TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Maksim Dmitrijev 211959IABM

Turvateabe ja- sündmuste haldus avatud lähtekoodiga tööriistadele baasil

[Magistritöö]

Juhendaja: Oleg Švets

TalTech Virumaa kolledž, MSc

Tallinn 2020

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Maksim Dmitrijev

08.01.2023

Annotatsioon

Alates 2022. aasta veebruarist on küberrünnakute arv kogu maailmas kasvanud. Kui võrrelda 2022. aasta kolmandat kvartalit 2021. aasta sama perioodiga, siis rünnakute arv kasvas 28%. Statistika kohaselt oli ründaja enne avastamist ohvri võrgus üle 180 päeva. Käsitsi, ilma süsteemi sündmuste automaatse analüüsita, on nakkust varajases staadiumis väga raske tuvastada.

Autor on üks neist, kes igapäevaselt ettevõttes küberturvalisuse probleeme lahendab. Sellest tulenevalt on autori jaoks automatiseerimine ja kiire reageerimine väga oluline.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 67 leheküljel, 7 peatükki, 18 joonist, 2 tabelit.

Abstract

Security Information and Event Management based on open-source tools

Since February 2022, the number of cyber attacks worldwide has increased. Compared to the same period in 2021, the number of attacks grew by 28% in the third quarter of 2022. [1] Statistics show that attackers were present on the victim's network for over 180 days before being discovered. It is very difficult to detect infections in the early stages without automated event analysis.

The author is one of those who deals with cybersecurity issues on a daily basis. Therefore, automation and rapid response are essential for the author.

The thesis is in Estonian language and contains 67 pages of text, 7 chapters, 20 figures, 2 tables.

Lühendite ja mõistete sõnastik

SIEM	*Security information and event management*, turvateabe ja sündmuste haldamise süsteem
SOAR	*Security Orchestration, Automation and Response*, Turvakorraldus, automatiseerimine ja reageerimine
CIS	*Center for Internet Security*
JVM	Java Virtual Machine
XDR	Extended Detection and Response
EDR	Endpoint Detection and Response
NIST	National Institute of Standards and Technology, Riiklik Standardi- ja Tehnikainstituut

Sisukord

Jooniste loetelu

Tabelite loetelu

1 Sissejuhatus

Küber rünnakute arv on alates 2022. aasta veebruarist kogu maailmas suurenenud. Võrreldes 2021. aasta sama perioodiga on rünnakute arv 2022. aasta kolmandas kvartalis kasvanud 28%[1]. Statistika kohaselt võivad kurjategijad olla ohvri võrgus pikka aega enne avastamist. See võib tavaliselt võtta mitu kuud kuni mitu aastat. See on seotud sellega, et kurjategijad kasutavad erinevaid tehnikaid oma tegevuse varjamiseks ja avastamise vältimiseks. Selline ajaperiood võimaldab kurjategijatel juurdepääsu konfidentsiaalsele teabele ning tekitada ettevõttele või organisatsioonile tõsist kahju. Seetõttu on oluline võrgu regulaarne jälgimine ja kaasaegsete kaitsevahendite kasutamine küberkuritegevuse vastu. Siiski on ilma süsteemisündmuste automaatse analüüsita varajases staadiumis nakatumise avastamine väga keeruline.

Autor on üks neist, kes igapäevaselt ettevõttes küberturvalisuse probleeme lahendab. Sellest tulenevalt on autori jaoks automatiseerimine ja kiire reageerimine väga oluline.

Enamikus kaasaegsetes era- ja riigiettevõtetes on installeeritud viirusetõrjed, tulemüürid ja muud infokaitsevahendid, kuid ühest pilti infrastruktuuris toimuvast pole. Kõik kaitseelemendid on individuaalselt seadistatud ja töötavad korrektselt, kuid nende vahel puudub ühine seos. Sel põhjusel langeb kaitsevahendite komplekti kasutamise efektiivsus märkimisväärselt ning puudub võimalus nakkust või rünnakut kiiresti tuvastada ja ennetusmeetmeid rakendada. Sündmuste logi analüüs on aluseks küberturbe toimingute planeerimisel. Kaasaegsed turvateabe ja sündmuste haldamise (SIEM) süsteemid[2] pakuvad lihtsat lähenemist küberrünnakute tuvastamiseks ja ennetamiseks, kogudes ja analüüsides seotud sündmusi tsentraalselt. SIEM on suunatud intsidentide jälgimisele, avastamisele ja neile kiirele reageerimisele ning selle tulemusena võimalike intsidendi tagajärgede vähendamisele.

Selle töö ülesanne on:

- Luua avatud lähtekoodiga süsteem erinevatest allikatest pärit logide tsentraalseks kogumiseks.

- Seadistada avatud lähtekoodiga SIEM-süsteem koos sündmuste sidumisega MITER ATTACK maatriksiga. Paigaldada ühendatud seadmetesse haavatavuste skanner.
- Luua SIEM-iga ühendatud seadmete haavatavuste jälgimise ja analüüsimise süsteem CIS-i standardite alusel (Center for Internet Security).
- Luua aruannete ja teadete süsteem

Vastata järgmistele uurimusküsimustele:

- Kuidas rakendada avatud lähtekoodiga lahendusi turvaelementide tsentraliseeritud haldamiseks?
- Kuidas tuvastada SIEM-i abil sissetungijate rünnakuid?
- Kuidas automatiseerida süsteemisündmuste analüüsi?

Andmeallikana kasutab autor Windowsi, Linuxi süsteemide, sissetungi ennetussüsteemide (IPS) ja viirusetõrje sündmuste logisid. Logianalüüs on arvuti loodud sündmuste logide vaatamine, et ennetavalt tuvastada vigu, turvariske või muid riske. Logifailide arvu ja suuruse kasvades muutub logifailide sõelumine üha keerulisemaks. On äärmiselt oluline, et analüütik järgiks tugevat logianalüüsi metoodikat, mida toetab võimas platvorm, et edukalt töödelda logifaile ja otsida väärtuslikke „artefakte“ täpsete tulemuste saamiseks.

Andmete analüüsi metoodika järgimine: Wazuhi[3] kasutatakse logide kogumiseks, indekseerimiseks ja tsentraliseeritud hoidmiseks. Graylog[4] vastutab seadmetega ühenduse loomise, korrelatsiooni ja logide edasise ettevalmistamise eest nendel seadmetel, kuhu Wazuh-agendi ei saa installida. Automaatseks juhtimiseks ja intsidentide uurimiseks logide analüüsi põhjal tuleb seadistada integratsioon Wazuh ja spetsialiseeritud digitaalsete kuritegude analüüsi ja uurimise tööriista TheHive vahel, mis tagab kiire ja täpse digitaalsete andmete analüüsi, kõigi leitud andmete kogumise ja hoidmise ühes kohas. Selle tulemusena saadakse andmemudel, kus kahjuliku faili või kahjuliku lingi avastamisel suunatakse sündmus turvaintsidentidele reageerimise platvormile TheHive. TheHive'i kasutades saab SOC meeskond kaasaegse probleemihaldussüsteemi, kus saab prioriteete seada, lahendajaid määrata ja ülesannete

olekut jälgida. Sisseehitatud aruandlussüsteem aitab tuvastada töötajate KPI-sid. Kogu töö tulemusena kuvatakse turvaintsidentide sündmused ühel töölaual TheHive'is, kus on võimalik vaadata digitaalsete jälgede analüüsi aruandeid, graafilisi diagramme ja muid andmete visualiseerimise vorme, mis võivad aidata haavatavuste analüüsis ja avastamises. See lahendus kontrollib Linuxi ja Windowsi süsteeme automaatselt tuntud haavatavuste suhtes, kasutades CIS-i turvalisuse kontrollnimekirju. Need on rahvusvaheliselt tunnustatud ja konsensuslikult parimad tavad, mille on välja töötanud Turvalisuse Internetikeskus (CIS)[5], et aidata turvainseneridel oma küberturvalisust tõhustada ja hallata. Loodud süsteemi toimimise valideerimiseks teostatakse katsed käivitada mitmesugused pahatahtlikke koode ning teostatakse süsteemidesse sissetungi katsed. See töö on kasulik infoturbekeskustele, andmekeskustele, riigi- ja eraettevõtetele. Kuna kasutatakse tasuta ja avatud lähtekoodiga tarkvara, saab organisatsioon säästa litsentside ostult. Litsentside hind põhineb tavaliselt seadmete arvul, millest sündmuste logisid kogutakse. Analüüsiprotsesside automatiseerimine aitab säästa tööjõudu.

Selles lõputöös on teemad jaotatud järgmiselt:

- Peatükk 2 annab ülevaate lõputööga seotud tööst.
- Peatükk 3 sisaldab logianalüüsi metoodika täpsemat kirjeldust.
- Peatükk 4 sisaldab Wazuhi logide kirjeldust, konfigureerimist, keskset kogumist ja indekseerimist.
- Peatükk 5 kirjeldab sündmuste jälgimist ja automaatset analüüsi reeglite ja MITER ATT&CK maatriksi alusel. Automatiseerimisplatvormi sündmuste edastamiseks Wazuhist TheHive'i, skaleeritavale turvaintsidentidele reageerimise platvormile. Räsi- ja dns-kirjete automaatne analüüs MISP-i ja Cortexi abil.
- Peatükk 6 annab ülevaate testidest ja lõpliku soovituse aruannete koostamisel.

2 Seotud tööd

Enne projekti elluviimist vaadati läbi mitmed paberid ja uuringud, et samm-sammult õppida, milliseid samme uuringu käigus järgida. Nendest allikatest saadud teave oleks pidanud andma rohkem teavet selle kohta, kuidas kõige paremini kasutada süsteemiloge ohutuvastusvahendina, ja muid võimalikke katseid, mis aitaksid kaasa automatiseeritud logianalüüsi uurimisele. Lisaks on kogutud erinevaid pabereid sündmustega manipuleerimise rünnakute ärahoidmise meetoditest ja sellest, kuidas need meetodid antud olukordades suuremat turvalisust pakuvad.

Selles artiklis[6],[7] kirjeldatakse NIST Security Framework dokumendi uue versiooni uurimist, SOC ja SIEM turbetehnoloogiate ja -lahenduste suundumusi ning tutvustatakse ka avatud lähtekoodiga tööriista suurandmete reaalajas kaitsmiseks.

Artikli[8] autorid on töös pakutud uue visuaalse lähenemisviisi intuitiivsele ohu jälgimisele ja kahtlaste IP-aadresside tuvastamisele, mis on tõsine probleem küberturvalisuse jälgimisel, et lahendada analüütiku töökoormuse probleemi. Selline lähenemisviis võimaldab kahtlaseid IP-aadresse statistiliselt tuvastada, jälgida ja analüüsida reaalajas. See lähenemisviis võimaldab teil tuvastada, jälgida ja analüüsida kahtlasi IP-aadresse statistiliselt reaalajas. Selle tulemusena rakendatakse pakutud meetodiga rakendatud süsteemi asjakohaselt ja kasutatakse reaalses keskkonnas. Lisaks kinnitab lähenemise kasutatavust erinevate ründe IP-aadresside edukas tuvastamine ja analüüs.

ELK Stacki avatud lähtekoodiga tehnoloogia kasutamine suurandmete, näiteks infoturbesüsteemis, terminalis ja serveris esinevate struktureerimata andmete analüüsimiseks. Teadlased Jeong-Hoon Hyun ja Hyoung-Joong Kim[9] suutsid luua infoturbe juhtimissüsteemi, mis on optimeeritud ärikeskkonna jaoks oma personali ja tehnoloogiaga. Lootmata kallitele kommertslahendustele, leidsime võimaluse küberrünnakute vastu kaitseks tehnoloogiaid akumuleerida, juurutades otse omal jõul tasuta kaitsehaldussüsteemi.

Korea Institute of Information Security & Cryptology teadluses oma artiklis[10] käsitletakse paljude haavatavuste olemasolu, mis on tingitud tööstusjuhtimissüsteemidesse jäänud vananenud süsteemide suurest hulgast. Kui neid haavatavaid süsteeme ei looda uuesti vastavalt turvasüsteemile, on vaja neile haavatavatele süsteemidele reageerida ning seetõttu testiti ja pakuti välja käideldavuspõhine turvalahendus. Sysmoni ja ELK-i kasutades suudavad turvalahendused tuvastada küberohte, mida on struktureerimata ICS-is raske tuvastada.

Kuna ettevõtetel on muutunud vajalikuks luua turvalahendusi kliendi teabe kaitsmiseks. Selles artiklis[11] pakuti välja automatiseeritud süsteem, mis kogub logisid suurandmete abil ja analüüsib kogutud logisid Mahouti abil. Sest käsitsi analüüs, mille käigus administraator jälgib logisid, loob piiranguid kogunenud logide analüüsile või suure hulga logide loomisele.

Lee, Sang-Yun ja Yoon, Hong-Joo oma artikkel[12] uurivad tulevase e-valitsuse soovitavat vormi intelligentsete valitsuse uuringute osas vastuseks uutele intelligentsetele küberturbeteenustele neljandas tööstusrevolutsioonis. Samuti on tulevase e-riigi strateegilist planeerimist vaadeldud tsentraliseerimise ja intellektualiseerimise aspektist, mis on neljanda tööstusrevolutsiooni olulised tunnused. Töös soovitatakse uut süsteemikonstruktsiooni, mida rakendatakse turvaanalüüsi tehnoloogiaga, kasutades täiustatud suhteanalüüsi kaudu suurandmeid. Artiklis soovitatakse luua süsteem, nagu SIEM (Security Information & Event Management), mis ennetavalt tuvastab turvaohu, kasutades logiteavet suurandmete analüüsi kaudu. Kui soovitatud süsteem teoks saab, on võimalik laiendada suurandmeobjekti, võimaldada tsentraliseerimist e-valitsuse turvalisuse osas neljandas tööstusrevolutsioonis, suurendada andmetöötlust, kiirust ja järelvastust, mis võimaldab süsteemil ennetavalt toimida.

Fernando Bauzá Sainz de Baranda püüab oma magistritöös [13] analüüsida logikogujate käitumist Microsofti võrkudes, uurides nendest rünnakutest jäetud jälgi ja olukorda, milles manipuleeritud sündmused aset leiavad. Selleks viidi läbi uuring, kus kasutati rünnakuid sündmustevoo erinevatele turvaaukudele: andmeallikale, transiidile ja logikogujatele endile, kasutades Winlogbeati ja Filebeati logikogujaid sisevõrgus, mis simuleerib väikeettevõtet. Selle tulemusena saime demonstratsiooni võimalusest muuta andmeallika sündmusi ja logikogujale suunatud rünnakuid. Sellest lähtuvalt peaksite krüptimise pärast muretsema nii logide edastamisel kui ka enda logimisel. Seda meetodit

käsitleb oma magistritöös Maarja-Liisa Tammepõld[14]. Artiklis käsitletakse ka väga olulist punkti analüütikute turvalisel autentimisel keskse andmekogumisteenusega ühenduse loomisel.

Logifailide arvu ja suuruse kasvades muutub logifailide sõelumine üha keerulisemaks. On äärmiselt oluline, et analüütik järgiks tugevat logianalüüsi metoodikat, mida toetab võimas platvorm, et edukalt töödelda logifaile ja otsida väärtuslikke artefakte täpsete tulemuste saamiseks. Edukas logifaili analüüs eeldab, et analüütik järgib logianalüüsi metoodikat. Andmete kogumise ja analüüsimise metoodika koostamiseks uuriti töös lisamaterjali[15], mis võimaldas koostada süsteemi logide analüüsi etappide diagrammi (vt Joonis 1).

Joonis 1. Logide analüüsi etappide diagramm

Paljude käesoleva lõputöö teemaga seotud dokumentide hindamine ja otsimine näitab, et kesksete sündmuste logihoidlate loomine on kuum teema. Põhimõtteliselt on artiklites hoidlad keskendunud ühele logide kogumise süsteemile, need on kas Linuxi või Windowsi sündmuste logid. Väga harva kaalutakse meetodeid, mis võimaldavad ühes aknas kombineerida erinevatest andmeallikatest pärit sündmusi. Kuna erinevad riistvaratootjad mõjutavad logide vormingut ja sellest tulenevalt kulub logide standardiseerimiseks rohkem aega. Käesoleva magistritöö eesmärk on täita lünk, andes ülevaate mitmesuguste sündmuste logi allikatega toimetuleva süsteemi ehitamisest.

3 Logianalüüsi metoodika

Süsteemi logide analüüsi metoodika eesmärk on süstemaatiline ja efektiivne lähenemine logide analüüsile, et avastada ja analüüsida turvaintsidente, vigu ja jõudlusprobleeme ning tuvastada turvapoliitika rikkumisi ja vastavust regulatiivsetele nõuetele[16].

Logianalüüsi metoodika hõlmab logifailidest andmete kogumist, indekseerimist, tsentraliseeritud salvestamist, andmete analüüsi ja tõlgendamist ning soovituste ja meetmete pakkumist süsteemi turvalisuse ja jõudluse parandamiseks[17].

Eesmärkide ja analüüsiülesannete määratlemine on samuti logide analüüsi metodoloogias sisaldatud ning see määrab vajaduse valiku järele, milliseid vahendeid ja tehnoloogiaid kasutada logide kogumiseks ja töötlemiseks, analüüsikriteeriumide ja läviväärtuste määratlemise ning protseduuride ja kohustuste määratlemise juhuks, kui avastatakse turvaaugud ja turvaintsidentid. See on seotud sellega, et traditsioonilised andmeanalüüsi vahendid ei suuda tagada tõhusat töötlust kiiresti kasvava mahuga ja mitmekesisusega masinlogide puhul. [18].

