Ympäristöön tutustuminen

Ryhmä 13

Leevi Kauranen, AC7750
Samir Benjenna, AD1437
Eelis Suhonen, AA3910
Juho Eräjärvi, AD1276
Mikke Kuula, AC7806

Poikkeamienhallinta ja kyberturvakeskukset TTC6060-3007
03.12.2024
Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

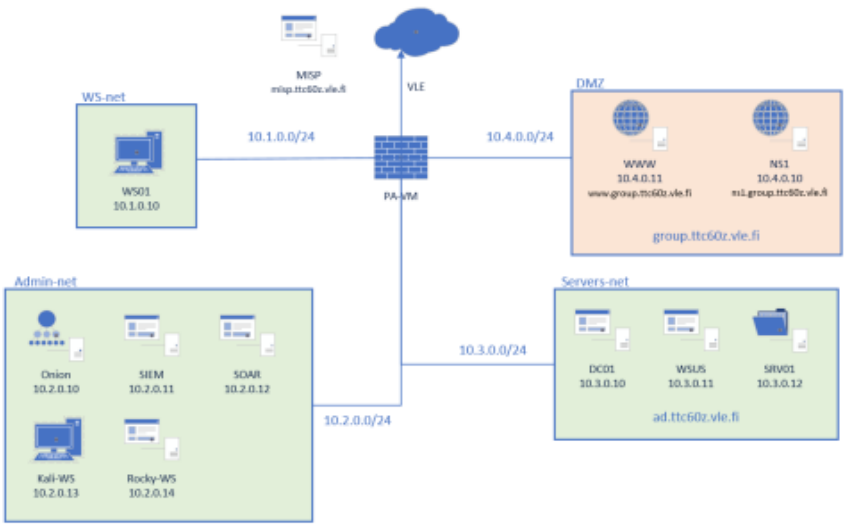
Kuviot

1 Johdanto

Tämän harjoitustyön tavoite on tutustua syvemmin VLE ympäristöstämme löytyviin poikkeamienhallintatyökaluihin Security Onion, ElasticSIEM sekä Wazuh. Tutustumme näiden työkalujen toimintaan ja siihen, miten ne liittyvät toisiinsa. Työkalut on valmiiksi konfiguroitu tietoturvakontrollien harjoitustöiden yhteydessä.

Tutkimme myös työkalujen käyttöliittymiä ja käyttöliittymästä löytyviä ominaisuuksia, pohdimme myös automatisoinnin tuomia etuja.

Kuviossa 1 on kuvattu harjoituksessa käytetty VLE ympäristö.



Kuvio 1. VLE-ympäristö

2 Työkalut

Seuraavaksi käymme läpi ympäristömme työkaluja, joiden tarkoitus on lisätä VLE-ympäristömme turvallisuutta ja kyberpuolustus kapasiteettiä. Näitä työkaluja on konfiguroitu ja käytetty osana

muita harjoitustöitä, ja ne muodostavat monipuolisen ja integroidun ympäristön verkkoturvallisuuden hallintaan ja poikkeamien monitorointiin.

2.1 Security Onion

Security Onion on avoimen lähdekoodin verkkoturvallisuusmonitorointityökalu, jonka käyttö, muokkaus ja kehittäminen on mahdollista kaikille. Se on suunniteltu yksinkertaistamaan kattavan NSM (Network Security Monitoring)-infrastruktuurin käyttöönottoa ja hallintaa, mahdollistaen organisaation tehokkaan tietoturvauhkien havaitsemisen, analysoinnin ja niihin reagoimisen.

Tärkeimpiä komponentteja:

1. **Suricata:** Tunkeutumisen havaitsemis- ja estojärjestelmä (IDS/IPS)
2. **Zeek:** Verkon analysointityökalu
3. **Snort:** Toinen IDS/IPS-moottori
4. **Elasticsearch:** Hajautettu haku- ja analytiikkamoottori
5. **Kibana:** Tiedon visualisointityökalu
6. **Logstash:** Lokitietojen keräys- ja käsittelytyökalu
7. **Squert**: Verkkosovellusliittymä

Security Onion toimii ”anturina” verkossa, keräten dataa ja generoiden hälytyksiä epäilyttävästä toiminnasta. Kerätty data lähetetään keskuspalvelimelle tallennusta, analyysiä ja visualisointia varten.

Hyödyt:

- Avoimen lähdekoodin ja kustannustehokas ratkaisu
- Kattava verkon näkyvyys
- Reaaliaikainen uhkien havaitseminen
- Laaja yhteisön tuki
- Muokattavuus ja joustavuus

(MSBJ. 2023)

2.2 ElasticSIEM

Elastic Security SIEM (Security and Event Management) on Elastic Stack alustalle rakennettu tuote, joka tarjoaa tietoturvanäkemyksiä ja reaaliaikaista uhkien havaitsemista. Se kerää, normalisoi ja analysoi dataa organisaation IT-ympäristön eri lähteistä, kuten lokeista, verkkoliikenteestä ja päätelaitteiden tiedoista.

ElasticSIEMin päätarkoitus on tarjota keskitetty alusta tietoturvatapahtumien seurantaan ja hallintaan. Se parantaa organisaatioiden kykyä havaita nopeasti ja tehokkaasti mahdollisesti haitallista toimintaa.

ElasticSIEMin tärkeimpiä komponentteja ovat:

1. **Elastic Endpoint Security –agentti:** Ne keräävät erilaisia tapahtumia isäntäjärjestelmistä, kuten prosessi ja verkkotietoja.
2. **Beat-moduulit:** Kevyet tiedonkerääjät, jotka keräävät ja jäsentävät tehokkaasti tiettyjä tietojoukkoja.
3. **Fleet-sovellus:** Käytetään agenttien ja niiden integraatioiden asentamiseen, hallintaan ja valvontaan isäntäkoneilla.
4. **Kibana:** On Elastic Stackin visualisointityökalu, joka tarjoaa käyttöliittymän Elasticsearchiin tallennetun datan tutkimiseen ja analysointiin.

