USPOREDBA SIEM ALATA OTVORENOG KODA

Farkaš, Matija

VELEUČILIŠTE U RIJECI

Matija Farkaš

USPOREDBA SIEM ALATA OTVORENOG KODA

završni rad

Rijeka, 2022.

VELEUČILIŠTE U RIJECI

Poslovni odjel

Preddiplomski stručni studij Informatika

USPOREDBA SIEM ALATA OTVORENOG KODA

završni rad

MENTOR

dr.sc Bernard Vukelić, prof.v.š

STUDENT

Ime i prezime: Matija Farkaš

MBS: 2422000056/18

Rijeka, 2022.

SAŽETAK

U današnje vrijeme IT odjeli prikupljaju ogromne količine podataka, te je sve teže prepoznati ključne podatke. Sigurnost podataka poduzeća može se poboljšati korištenjem alata koji pomažu u upravljanju i prikazu ključnih informacija i događaja. Tu funkciju obnašaju Sustavi za upravljanje sigurnosnim informacijama i događajima (Security Information and Event Management (SIEM)). SIEM proces služi za prikazivanje sigurnosti u organizaciji kako bi se lakše obavila sigurnosna analiza. Alati koji služe za obavljanje SIEM postupka prikupljaju, analiziraju te uspoređuju i normaliziraju sve datoteke te prikupljaju podatke sa različitih uređaja i daju centralizirani uvid u sve zapise koje su prikupili. U završnom radu, objasniti će se što je SIEM, povijest SIEM alata te njihovu evoluciju. Također će biti objašnjenje prikladne svrhe za korištenje određenih SIEM alata, te će se spomenuti nekoliko alata i usporediti najprikladnije alate za različite slučajeve i različita poduzeća. U praktičnom dijelu rada će se vršiti usporedba različitih SIEM alata otvorenog koda, te će se prikazati vrline i mane svakog od alata na kojima se bude radila usporedba.

Ključne riječi: informacijska sigurnost; sigurnosni incidenti; SIEM; SIM; SEM;

SADRŽAJ

1. Uvod

Kako bi se poduzeća osigurala od raznih prijetnji, koje su u današnje doba sve češće, potrebno je imati dobar sustav obrane. Jedna od komponenti tog sustava svakako bi trebali biti i SIEM alati. Oni omogućavaju prepoznavanje potencijalnih prijetnji uz pomoć skeniranja zapisa sa lokalne mreže.

Svrha ovog završnog rada je usporediti SIEM alate otvorenog koda kako bi se odredila primjerena okolina u kojoj bi se svaki alat mogao najučinkovitije koristiti, svrha završnog rada je također provjeriti kojoj vrsti poduzeća (malom, srednjem ili velikom poduzeću) najbolje odgovara koji alat. Cilj završnog rada je prikazati koje mogućnosti i načine zaštite pružaju SIEM alati koji se uspoređuju i koliko su učinkoviti u otkrivanju prijetnji na lokalnoj mreži na kojoj su implementirani.

Tema diplomskog rada je upravljanje sigurnosnim incidentima, te alati koji služe za obavljanje istog. Također, rad će se baviti SIEM alatima otvorenog koda, te će analizirati alate otvorenog koda i međusobno ih usporediti.

Rad se sastoji od 7 poglavlja. Nakon prvog i uvodnog poglavlja, opisati će se što je SIEM, te kada se on koristi i zašto je potreban u svijetu informacijske sigurnosti, kombiniranjem kojih alata su nastali SIEM alati itd.

Treće poglavlje bavi se povijesti SIEM alata, njihovim začecima, i evolucijama koje su se događale kroz godine postojanja SIEM alata.

U četvrtom poglavlju, biti će navedene i objašnjene sve mogućnosti SIEM alata, od onih osnovnih, poput prikupljanja zapisa datoteka, pa sve do naprednijih poput implementiranja strojnog učenja u same alate.

Peto poglavlje započinje se baviti praktičnim dijelom rada. U ovom poglavlju govori se o alatima koji će se uspoređivati, a to su Wazuh i AlienVault OSSIM. Također će se pokazati koraci instalacije alata, te njihove mogućnosti i opcije koje posjeduju.

Šesto poglavlje donosi usporedbu oba alata, u usporedbi se spominju same mogućnosti alata, kao i sigurnost koju pružaju, izgled njihovih sučelja, kao i najbolja primjena za svaki alat.

Posljednje poglavlje je zaključak završnog rada.