Logianalüüsi metoodika eesmärkide hulka kuulub ka tõhusa ja süstemaatilise lähenemisviisi tagamine logide analüüsile, mis võimaldab reaalajas või minevikus tuvastada ja reageerida turvariskidele ja muudele süsteemiprobleemidele[19].

Samuti tagab see infoturbe süsteemi turvalisuse, avastades ja ennetades rünnakuid, kasutajate ebanormaalset käitumist ja muid potentsiaalselt ohtlikke sündmusi. Seda saab kasutada ka süsteemi jõudluse jälgimiseks ja probleemide tuvastamiseks, mis võivad põhjustada tõrkeid.

Süsteemi logide analüüsi jaoks võib teabeallikateks olla erinevad logid ja ajakirjad, mis on kogutud erinevatelt seadmetelt ja rakendustelt infoturbe süsteemis. Need võivad olla operatsioonisüsteemi, andmebaasi, veebiserveri, rakenduste ja teiste süsteemi komponentide logid. Samuti võivad kasutada andmeid võrguliikluse ja turvariskide kohta, mida erinevad võrgu perimeetri kaitse seadmed avastavad[20].

3.1 Logianalüüs

Logianalüüs on protsess, kus süsteemi või võrgu logifailidest kogutakse, töödeldakse ja analüüsitakse andmeid, et tuvastada turvaintsidente, toimivusprobleeme ja muid olulisi sündmusi. Logid on kirjalikud salvestised, kus fikseeritakse süsteemi toimimist puudutav informatsioon, nagu sisse- ja väljalogimised, juurdepääsukatsed, vigu, hoiatusi ja muud sündmused. Logianalüüs aitab parandada süsteemi turvalisust, jõudlust ja usaldusväärsust ning võimaldab tuvastada probleeme varajases staadiumis, enne kui need kasvavad tõsisteks ohuks.

3.2 Logide analüüsi protsess

Logianalüüs võimaldab koguda ja analüüsida logifaile, mis sisaldavad teavet erinevate sündmuste kohta, mis toimuvad süsteemis või rakenduses. Logifaile saab koguda erinevatest allikatest, sealhulgas serveritest, võrguseadmetest ja rakendustest.

Logianalüüs töötab järgmiselt:

- Kogumine: Logifaile kogutakse erinevatest allikatest, tavaliselt kasutades spetsiaalseid tarkvaralahendusi, mis suudavad logifailide andmeid korralikult koguda ja salvestada.

- Agregatsioon: Kogutud logifailide andmeid töödeldakse ja koondatakse ühte kohta, et hõlbustada nende edasist analüüsi. Selles etapis on oluline mõista, millised sündmused on kriitilised ja millised võivad olla vähem olulised.

- Korrelatsioon: Logianalüüs tähendab ka erinevate logisündmuste seostamist ja korrelatsiooni uurimist, et saada aru, millised sündmused võivad olla seotud või millised sündmused võivad olla põhjustanud muid sündmusi.

- Analüüs: See etapp hõlmab logisündmuste põhjalikku uurimist ja analüüsi, et tuvastada võimalikke ohutusprobleeme, vigu, jõudlusküsimusi ja muid probleeme.

- Hoiatused ja teavitused: Kui tuvastatakse mõni tõsine probleem, saadetakse vastavad hoiatused ja teavitused, et rakendada kiiret reageerimist ja kõrvaldada probleemid.

3.3 Logi analüüsi meetodid

Tänapäeva digimaailmas genereeritud andmemahu tõttu ei saa IT-spetsialistid suures IT-infrastruktuuris logisid käsitsi jälgida ja analüüsida. Selle tulemusena vajasid nad keerukat logihaldussüsteemi ja strateegiaid, mis automatiseerivad võtmeandmete kogumist, vormindamist ja analüüsi. [20]

- Reeglitel põhinev analüüs: See meetod põhineb reeglite seadmisel, et tuvastada teatud tüüpi sündmusi logides. Reeglites võib olla määratud sündmuse kirjeldus,

mis vastab konkreetsele tingimusele. Kui logisse kirjutatakse sündmus, mis vastab reegli tingimustele, käivitatakse vastav toiming.

- Masinõppe meetodid: Masinõppe meetodid võimaldavad luua ennustusmudeleid, mis analüüsivad logi andmeid ja tuvastavad tavapärasest erinevaid sündmusi. See meetod on eriti kasulik avastamaks uusi ründe- ja pahavara tüüpe.

- Korrelatsioonianalüüs: See meetod kasutab mitmeid logifailide andmeid, et leida seoseid sündmuste vahel. See võib aidata tuvastada rünnakute algsündmusi, mis võivad olla peidus erinevates süsteemides.

- Visuaalne analüüs: Visuaalse analüüsi meetod hõlmab graafiliste esituste loomist logiandmetest. Selline lähenemine aitab tuvastada seoseid andmete vahel ja annab parema ülevaate sündmustest, mis aitavad kaasa otsustusprotsessidele.

Kokkuvõtvalt on logianalüüs meetod, mis võimaldab koguda, salvestada ja analüüsida sündmusi süsteemides, et tuvastada tavapärastest erinevaid käitumisi, rünnakuid või muid probleeme. Erinevad meetodid võivad olla kasulikud erinevates olukordades ja sõltuvalt analüüsi eesmärgist.

3.4 Logianalüüsi eelised

Logianalüüsi eelised võivad hõlmata[20]:

- Turvalisus: Logianalüüs võimaldab avastada varakult potentsiaalseid turvarikkumisi ja reageerida neile kiiresti. See võib aidata vältida suuri andmekaotusi, vargusi või ründeid.

- Jõudlus: Logianalüüs võib aidata parandada süsteemi jõudlust, identifitseerides protsessides ja rakendustes aeglaseid või ebakorrapäraseid käitumismustreid.

- Tõrkeotsing: Logianalüüs võib aidata IT-spetsialistidel tuvastada süsteemis esinevaid probleeme ja aidata tõrkeotsingul.

- Jälgimine: Logianalüüs võimaldab jälgida süsteemi toimimist ja tööd, aidates ettevõtetel paremini mõista, kuidas nende IT-keskkond toimib.

- Reguleerimisnõuete täitmine: Mõned tööstusharud, nagu finantsteenused ja tervishoid, nõuavad logide säilitamist ja analüüsimist vastavalt määrustele ja standarditele. Logianalüüs võib aidata ettevõtetel täita neid nõudeid.

Vastavalt reeglitele peavad enamik ettevõtteid salvestama ja analüüsima ajaloo- ehk logifaile. Süsteemsete logifailide regulaarne jälgimine ja analüüs võimaldab avastada vigu, anomaaliaid või kahtlaseid tegevusi, mis jäävad tavapärase tegevuse raamidest välja. Logifailide analüüsi abil saab taastada sündmuste järjestuse, mis viis probleemi tekkeni ning seda tõhusalt lahendada.

Lisaks sellele, kuigi logide analüüs võib tunduda puudutavat ainult organisatsiooni IT-komponenti, tegelikult hõlmab see kõiki teie äritegevuse aspekte, sealhulgas juriidilisi, finants-, müügi- ja turundusaspekte, personalijuhtimist, turvalisust ja tegevusi. Logifailide analüüs võimaldab probleeme avastada ennetavalt või nende tekkimise ajal, säästes aega, vältides tarbetuid viivitusi ja lisakulusid.

Logianalüüs võimaldab ettevõtetel paremini mõista nende IT-keskkonda, parandada turvalisust ja jõudlust ning täita reguleerimisnõudeid.

4 Keskkonna seadistamine

Wazuh on avatud lähtekoodiga tasuta turvalisuse platvorm, mis ühendab XDR-i ja SIEM-i võimalused. See kaitseb töökoormusi kohalikes, virtualiseeritud, konteiner- ja pilvekeskkondades. Wazuh aitab organisatsioonidel ja eraisikutel kaitsta oma andmevarasid turvariskide eest. See on laialdaselt kasutusel tuhandetes organisatsioonides üle maailma, alates väikestest ettevõtetest kuni suurettevõteteni[21].

Wazuhi meeskond ehitas oma toote OpenSearchi tarkvaraprojekti koodibaasi abil, mis omakorda põhines projekti Elasticsearch versioonil 7.10.2. Wazuh on tasuta ja avatud lähtekoodiga ettevõtte turvaseire lahendus ohtude tuvastamiseks, terviklikkuse jälgimiseks, intsidentidele reageerimiseks ja nõuetele vastavuseks. Lahendus koosneb ühest universaalsest agendist ja kolmest kesksest komponendist: Wazuh Server, Wazuh Indexer ja Wazuh Dashboard[22].

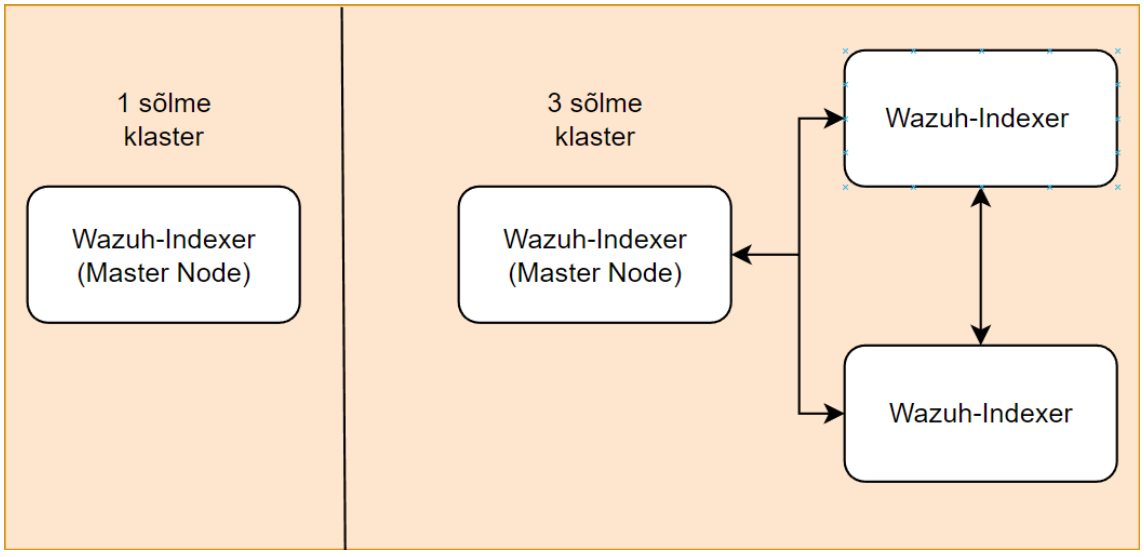
4.1 Wazuh Indexer – SIEM-i tagasüsteem seadistamine

Kõigi turvalogide salvestamiseks on vaja tagasüsteemi. See võimaldab turvaanalüütikutel soovitud aegadel turvasündmusi otsida. Selleks on vaja kiiret ja usaldusväärset lahendust, mida saab hõlpsasti skaleerida, et käsitleda erinevatest allikatest kogutud palkide koormust.

Wazuh Indexer on SIEM-i tagasüsteem, mis kogub, indekseerib ja salvestab logifailid, mida kogub Wazuh agent, et võimaldada nende logide kiiret ja lihtsat otsimist ja analüüsi. SIEM-i tagasüsteemi seadistamine hõlmab Wazuh Indexeri paigaldamist, vajalike konfiguratsioonide määramist ja seadistamist vastavalt teie organisatsiooni vajadustele. Lisaks tuleb seadistada Wazuh Indexeri tulemüür ja võrgupoliitikad, et tagada andmete turvalisus. Lõpuks on oluline ka jälgida Wazuh Indexeri jõudlust, et tagada selle tõrgeteta töö.

Wazuhi indekseerimisklaster on ühe või mitme sõlme kogum, mis suhtlevad üksteisega indeksi lugemise ja kirjutamise toimingute tegemiseks (vt Joonis 2).

Väikesi Wazuhi juurutusi, mille töötlemiseks ei ole vaja suuri andmemahtusid, saab hõlpsasti hallata ühe sõlmeklastri abil. Mitme sõlmega klastreid soovitatakse kasutada, kui jälgitavaid lõpp-punkte on palju, kui oodatakse suurt hulka andmeid või kui on vaja suurt käideldavust.



Joonis 2. 1 sõlme ja 3 sõlme klaster.

Tootmiskeskkondade jaoks on soovitatav juurutada Wazuh Server, Wazuh Indexer ja Wazuh Dashboard erinevatele hostidele.

Wazuh Server, Wazuh Indexer ja Wazuh Dashboard saab erinevatel hostidel turvalisuse tagamiseks kaitsta TLS-krüpteeringuga. TLS-sertifikaadi saab iga hosti jaoks genereerida ise allkirjastatult, et seda TLS-sertifikaadina kasutada. Tootmises soovitatakse kindlasti kasutada ametlikult välja antud sertifikaate. Wazuh Server, Wazuh Indexer ja Wazuh Dashboard tuleb seadistada TLS-i kasutamiseks ning veenduda, et kõik ühendused hostide vahel kulgevad läbi krüpteeritud TLS-kanali. See aitab tagada Wazuh Serveri, Wazuh Indexeri ja Wazuh Dashboardi turvalisuse erinevatel hostidel TLS-krüpteeringuga ning kõik sõnumid hostide vahel edastatakse krüpteeritud kujul.

Minimaalne			**Soovitav**	
Component	RAM (GB)	CPU (cores)	RAM (GB)	CPU (cores)
Wazuh-Indexer	4	2	16	8

Tabel 1. Riistvara soovitused iga sõlme jaoks

Andmemaht sõltub genereeritud hoiatustest sekundis (APS). See tabel kirjeldab hinnangulist kettaruumi, mis on vaja agenti kohta, et salvestada Wazuhi indekseerija serverisse 90 päeva hoiatusi, olenevalt jälgitavate lõpp-punktide tüübist.

Monitored endpoints	**APS**	**Salvestus Wazuhi indekseerijas (GB/90 päeva)**
Servers	0.25	3.7
Workstations	0.1	1.5
Network devices	0.5	7.4

Tabel 2. Kettaruumi nõuded

Arendajad toovad näite, et keskkonnas, kus on 80 tööjaama, 10 serverit ja 10 võrguseadet, on Wazuhi indekseerija serveris 90 päeva hoiatuste jaoks vajalik salvestusruum 230 GB[23].

Praeguses konfiguratsioonis on wazuh-indexer installitud ühe sõlmega, mille baasOS on Debian 11. Teiste toetatud operatsioonisüsteemide hulka kuuluvad Ubuntu 16.x-22.x, Centos 7-8, Red Hat 7-9, Amazon Linux 2.

Wazuh keskkomponentide vahelise suhtluse krüptimiseks ja turvaliseks muutmiseks tuleb alla laadida skript wazuh-certs-tool.sh ja konfiguratsioonifail config.yml. Soovi korral on võimalik kasutada enda sisemist PKI-d. Wazuh pakub hõlpsasti kasutatavat bash-skripti, mida kasutatakse teie enda sisemiste sertifikaatide genereerimiseks, et krüpteerida wazuh-indexerile saadetud logisid. Ohutuse põhimõtteid on kirjeldatud varasemates uuringutes [13],[14]. Nende uuringute tulemuste põhjal on näha, et logi krüpteerimine ja kaitse on väga aktualnee teema.

Vaja on redigeerida config.yml faili ja asendada hostide nimed ja IP-aadresside väärtused vastavate nimede ja IP-aadressidega. See tuleb teha Wazuh skanneri, Wazuhi jälgimispaneeli sõlmede ja kõigi serverite jaoks, mis saadavad skannerile Wazuh logisid, näiteks Graylog.

```
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: node-1
      ip: <indexer-node-ip>
    # - name: node-2
    #   ip: <indexer-node-ip>
    # - name: node-3
    #   ip: <indexer-node-ip>

# Wazuh server nodes
  # Use node_type only with more than one Wazuh manager
  server:
    - name: wazuh-1
      ip: <wazuh-manager-ip>
    # node_type: master
    # - name: wazuh-2
    #   ip: <wazuh-manager-ip>
    # node_type: worker

# Wazuh dashboard node
  dashboard:
    - name: dashboard
      ip: <dashboard-node-ip>
```

Joonis 3. Aadress ja sõlme konfigureerimine

Pärast installimise lõpetamist peate redigeerima faili /etc/wazuh-indexer/opensearch.yml ja asendama väärtused:

- **network.host**: määrab selle sõlme aadressi nii HTTP- kui ka transpordiliikluse jaoks. Sõlm seostub selle aadressiga ja kasutab seda ka oma avaldamisaadressina. Aktsepteerib IP-aadressi või hostinime. Kasutage SSL-sertifikaatide loomiseks sama sõlme aadressi, mis on määratud failis config.yml.

- **Node.name**: Wazuhi indekseerimissõlme nimi, mis on määratletud failis config.yml. Näiteks node-1.

- **cluster.initial_master_nodes**: põhi-kõlblike sõlmede nimede loend. Need nimed on määratletud failis config.yml. Tühjendage ridade node 2 ja node 3 kommentaarid, muutke nimesid või lisage rohkem ridu vastavalt oma config.yml definitsioonidele.

- **discovery.seed_hosts**: hosti aadresside loend, mis võivad olla põhiaadressid. Iga element võib olla kas IP-aadress või hostinimi. Kui konfigureerite Wazuhi indekseerija ühe sõlmena, võite selle sätte kommenteerimata jätta. Mitme sõlmega konfiguratsioonide puhul tühistage see suvand ja määrake nende sõlmede aadressid, mis võivad olla juhtsõlmed.