(Elastic SIEM: Features, Components, Pricing, and Quick UI Guide. 2024)

2.3 Wazuh

Wazuh on ilmainen, avoimen lähdekoodin tietoturva-alusta, joka tarjoaa yhdistetyt XDR (Extended Detection and Response) ja SIEM (Security Information and Event Management) -ominaisuudet. Se

on suunniteltu suojaamaan erilaisia ympäristöjä, kuten julkisia ja yksityisiä pilviä sekä paikallisia datakeskuksia.

Tärkeimmät ominaisuudet:

- **Päätelaitteiden ja pilviympäristön suojaus**
- **Telemetrian ja lokitietojen analysointi**
- **Uhkien tiedustelu ja niihin reagointi**
- **Monialustainen päätelaitteiden valvonta**
- **Pilvitietoturva (AWS; Azure, GCP, Github)**
- **Uhkien metsästys ja käyttäytymisanalyysi**
- **Automatisoitu reagointi ja säännöstenmukaisuus**

Wazuh koostuu kolmesta pääkomponentista: indeksoijasta, palvelimesta ja kojelaudasta. Nämä yhdessä mahdollistavat tehokkaan tietoturvatietojen hallinnan, analysoinnin ja visualisoinnin

Wazuh myös integroituu saumattomasti muiden tietoturvatyökalujen kanssa ja skaalautuu organisaation tarpeiden mukaan. (Brandstaetter,S. 2024)

3 Käyttöliittymien ominaisuudet

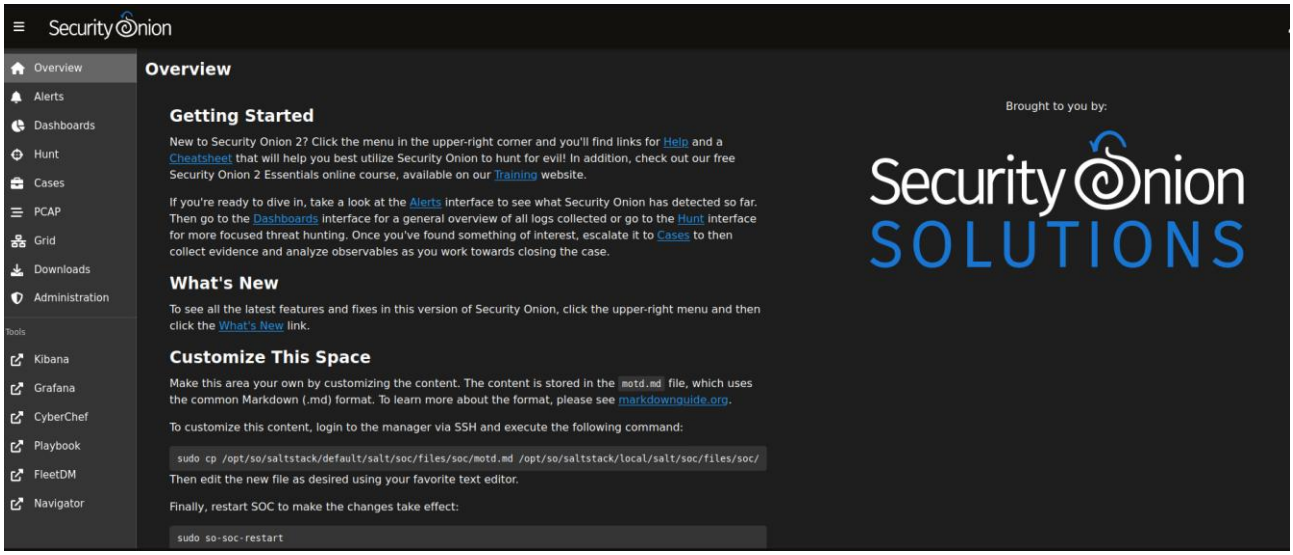
Ominaisuuksia löytyy jokaisesta runsaasti ja niihin syventyminen ja käytön hallitsemien voi viedä hieman aikaa. Ominaisuuksien tunteminen ja hyödyntäminen on kuitenkin todella tärkeä osata, mikäli haluaa saada kaiken hyödyn järjestelmästä.

Seuraavaksi perehdytään näihin ominaisuuksiin mitä aiemmin mainittujen järjestelmien käyttöliittymistä löytyy.