2. Što je SIEM?

Prema Nacionalnom institutu standarada i tehnologije (eng: National Institute of Standards and Technology) i njihovoj publikaciji „Guide to Computer Security Log Management“(Kent K., Murugiah S., 2006), sustavi za upravljanje sigurnosnim informacijama i događajima (Security Information and Event Management (SIEM)) spadaju pod granu sigurnosti informacijskih sustava u kojoj se zajedno koriste sustavi za upravljanje sigurnosnim informacijama (Security information management (SIM)) i alati za upravljanje sigurnosnim događajima (Security event management(SEM)). SIEM alati nude analizu sigurnosnih upozorenja svih uređaja i aplikacija koje se nalaze u lokalnoj mreži. U publikaciji se također navodi kako se analiza svih sigurnosnih upozorenja odvija u realnom vremenu.

Kako bi jasnije shvatili što je SIEM, potrebno je znati više o SIM i SEM sustavima.

2.1 SIM

Cyrus Peikari i Anton Chuvakin u svojoj knjizi „Security Warrior: Know Your Enemy“(Peikari C., Chuvakin A., 2004.) navode definiciju Sustava za upravljanje sigurnosnim informacijama (SIM) kao alata koji se koristi za prikupljanje zapisa sa računala lokalne mreže u centralno spremište, kako bi se mogla vršiti daljnja analiza trendova.

U istoj knjizi također se navodi kako SIM alati funkcioniraju u pozadini, te su neprimjetni u radu računala. SIM alati prikupljaju zapise iz gotovo svih komponenti hardverske mreže (servera, usmjernika, preklopnika, osobnih računala) i iz raznih aplikacija poput antivirusnih programa. Kada alat prikupi podatke, šalje ih na centralizirani server, koji služi kao „sigurnosna konzola“. S obzirom da na centralizirani server stiže ogromna količina podataka, iz koje korisnik nema dobar uvid u sigurnosnu situaciju, u konzoli se podaci prikazuju u obliku grafikona, tablica i raznih izvještaja u stvarnom vremenu.

Konzolu nadgledaju i s njom upravljaju sistemski administratori, koji pregledavaju informacije i poduzimaju odgovarajuće korake za prevenciju sigurnosnih incidenata, ovisno o tipu upozorenja koje je izdao sustav. SIM alati jako su korisni sistemskim administratorima,

jer im pomažu predočiti što se događa u njihovom okruženju te s kojim prijetnjama se suočavaju.

Amir Jamil u članku „The difference between SEM, SIM and SIEM“ (Jamil A., 2011.) navodi kako se termin SIM odnosi se samo na proces otkrivanja nepravilnosti i kršenja pravila postavljenih od strane sistemskog administratora. Za otklanjanje istih nepravilnosti služe SEM alati.

2.2 SEM

Sustavi za upravljanje sigurnosnim događajima (Security event manager (SEM)), za razliku od SIM alata, koji se pretežno fokusiraju na prikupljanje podataka radi izvještavanja o problemima i analizi istih, kao primarni fokus imaju nadziranje u stvarnom vremenu, analiza korelacije različitih događaja, te slanje obavijesti i konzolni prikaz.

Oba sustava započinju rad na isti način. SEM alati, kao i SIM, prikupljaju zapise sa hardverskih komponenti lokalne mreže i šalju zapise na centralizirani server.

Razlika nastaje kada zapisi dođu do centraliziranog servera. SIM alati rade na jednostavniji način, te samo prikupljaju zapise. Amir Jamil u članku „The difference between SEM, SIM and SIEM“(Jamil A., 2011.) navodi kako za razliku od SIM alata, SEM alati rade detaljniju analizu zapisa kako bi pronašli specifične događaje koji su se odvijali na mreži. Primjer neke od tih nepravilnosti bio bi pronalaženje autentifikacija korisnika koje se odvijaju izvan radnog vremena, prijava sumnjivih korisničkih računa na mrežu itd.

Jednostavnije rečeno, SEM sustavi traže specifična ponašanja koja bi mogla biti od važnosti sistemskim administratorima, dok SIM sustavi prikupljaju zapise sa mreže i prikazuju ih u konzoli.

Uz obavijest o sumnjivom događaju, SEM alati dobavljaju i dodatne informacije, kao što su informacije o identitetu korisnika koji je počinio sumnjivu radnju, lokaciji odakle je radnja izvršena, itd.