- **plugins.security.nodes_dn**: kõigi Wazuhi indekseerimisklastri sõlmede sertifikaatide eristavate nimede loend. Tühjendage node-2 ja node-3 read ning muutke üldnimetusi (CN) ja väärtusi, et need vastaksid teie seadetele ja config.yml definitsioonidele. Sertide CN-i vaatamiseks käivitage käsk

Wazuh-indekser ei tööta korralikult, kui süsteem vahetab mälu. Sõlme tervise seisukohalt on ülioluline, et ükski JVM ei lehitseks kunagi kettale. Järgmised sammud näitavad, kuidas määrata bootstrap.memory_lock väärtuseks true, et wazuh-indexer lukustaks protsessi aadressiruumi RAM-is. See takistab wazuh-indexermälu mahalaadimist. JVM-i kuhi piirangud aitavad piirata mälukasutust ja seda olukorda vältida. Wazuh-indekseri kuhi suuruse määramisel tuleb järgida kahte reeglit:

- Kasutage mitte rohkem kui 50% saadaolevast RAM-ist.

- Kasutage mitte rohkem kui 32 GB.

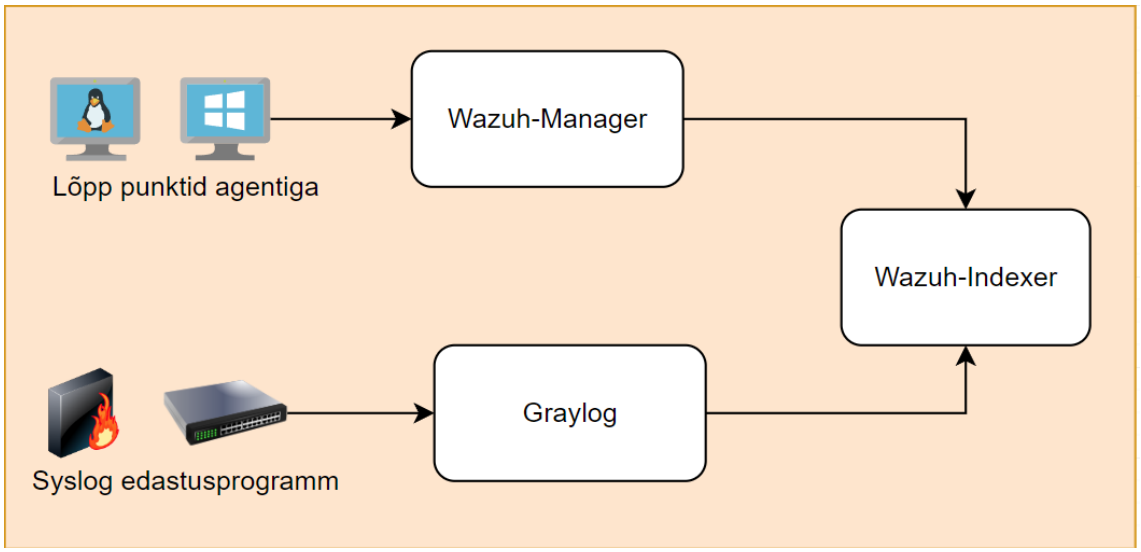
4.2 Graylog seadistamine

Kuna süsteemi logid kogutakse erinevatest süsteemidest, on vajalik paigaldada logide tsentraliseeritud haldamise süsteem (LMS), näiteks Graylog, mis võimaldab koguda, süstematiseerida ja analüüsida kõiki neid andmeid. Graylog on oluline komponent, mis täiendab Wazuh funktsionaalsust ja tagab laiema valiku võimalusi süsteemi turvalisuse ja jälgimise jaoks.

Andmete normaliseerimine on kohustuslik. Tuleb pakkuda ühist vastet logide ühistele andmeväljadele (sõltumata allikast), et oleks võimalik luua infopaneele ja standardeid, mis kehtivad kõigi logitüüpide suhtes. Näiteks tulemüüri logi kirjutab ühenduse algataja algse IP-aadressi source_ip_ipv4 ja Sysmon-i sündmused, mis on kogutud lõppseadmetest, kirjutavad algse IP-aadressi väljale data_win_eventdata_sourceIp. Kuna need väljad sisaldavad samu metaandmeid (allika IP-aadress), on kasulik salvestada need

väärtused standardväljale, nagu src_ip. Nüüd saab SOC meeskond ühe päringuga kiiresti leida algse IP-aadressi, mitte kahega.

Logide kogumise ja analüüsi automatiseerimine on turvaseire süsteemi oluline osa. Graylogi kasutamine andmete edastamiseks Wazuhile võimaldab erinevatest allikatest pärinevaid andmeid kombineerida, normaliseerida ja analüüsida võimalike ohtude tuvastamiseks. Ühendus teiste teenustega, nagu MISP ja Virustotal, võimaldab avastada teadaolevaid kahjulikke IP-aadresse, domeene ja faile, mis aitab tõhusamalt võidelda küberohtudega.



Joonis 4. Loogikogumine süsteem.

Graylogs 5.0 installimiseks on vaja eraldi Debian 11 serverit. Graylog kasutab MongoDB-d konfiguratsiooniandmete, mitte logiandmete salvestamiseks. Salvestatakse ainult metaandmed, näiteks kasutajateave või voo konfiguratsioonid. Selle saab installida spetsiaalsesse serverisse või Graylogiga samasse hosti.

Graylog on võimas ja paindlik tööriist logide töötlemiseks, mis sisaldab mitmeid sisseehitatud funktsioone andmete analüüsimiseks ja täiendamiseks. Tänu nendele funktsioonidele saame lisada intelligentsed funktsioonid lõplikesse logidesse, enne kui need salvestatakse meie serveri hoidlasse, mis on oluline ehitusplokk edukaks SIEM-iks.

4.3 Wazuh Manager seadistamine

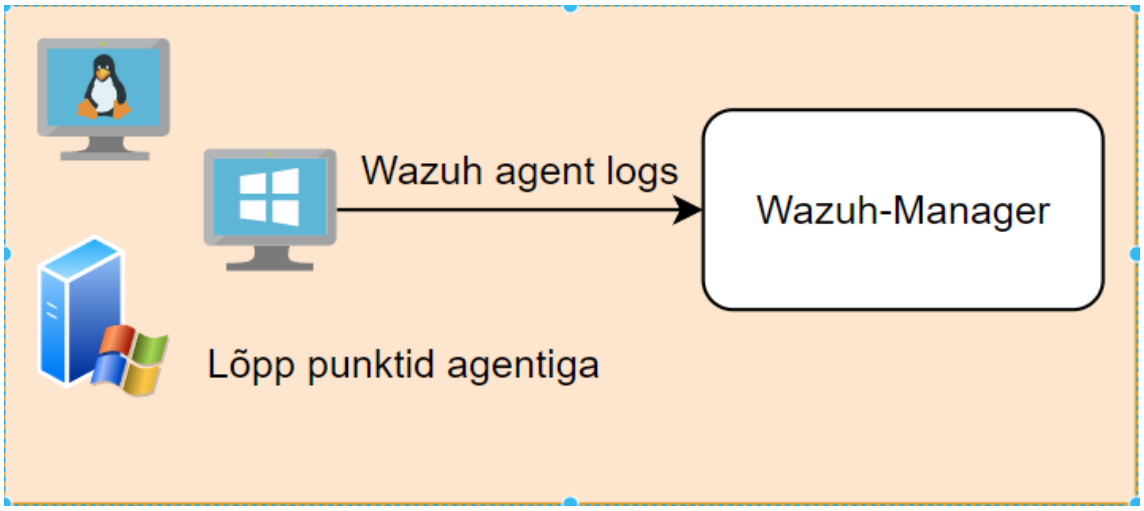
Wazuh Manager on Wazuh süsteemi komponent, mis vastutab reaalajas arvutites ja serverites turvalisuse andmete kogumise, analüüsi ja salvestamise eest. Wazuh Manager

saab töödelda andmeid erinevatest allikatest, sealhulgas süsteemi logifailidest, viirusetõrje logidest, sise- ja välislogidest jne. Ta saab analüüsida andmeid võimalike ohtude osas ja teavitada kahtlasest tegevusest. Wazuh Managerit kasutatakse tavaliselt koos teiste Wazuh komponentidega, nagu Wazuh API ja Wazuh Agent, keskse turvaseire süsteemi loomiseks.

EDR-lahendus peab tagama pideva ja igakülgse ülevaate lõpp-punktides toimuvast reaalajas.

EDR-id koosnevad tavaliselt kahest põhiosast:

- Endpoint Agent – kogub lõpp-punktidest logisid.
- Collection Manager – hangib lõpp-punktidest logisid ja analüüsib pahatahtlikku tegevust.



Joonis 5. Wazuh agenti töö

Põhjalik kaitse on tänapäeva küberkliimas kohustuslik. AV on loodud arvutis pahavara tuvastamiseks, kuid küberohtude osalised muutuvad üha keerukamaks. Lisaks kasutavad pahavara arendajad erinevaid meetodeid, näiteks failivaba pahavara, et vältida viirusetõrjelahenduste tuvastamist. EDR võimaldab kergitada loori lõpp-punktidelt ja jälgida kõiki süsteemis toimuvaid toiminguid. Analüütikud peavad mõistma lõpp-punktides toimuvat tegevust, et pahatahtlikku tegevust täpselt tuvastada. Kogudes mõned alltoodud allikatest, aitavad need leida varjatud ohu, mida viirusetõrje ei paku:

- Võrguühendused

- DNS-päringud
- Käsud käivita
- Kasutajate sisselogimised
- Powershell Spawns
- Protsessi kudesid

Wazuh on autori sõnul praegu parim avatud lähtekoodiga EDR. Wazuh pakub platvormi, mis võimaldab teil jälgida lõpp-punkte, integreerida kolmandate osapoolte rakendustega ja järgida vastavusstandardeid. Wazuh toetab kõige levinumaid operatsioonisüsteeme. Vaikimisi on Wazuhis eelinstallitud järgmised komponendid:

- Logiandmete analüüs
- Failide terviklikkuse jälgimine
- Haavatavuse tuvastamine
- CIS Benchmark hindamine
- Vastavus eeskirjadele
- Konteinerite turvalisus

Wazuh võimaldab teil luua ka oma tuvastamisreegleid, integratsioone ja konfiguratsioone, mis sobivad iga kasutusjuhtumiga.

Parem on installida Wazuh Manager eraldi serverisse, kuid ühte serverisse on võimalik installida ka Indexer, Dashboard ja Manager, kuid autor soovitab eraldada iga teenuse jaoks eraldi server.

Lõpp-agendid peavad enne logide saatmist registreeruma Wazuh Manageris. Vaikimisi saab iga Wazuhi agent registreeruda halduri juures. Muudame seda nii, et meie halduriga saaksid ühendust võtta ainult meie kontrolli all olevad agendid.

- Lubage parooli autentimise suvand, lisades allpool esiletõstetud konfiguratsiooni halduri konfiguratsioonifaili /var/ossec/etc/ossec.conf jaotisesse <auth>.

- Enda parooli määramine. Seda tehakse, luues oma parooliga halduris faili /var/ossec/etc/authd.pass.

- Muutke faili authd.pass õigusi ja omandiõigust.

See annab võimaluse täiendavalt turvata logide ülekandmist, et vältida sissetungijate ründamist süsteemilogidesse, nagu töös kirjeldatud[14].

Järgmine samm on võimaldada haavatavuste otsimise võimalus lõppseadmetes, kuhu agendid installitakse..

Wazuh võimaldab ka tsentraalselt hallata agentide konfiguratsiooni lõppseadmetes.

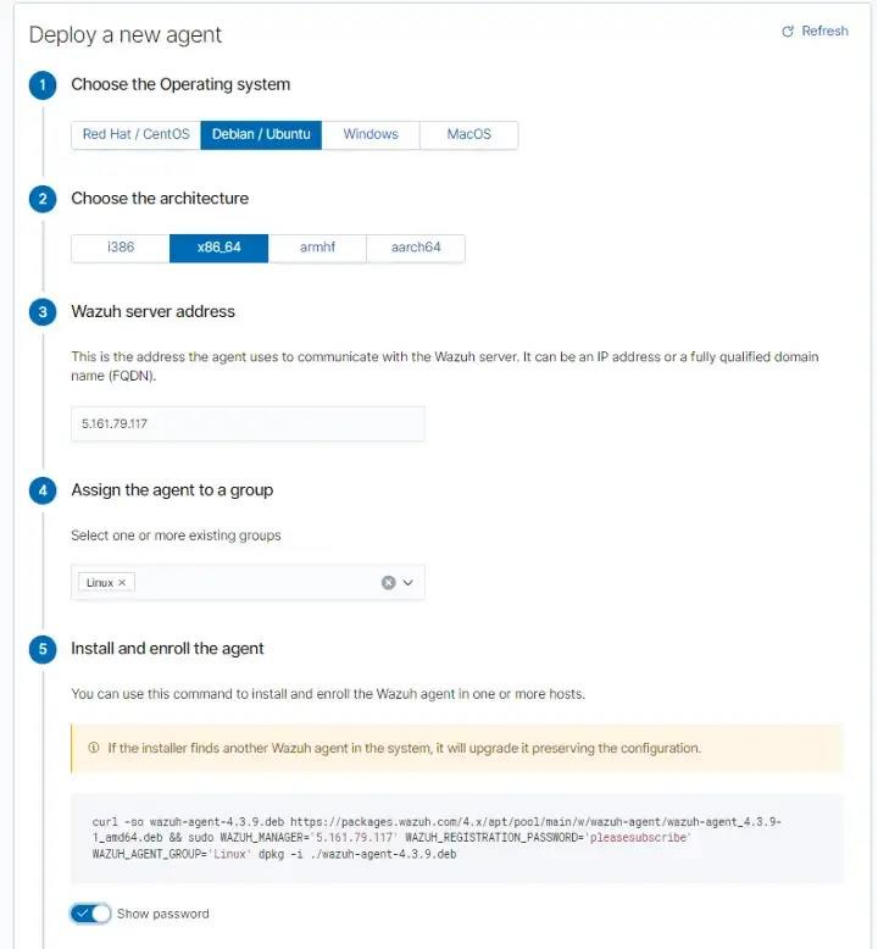
4.4 Wazuh Agent Install – lõpp-punkti jälgimine

Wazuh Agent - see turvaaagent, mis installitakse sihtseadmetele (arvutid, serverid jne) turvalisuse andmete kogumiseks ja saatmiseks Wazuh Managerile. Agent saab koguda andmeid erinevatest allikatest, sealhulgas süsteemiloggidest, viirusetõrje logidest, võrgupakettidest jne. See võib samuti avastada turvariske ja saata reaalajas hoiatusi Wazuh Managerile. Wazuh Agent toetab erinevaid operatsioonisüsteeme, sealhulgas Windows, Linux, macOS ja Solaris. See pakub laia valikut konfigureerimis- ja juhtimisfunktsioone, nagu turvaseaded, jõudluse jälgimine jne[25].

Wazuhi agendi installimine on lihtne, kuid kõigepealt peate mõistma mõningaid põhitõdesid selle kohta, kuidas Wazuhi agent halduriga suhtleb.

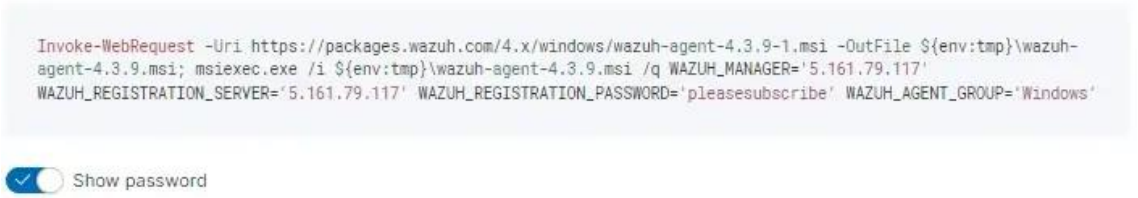
Manager ja agent krüpteerivad omavahelist suhtlust. Selleks peab manageril ja agendil olema ühine kliendivõti. See sümmeetriline võti krüpteerib logid, mille agent dispetšerile edastab. Kui Wazuh-Agent esimest korda käivitub, küsib see dispetšerilt kliendivõtit (TCP 1515). Kui on vaja autentimist, parooli autentimist või sertifikaadi autentimist, kinnitab manager agendi ja heakskiitmise korral genereerib kliendivõtme, mille see agendile tagasi saadab. Wazuhi agent edastab logid nüüd Wazuhi haldurile. See liiklus liigub agendilt haldurile TCP-pordis 1514. Enne massinstalli juurutamist veenduge, et nii logimise kui ka logi edastamise jaoks on määratud sobivad tulemüürireeglid. Wazuh on

kokku pannud laheda tööriista, mida saab Wazuhi veebirakenduse kaudu kasutada ühere alise installikäskluse loomiseks. See installib agendi lõpp-punkti ja näitab õige manager, mida kasutada (Vt. Lisa 3).



Joonis 6. Wazuh agenti automaatne konfigureerimine

Windowsi agendi installimiseks peate avada PowerShelli ja käivitama automatselt loodud installikäskluse:



Joonis 7. PowerShelli loodud installikäsk

Vaikimisi Wazuh agendi kogub ainult Windowsi logisid ja süsteemilogisid, mis ei anna täielikku pilti sellest, mis toimub lõppseadmel. Väärteoaktiivsuse täpsemaks avastamiseks on vaja koguda täiendavaid andmeid, nagu võrguühendused, protsessivood

ja käsuridade täitmine. Selleks saab kasutada muid teenuseid, nagu Sysmon ja Packetbeat, mida saab koos Wazuh agendiga laiendada selle jälgimisvõimalusi.