3.1 Security Onion

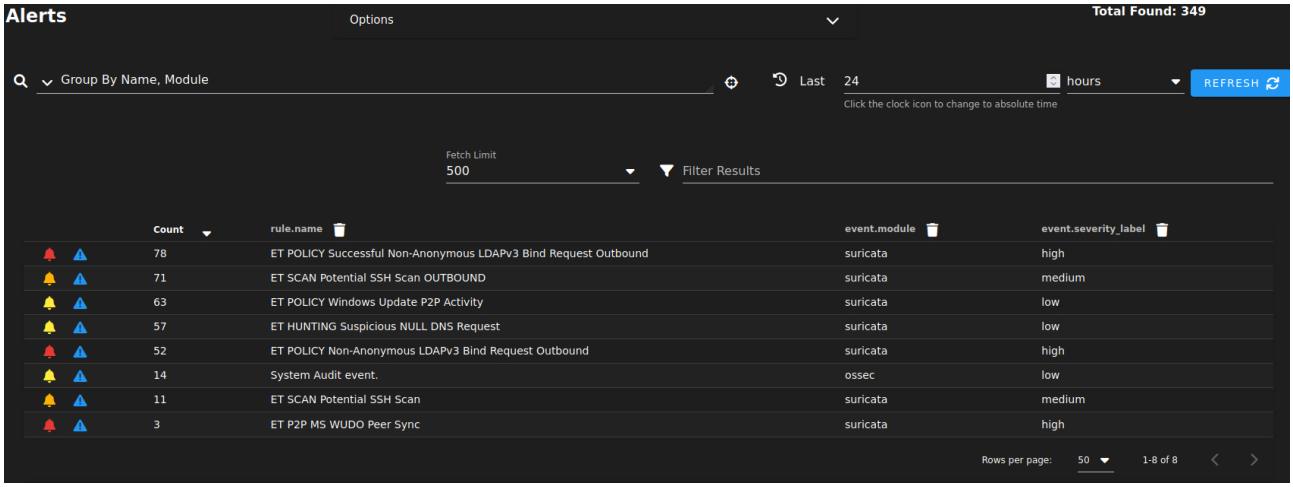
Perehdytään Security Onionin käyttöliittymän ominaisuuksiin.

Kun järjestelmään kirjautuu, tulee ensimmäisenä sivu, jolta löytyy ohjeistuksia ja päivitystietoja sekä sivupalkki, jossa näkyy useita eri toimintoja. (Kuvio 2).



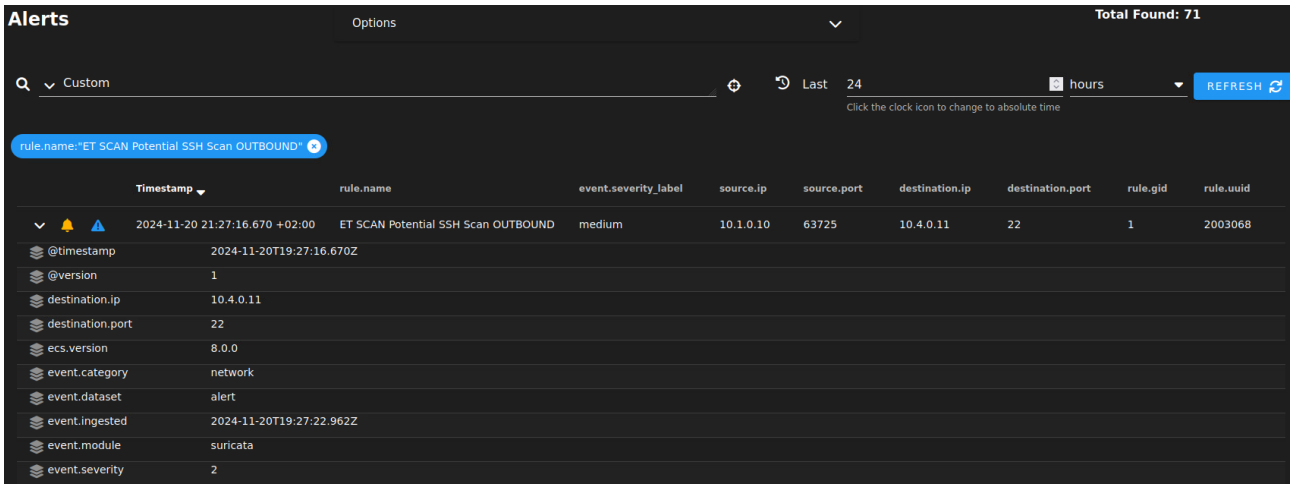
Kuvio 2. Overview-välilehti

Alerts välilehdeltä löytyy hälytyksiä, jotka aiheutuvat turvallisuus sääntöjen vuoksi. Järjestelmä seuraa verkko- ja järjestelmädataa, ja aiheuttaa hälytyksen, mikäli joku turvallisuussäännöistä täytyy. (Kuvio 3)



