. Esimerkiksi mahdollisesti hyödyllinen Osquery-palvelu, joka hakee laitteiden tietoja, on oletuksena poistettu käytöstä. Sen voi ottaa käyttöön muuttamalla teksti no muotoon yes riviltä 81. Asetuksia voi katsoa lista muodossa, mutta valitettavasti niitä ei voi muokata siitä.




KUVA 3. Wazuhin konfiguraatiokoodi. Muutokset haluamiinsa palveluihin tehdään muuttamalla tätä tekstiä.

Tärkeä osa Wazuhin toimintaa ovat sen hälytystoiminnot. Kojelautaa ei luonnollisesti tarkastella koko aikaa, joten tärkeät tapahtumat voivat helposti jäädä huomaamatta. Tämän vuoksi on hyvä asettaa hälytykset itselle tärkeille poikkeamille. Hälytykset eivät ole oletuksena toiminnassa ja ne tarvitsevat lisää konfiguraatiota, jos niiden haluaa tulevan yleisesti käytettyihin sähköpostipalveluihin. Prosessiin on olemassa ohjeet Wazuhin verkkosivuilla, mutta ei suoraan ohjelmassa. Asennuksen aikana voi valita hälytystason, jonka mukaan määräytyy minimitärkeys niistä hälytyksistä, jotka lähtevät sähköpostiin. Lisäksi voi tehdä omia sääntöjä. Esimerkiksi voi määrätä sähköpostin lähetettäväksi aina kun tapahtuu epäonnistunut kirjautumisyritys tietyllä agentilla. Jokainen asennus on erilainen riippuen käytettävästä sähköpostipalvelusta ja -osoitteesta, mutta hälytyksien kuulumattomuus oletuspakettiin vaikeuttaa käyttöönottoprosessia.

## 4.3 Wazuh-testit

Teoriassa ohjelman käyttöönotto ja käyttäminen vaikuttavat suhteellisen helpolta, mutta parhaiten käytännön puolta näkee testaamalla. Testeiksi valittiin erilaisia oikean elämän tilanteita, joista ohjelmiston pitäisi huomauttaa. Testataan siis ensinnäkin hälytysten ilmestymistä ja niiden tarkkuutta. Kaikki muu lisätieto on myös hyödyllistä.

### 4.3.1 EICAR

EICAR (European Institute for Computer Antivirus Research) on yhdistys, joka tekee tutkimusta virustorjuntaan liittyen. Heidän kehittämänsä testitiedosto vastaa oikeaa virusta sen rakenteessa. Sen voi ladata heidän nettisivultaan ja tämän testin tarkoituksena on katsoa Wazuhin reaktio siihen. Alkuoletuksena on hälytys vaarallisesta tiedostosta ja mahdollisesti lisätietoa sen alkuperästä. Varsinaista käytännön toimintaa ei tule tapahtumaan, sillä se vaatisi erillisen säännön konfiguraatiotiedostoon.

Testitiedostoja on tarjolla neljää erilaista:

- COM-tyyppinen suoritettava tiedosto
- tekstitiedosto
- pakattu tiedosto
- syvemmin pakattu tiedosto.