4.5 Sysmon seadastamine

Sysmon - see süsteemi jälgimisvahend Windowsi operatsioonisüsteemidele, mille on välja töötanud Microsoft. See on mõeldud süsteemi protsesside ja sündmuste info kogumiseks, mis võivad viidata süsteemi ohustamisele või muudele turvaprobleemidele. Sysmon võimaldab saada üksikasjalikku teavet käivitatud protsesside, võrguühenduste, failioperatsioonide, registri muudatuste ja muude sündmuste kohta, mida saab kasutada turvaintsidentide tuvastamiseks ja uurimiseks. Sysmoni saab integreerida teiste turvavahendite ja jälgimissüsteemidega, nagu Wazuh, et tuvastada ja reageerida turvaohtudele tõhusamalt.[24]

Sysmoni installimisel mängib olulist rolli konfiguratsioonifail sysmonconfig.xml[26]. Praegu failis on rohkem kui 2500 read.

sysmonconfig-export.xml

```
<Sysmon schemaversion="4.60">
  <HashAlgorithms>*</HashAlgorithms>
  <!-- This now also determines the file names of the files preserved (String) -->
  <CheckRevocation>False</CheckRevocation>
  <!-- Setting this to true might impact performance -->
  <DnsLookup>False</DnsLookup>
  <!-- Disables lookup behavior, default is True (Boolean) -->
  <ArchiveDirectory>Sysmon</ArchiveDirectory>
  <!-- Sets the name of the directory in the C:\ root where preserved files will be saved (String)-->
  <EventFiltering>
    <!-- Event ID 1 == Process Creation - Includes -->
    <RuleGroup groupRelation="or">
      <ProcessCreate onmatch="include">
        <ParentImage name="technique_id=T1546.008,technique_name=Accessibility Features" condition="image">sethc.exe</ParentImage>
        <ParentImage name="technique_id=T1546.008,technique_name=Accessibility Features" condition="image">utilman.exe</ParentImage>
        <ParentImage name="technique_id=T1546.008,technique_name=Accessibility Features" condition="image">osk.exe</ParentImage>
        <ParentImage name="technique_id=T1546.008,technique_name=Accessibility Features" condition="image">Magnify.exe</ParentImage>
        <ParentImage name="technique_id=T1546.008,technique_name=Accessibility Features" condition="image">DisplaySwitch.exe</ParentImage>
        <ParentImage name="technique_id=T1546.008,technique_name=Accessibility Features" condition="image">Narrator.exe</ParentImage>
        <ParentImage name="technique_id=T1546.008,technique_name=Accessibility Features" condition="image">AtBroker.exe</ParentImage>
        <OriginalFileName name="technique_id=T1546.011,technique_name=Application Shimming" condition="is">sdbinst.exe</OriginalFileName>
        <OriginalFileName name="technique_id=T1197,technique_name=BITS Jobs" condition="is">bitsadmin.exe</OriginalFileName>
        <Rule name="Eventviewer Bypass UAC" groupRelation="and">
          <ParentImage name="technique_id=T1548.002,technique_name=Bypass User Access Control" condition="image">eventvwr.exe</ParentImage>
          <Image condition="is not">c:\windows\system32\mmc.exe</Image>
        </Rule>
        <ParentImage name="technique_id=T1548.002,technique_name=Bypass User Access Control" condition="image">fodhelper.exe</ParentImage>
        <Rule name="technique_id=T1021.003,technique_name=Distributed Component Object Model" groupRelation="and">
          <ParentCommandLine condition="contains">-Embedding</ParentCommandLine>
          <ParentImage condition="is">c:\windows\system32\mmc.exe</ParentImage>
        </Rule>
        <Rule groupRelation="and">
          <CommandLine condition="contains">Set-MpPreference</CommandLine>
          <CommandLine condition="contains any">-DisableRealTimeMonitoring $true;-DisableBehaviorMonitoring $true;-DisableBlockAtFirstSeen $true;-DisableIOAVProtection $true;-DisablePrivacyMode $true;
-SignatureDisableUpdateOnStartupWithoutEngine $true;-DisableArchiveScanning $true;-DisableIntrusionPreventionSystem $true;-DisableScriptScanning $true</CommandLine>
        </Rule>
        <CommandLine name="technique_id=T1027,technique_name=Obfuscated Files or Information" condition="contains">^</CommandLine>
        <CommandLine name="technique_id=T1027,technique_name=Obfuscated Files or Information" condition="contains">../../</CommandLine>
        <ParentCommandLine name="technique_id=T1204,technique_name=User Execution" condition="is">C:\Windows\explorer.exe</ParentCommandLine>
        <ParentImage name="technique_id=T1204,technique_name=User Execution" condition="is">C:\Windows\explorer.exe</ParentImage>
```

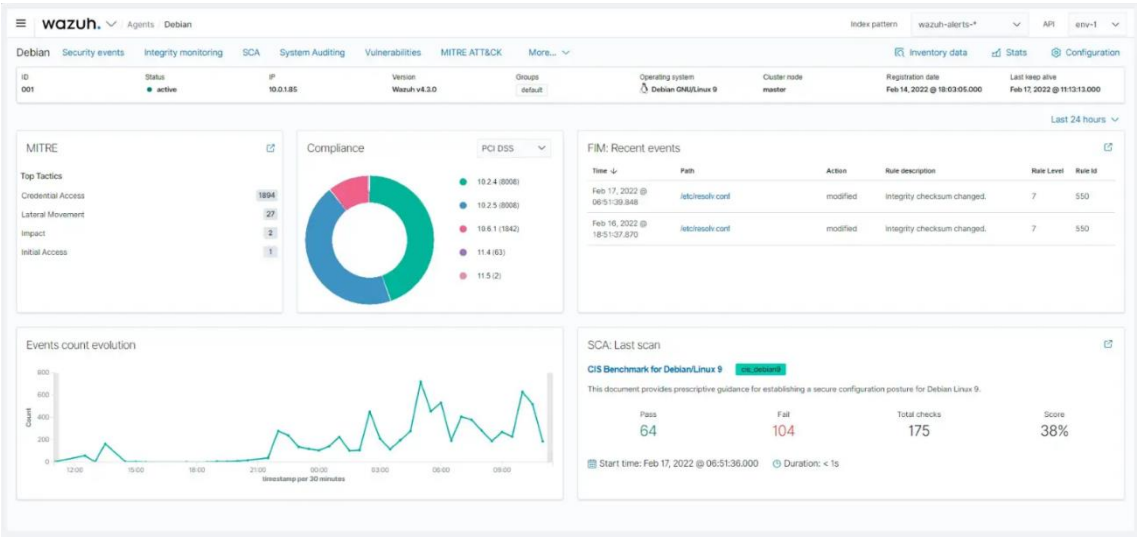
Joonis 8. Sysmoni konfiguratsionifail

Aluseks võeti avalikust hoidlast konfiguratsioonifail, kuid nagu autor ise kirjutab, on see vaid lähtepunkt ning Valepositiivsete (False Positive) sündmuste filtreerimiseks on soovitav edaspidi sätteid täiendada või eemaldada.(Vt. Lisa 4)

4.6 Wazuh-Dahboard – SIEM-i eessüsteem seadistamine

Wazuhi juhtpaneel on paindlik ja intuitiivne kasutajaliides, mis võimaldab Wazuhi platvormi kogutud turvandmete ja hoiatuste andmeid analüüsida, kokku võtta ja visualiseerida. Seda kasutatakse ka Wazuhi platvormi jälgimiseks ja haldamiseks. Wazuhi juhtpaneelil on rollipõhine juurdepääsu haldamise (RBAC) ja ühekordse sisselogimise (SSO) funktsionaalsus, mis võimaldab organisatsioonidel kontrollida juurdepääsu ja Wazuhi platvormi kasutamist.

Lisaks pakub Wazuhi juhtpaneel veebiliidest Wazuhi indekseerimisõõnaste suhtlemiseks, mis hõlbustab turvandmetega töötamist ja nende analüüsimist. Wazuhi juhtpaneelil on lai valik funktsioone, sealhulgas reaalajas kuvamine, sündmuste filtreerimine ja otsing, kohandatavate armatuurlaudade ja teadete loomine. Samuti on sellel graafilised ja analüütilised võimalused turvandmetega töötamise hõlbustamiseks.



Joonis 9. Wazuh Dashboard

Wazuh-koondpaneelide teenus peab suhtlema meie varem juurutatud wazuh-indekseri klastriga. Selle saab installida sõlme, kus juba töötab wazuh-indexer, või juurutada eraldi serverisse.

5 Turvaintsidentidele reageerimise platvorm

Küberintsidentide haldamise platvorm on süsteem, mis on loodud küberintsidentide avastamise ja neile reageerimise tegevuste koordineerimiseks ja haldamiseks. See sisaldab tööriistade ja protseduuride komplekti, mis aitavad turbemeeskondadel küberintsidente tuvastada, analüüsida ja lahendada.

Sellistel platvormidel on tavaliselt järgmised põhifunktsioonid:

- Intsidentide tuvastamine: küberohtude automaatne tuvastamine erinevate andmeallikate põhjal, nagu süsteemilogid, võrguliiklus, ohuseiresüsteemid jne.
- Intsidentide haldamine: küberintsidentide jälgimise ja haldamise süsteem, mis võimaldab turvameeskondadel töötada intsidentidega tsentraliseeritud keskkonnas, koordineerida tegevusi ja jälgida probleemide lahendamise edenemist.
- Probleemide analüüs ja lahendamine: probleemide analüüsi- ja lahendussüsteem, mis võimaldab turvameeskondadel andmeid analüüsida, tuvastada probleemide juuri, töötada välja strateegiaid haavatavuste kõrvaldamiseks ja parandada neid.
- Koostöö: mitme meeskonnaliikme võimalus töötada samaaegselt probleemide lahendamiseks, teabe jagamiseks ja juhtumi oleku värskendamiseks.
- Aruandlus: võime luua aruandeid toimunud vahejuhtumite, nende analüüsi, probleemide lahendamiseks võetud meetmete ja nende tulemuste kohta.
- Küberintsidentide haldamise platvorme saab arendada avatud lähtekoodiga, võimaldades kogukonnal luua oma versioone, või neid saab esitada erineva toe ja funktsionaalsusega kommertstarkvarana.

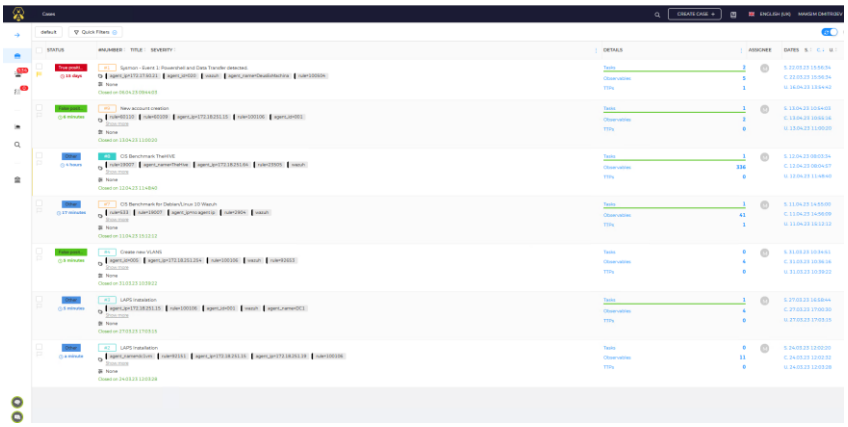
Kavandatud konfiguratsioonis kasutatakse TheHive: Community Edition. See on avatud lähtekoodiga turbeintsidentidele reageerimise platvorm, mis pakub turvaanalüütikutele, ohuküttidele ja intsidentidele reageerijatele otspunktlahendust turvaintsidentide tõhusaks ja tõhusaks koostööks, uurimiseks ja parandamiseks. Platvorm on loodud intsidentidele reageerimise protsessi automatiseerimiseks ja korraldamiseks, reageerimisaja vähendamiseks ja turvalisuse suurendamiseks[27].

5.1 TheHive ülevaade

TheHive on avatud platvorm küberrünnete ja turvaintsidentide kohta teabe kogumiseks ja analüüsimiseks. See võimaldab teil kiiresti ja tõhusalt koguda intsidentide teavet, hallata uurimisülesandeid ja tegevusi ning suhelda kolleegidega reaalajas. TheHive'i eeliste hulgas on:

- Kasutajasõbralik kasutajaliides: TheHive'il on intuitiivne ja hõlpsasti kasutatav liides, mis muudab sellega töötamise tõhusamaks.
- Lai valik integratsioone: TheHive'il on palju integratsioone erinevate turvatööriistadega, mis võimaldab teil automatiseerida paljusid ülesandeid ja muuta andmetega töötamise lihtsaks.
- Avatud lähtekoodiga: TheHive on avatud lähtekoodiga projekt, mis võimaldab arendajate kogukonnal platvormi funktsionaalsust parandada ja laiendada.
- Hajutatud töövõime: TheHive võimaldab teil jagada ülesandeid meeskonnaliikmete vahel, võimaldades teil intsidentidele kiiremini reageerida ja töö efektiivsust parandada.
- Kohandamise paindlikkus: TheHive võimaldab teil kohandada reegleid ja protsesse vastavalt oma meeskonna nõuetele ja teie individuaalsetele vajadustele.
- Võimalus konfigureerida kaheastmelist autentimist.

TheHive'is on aga funktsionaalsuse piirangud, mis võeti kasutusele versioonis 3.0.0, mis ilmus 2018. aasta veebruaris. TheHive'i arendajad põhjendasid seda otsust asjaoluga, et platvormi kaubandusliku elujõulisuse säilitamiseks ning toe ja tootearenduse jätkamiseks oli vaja eristada tasuta ja tasulisi versioone. Praegu on kaks versiooni: TheHive Community Edition ja Enterprise Edition.



Joonis 10. TheHive Case Management

TheHive'i tasuta versioonis, tuntud ka kui "Community Edition", on saadaval palju funktsioone, kuid on ka mõned piirangud. Siin on peamised funktsioonid, mis pole tasuta versioonis saadaval:

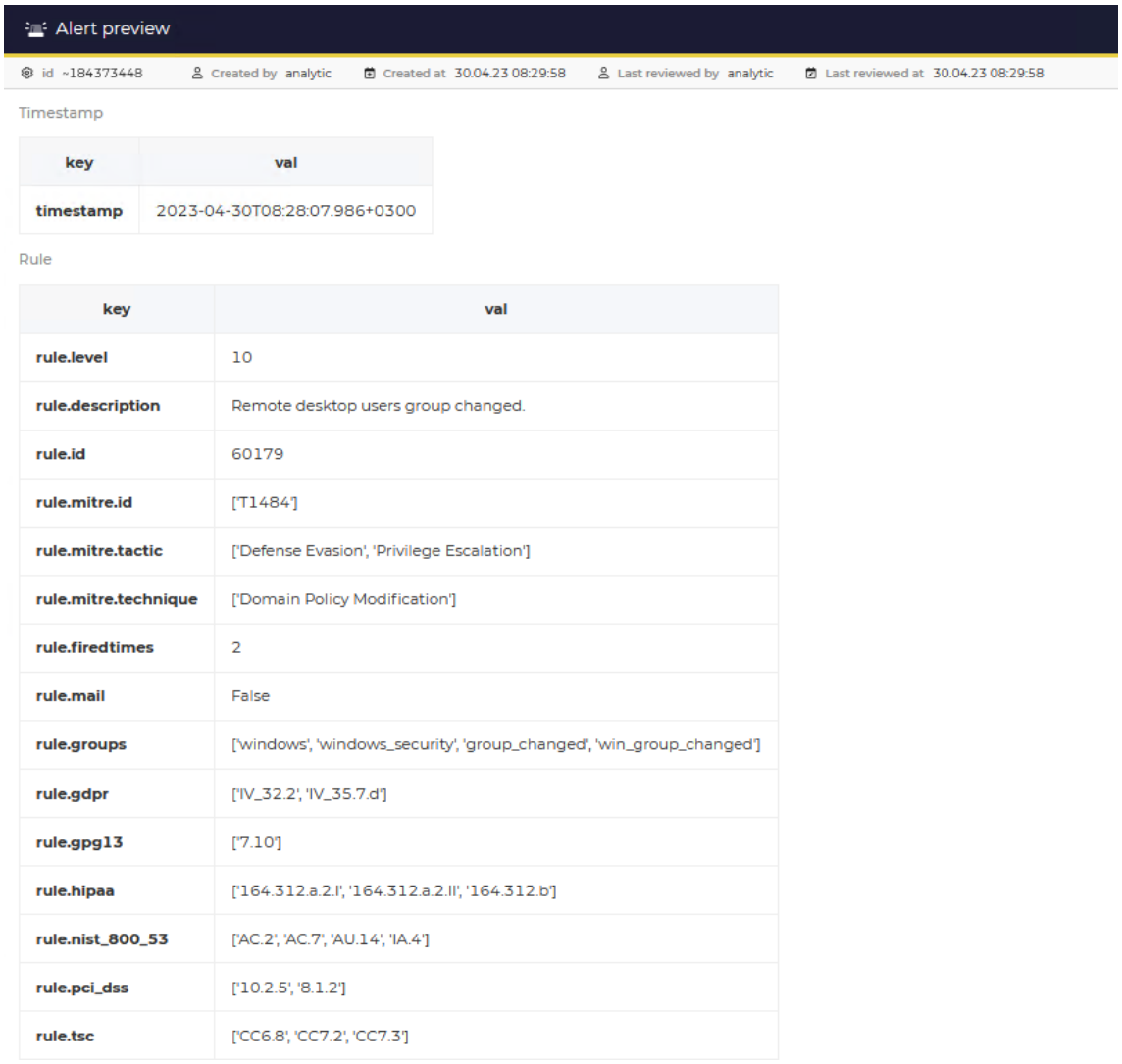
- Käsurea tugi: käsurea tugi on saadaval TheHive'i kommertsversioonis, mis võimaldab kasutajatel hallata intsidente ja ülesandeid konsooli kaudu.