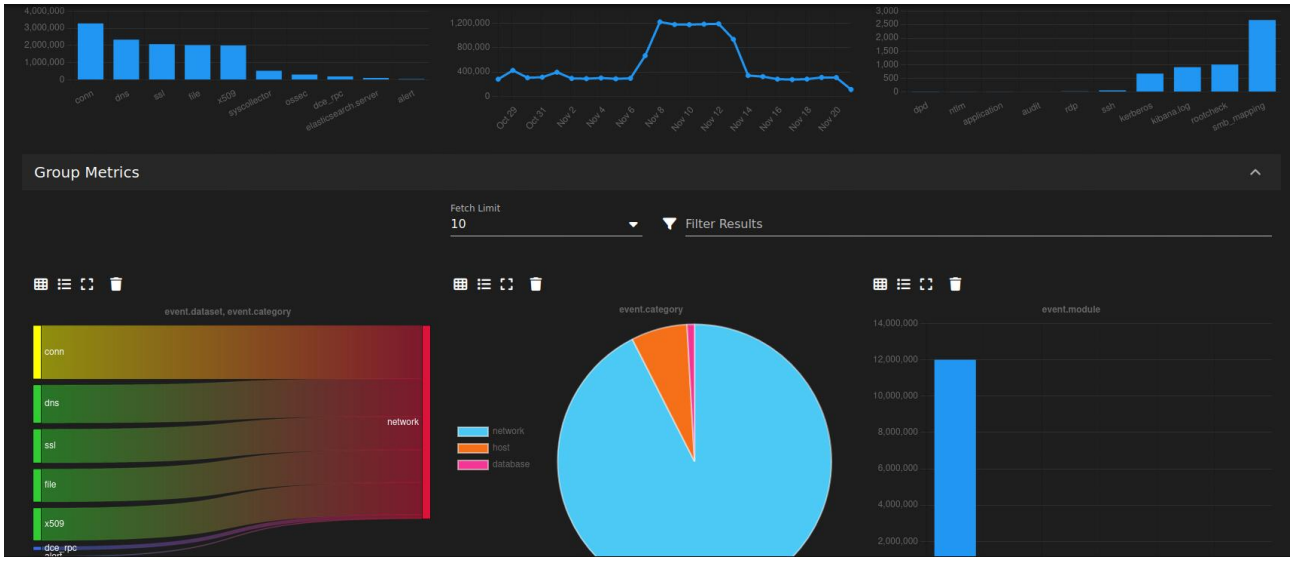
Kuvio 3. Alerts-välilehti

Kun hälytystä tupla klikkaa saa auki tarkemmat tiedot ja kaikki kyseisen hälytyksen laukaisseet tapahtumat. Kuviossa 4 näkyy yksi tapahtuma tarkastelussa, josta selviää esimerkiksi lähde- ja kohde IP-osoite, portti, ja paljon muuta.



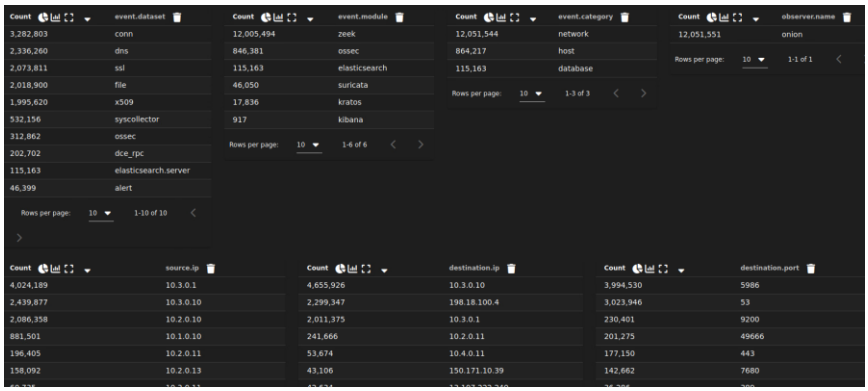
Kuvio 4. Hälytyksen tiedot

Dashboards-välilehdeltä löytyy erilaisia visualisointeja tarkkailtuun liikenteeseen perustuen. (Kuvio 5).



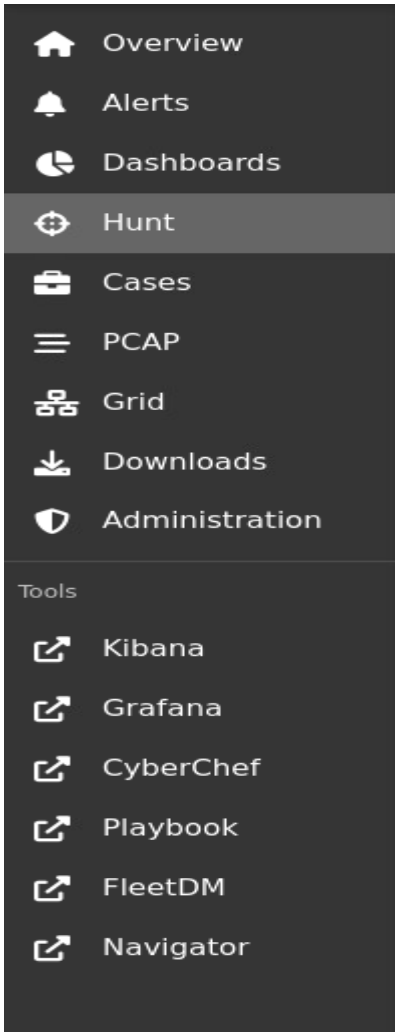
Kuvio 5. Dashboards-välilehti

Dashboards-välilehden alaosasta löytyy lisätietoa lokeista, kuten liikenne tietyistä IP-osoitteista/osoitteisiin ja tapahtumaa tarkkailleet moduulit. (Kuvio 6).



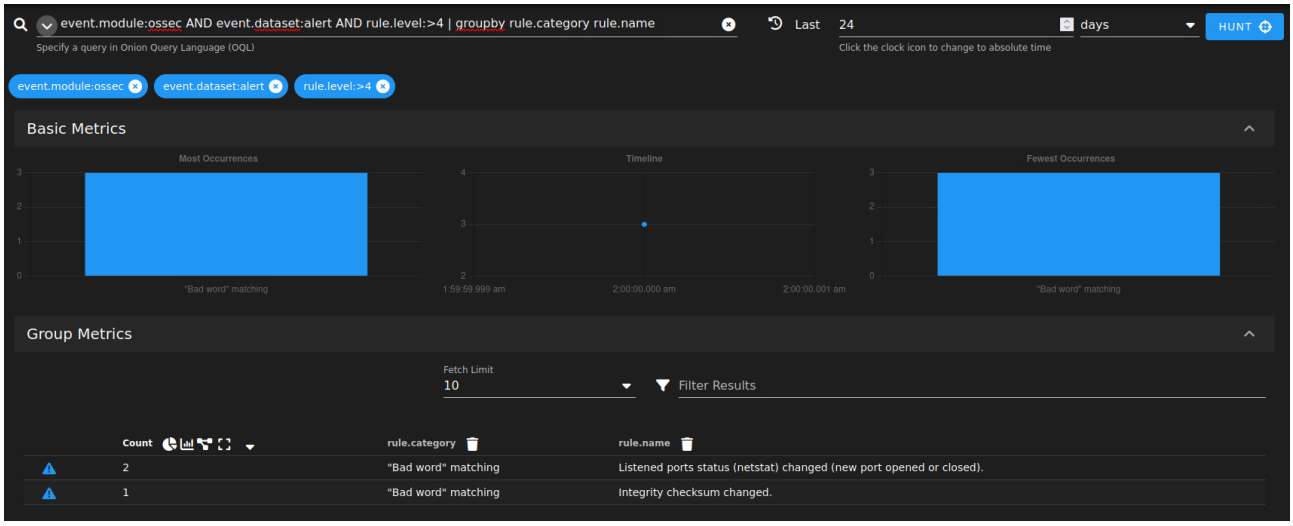
Kuvio 6. Dashboards-välilehden lisätiedot

Käyttöliittymän sivupaneelista löytyy myös paljon muita hyödyllisiä osioita kuten hunt, cases ja pcap.