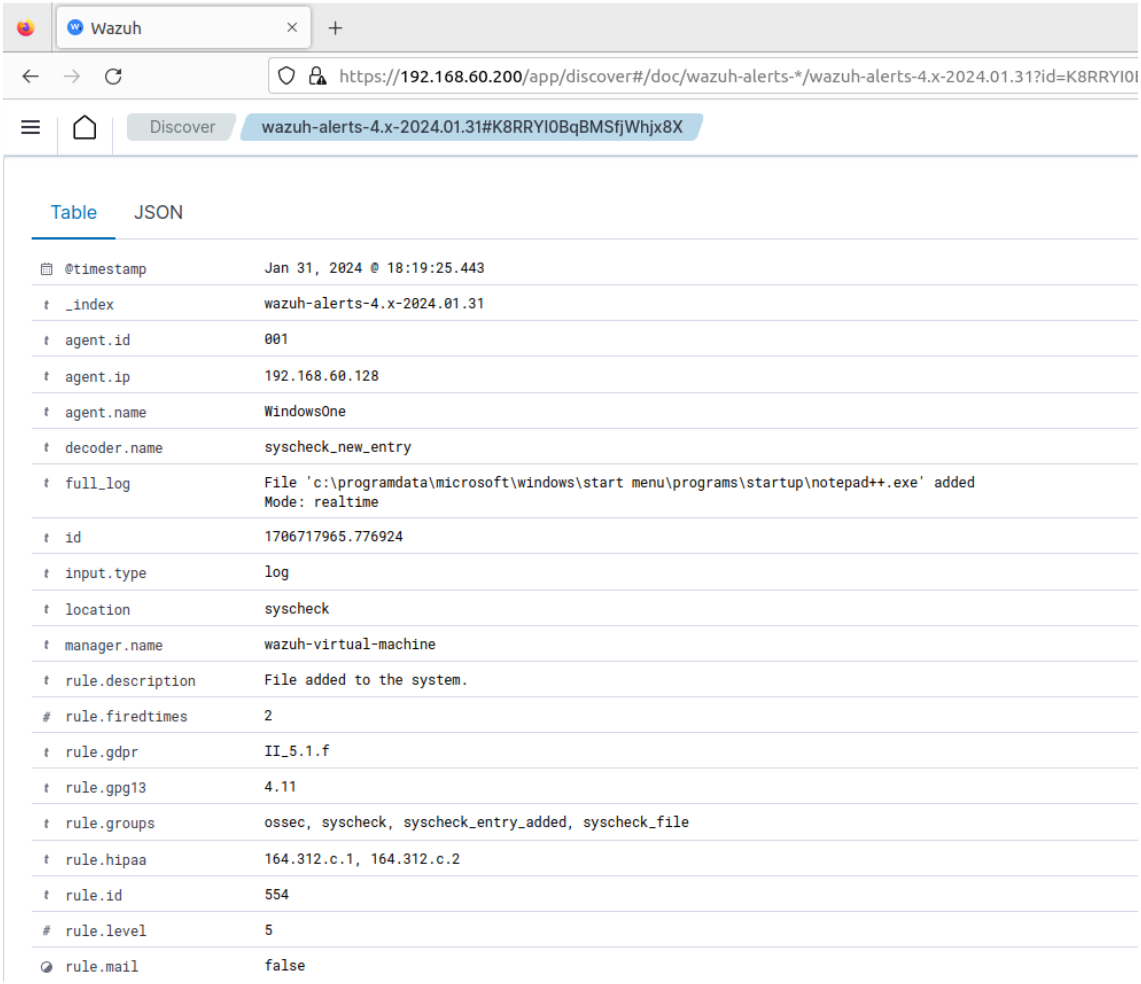
Eri tiedostot testaavat torjuntaohjelmaa eri tavalla. Suoritettavia tiedostoja on tärkeä tarkkailla, koska niitä käynnistäessä voi tapahtua suurta vahinkoa. Ne ovat siis olennaisia tarkastaa jo latausvaiheessa. Tekstitiedosto on tässä tapauksessa ensimmäinen tiedosto toisessa muodossa. Pakattu tiedosto on taas tiivistetty versio, joka täytyy tarkastaa eri tavalla. Lisäksi viimeinen kohde on vaikeampi käydä läpi, koska haitallinen osuus on asetettu syvemmälle tiedostorakenteeseen.

Windows-koneelle oletuksena asennettu virustorjuntaohjelmisto Windows Defender varoitti kaikista tiedostoista ja asetti ne automaattisesti karanteeniin latauksen yhteydessä. Tässä vaiheessa Wazuh ilmoitti vain normaalia korkeampien oikeuksien käyttämisestä, mikä liittyy Defenderin toimintaan. Testiä varten piti siis ensin ottaa virustorjunta pois päältä. Kiinnostavasti Wazuh ei huomauttanut virustorjunnan ja palomuurin sammuttamisesta. Siihen olisi hyvä asettaa sääntö, jos Wazuhin ottaisi itse käyttöön. Tämän jälkeen tiedostot sai ladattua koneelle, mutta alkuoletusta vastaan Wazuhun ei tullut tästä turvallisuusilmoitusta. Tästä päätellen Wazuh ei oletuksena tarkastele ladattuja tiedostoja. Täytyisi siis asettaa sääntö tarkastelemaan kaikkia uusia tiedostoja tietyissä kansioissa tai koko järjestelmätasolla. Toinen vaihtoehto olisi Windows Defenderin lokien ohjaaminen Wazuhun, jolloin karanteenista tulisi ilmoitus.