- Integratsioon Jira ja Microsoft Teamsiga: Integratsioon Jira ja Microsoft Teamsiga on saadaval TheHive'i kommertsversioonis, mis võimaldab kasutajatel integreerida TheHive'i oma olemasolevatesse infrastruktuuridesse.

- LDAP / AD tugi: LDAP / AD tugi on saadaval TheHive'i kommertsversioonis, mis võimaldab kasutajatel integreerida TheHive'i oma olemasolevatesse turvainfrastruktuuridesse.

- Reeglite seadistamine automaat-tegumite loomiseks: TheHive'i kommertsversioonis saate seadistada reeglid automaatsete ülesannete loomiseks, võimaldades kasutajatel intsidentide käsitlemise protsessi automatiseerida.

Üldiselt on TheHive võimas tööriist intsidentide haldamiseks ja neile reageerimiseks, kuid selle platvormi rakendamist tuleb hinnata organisatsiooni konkreetsete vajaduste ja nõuete kontekstis.



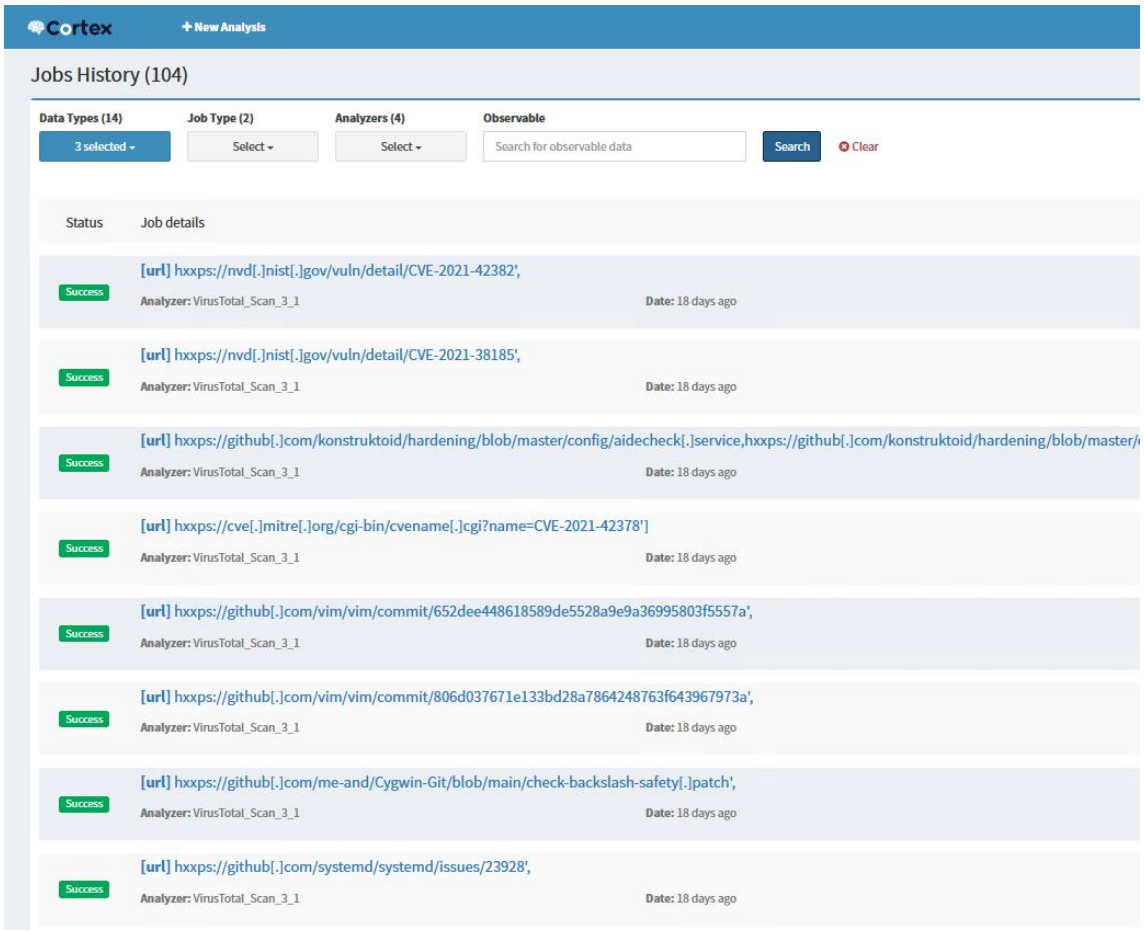
Joonis 11. TheHive alert naide

Platvormiga töötamise tõhususe parandamiseks saab seda integreerida Cortexi ja MISP-ga. See on tööriist, mis peab olema kohandatud SOC meeskonna konkreetsetele vajadustele. Parimate tavade järgimine aitab luua kõige tõhusama ja kasulikuma armatuurlaua. Selleks tasub kindlaks määrata, milliseid mõõdikuid tuleb pidevalt jälgida ja milliseid eesmärke tuleb saavutada. Selleks on TheHive'is saadaval erinevat tüüpi graafikud ja tabelid, näiteks Kuvati ainult vajalik teave. Näiteks saate kuvada ainult avatud juhtumeid, millel on kõrge prioriteet. Loomulikult peate armatuurlauda pidevalt analüüsima ja täiustama. Analüüsides armatuurlaua tõhusust ja tehes muudatusi selle parandamiseks ning kasulikumaks ja informatiivsemaks muutmiseks. Pop-diagrammid, sektordiagrammid, tabelid jne[27].

Joonis 12. TheHive armatuurlaud naide

5.2 Cortex ülevaade

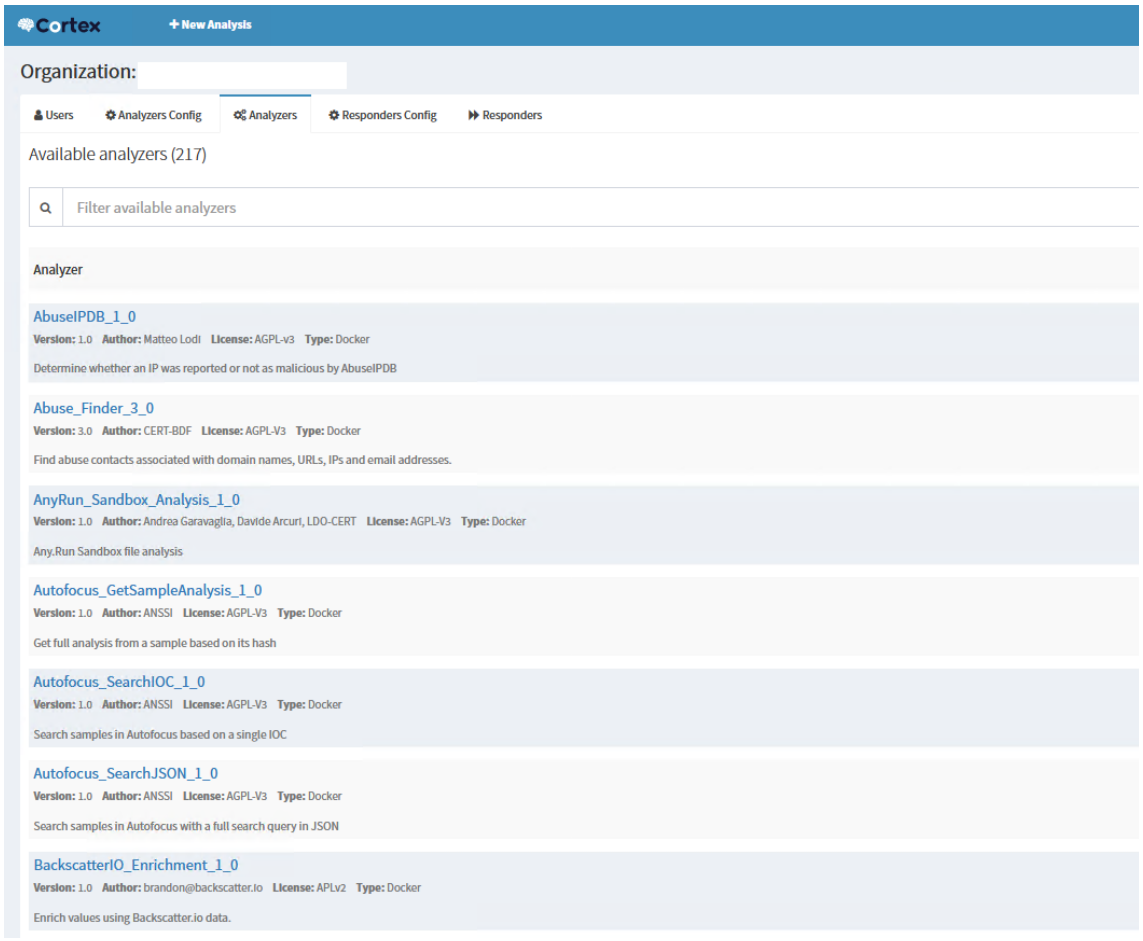
TheHive Cortex on integratsiooniplatvorm infoturbe ülesannete automatiseerimiseks ja korraldamiseks. See platvorm võimaldab teil seadistada ja käivitada automatiseeritud andmeanalüsaatoreid, mis aitavad turvasündmuste ja muude andmete töötlemisel ja klassifitseerimisel.



Joonis 13. Cortex töö ajalugu

TheHive Cortex võimaldab kasutajatel turbeülesannete automatiseerimiseks integreerida mitmesuguseid tööriistu ja teenuseid. See võib olla kasulik erinevatest allikatest pärit andmete töötlemiseks ja analüüsimiseks, näiteks turvalogid, turvaseiresüsteemid ja teised.

TheHive Cortex pakub ulatuslikku analüsaatorite raamatukogu, mida saab kasutada andmetöötluseks. Lisaks võimaldab platvorm kasutajatel luua kohandatud skriptide ja tööriistade põhjal oma analüsaatorid.



Joonis 14. Cortex analüsaatorite kollektsioon

TheHive Cortex integreerub ka TheHive'i intsidentide haldamise platvormiga, võimaldades kasutajatel töödeldud andmete põhjal turvaintsidente tõhusalt hallata ja jälgida.

TheHive Cortexi põhijooned:

- Kohandatavad analüsaatorid: Platvorm pakub ulatuslikku analüsaatorite raamatukogu, mida saab konfigureerida ja kasutada andmete töötlemiseks.

- Kohandatud analüsaatorid: kasutajad saavad luua kohandatud analüsaatoreid, mis põhinevad kohandatud skriptidel ja tööriistadel. Lisas on toodud näide TheHive Cortexi kohandatud skriptist, mis teostab domeeninime valideerimist tööriista Whois abil ja tagastab domeeni kohta teavet.

- TheHive'i integratsioon: Platvorm integreerub TheHive'i intsidentide haldamise platvormiga, võimaldades kasutajatel töödeldud andmete põhjal turvaintsidente tõhusalt hallata ja jälgida.

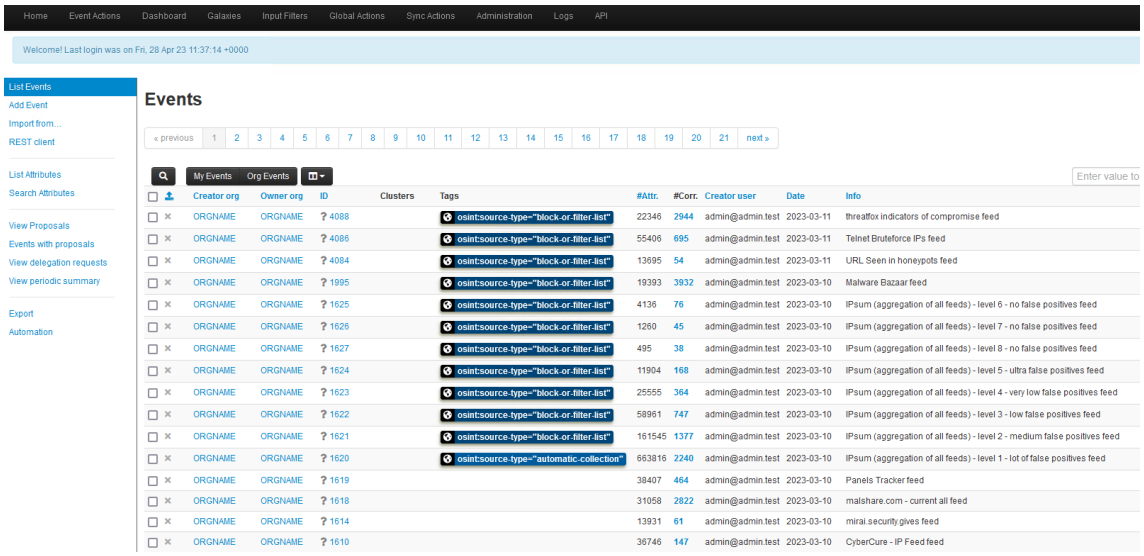
- Integreerimine teiste turvatööriistadega: TheHive Cortex integreerub mitmesuguste turvatööriistadega, võimaldades kasutajatel kasutada mitmesuguseid tööriistu turvaülesannete automatiseerimiseks ja orkestreerimiseks.

TheHive Cortex on võimas ja paindlik platvorm turvaülesannete automatiseerimiseks ja korraldamiseks. Selle kohandatavad analüsaatorid ja võime luua oma analüsaatoreid võimaldavad kasutajatel tõhusalt töödelda ja klassifitseerida erinevatest allikatest pärit turvaandmeid ning integreerimine teiste turvatööriistadega tagab veelgi suurema paindlikkuse ja funktsionaalsuse infoturbe valdkonnas.

5.3 MISP ülevaade

MISP (Malware Information Sharing Platform) on tasuta ja avatud turbeteabe jagamise platvorm, mis on mõeldud organisatsioonide koostööks küberturvalisuse valdkonnas.

MISP pakub võimalust vahetada erinevat tüüpi andmeid, nagu ohud, intsidendid, haavatavused, rünnakud ja muud turbeandmed. Selle platvormi abil saate luua ja jagada erinevaid andmebaase, mis võimaldab teil parandada analüüsi kvaliteeti ja küberohtudele reageerimise kiirust[29].



Joonis 15. MISP

MISP on väga kohandatav, mis võimaldab kasutajal kohandada platvormi vastavalt oma konkreetsetele turvavajadustele. MISP toetab integreerimist teiste turvatööriistadega, mis võimaldab vastuvõetud andmeid ja teateid kiiresti edastada teistele turvasüsteemidele.

Platvormil on kaasaegne kasutajaliides ja seda on lihtne hallata, võimaldades kasutajatel kiiresti leida vajalikku teavet. MISP pakub ka võimalust luua ja jagada automatiseeritud aruandeid, mis lihtsustab oluliselt andmete analüüsimise ja töötlemise protsessi.

MISP on üks populaarsemaid ja laialdasemalt kasutatavaid tööriistu turbeteabe jagamiseks küberturvalisuse kogukonnas. Seda arendab ja toetab aktiivselt arendajate kogukond, mis tagab selle edasise arengu ja paranemise tulevikus.

Üldiselt on MISP tugev ja tõhus turbeteabe jagamise platvorm, mis aitab küberturvalisuse organisatsioonidel ja kogukondadel koostööd teha ja suurendada oma kaitsetaset küberohtude eest.

5.4 TheHive'i, Cortexi, MISP installimine ja konfigureerimine

Installime ja käivitame rakendusi Dockeris[30] - kuna see on tõhus ja mugav viis rakenduste ja nende sõltuvuste haldamiseks, mis tagab suure kaasaskantavuse, paindlikkuse, skaleeritavuse ja haldamise lihtsuse. Docker võimaldab teil isoleerida rakendusi ja nende sõltuvusi hostisüsteemist, mis väldib konflikte erinevate rakenduste vahel ja tagab nende stabiilsema toimimise. See pakub ka turvalisust, kuna rakendused töötavad isoleeritud konteinerites. Dockeri rakendusi saab käivitada mis tahes hostisüsteemis, mis toetab Dockerit, muutes rakenduste juurutamise ja migreerimise lihtsaks. Samuti pakub see võimalust käivitada sama rakendust erinevates arendus-, testimis- ja tootmiskeskkondades. Võimaldab konteinereid kiiresti luua, käivitada ja peatada, muutes rakenduste arendamise ja testimise protsessi paindlikumaks ja tõhusamaks. Samuti pakub see võimalust rakendusi teie vajaduste põhjal kiiresti skaleerida.

TheHive, Cortex ja MISP installimiseks Dockeri konteinerite abil kasutage tööriista Docker Compose ja kasutage konfiguratsiooni. YAML juurutusparameetrite määratlemiseks. Näidiskonfiguratsioon on lisas (Vt. Lisa 5)[31],[32].

5.5 TheHive'i, Cortexi, MISP integreerimine.

TheHive'i, Cortexi ja MISP-i integreerimise kohandamine võib oluliselt parandada ohtude käsitlemise protsessi ja kiirendada intsidentidele reageerimise aega. Selleks toimige järgmiselt[33].

- Konfigureerige MISP integreerimine Cortexiga. Selleks peate MISP-is looma kohandatud API-võtme ja lisama selle Cortexi. Samuti peate Cortexis looma kohandatud API-võtme ja lisama selle MISP-i.

- Seadistage Cortexi integratsioon TheHive'iga. Selleks peate TheHive'is looma kohandatud API-võtme ja lisama selle Cortexi. Samuti peate TheHive'ile juurdepääsemiseks lisama Cortexile mandaadid.

- Konfigureerige MISP integratsioon TheHive'iga. Selleks peate TheHive'is looma kohandatud API-võtme ja lisama selle MISP-i. Samuti peate oma MISP-i lisama mandaadid, et pääseda juurde TheHive'ile.