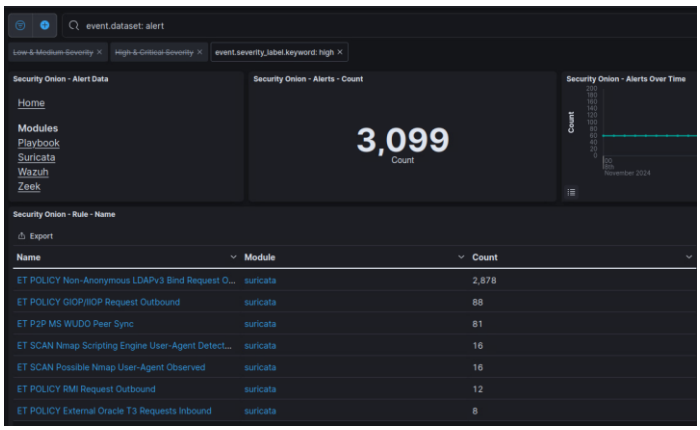
Kuvio 7. Sivupaneeli

Hunt-välilehdellä pystymme perehtymään syvällisemmin tapahtuneeseen hälytykseen. Esimerkiksi kuviossa 8 on filtteröity moduulin ossec-hälytykset. Alempi hälytys on syntynyt säännöstä, joka tarkkailee tiedostojen muokkauksia. Hälytys aiheutui, kun etc/sysconfig/iptables tiedostoa muokattiin.



Kuvio 8. Hunt-välilehti

Sivupalkista löytyy myös erilaisia työkaluja, jotka ovat integroitu Security Onion järjestelmään, kuten MITRE ATT&CK Navigator ja Cyberchef. Security Onionista löytyy myös kibana käyttöliittymä. Kuviossa 9 on tarkasteltuna hälytykset, joiden vakavuustaso on korkea (high).

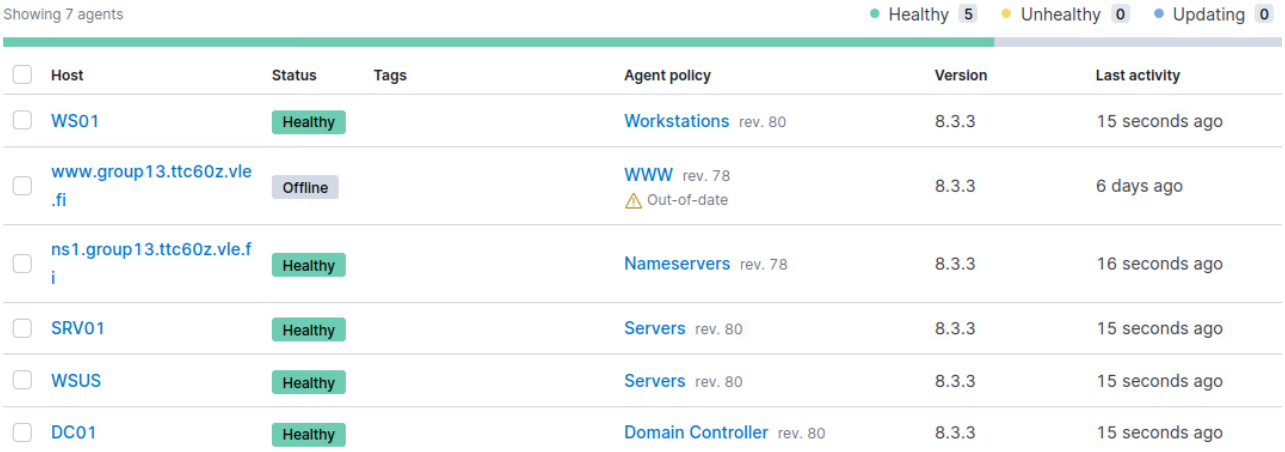


Kuvio 9. Korkean vakavuustason hälytykset

3.2 ElasticSIEM

ElasticSIEM:n visuaaliseen käyttöliittymään pääsee kirjautumaan Kali-virtuaalitietokoneen kautta selaimella osoittessa http://10.2.0.11:5601.

Elasticissa ”fleet”, johon voidaan intergroida palvelimia ja päätelaitteita, joilta voidaan kerätä loki-dataa ja metriikkaa. (Kuvio 10).