### 4.3.2 Tiedoston lisääminen suojattuun kansioon

Edellinen testi ei antanut ilmoitusta kojelautaan, koska tehtyä toimenpidettä ei vastannut sääntö ohjelman asetuksissa. Tällä kertaa kokeillaan tiedoston lisäämistä Windowsin ‘Startup’ kansioon, joka on oletuksena Wazuhin tarkkailun alla. Kyseisen kansion tiedostot ja ohjelmat avataan automaattisesti tietokoneen käynnistyksen yhteydessä, mikä tekee siitä oivan paikan haittaohjelmille. Kojelautaan toivotaan jälleen ilmoitusta lisäyksestä, sekä mahdollisimman paljon lisätietoa. Internetistä ladattu Notepad++-ohjelma on yksinkertainen tekstinkäsittelyohjelma ja siinä mukana tuleva .exe-päätteinen ohjelmatiedosto on hyvä testauskohde.

Tiedoston lisäämisestä ilmestyi lokitieto Wazuhun. Ote ilmoituksen tiedoista on esitetty kuvassa 4. Tiedoista voidaan päätellä muun muassa tapahtuman tarkka ajankohta, kyseessä oleva laite, tarkka tiedoston nimi ja polku sekä ilmoituksen sääntötaso. Tiedot ovat hyödyllisiä ja tarpeen tullessa aikaleimaa voisi verrata reaalimaailmaan, josta voisi päätellä esimerkiksi mahdollisen tietokoneen käyttäjän, jolla on ollut pääsy koneelle silloin. Muutos vastaa sääntötaso viisi, joka on suhteellisen alhainen verrattuna esimerkiksi haittaohjelman lisäyksen vaaraa kansioon. Toisaalta sääntöä voisi muokata, jolloin sääntötaso olisi suurempi. Tai voisi ottaa myös käyttöön erillisen tietouhkapankin, joka vertailisi uusia tiedostoja tunnettuun uhkakantaan. Tällöin tulisi vielä erillinen ilmoitus haitallisista tiedostoista.