Kui kõik integratsioonid on seadistatud, saate selle süsteemiga tööd alustada. Näiteks kui ilmub uus juhtum, saab seda kiiresti ja tõhusalt käsitseda, kasutades kõiki MISP-i saadaolevaid andmeid, Cortexi analüsaatoreid ja TheHive'i intsidentide haldamise süsteemi.

Lisaks võimaldab see integratsioon automatiseerida paljusid protsesse, näiteks ohukäsitlust ja intsidentide teatisi, mis lihtsustab administraatorite tööd ja suurendab ohtude käsitlemise tõhusust.

Üldiselt pakub TheHive'i, Cortexi ja MISP-i integreerimine võimsat ohtude käsitlemise ja intsidentide haldamise tööriista, mis võib dramaatiliselt kiirendada intsidentidele reageerimise aega ja parandada ohtude tõhusust.

5.6 Wazuhi integreerimine TheHive'iga.

Wazuhi integratsioon TheHive'iga pakub võimsat turvasündmuste töötlemise tööriista, mis võib parandada turvaanalüütikute tõhusust ja vähendada ohtudele reageerimise aega. Kuid enne selle kasutamise alustamist peate integratsiooni hoolikalt konfigureerima ja kasutajaid koolitama, et sellest maksimumi võtta. Järgides blogis kirjeldatud samm-

sammult dokumentatsiooni "Wazuh ja TheHive'i kasutamine ohukaitseks ja intsidentidele reageerimiseks"[34] ja projekti "croud1011"[35] kirjeldus Integratsioon on konfigureeritud. Integratsiooni seadistamisel peaksite arvestama, et Wazuhi projekt on varem sündmused klassifitseerinud. Reeglid liigitatakse mitmeks tasandiks, alates madalaimast (0) kuni maksimumini (15). Mõned tasemed ei ole praegu kasutusel. Järgmises tabelis kirjeldatakse neid kõiki, mis võivad olla kasulikud iga käivitatud hoiatuse tõsiduse mõistmiseks või kohandatud reeglite loomiseks.

Tulevikus on võimalik iseseisvalt määrata konkreetse ohu tase vastavalt failis /var/ossec/etc/rules/local_rules.xml olevatele reeglitele.

Kui Wazuh-TheHive'i integratsioon on konfigureeritud, loovad Wazuhi tuvastatud ja töödeldud sündmused TheHive'is automaatselt ülesandeid, lihtsustades turvalisuse analüüsimise ja haavatavustega tegelemise protsessi[36]. Klassifitseerimistabeli leiab Wazuhi ametlikult dokumendivaramust veebilehel[36].

5.7 TheHive'i kasutava töötaja igapäevatöö.

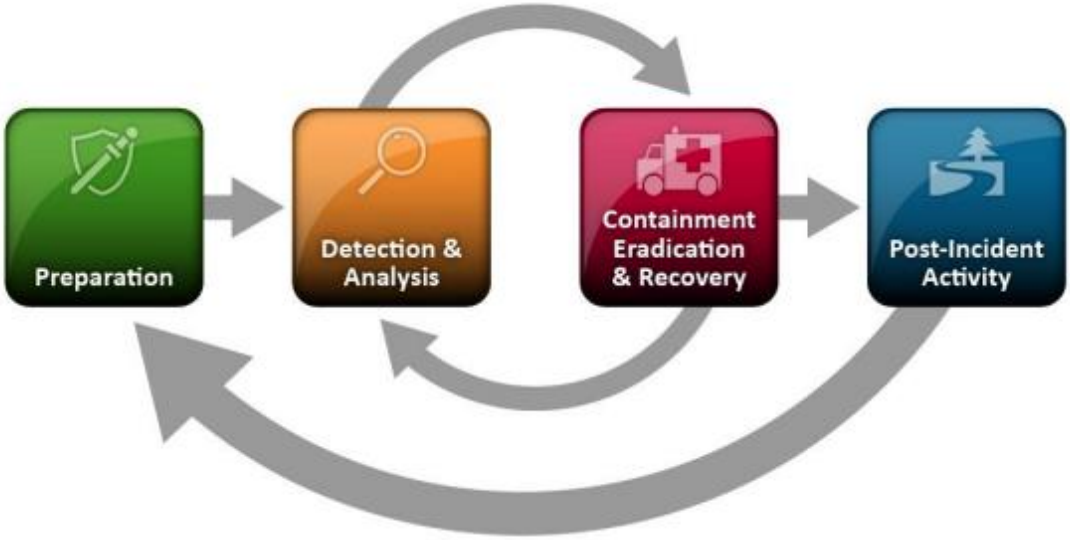
Töötaja igapäevatöö võib sisaldada järgmisi etappe:

- Looge TheHive'is uus juhtum, kui see märkab kahtlast tegevust või tuvastab juhtumi, mida tuleb uurida.
- Juhtumi kirjeldus, märge selle prioriteedi ja klassifikatsiooni kohta ning vastutava ametniku määramine.
- Analüüsige toorandmeid ja hankige juhtumiga seotud lisateavet, vajadusel käivitage Cortexi analüsaatorid või otsige sarnaseid juhtumeid MISP abil.
- Tehke koostööd teiste osakondade (nt infoturbemeeskonna) inimestega, et koguda täiendavaid andmeid ja määratleda intsidentidele reageerimise strateegia.
- Tegevuskava kavandamine ja tegevuskava väljatöötamine probleemi lahendamiseks.
- Täitke tegevuskava ülesanded ja värskendage juhtumiteavet TheHive'is.
- Meetmete rakendamise kontroll ja probleemi kõrvaldamine.

- Kogu probleemi lahendamise protsessi dokumenteerimine ja juhtumi sulgemine TheHive'is.

- Analüüsige tööprotsessi ja leidke viise, kuidas tulevaste juhtumite jaoks paremaks muuta.

Tavaliselt seisneb TheHive kasutava töötaja roll juhtumite töötlemises, ülesannete haldamises ja suhtlemises teiste töötajatega probleemi lahendamiseks. See katavad täielikult elutsükli reageerimist intsidentidele, mis on kirjeldatud NIST SP 800-61[37] standardis, mis kirjeldab infoturbe intsidentide haldamise protsesse (Vt. Joonis 16).



Joonis 16. juhtumi lahendamise elutsükkel[18].

Seega tagab TheHive tõhusa ja struktureeritud meeskonnatöö vastavalt NIST standardile infoturbe intsidentide ja ülesannete haldamiseks järgmiselt:

Identifitseerimine ja kaitse: TheHive võib aidata infoturbe intsidentide ja ülesannete avastamisel ja identifitseerimisel ning sõnastada kaitseplaane potentsiaalsete ohtude vastu.

Avastamine ja vastus: TheHive võib kasutada automatiseeritud andmete kogumise, analüüsi ja juhtimise jaoks infoturbe intsidentide puhul, et aidata reageerida ohtudele kiiresti ja võtta õigeaegselt meetmeid.

Reageerimine ja taastamine: TheHive võimaldab automatiseerida infoturbe intsidentide ja ülesannete reageerimisprotsessi, määratledes õiged sammud jälgimiseks, juhtimiseks ja ohtude kontrollimiseks ning süsteemi taastamiseks pärast intsidenti.

Teabe ja dokumentatsiooni haldus: TheHive võimaldab koguda, säilitada ja analüüsida teavet intsidentide kohta ning esitada dokumentatsiooni infoturbe intsidentide ja ülesannete reageerimisprotsessi juhtimiseks.

Seega võib TheHive'i kasutamine vastavalt NIST standardile aidata organisatsioonidel tõhusalt juhtida infoturbe intsidente ja ülesandeid ning tagada andmete turvalisus ja kaitse.

6 Testimine ja platvormi töövõime analüüs

Selles peatükis kirjeldatakse Wazuh, TheHive, Cortexi ja MISP keskkonna töövõime testimist. Järgmised testid viiakse läbi:

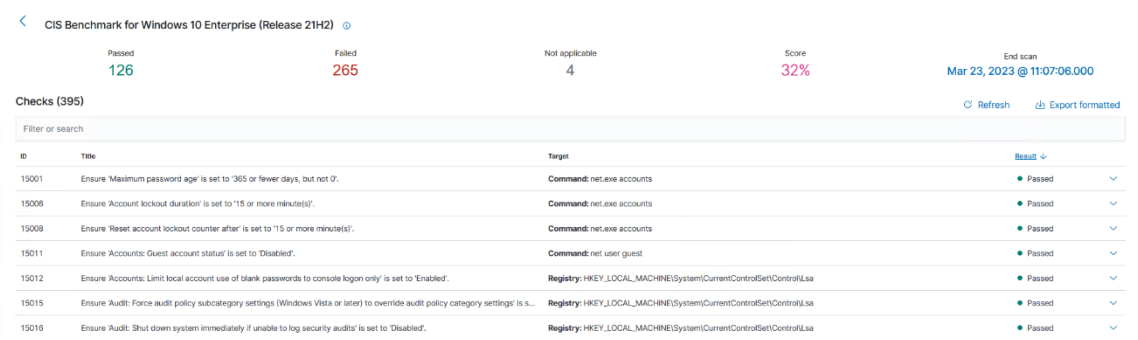
- Uue agendi ühendamine
- Süsteemi konfiguratsiooni kontroll vastavalt CIS Benchmarkile[38]
- Haavatavuste kontroll
- Exploidi käivitamine ja Wazuh TheHive Cortexi MISP automatiseerimise kontrollimine
- Võrdlemine pilveantiviirusega.

Infrastruktuur on välja ehitatud VMware vSphere 6.7 testiklastri peal ESXi 6.0-l. Autor lõi 3 Debian 11.5 virtuaalset masinat, millel on 200 GB kõvaketast, 32 GB RAM-i ja 12 protsessorit. Testimise objektiks on virtuaalne masin, millel on paigaldatud Windows 10 Pro 22H2. Kõik masinad on varustatud viimaste kriitiliste värskendustega.

Virtuaalsed masinad:

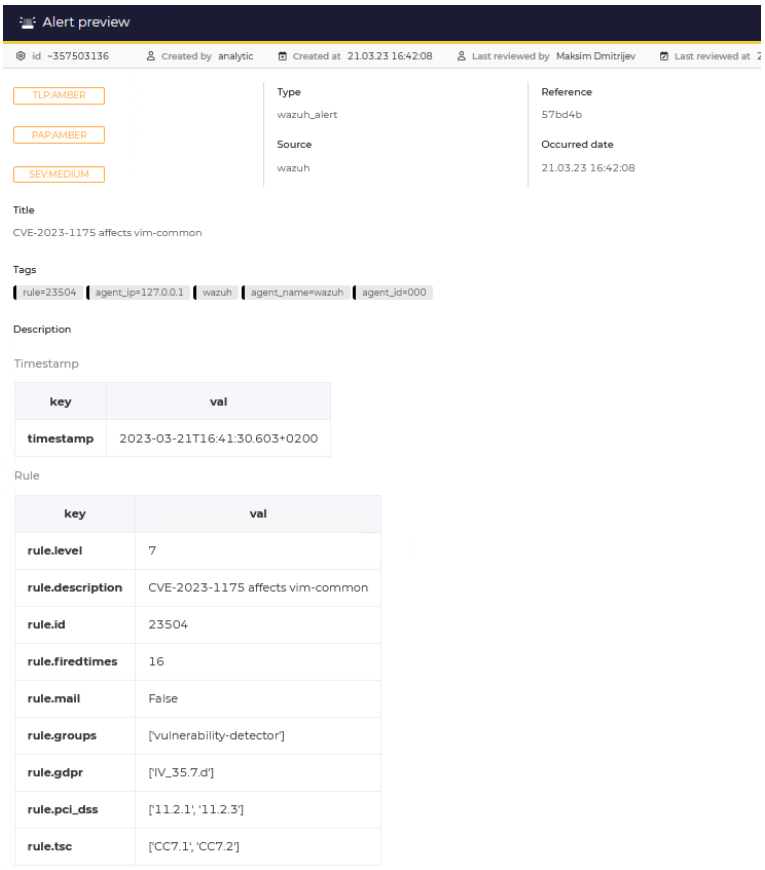
- Wazuh Indexer
- Wazuh Dashboard
- TheHive Cortex Misp Docker
- Virtuaalne masin testide käivitamiseks
- Ärikasutuseks mõeldud pilvepõhine AV+EDR (antiviirus ja Endpoint Detection and Response) lahendus

Pärast uue Wazuh agendi ühendamist lülitati automaatselt sisse CIS benchmark, mis võrdleb praegust konfiguratsiooni turvalisuse ekspertide poolt kontrollitud ja tõhusaks osutunud turvalise konfiguratsiooniga. Testimistulemused laaditi automaatselt TheHive'isse ja koondati eraldi juhtumisse (Case). Rohkem teavet saab vaadata Wazuhi halduris CIS benchmarki jaotises ning alla laadida CSV-faili soovitustega.



Joonis 17. CIS Benchmark aruanne

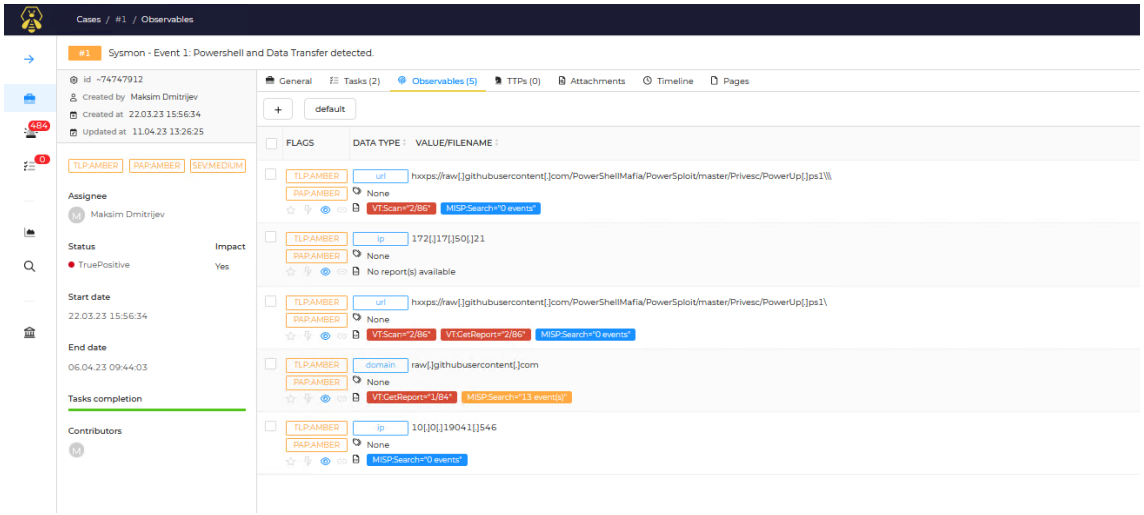
Virtuaalseadmesse testimiseks installiti aegunud tarkvara Mozzila Firefox 73 (dokumendi kirjutamise ajal oli praegune versioon 102). Pärast paigaldamist käivitus turvalisuse skanner, mis tuvastas haavatavused ja saatis tulemused TheHive'i. Haavatavused määrati CVE-de järgi, millele on vastuvõtlik antud versioon Mozilla Firefoxist.



Joonis 18. Sisseehitatud skanneri abil leiti haavatavus

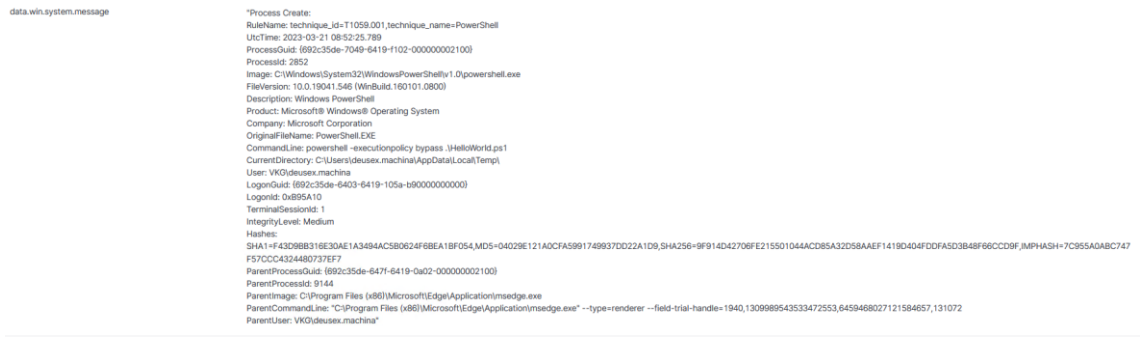
PowerShell exploit võeti GitHubi ressursilt PowerShellMafia[39], et proovida nakatada testimiseks kasutatavat virtuaalset masinat. Pärast Wazuh-agenti käivitamist edastati teave juhisele. Wazuh koostas Mittre maatriksi põhjal ohumudeli, näidates, millised tehnikad selles nakatumises kasutati. Wazuh Dashboardi avamisel saab tutvuda mudeli ja

infograafikutega. Wazuh tuvastas selle potentsiaalse ohu automaatselt ja edastas andmed TheHive'ile. TheHive loodi Case ja käivitati automaatsed analüsaatorid Cortex ja Misp. Cortexi analüsaatorid käivitasid hashsummi võrdlemise VirusTotali andmetega ja koostasid aruande. Misp leidis kõik avatud juhtumid, kus kasutati neid tehnikaid, ja näitas suurt seotud graafi.



Joonis 19. VirusTotal ja MISP aruanne TheHive`s

Wazuh Manageri aruandes märgiti ka, et PowerShell exploit käivitamise tulemusel avastati süsteemi turvalisusele ohtliku käsu käivitamise katse.