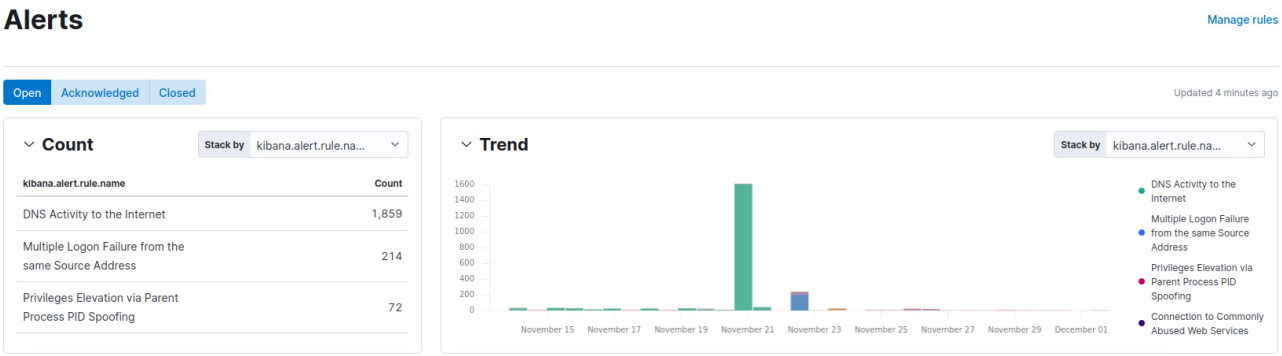


Kuvio 10. Elastic fleet

Elasticista löytyy myös laaja tarjonta erilaisia integraatioita, joiden avulla voidaan kerätä erilaista tietoa järjestelmistä. (Kuvio 11).

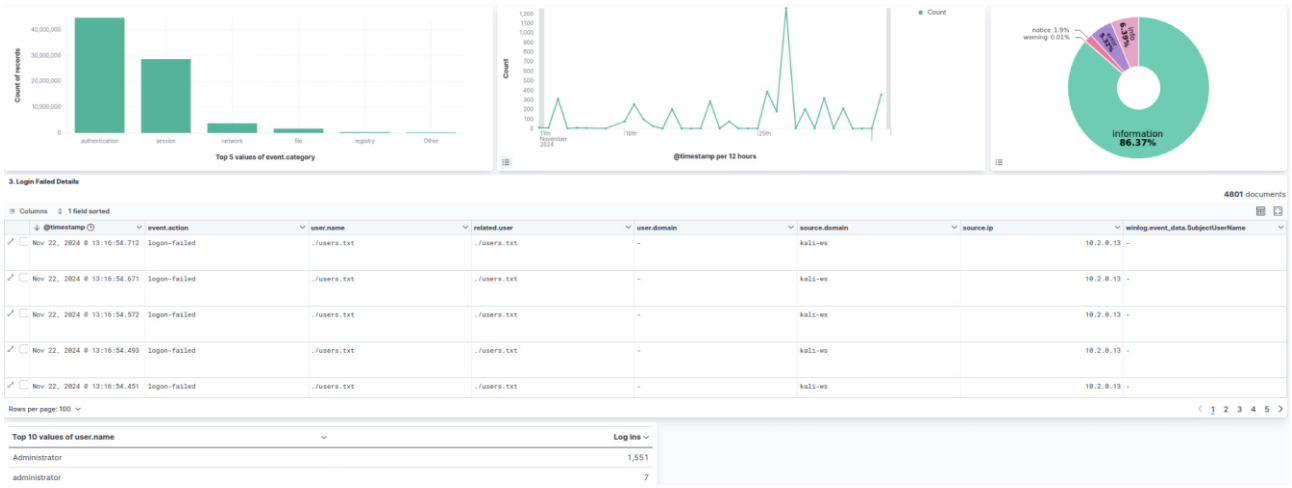
Kuvio 11. Elasticin integraatiot

Elasticista löytyy myös hälytyksiä, jotka perustuvat valmiiksi luotuihin sääntöihin. Sääntöjä voi luoda myös itse, jolloin ne voidaan kustomoida organisaation tarpeita vastaaviksi. Valmiiksi luodut säännöt ovat myös hyödyllisiä ja niiden avulla saatuja hälytyksiä on helppo seurata Security otsikon alta löytyvältä Alerts-välilehdeltä. (Kuvio 12).



Kuvio 12. Elasticin hälytykset

Elasticiin on mahdollista myös luoda omia ohjausnäkymiä (dashboard), jotka helpottavat järjestelmässä tapahtuvan liikenteen seuraamista. Myös ohjausnäkymistä löytyy valmis laaja valikoima, mistä valita. Ohjausnäkymiä voi myös luoda itse omien tarpeiden mukaan. Kuviossa 13 on esiteltynä itse tehty ohjausnäkymä, jonka avulla voi tarkkailla onnistuneita ja epäonnistuneita kirjautumisia. (Kuvio 13).