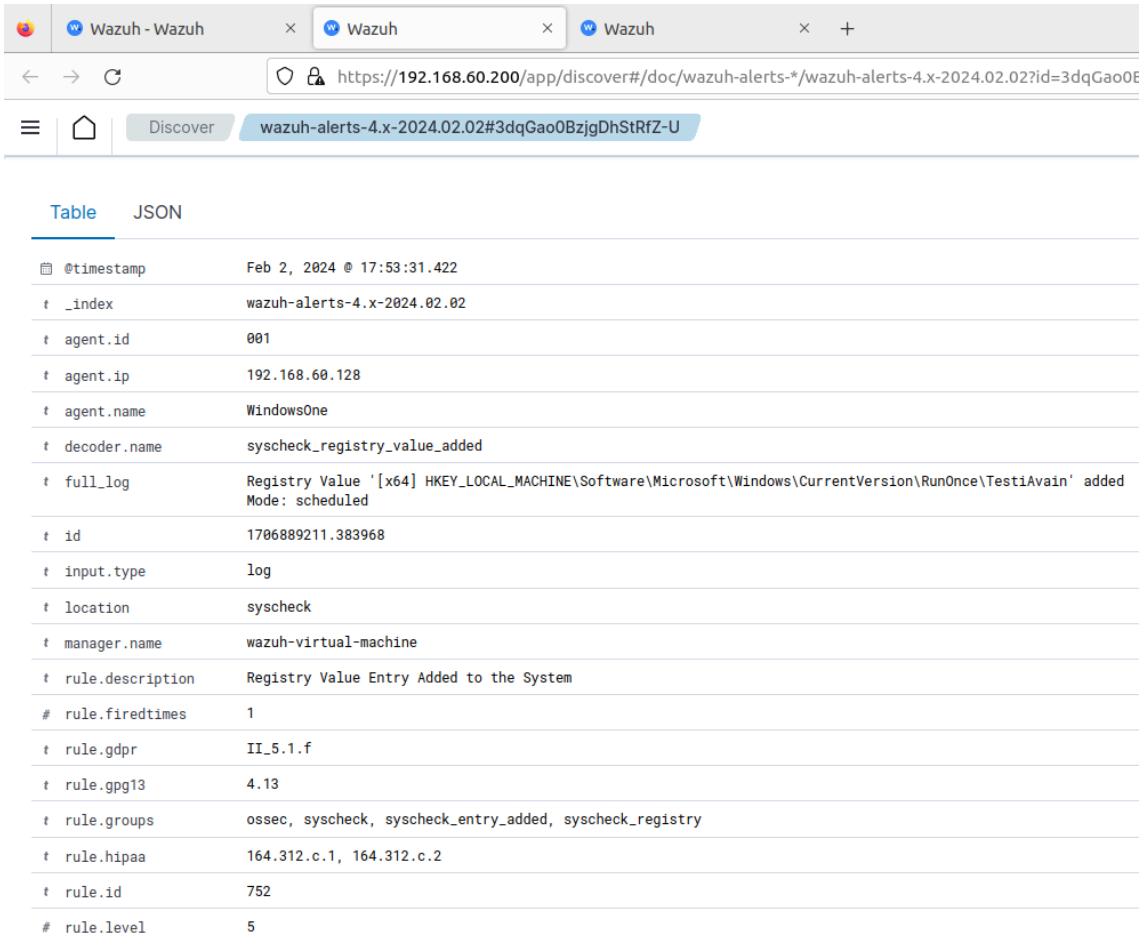



Kuva 4. Wazuh-näkymä keskitettynä yhteen tapahtumaan. Kyseessä on ‘Notepad++’-ohjelman lisääminen suojattuun kansioon ja siitä seuraava lokitieto.

### 4.3.3 Rekisteriavaimen muutos

Wazuh tarkkailee agenttien yhtenäisyyttä oletuksena 12 tunnin välein. Yksi osa sitä on Windowsin rekisteriavainten muutosten seuranta. Rekisteristö pitää sisällään tärkeitä asetuksia, vaihtoehtoja ja muita tietoja liittyen järjestelmän ohjelmiin ja toimintaan. Suunnittelematon tietojen muutos siellä voi olla hälyttävä merkki. Tässä testissä lisätään uusi arvo RunOnce-avaimeen, jonka tarkoitus on käynnistää ohjelma yhden kerran kirjautumisen yhteydessä ja sen jälkeen poistaa avain. Haitallinen taho voisi esimerkiksi lisätä tänne avaimen, joka käynnistää haittaohjelman käyttäjän kirjautuessa.

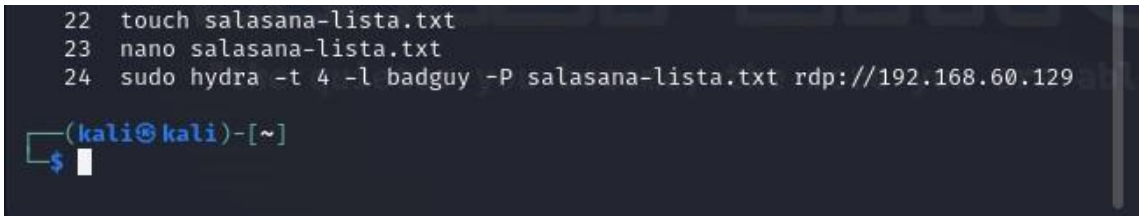
Tarkastelemalla Wazuhin kojelautaa pystyi näkemään ilmoituksen rekisterimuutoksesta. Ilmoitus ilmestyi järjestelmän yhtenäisyystarkasteluun ja yleisiin turvallisuustapahtumiin. Kuvan 5 esittämässä lokitiedossa näkyy uuden arvon olevan nimetty TestiAvain-nimellä ja sääntötason olevan viisi. Windows voi tehdä myös itse muutoksia esimerkiksi päivitysten yhteydessä, joten kaikki rekisterimuutokset eivät ole välittömästi paha enne. Tarpeen mukaan voisi asettaa suurempia sääntötasoja tietyille tärkeille avaimille, jos haluaisi niistä vaikka sähköposti-ilmoituksia. Kuitenkin on hyvä nähdä, että tapahtumasta jäi tarkka lokitieto järjestelmään.