Joonis 20. Logianalüüs Wazuhiga

Wazuh Manageri aruandes märgiti ka seda, et PowerShelli eksponeerimise käigus avastati käsu täitmise katse, mis kujutab endast süsteemi turvalisuse ohtu. Logide analüüs näitas, et käsk käivitati MS Edge'i alamprotsessina.

Kui võrrelda informatsiooni kiirust, mis saadakse Wazuh-agentilt ja tasulise viirusetõrje programmist seadmes toimuvatest sündmustest, siis tasuline pilvepõhine lahendus andis mõnikord teavet viivitusega kuni 5 minutit. Tasuline lahendus ei jäänud tasuta

lahendusele alla ohu tuvastamise ja avastamise osas, kuid teatas oma tegevustest ja süsteemis toimuvatest sündmustest viivitusega.

Seega näitas selles olukorras Wazuh agent võimalike ohtude ja süsteemis toimuvate sündmuste suhtes kiiremat reageerimist kui tasuline viirusetõrje. Lisaks pakkus Wazuh agent üksikasjalikumat teavet sündmuste ja ohtude kohta, mis võimaldas neile kiiremini ja tõhusamalt reageerida.

Siiski ei tohiks unustada, et Wazuh agenti efektiivsus sõltub suuresti süsteemi seadetest ja konfiguratsioonist, kuhu see on installitud. Seetõttu on maksimaalse efektiivsuse ja võimalike ohtude eest kaitsmise tagamiseks vaja süsteemi ja turvakomponente regulaarselt konfigureerida ja uuendada ning Wazuh agenti andmebaase ja seadeid regulaarselt ajakohastada.

Sellest lähtuvalt võib öelda, et Wazuh agenti kasutamine võib olla heaks lisandiks viirusetõrjele.

7 Kokkuvõte

Antud lõputöös uuriti tööriistu Wazuh, TheHive, Cortex ja MISP, mis võivad olla kasutatud OpenSource SIEM süsteemina organisatsioonide infosüsteemides esinevate intsidentide avastamiseks ja analüüsimiseks.

Üks peamisi eeliseid Wazuh, TheHive, Cortex ja MISP kasutamisel on võime koguda ja analüüsida suuri andmemahte erinevatest allikatest, mis võimaldab kiiresti ja täpselt avastada ohte ja rünnakuid infosüsteemis. Lisaks on neil tööriistadel avatud lähtekood, mis võimaldab süsteemi vastavalt organisatsiooni vajadustele konfigureerida ja koodi muudatusi teha, kui see on vajalik.

Vastused esitatud küsimustele on antud:

- OpenSource SIEM-lahenduste edukaks rakendamiseks valiti vastavad tööriistad ja nende tööd seadistati. Samuti tagati süsteemi turvalisus ja konfigureeriti vajalikud komponendid.

- Ohtude avastamiseks SIEM-i abil seadistati süsteem, mis kogub ja analüüsib andmeid erinevatest allikatest, sealhulgas sündmustest logisüsteemidest ja võrguühenduste ja -liikluse jälgimisest.

- Süsteemsete sündmuste analüüsi automatiseerimine saavutati erinevate tööriistade, nagu TheHive, MISP ja Cortex, integratsiooni abil, mis võimaldas luua ja seadistada automaatseid ohu- ja rünnakuavastamise reegleid.

Siiski on OpenSource SIEM süsteemide kasutamisel ka mõningaid puudusi. Näiteks erinevalt kaubanduslikest lahendustest, nagu Splunk[40] või QRadar[41], ei pruugi OpenSource süsteemidel olla ametlikku tootjatuge ja kasutajad võivad probleemide korral jääda abita. Lisaks võib avatud lähtekoodi kasutamine viia süsteemi haavatavusteni, kui koodi ja süsteemi seadeid ei kaitsta piisavalt.

Siiski näitavad käesoleva lõputöö tulemused, et Wazuh, TheHive, Cortex ja MISP kasutamine võib olla paljudele organisatsioonidele tõhus lahendus, eriti neile, kes ei saa kasutada kaubanduslikke lahendusi. See süsteem võimaldab oluliselt parandada infosüsteemi turvalisust ja avastada intsidente, mis on oluline tegur andmete kaitsmiseks ja organisatsiooni maine säilitamiseks.

Kasutatud kirjandus

[1] Check Point Research: Third quarter of 2022 reveals increase in cyberattacks and unexpected developments in global trends. https://blog.checkpoint.com/2022/10/26/third-quarter-of-2022-reveals-increase-in-cyberattacks/

[2] Don’t let SIEM myths impede modernizing your SOC. IBM Security QRadar SIEM. https://www.ibm.com/topics/siem

[3] Wazuh official webpage. https://wazuh.com/platform/

[4] Graylog Docs https://go2docs.graylog.org/

[5] Center for Internet Security. https://www.cisecurity.org/

[6] NIST Security Framework. https://www.nist.gov/cyberframework

[7] Trends of SOC & SIEM Technology for Cybersecurity. Smart Media Journal. Volume 6 Issue 4 / Pages.41-49 / 2017 / 2287-1322(pISSN) / 2288-9671(eISSN) Cha, ByungRae; Choi, MyeongSoo ; Kang, EunJu ; Park, Sun ; Kim, JongWon https://koreascience.kr/article/JAKO201708260282339.page

[8] A Real-Time and Statistical Visualization Methodology of Cyber Threats Based on IP Addresses. Journal of the Korea Institute of Information Security & Cryptology Volume 30 Issue 3 / Pages.465-479 / 2020 / 1598-3986(pISSN) / 2288-2715(eISSN) Moon, Hyeongwoo (Korea Institute of Science and Technology Information(KISTI)) ; Kwon, Taewoong (Korea Institute of Science and Technology Information(KISTI)) ; Lee, Jun (Korea Institute of Science and Technology Information(KISTI)) ; Ryou, Jaecheol (Chungnam National University) ; Song, Jungsuk (Korea Institute of Science and Technology Information(KISTI)) https://koreascience.kr/article/JAKO202019163740262.page

[9] Security Operation Implementation through Big Data Analysis by Using Open Source ELK Stack. Jeong-Hoon Hyun, Hyoung-Joong Kim. Journal of Digital Contents Society Vol. 19, No. 1, pp. 181-191, Jan. 2018 https://koreascience.kr/article/JAKO201808962641919.pdf

[10] Y. Kim and T. Shon, “Cyber-Threat Detection of ICS Using Sysmon and ELK,” Journal of the Korea Institute of Information Security & Cryptology, vol. 29, no. 2, pp. 331–346, Apr. 2019. https://koreascience.kr/article/JAKO201914860237981.page

[11] D.-H. Kim, D.-K. Shin, and D.-I. Shin, “Security Log collection and analysis System Design Using Big Data System,” Proceedings of the Korea Information Processing Society Conference, pp. 321–323, Apr. 2016. https://koreascience.kr/article/CFKO201629368414382.page

[12] S.-Y. Lee and H.-J. Yoon, “A Study on the 4th Industrial Revolution and E-Government Security Strategy -In Terms of the Cyber Security Technology of Intelligent Government-,” The Journal of the Korea institute of electronic communication sciences, vol. 14, no. 2, pp. 369–376, Apr. 2019. https://koreascience.kr/article/JAKO201914260902437.page

[13] Bauzá Sainz de Baranda, Fernando. How to mess with log collectors and analyse their response in Microsoft networks with an example of the ELK stack. https://digikogu.taltech.ee/et/Item/86ec0590-a77a-4210-92d7-8fb84e64c353

[14] Tammepõld, Maarja-Liisa. Securing the centralized logging system by the example of Elasticsearch. 01.06.2020 https://digikogu.taltech.ee/et/Item/b4cbaadb-adcf-4a26-a817-113d6eed9f0e

[15] Guide to Computer Network Security (Texts in Computer Science). Joseph Migga Kizza. Jun 4, 2020

[16] Dennis Matotek, James Turnbull, Peter Lieverdink. Logging and Monitoring. 15 March 2017 https://doi.org/10.1007/978-1-4842-2008-5_18

[17] Richard Bejtlich. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. 2013

[18] Nisioti, Antonia & Mylonas, Alexios & Yoo, Paul & Katos, Vasilios. (2018). From Intrusion Detection to Attacker Attribution: A Comprehensive Survey of Unsupervised Methods. IEEE Communications Surveys & Tutorials. PP. 1-1. 10.1109/COMST.2018.2854724.

[19] SolarWinds. Loggly Blog https://www.loggly.com/blog/

[20] Janani. Atatus blog Content Writer. Log Analysis NOV 15, 2021 https://www.atatus.com/glossary/log-analysis/

[21] Wazuh documentation. Getting started with Wazuh. https://documentation.wazuh.com/current/getting-started/index.html

[22] Wazuh documentation. Architecture. https://documentation.wazuh.com/current/getting-started/architecture.html

[23] Wazuh documentation. Wazuh indexer. https://documentation.wazuh.com/current/getting-started/architecture.html

[24] Sysinternals Security Utilities. Microsoft Corp. https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

[25] Agent groups and centralized configuration. Braulio Vargas. https://wazuh.com/blog/agent-groups-and-centralized-configuration/

[26] Building A Perfect Sysmon Configuration File. CQURE ACADEMY. https://cqureacademy.com/blog/hacks/sysmon-configuration-file

[27] TheHive Blog. https://blog.thehive-project.org/

[28] Cortex overview https://github.com/TheHive-Project/Cortex

[29] MISP Documentation https://www.misp-project.org/documentation/

[30] Docker Compose overview https://docs.docker.com/compose/

[31] CoolAcid's MISP Docker images https://github.com/coolacid/docker-misp

[32] Guide how to use the docker image of TheHive. https://docs.strangebee.com/thehive/setup/installation/docker/

[33] TheHive Project Documentation https://docs.thehive-project.org/thehive/installation-and-configuration/

[34] Using Wazuh and TheHive for threat protection and incident response. https://wazuh.com/blog/using-wazuh-and-thehive-for-threat-protection-and-incident-response/

[35] Wazuh and TheHive integration https://github.com/crow1011/wazuh2thehive

[36] Rules classification https://documentation.wazuh.com/3.12/user-manual/ruleset/rules-classification.html

[37] NIST SP800-61, 08/06/12:SP 800-61 Rev.2 (Final) https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

[38] The Ultimate Manual for CIS Benchmarks and Compliance https://nira.com/cis-benchmarks-and-compliance/

[39] Collection of Microsoft PowerShell modules for penetration testers. https://github.com/PowerShellMafia/PowerSploit

[40] Splunk is named a Leader across three reports that evaluate security vendors in the SIEM space. https://www.splunk.com/en_us/products/cyber-security.html

[41] IBM Security QRadar: SIEM product overview. Karen Scarfone, Scarfone Cybersecurity https://www.techtarget.com/searchsecurity/feature/IBM-Security-QRadar-SIEM-product-overview

Lisa 1 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks[1]

Mina, Maksim Dmitrijev

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose "Turvateabe ja- sündmuste haldus avatud lahtikoodiga tööristadele baasil", mille juhendaja on Oleg Švets
   1.1. reprodutseerimiseks lõputöö säilitamise ja elektroonse avaldamise eesmärgil, sh Tallinna Tehnikaülikooli raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
   1.2. üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.
2. Olen teadlik, et käesoleva lihtlitsentsi punktis 1 nimetatud õigused jäävad alles ka autorile.
3. Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest ning muudest õigusaktidest tulenevaid õigusi.

30.04.2023

1 Lihtlitsents ei kehti juurdepääsupiirangu kehtivuse ajal vastavalt üliõpilase taotlusele lõputööle juurdepääsupiirangu kehtestamiseks, mis on allkirjastatud teaduskonna dekaani poolt, välja arvatud ülikooli õigus lõputööd reprodutseerida üksnes säilitamise eesmärgil. Kui lõputöö on loonud kaks või enam isikut oma ühise loomingulise tegevusega ning lõputöö kaas- või ühisautor(id) ei ole andnud lõputööd kaitsvale üliõpilasele kindlaksmääratud tähtajaks nõusolekut lõputöö reprodutseerimiseks ja avalikustamiseks vastavalt lihtlitsentsi punktidele 1.1. ja 1.2, siis lihtlitsents nimetatud tähtaja jooksul ei kehti.

Lisa 2 – Wazuh haavatussüsteemi aktiveerimine

Seda tehakse konfiguratsioonifailis /var/ossec/etc/ossec.conf. Nagu näete, on kõik konfiguratsioonifailid saadaval ja aktiveerida saab ainult neid süsteeme, kuhu agendid installitakse[25].

```
<vulnerability-detector>
    <enabled>yes</enabled>
    <interval>5m</interval>
    <min_full_scan_interval>6h</min_full_scan_interval>
    <run_on_start>yes</run_on_start>
    <!-- Ubuntu OS vulnerabilities -->
    <provider name="canonical">
      <enabled>yes</enabled>
      <os>trusty</os>
      <os>xenial</os>
      <os>bionic</os>
      <os>focal</os>
      <os>jammy</os>
      <update_interval>1h</update_interval>
    </provider>
    <!-- Debian OS vulnerabilities -->
    <provider name="debian">
      <enabled>yes</enabled>
      <os>stretch</os>
      <os>buster</os>
      <os>bullseye</os>
      <update_interval>1h</update_interval>
    </provider>
    <!-- RedHat OS vulnerabilities -->
    <provider name="redhat">
      <enabled>yes</enabled>
      <os>5</os>
      <os>6</os>
      <os>7</os>
      <os>8</os>
      <os>9</os>
      <update_interval>1h</update_interval>
    </provider>
    <!-- Amazon Linux OS vulnerabilities -->
    <provider name="alas">
      <enabled>yes</enabled>
      <os>amazon-linux</os>
      <os>amazon-linux-2</os>
      <update_interval>1h</update_interval>
    </provider>
    <!-- Arch OS vulnerabilities -->
    <provider name="arch">
      <enabled>yes</enabled>
      <update_interval>1h</update_interval>
    </provider>
```

```
    <!-- Windows OS vulnerabilities -->
    <provider name="msu">
      <enabled>yes</enabled>
      <update_interval>1h</update_interval>
    </provider>
    <!-- Aggregate vulnerabilities -->
    <provider name="nvd">
      <enabled>yes</enabled>
      <update_from_year>2010</update_from_year>
      <update_interval>1h</update_interval>
    </provider>
  </vulnerability-detector>
```