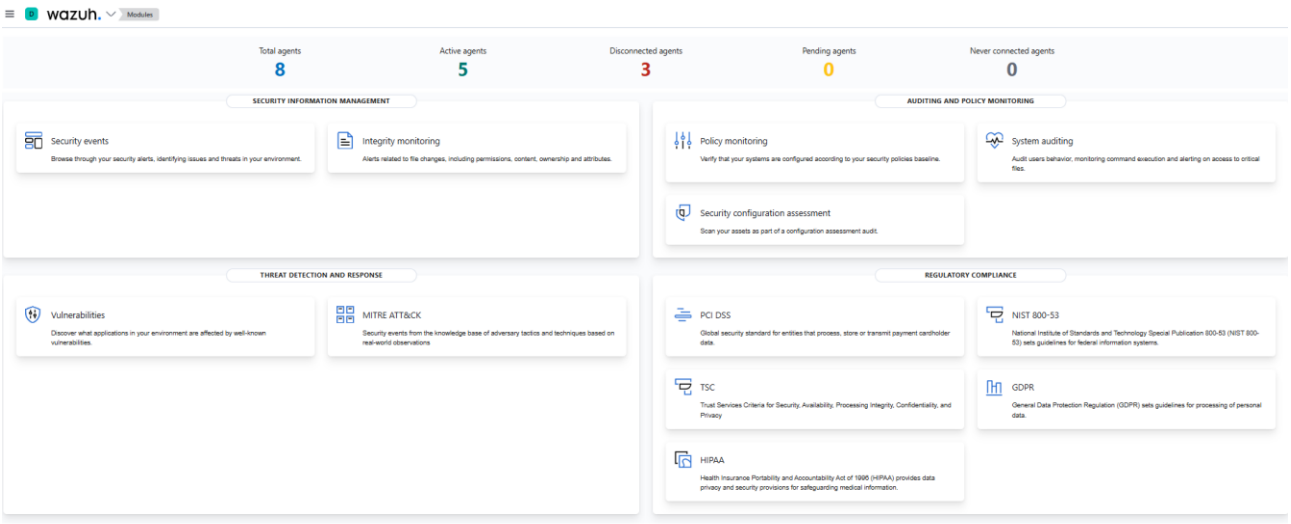


Kuvio 13. Esimerkki ohjausnäkymästä

3.3 Wazuh

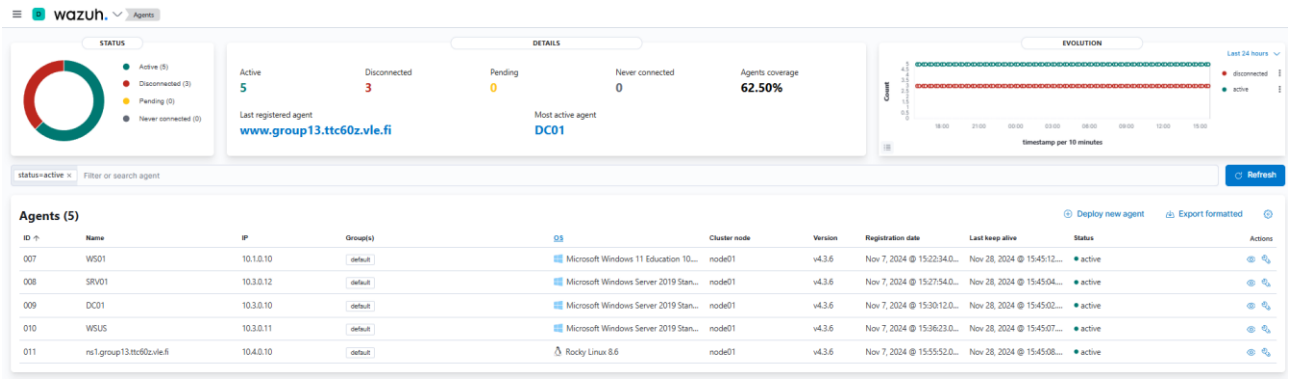
Wazuhiin pääsee käsiksi osoitteella https://10.2.0.12/ omalta tietokoneelta, kun tietokone on yhdistetty VLE-ympäristöön GlobalProtectin avulla.

Etusivulle aukeaa näkymä, josta ilmenee agenttien tila, ja erilaisia työkaluja ja ominaisuuksia. (Kuvio 14).



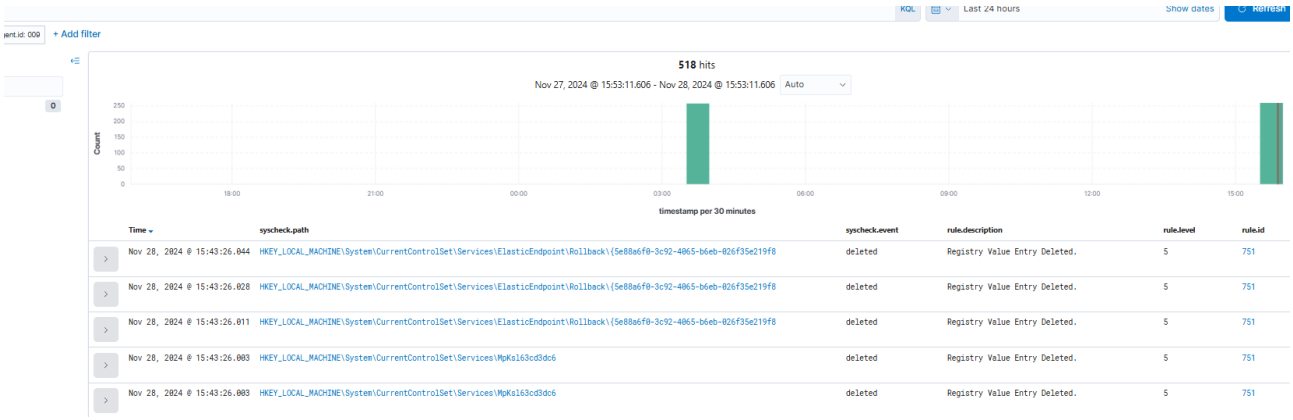
Kuvio 14. Wazuh:n etusivu

Kun painamme active agents alta numeroa 5, pääsemme katsomaan aktiivisia agentteja, eli Wazuh:n liitettyjä laitteita. Ympäristössämme on normaalisti 6 agenttia, mutta tehtävän tekohetkellä WWW-palvelin oli resetoitu, eikä sitä ollut yhdistetty. (Kuvio 15).