Kuva 5. Wazuhin kojelaudan lokitieto rekisteriavainmuutoksesta. Hälytyksestä näkee uuden TestiAvain-nimisen arvon ilmaantumisen RunOnce-avaimeen.

### 4.3.4 Salasanahyökkäys

Tässä testissä simuloitiin tilannetta, jossa hyökkääjä pyrkii saaman hallinnan Windows-koneesta. Kohteena oli RDP-protokolla, joka antaa tietokoneen työpöydän käyttöhallinnan tunnuksien avulla. Linux Kali-tietokone toimi tässä testissä hyökkäyslaitteena. Hyökkääjä pyrkii Hydra-työkalulla arvaamaan käyttäjätunnukset niin sanotulla brute force-taktiikalla. Hydra kokeilee sille annettuja käyttäjätunnus ja salasanayhdistelmiä. Tämänkaltainen strategia toimii tehokkaimmin järjestelmiin, joissa käytetään joko oletussalasanaa tai muita yleisesti käytettyjä helposti muistettavia salasanoja. Hyökkäykseen tarvittavat komennot on esitetty kuvassa 6.

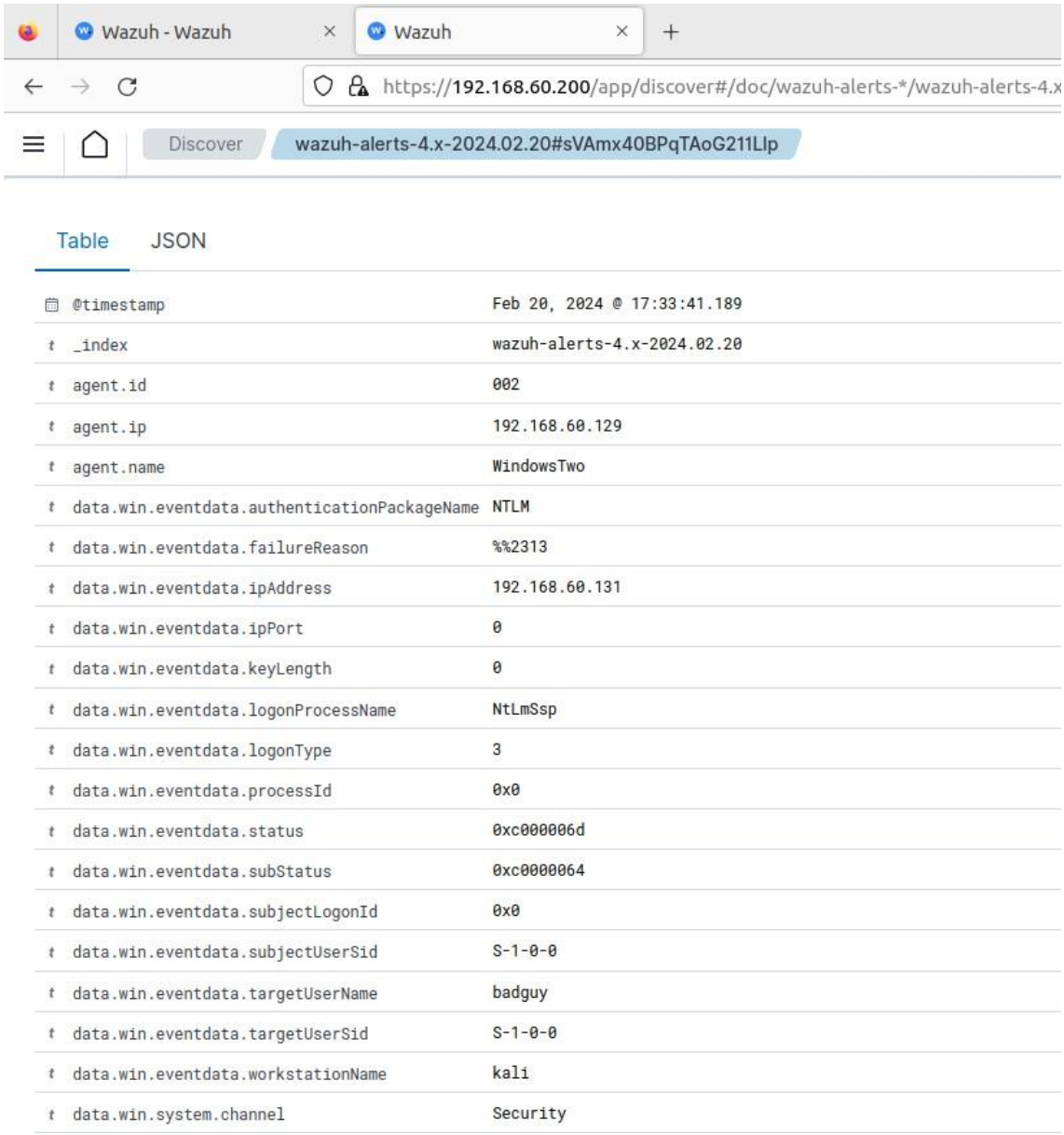



Kuva 6. Kalilla käytetyt komennot hyökkäykseen. touch-komento tekee tekstitiedoston, nano-komennolla voi kirjoittaa salasanoja tiedostoon ja hydra-komento käynnistää hyökkäyksen annettuun IP-osoitteeseen.

Hyökkäys ei onnistunut arvaamaan Windowsin salasanaa ja jokaisesta kirjautumisyrityksestä jäi lokitieto Wazuhun. Kirjautumisyritykset näkyvät kuvassa 7. Wazuh ei linkittänyt kyseisiä tapahtumia yhdeksi hyökkäykseksi, mutta lisätiedoista näkyy kaikille samanlaisia