Lisa 3 – Wazuhi agentide tsentraliseeritud konfiguratsioonihaldus lõppseadmetes

```
Autor jagas kahte rühma Linux Group ja Windows Group[25].
Linux Group:
<agent_config>
       <client_buffer>
              <!-- Agent buffer options -->
              <disabled>no</disabled>
              <queue_size>5000</queue_size>
              <events_per_second>500</events_per_second>
       </client_buffer>
       <!-- Policy monitoring -->
       <rootcheck>
              <disabled>no</disabled>
              <!-- Frequency that rootcheck is executed - every 12 hours -->
              <frequency>43200</frequency>
<rootkit_files>/var/ossec/etc/shared/rootkit_files.txt</rootkit_files>
<rootkit_trojans>/var/ossec/etc/shared/rootkit_trojans.txt</rootkit_trojans>
<system_audit>/var/ossec/etc/shared/system_audit_rcl.txt</system_audit>
<system_audit>/var/ossec/etc/shared/system_audit_ssh.txt</system_audit>
<system_audit>/var/ossec/etc/shared/cis_debian_linux_rcl.txt</system_audit>
              <skip_nfs>yes</skip_nfs>
       </rootcheck>
       <wodle name="open-scap">
              <disabled>yes</disabled>
              <timeout>1800</timeout>
              <interval>1d</interval>
              <scan-on-start>yes</scan-on-start>
              <content type="xccdf" path="ssg-debian-8-ds.xml">
       <profile>xccdf_org.ssgproject.content_profile_common</profile>
              </content>
```

```
            <content type="oval" path="cve-debian-oval.xml"/>
      </wodle>
      <!-- File integrity monitoring -->
      <syscheck>
            <disabled>no</disabled>
<!-- Frequency that syscheck is executed default every 12 hours -->
            <frequency>43200</frequency>
            <scan_on_start>yes</scan_on_start>
<!-- Directories to check  (perform all possible verifications) -->
            <directories>/etc,/usr/bin,/usr/sbin</directories>
            <directories>/bin,/sbin,/boot</directories>
            <!-- Files/directories to ignore -->
            <ignore>/etc/mtab</ignore>
            <ignore>/etc/hosts.deny</ignore>
            <ignore>/etc/mail/statistics</ignore>
            <ignore>/etc/random-seed</ignore>
            <ignore>/etc/random.seed</ignore>
            <ignore>/etc/adjtime</ignore>
            <ignore>/etc/httpd/logs</ignore>
            <ignore>/etc/utmpx</ignore>
            <ignore>/etc/wtmpx</ignore>
            <ignore>/etc/cups/certs</ignore>
            <ignore>/etc/dumpdates</ignore>
            <ignore>/etc/svc/volatile</ignore>
            <ignore>/sys/kernel/security</ignore>
            <ignore>/sys/kernel/debug</ignore>
            <!-- File types to ignore -->
            <ignore type="sregex">.log$|.swp$</ignore>
            <!-- Check the file, but never compute the diff -->
            <nodiff>/etc/ssl/private.key</nodiff>
            <skip_nfs>yes</skip_nfs>
            <skip_dev>yes</skip_dev>
            <skip_proc>yes</skip_proc>
            <skip_sys>yes</skip_sys>
            <!-- Nice value for Syscheck process -->
            <process_priority>10</process_priority>
            <!-- Maximum output throughput -->
            <max_eps>100</max_eps>
            <!-- Database synchronization settings -->
            <synchronization>
                  <enabled>yes</enabled>
                  <interval>5m</interval>
                  <response_timeout>30</response_timeout>
                  <queue_size>16384</queue_size>
                  <max_eps>10</max_eps>
            </synchronization>
      </syscheck>
      <!-- Log analysis -->
      <localfile>
            <log_format>syslog</log_format>
            <location>/var/ossec/logs/active-responses.log</location>
```

```
	</localfile>
	<localfile>
		<log_format>syslog</log_format>
		<location>/var/log/messages</location>
	</localfile>
	<localfile>
		<log_format>syslog</log_format>
		<location>/var/log/auth.log</location>
	</localfile>
	<localfile>
		<log_format>syslog</log_format>
		<location>/var/log/syslog</location>
	</localfile>
	<localfile>
		<log_format>command</log_format>
		<command>df -P</command>
		<frequency>360</frequency>
	</localfile>
	<localfile>
		<log_format>full_command</log_format>
		<command>netstat -tan |grep LISTEN |grep -v 127.0.0.1 |
sort</command>
		<frequency>360</frequency>
	</localfile>
	<localfile>
		<log_format>full_command</log_format>
		<command>last -n 5</command>
		<frequency>360</frequency>
	</localfile>
	<wodle name="osquery">
		<disabled>yes</disabled>
		<run_daemon>yes</run_daemon>
		<log_path>/var/log/osquery/osqueryd.results.log</log_path>
		<config_path>/etc/osquery/osquery.conf</config_path>
		<add_labels>yes</add_labels>
	</wodle>
	<wodle name="syscollector">
		<disabled>no</disabled>
		<interval>24h</interval>
		<scan_on_start>yes</scan_on_start>
		<packages>yes</packages>
		<os>yes</os>
		<hotfixes>yes</hotfixes>
		<ports all="no">yes</ports>
		<processes>yes</processes>
	</wodle>
</agent_config>

Windows Group:
<agent_config>
	<client_buffer>
```

```
            <!-- Agent buffer options -->
            <disabled>no</disabled>
            <queue_size>5000</queue_size>
            <events_per_second>500</events_per_second>
      </client_buffer>
      <!-- Policy monitoring -->
      <rootcheck>
            <disabled>no</disabled>
            <windows_apps>./shared/win_applications_rcl.txt</windows_apps>
            <windows_malware>./shared/win_malware_rcl.txt</windows_malware>
      </rootcheck>
      <sca>
            <enabled>yes</enabled>
            <scan_on_start>yes</scan_on_start>
            <interval>12h</interval>
            <skip_nfs>yes</skip_nfs>
      </sca>
<!-- File integrity monitoring -->
<syscheck>
      <disabled>no</disabled>
<!-- Frequency that syscheck is executed default every 12 hours -->
<frequency>43200</frequency>
            <!-- Default files to be monitored. -->
<directories recursion_level="0"
restrict="regedit.exe$|system.ini$|win.ini$">%WINDIR%</directories>
<directories recursion_level="0"
restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|l
sass.exe$|net.exe$|net1.exe$|netsh.exe$|reg.exe$|regedt32.exe|regsvr32.exe|ru
nas.exe|sc.exe|schtasks.exe|sethc.exe|subst.exe$">%WINDIR%\SysNative</directo
ries>
<directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>
<directories recursion_level="0"
restrict="WMIC.exe$">%WINDIR%\SysNative\wbem</directories>
<directories recursion_level="0"
restrict="powershell.exe$">%WINDIR%\SysNative\WindowsPowerShell\v1.0</directo
ries>
<directories recursion_level="0"
restrict="winrm.vbs$">%WINDIR%\SysNative</directories>
<!-- 32-bit programs. -->
<directories recursion_level="0"
restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|l
sass.exe$|net.exe$|net1.exe$|netsh.exe$|reg.exe$|regedit.exe$|regedt32.exe$|r
egsvr32.exe$|runas.exe$|sc.exe$|schtasks.exe$|sethc.exe$|subst.exe$">%WINDIR%
\System32</directories>
<directories recursion_level="0">%WINDIR%\System32\drivers\etc</directories>
<directories recursion_level="0"
restrict="WMIC.exe$">%WINDIR%\System32\wbem</directories>
<directories recursion_level="0"
restrict="powershell.exe$">%WINDIR%\System32\WindowsPowerShell\v1.0</director
ies>
<directories recursion_level="0"
restrict="winrm.vbs$">%WINDIR%\System32</directories>
```

```
<directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start
Menu\Programs\Startup</directories>
<ignore>%PROGRAMDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\desktop.ini</ignore>
<ignore type="sregex">.log$|.htm$|.jpg$|.png$|.chm$|.pnf$|.evtx$</ignore>
<!-- Windows registry entries to monitor. -->
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\batfile</windows_regist
ry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\cmdfile</windows_regist
ry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\comfile</windows_regist
ry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\exefile</windows_regist
ry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\piffile</windows_regist
ry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\AllFilesystemObjects</w
indows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\Directory</windows_regi
stry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\Folder</windows_registr
y>
<windows_registry
arch="both">HKEY_LOCAL_MACHINE\Software\Classes\Protocols</windows_registry>
<windows_registry
arch="both">HKEY_LOCAL_MACHINE\Software\Policies</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Security</windows_registry>
<windows_registry arch="both">HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services</windo
ws_registry>
<windows_registry>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session
Manager\KnownDLLs</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecureP
ipeServers\winreg</windows_registry>
<windows_registry
arch="both">HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run<
/windows_registry>
<windows_registry
arch="both">HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunO
nce</windows_registry>
      <windows_registry>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Curren
tVersion\RunOnceEx</windows_registry>
<windows_registry
arch="both">HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\URL<
/windows_registry>
<windows_registry
arch="both">HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Poli
cies</windows_registry>
<windows_registry arch="both">HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Windows</windows_registry>
<windows_registry arch="both">HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon</windows_registry>
<windows_registry arch="both">HKEY_LOCAL_MACHINE\Software\Microsoft\Active
Setup\Installed Components</windows_registry>
<!-- Windows registry entries to ignore. -->
```

```
      <registry_ignore>HKEY_LOCAL_MACHINE\Security\Policy\Secrets</registry_
ignore>
      <registry_ignore>HKEY_LOCAL_MACHINE\Security\SAM\Domains\Account\Users
</registry_ignore>
            <registry_ignore type="sregex">\Enum$</registry_ignore>
      <registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\
MpsSvc\Parameters\AppCs</registry_ignore>
      <registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\
MpsSvc\Parameters\PortKeywords\DHCP</registry_ignore>
      <registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\
MpsSvc\Parameters\PortKeywords\IPTLSIn</registry_ignore>
      <registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\
MpsSvc\Parameters\PortKeywords\IPTLSOut</registry_ignore>
      <registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\
MpsSvc\Parameters\PortKeywords\RPC-EPMap</registry_ignore>
      <registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\
MpsSvc\Parameters\PortKeywords\Teredo</registry_ignore>
      <registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\
PolicyAgent\Parameters\Cache</registry_ignore>
      <registry_ignore>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current
Version\RunOnceEx</registry_ignore>
      <registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\
ADOVMPPackage\Final</registry_ignore>
            <!-- Frequency for ACL checking (seconds) -->
            <windows_audit_interval>60</windows_audit_interval>
            <!-- Nice value for Syscheck module -->
            <process_priority>10</process_priority>
            <!-- Maximum output throughput -->
            <max_eps>100</max_eps>
            <!-- Database synchronization settings -->
            <synchronization>
                  <enabled>yes</enabled>
                  <interval>5m</interval>
                  <max_interval>1h</max_interval>
                  <max_eps>10</max_eps>
            </synchronization>
      </syscheck>
      <!-- System inventory -->
      <wodle name="syscollector">
            <disabled>no</disabled>
            <interval>1h</interval>
            <scan_on_start>yes</scan_on_start>
            <hardware>yes</hardware>
            <os>yes</os>
            <network>yes</network>
            <packages>yes</packages>
            <ports all="no">yes</ports>
            <processes>yes</processes>
            <!-- Database synchronization settings -->
            <synchronization>
                  <max_eps>10</max_eps>
            </synchronization>
      </wodle>
```

```
	<!-- CIS policies evaluation -->
	<wodle name="cis-cat">
		<disabled>yes</disabled>
		<timeout>1800</timeout>
		<interval>1d</interval>
		<scan-on-start>yes</scan-on-start>
		<java_path>\\server\jre\bin\java.exe</java_path>
		<ciscat_path>C:\cis-cat</ciscat_path>
	</wodle>
	<!-- Osquery integration -->
	<wodle name="osquery">
		<disabled>yes</disabled>
		<run_daemon>yes</run_daemon>
		<bin_path>C:\Program Files\osquery\osqueryd</bin_path>
		<log_path>C:\Program
Files\osquery\log\osqueryd.results.log</log_path>
		<config_path>C:\Program Files\osquery\osquery.conf</config_path>
		<add_labels>yes</add_labels>
	</wodle>
	<!-- Active response -->
	<active-response>
		<disabled>no</disabled>
		<ca_store>wpk_root.pem</ca_store>
		<ca_verification>yes</ca_verification>
	</active-response>
	<!-- Log analysis -->
	<localfile>
		<location>Microsoft-Windows-Sysmon/Operational</location>
		<log_format>eventchannel</log_format>
	</localfile>
	<localfile>
		<location>Windows PowerShell</location>
		<log_format>eventchannel</log_format>
	</localfile>
	<localfile>
		<location>Microsoft-Windows-CodeIntegrity/Operational</location>
		<log_format>eventchannel</log_format>
	</localfile>
	<localfile>
		<location>Microsoft-Windows-TaskScheduler/Operational</location>
		<log_format>eventchannel</log_format>
	</localfile>
	<localfile>
		<location>Microsoft-Windows-PowerShell/Operational</location>
		<log_format>eventchannel</log_format>
	</localfile>
	<localfile>
		<location>Microsoft-Windows-Windows Firewall With Advanced
Security/Firewall</location>
		<log_format>eventchannel</log_format>
	</localfile>
```

```
	<localfile>
		<location>Microsoft-Windows-Windows
Defender/Operational</location>
		<log_format>eventchannel</log_format>
	</localfile>
</agent_config>
```

Lisa 4 – Sysmon konfigorutsioni faili seadastamine

```
Massinstallimiseks sama domeeni klientidele saate luua GPO (grupipoliitika)
PowerShelli skripti ühe käivitamisega.
$sysinternals_repo = 'download.sysinternals.com'
$sysinternals_downloadlink =
'https://download.sysinternals.com/files/SysinternalsSuite.zip'
$sysinternals_folder = 'C:\Program Files\sysinternals'
$sysinternals_zip = 'SysinternalsSuite.zip'
$sysmonconfig_file = 'sysmonconfig-export.xml'
 [Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::Tls12
 if (Test-Path -Path $sysinternals_folder) {
    write-host ('Sysinternals folder already exists')
} else {
  $OutPath = $env:TMP
  $output = $sysinternals_zip
  New-Item -Path "C:\Program Files" -Name "sysinternals" -ItemType
"directory"
  $X = 0
  do {
    Write-Output "Waiting for network"
    Start-Sleep -s 5
    $X += 1
  } until(($connectreult = Test-NetConnection $sysinternals_repo -Port 443 |
? { $_.TcpTestSucceeded }) -or $X -eq 3)
   if ($connectreult.TcpTestSucceeded -eq $true){
    Try
    {
    write-host ('Downloading and copying Sysinternals Tools to C:\Program
Files\sysinternals...')
    Invoke-WebRequest -Uri $sysinternals_downloadlink -OutFile
$OutPath\$output
    Expand-Archive -path $OutPath\$output -destinationpath
$sysinternals_folder
    Start-Sleep -s 10
    Invoke-WebRequest -Uri $sysmonconfig_downloadlink -OutFile
$OutPath\$sysmonconfig_file
    $serviceName = 'Sysmon64'
    If (Get-Service $serviceName -ErrorAction SilentlyContinue) {
    write-host ('Sysmon Is Already Installed')
```

```
    } else {
    Invoke-Command {reg.exe ADD HKCU\Software\Sysinternals /v EulaAccepted /t
REG_DWORD /d 1 /f}
    Invoke-Command {reg.exe ADD HKU\.DEFAULT\Software\Sysinternals /v
EulaAccepted /t REG_DWORD /d 1 /f}
    Start-Process -FilePath $sysinternals_folder\Sysmon64.exe -Argumentlist
@("-i", "$OutPath\$sysmonconfig_file")
    }
    }
    Catch
    {
        $ErrorMessage = $_.Exception.Message
        $FailedItem = $_.Exception.ItemName
        Write-Error -Message "$ErrorMessage $FailedItem"
        exit 1
    }
    Finally
    {
        Remove-Item -Path $OutPath\$output
    }
  } else {
      Write-Output "Unable to connect to Sysinternals Repo"
  }
}
```

Sysmon kirjutab nüüd sündmusi rakenduste ja teenuste logidesse Microsoft-Windows-Sysmon/Operational.

Lisa 5 – Docker konfigorutsioni faili seadastamine

```
Konfiguratsioonifail on koostatud TheHive'i, Cortexi ja MISP ametlike
dokumentatsioonide põhjal[28],[29],[30],[31],[32].
version: "3.7"
services:
  thehive:
    image: strangebee/thehive:latest
    restart: unless-stopped
    depends_on:
      - cassandra
      - elasticsearch
      - minio
      - cortex.local
    ports:
      - "0.0.0.0:9000:9000"
    environment:
      - JVM_OPTS="-Xms1024M -Xmx1024M"
    command:
      - --secret
      - "lab123456789"
      - "--cql-hostnames"
      - "cassandra"
      - "--index-backend"
      - "elasticsearch"
      - "--es-hostnames"
      - "elasticsearch"
      - "--s3-endpoint"
      - "http://minio:9002"
      - "--s3-access-key"
      - "minioadmin"
      - "--s3-secret-key"
      - "minioadmin"
      - "--s3-use-path-access-style"
    volumes:
      - thehivedata:/etc/thehive/application.conf
    networks:
      - SOC_NET
  cassandra:
    image: 'cassandra:4'
    restart: unless-stopped
    ports:
      - "0.0.0.0:9042:9042"
    environment:
      - CASSANDRA_CLUSTER_NAME=TheHive
    volumes:
      - cassandradata:/var/lib/cassandra
    networks:
      - SOC_NET
```

```
elasticsearch:
  image: docker.elastic.co/elasticsearch/elasticsearch:7.17.4
  restart: unless-stopped
  ports:
    - "0.0.0.0:9200:9200"
  environment:
    - discovery.type=single-node
    - xpack.security.enabled=false
    - cluster.name=hive
    - http.host=0.0.0.0
    - "ES_JAVA_OPTS=-Xms256m -Xmx256m"
  volumes:
    - elasticsearchdata:/usr/share/elasticsearch/data
  networks:
    - SOC_NET
minio:
  image: quay.io/minio/minio
  restart: unless-stopped
  command: ["minio", "server", "/data", "--console-address", ":9002"]
  environment:
    - MINIO_ROOT_USER=
    - MINIO_ROOT_PASSWORD=
  ports:
    - "0.0.0.0:9002:9002"
  volumes:
    - "miniodata:/data"
  networks:
    - SOC_NET
cortex.local:
  image: thehiveproject/cortex:latest
  restart: unless-stopped
  environment:
    - job_directory=/tmp/cortex-jobs
    - docker_job_directory=/tmp/cortex-jobs
  volumes:
    - /var/run/docker.sock:/var/run/docker.sock
    - /tmp/cortex-jobs:/tmp/cortex-jobs
    - ./cortex/logs:/var/log/cortex
    - ./cortex/application.conf:/cortex/application.conf
  depends_on:
    - elasticsearch
  ports:
    - "0.0.0.0:9001:9001"
  networks:
    - SOC_NET
misp.local:
  image: coolacid/misp-docker:core-latest
  restart: unless-stopped
  depends_on:
    - misp_mysql
  ports:
```

```
      - "0.0.0.0:80:80"
      - "0.0.0.0:443:443"
    volumes:
      - "./server-configs/:/var/www/MISP/app/Config/"
      - "./logs/:/var/www/MISP/app/tmp/logs/"
      - "./files/:/var/www/MISP/app/files"
      - "./ssl/:/etc/nginx/certs"
    environment:
      - MYSQL_HOST=misp_mysql
      - MYSQL_DATABASE=misp_db
      - MYSQL_USER=misp_user
      - MYSQL_PASSWORD=misp_pass
      - MISP_ADMIN_EMAIL=mispadmin@Test.local
      - MISP_ADMIN_PASSPHRASE=misp_admin
      - MISP_BASEURL=localhost
      - TIMEZONE=Europe/Riga
      - "INIT=true"
      - "CRON_USER_ID=1"
      - "REDIS_FQDN=redis"
      - "HOSTNAME= "
    networks:
      - SOC_NET

  misp_mysql:
    image: mysql/mysql-server:5.7
    restart: unless-stopped
    volumes:
      - mispsqldata:/var/lib/mysql
    environment:
      - MYSQL_DATABASE=misp_db
      - MYSQL_USER=misp_user
      - MYSQL_PASSWORD=misp_pass
      - MYSQL_ROOT_PASSWORD=misp_pass
    networks:
      - SOC_NET
  redis:
    image: redis:5.0.6
    networks:
      - SOC_NET
  misp-modules:
    image: coolacid/misp-docker:modules-latest
    environment:
      - "REDIS_BACKEND=redis"
    depends_on:
      - redis
      - misp_mysql
    networks:
      - SOC_NET
volumes:
  miniodata:
  cassandradata:
```

```
  elasticsearchdata:
  thehivedata:
  mispsqldata:

networks:
    SOC_NET:
          driver: bridge
```