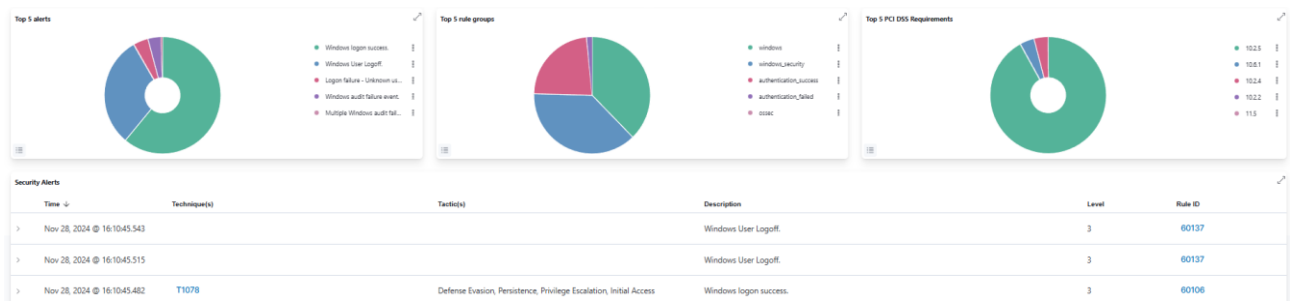
Kuvio 15. Agentit

Kun avaamme DC01-agentin tarkasteluun, pääsemme tarkastelemaan esimerkiksi kuviossa 16 näkyvää integrity monitoria, jossa ilmenee tiedostojen muokkaukset ja poistot. Integrity Monitorilla pystyy seuraamaan järjestelmän eheyttä.



Kuvio 16. Integrity

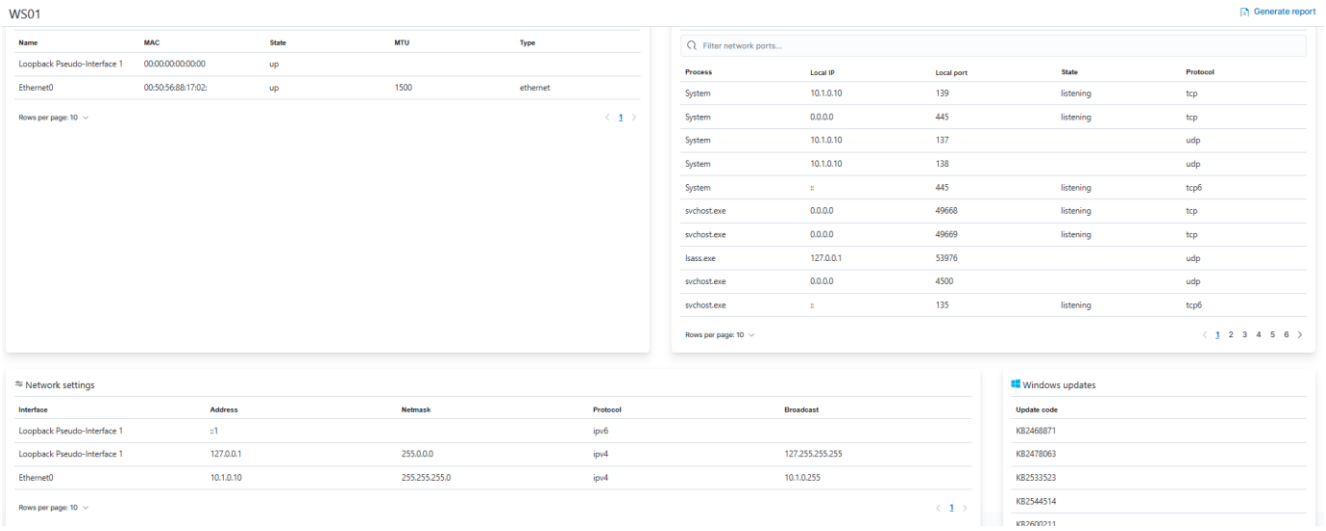
Security events osiossa pääsemme tarkastelemaan agentin havaitsemia tapahtumia DC01:ssä, kuten kirjautumisia. Kuten kuviosta 17 ilmenee, kirjautumislokeja tulee todella paljon, esimerkiksi Palo Alto AD-integraation vuoksi, jossa käyttäjä hakee Active Directory käyttäjä tietoja Palo Alto p. Näitä tulee suodattaa pois, jotta voidaan keskittyä oikeisiin ilmoituksiin niin sanotun ”melun” keskeltä.



Kuvio 17. DC01:n turvallisuustapahtumat

4 Automatisoinnin edut

Automatisointi tuo merkittäviä etuja tietoturvajärjestelmien hallintaan ja operointiin. Esimerkiksi Wazuh tarkistaa automaattisesti työaseman WS01 inventaariotiedot kuviossa 18.



Kuvio 18.inventaario

Kuviossa ilmenee inventaariodatasta esimerkiksi WS01-laitteen verkkokortit ja yhteydet, kuuntelevat verkkoportit, Windows-päivitykset sekä verkkoasetukset.

Esille tulleita etuja:

- **Reaaliaikainen tieto ja nopeus**
- **Tiedon tarkkuus ja kattavuus**
- **Tehokkuus ja ajan säästö**
- **Haavoittuvuuksien nopeampi tunnistaminen**
- **Järjestelmien yhdenmukaisuus ja dokumentointi**
- **Poikkeamien ennakoiva tunnistus**

Lähteet

Brandstaetter, S. Understanding Wazuh: The Free, Open Source Security Platform for XDR & SIEM. Medium.com sivuston artikkeli. 25.2.2024. Viitattu 1.12.2024. https://osintph.medium.com/understanding-wazuh-the-free-open-source-security-platform-for-xdr-siem-48b3c3dfba9d.

Elastic SIEM: Features, Components, Pricing, and Quick UI Guide. Cynet.com sivuston artikkeli. 9.7.2024. Viitattu 1.12.2024. https://www.cynet.com/siem/elastic-siem-features-components-pricing-and-quick-ui-guide/.

MSBJ. Exploring Security Onion. Medium.com sivuston artikkeli. 2.8.2023. Viitattu 1.12.2024. https://medium.com/@msbj/exploring-security-onion-d406412fdebb.