piirteitä. Yksittäisen tapahtuman näkymässä näkee muun muassa hyökkäävän tahon IP-osoitteen, tietokoneen nimen ja yritetyn käyttäjänimen. Tämä on kuvattu kuvassa 8. Wazuh tunnisti siis tapahtumat. Olisi kuitenkin ollut kätevää, jos tapahtumat olisi yhdistetty yhteen ja merkattu mahdollisesti haitallisiksi. Kirjautumisyritykset tulivat koneelta, jonka kanssa ei olla ennen tehty vastaavaa kommunikaatiota. Oikeissa hyökkäystilanteissa kirjautumisyritykset tulisivat myös tuntemattomista IP-osoitteista.

| | | | |
|---|---|---|---|
| Feb 20, 2024 @ 17:33:42.592 | Logon failure - Unknown user or bad password. | 5 | 60122 |
| Feb 20, 2024 @ 17:33:42.590 | Logon failure - Unknown user or bad password. | 5 | 60122 |
| Feb 20, 2024 @ 17:33:41.236 | Logon failure - Unknown user or bad password. | 5 | 60122 |
| Feb 20, 2024 @ 17:33:41.220 | Logon failure - Unknown user or bad password. | 5 | 60122 |
| Feb 20, 2024 @ 17:33:41.205 | Logon failure - Unknown user or bad password. | 5 | 60122 |
| Feb 20, 2024 @ 17:33:41.189 | Logon failure - Unknown user or bad password. | 5 | 60122 |

Kuva 7. Wazuhin kojelaudan ilmoitukset Hydra-hyökkäyksestä. Jokaista kirjautumisyritystä vastaa oma ilmoitus.




Kuva 8. Otos yksittäisestä kirjautumisyrityksestä osana hyökkäystä. Wazuhin kojelauta antaa lisätietoja hyökkäyksen piirteistä.

# 5 POHDINTA

Nykymaailman tietoturvaympäristön lomassa SIEM-ohjelmistot ovat osa suurten yritysten toimintaa, mutta pienempien yritysten ja myös yksityiskäyttäjien pitää miettiä muutamaa seikkaa ennen käyttöönottoa. Esimerkkinä käytetty Wazuh-ohjelmisto toi paljon ominaisuuksia suoraan paketista, mutta kaikkea ei saa suoraan. Muun muassa tietokoneen kansioita suojellaan vain tietyissä paikoissa ja viestihälytykset sähköpostien muodossa eivät ole oletuksena käytössä. Kaikki esille tulleet puutteet ovat lyhyehkön konfiguroinnin takana, mutta se vaatii lisää perehtymistä käyttäjältä. Kuitenkin ohjelmaa oli selkeä asentaa ja myös tarkkailla sen jälkeen. Wazuh ei korvannut virustorjuntajärjestelmää, vaan toimi sen rinnalla antaen lisätietoja kotiverkon liikenteestä.

Tarkemmin tarkasteltuna Wazuhin asennus ja kojelaudan ymmärtäminen vaatii perustasoa enemmän tietotekniikan tietämystä. Täytyy tietää miten Linux-pohjaisen koneen saa käyttöön omaan kotiverkkoon palvelimeksi ja lisäksi täytyy suorittaa komentoja asennusprosessissa. Myös uusien sääntöjen konfiguroiminen vaatii oman ymmärryksensä ohjelmasta, mitä ei suoraan kerrota kojelaudalla. Maksulliset kilpailijat voivat olla selkeämpiä kokonaisuuksia ja tarjota käyttäjätukea, mutta hintatasot eivät ole kuluttajaluokkaa.

Kaiken tämän huomioon ottaen koen SIEM-ohjelmiston olevan kiinnostava idea kotiverkkoon harrastajalle, mutta vaatii yksinkertaistamista arkisille tietokoneenkäyttäjille. Ymmärrettävyys vaihtelee henkilöittäin, mutta tämän hetken kiinnostuksen tietoturvaan perustuen koen päätelmän olevan luotettava. Paljon turvaudutaan vain virustorjunnan riittävyyteen. Teknologia tulee enemmän osaksi arkea koko ajan ja tietämys kasvaa ihmisillä samalla. SIEM-ohjelmistoilla voi olla tärkeä tehtävä kodeissa tulevaisuudessa, mutta tällä hetkellä ne vaativat käyttäjältä aiheeseen perehtymistä.

**LÄHTEET**

Gailey, S. 2020. A Brief History of SIEM. CyberSecurity Magazine 19.1.2020. https://cybersecurity-magazine.com/a-brief-history-of-siem/

Hyppönen, M. 2022. If It's Smart, It's Vulnerable. 1st Edition. E-kirja. Newark: John Wiley & Sons, Incorporated. Vaatii käyttöoikeuden. https://andor.tuni.fi/permalink/358FIN_TAMPO/176jdvt/cdi_skillsoft_books24x7_bkb000163545

López Velásquez, J.M., Martínez Monterrubio, S.M., Sánchez Crespo, L.E. et al. Systematic review of SIEM technology: SIEM-SC birth. Int. J. Inf. Secur. 22, 691–711 (2023). Vaatii käyttöoikeuden. https://doi-org.libproxy.tuni.fi/10.1007/s10207-022-00657-9

Packetlabs. 2023. A "Who's Who" of Open-Source EDR Solutions. Verkkosivu. Viitattu 19.2.2024. https://www.packetlabs.net/posts/open-source-edr-solutions/

Suskalo, D[ario]; Moric, Z[latan]; Redzepagic, J[asmin] & Regvart, D[amir] (2023). Comparative Analysis of IBM Qradar and Wazuh for Security Information and Event Management, Proceedings
of the 34th DAAAM International Symposium, pp.0096-0102, B. Katalinic (Ed.), Published by DAAAM International,
ISBN 978-3-902734-41-9, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/34th.daaam.proceedings.014

Williams, A & Nicolett, M. 2005. Improve IT Security With Vulnerability Management. Gartner 2.5.2005.

**LIITTEET**