2.3 SIEM

Sustavi za upravljanje sigurnosnim informacijama i događajima (Security infomation event management (SIEM)), prema članku autora AmriTw „The Future of SIEM – The market will begin to diverge“ (Amritw., 2007), nastali su kombiniranjem elemenata SIM i SEM sustava. Kao i kod prijašnja dva alata, SIEM alati također prikupljaju zapise sa svih hardverskih komponenti lokalne mreže i te podatke šalju na centralizirani server. Zatim se ti podaci u sigurnosnoj konzoli prikazuju pomoću grafikona i raznih izvještaja i čuvaju se na duže vrijeme radi daljnje analize trendova kao kod SIM alata. Ono što je SIEM alatima zajedničko sa SEM alatima je analiza korelacije različitih događaja i obavještavanje administratora o specifičnim sumnjivim aktivnostima koje su se događale na mreži. SIEM alati uzimaju najbolje iz oba sustava, te su zato naj korišteniji od ova tri alata.

3. Povijest SIEM-a

U začecima informatike i interneta, potreba za sigurnosnim alatima nije bila toliko velika kao danas. No, potreba za prikupljanjem i pregledavanjem zapisa pojavljuje se vrlo brzo nakon pojave interneta. Potreba za SIEM alatima pojavljuje se u novije vrijeme, s obzirom da je u početku broj zapisa bio dovoljno mali kako bi čovjek njima sam upravljao.

Logisign team u svom članku „Evolution of SIEM Over the Years“(Logisign Team, 2018.) tako navodi da se prikupljanje zapisa u začecima koristilo primarno kao način otkrivanja nepravilnosti u radu aplikacija, ali se sa razvojem operacijskih sustava i mreža, počelo razvijati i prikupljanje zapisa u sigurnosne svrhe. U članku se također spominje razvoj u prikupljanju zapisa, koji je doveo do mogućnosti praćenja aktivnosti gotovo svakog korisnika. Prve ideje o alatima za upravljanje zapisima javljaju se kasnih 1970-ih. Tada se i postavljaju kriteriji za nadgledanje programa te se otkrivaju načini na koje prikupljanje zapisa može pomoći u otkrivanju napada iznutra, otkrivanju uzroka problema i pravilnog odgovaranja na incidente.

Kako su se u kasnim 1990-im i ranim 2000-im sve više počeli implementirati alati za upravljanje rizicima (Risk management framework (RMF)), količina prikupljenih zapisa naglo je rasla te je broj platformi sa kojih su se prikupljali zapisi također rastao. Sve skupa je postalo jako

teško za kontrolirati i pratiti. Uskoro je nastala potreba za centraliziranjem podataka na jedan server kako bi se povećala preglednost i jednostavnost rada sa prikupljenim zapisima.

U ranije navedenom članku također se spominje da su se podaci počeli prikupljati na centralizirani server, te da je to bio veliki napredak u radu sa zapisima. U početku je samo postojao jednostavniji sustav za upravljanje sigurnosnim informacijama, SIM. Ubrzo se pojavio i drugi sustav za upravljanje sigurnosnim događajima, zvan SEM. Kao što je ranije spomenuto, kombiniranjem ova dva sustava, nastao je novi, bolji sustav za upravljanje sigurnosnim informacijama i događajima (SIEM). Evolucija SIEM alata odvijala se postepeno, sa nekoliko značajnih pomaka koji će biti objašnjeni u sljedećim poglavljima. Iako se u sljedećim poglavljima spominju generacije SIEM-a, službeno ne postoje generacije SIEM alata, već je tako jednostavnije prikazati značajne napretke u određenom vremenskom periodu. Pojam generacija SIEM alata spominje se u članku „A Brief Hsitory of SIEM“(Gailey S., 2020.) Stephena Gaileya, te se sljedeća tri poglavlja referiraju na spomenuti članak.

3.1 SIEM 1.0

Stephen Gailey (Gailey S., 2020.) tako navodi da se prva generacija SIEM-a pojavila se kombiniranjem SIM i SEM sustava prvom polovicom 2000-ih godina. Autor (Gailey S., 2020.) napominje kako je ova generacija SIEM-a bila ograničena jer nije postojala mogućnost horizontalnog skaliranja, već samo vertikalnog, odnosno, poslužitelj na koji su se slali podaci mogao se poboljšati jedino dodavanjem dodatnih ili poboljšanih komponenti, dok bi se horizontalnim skaliranjem isti učinak dobio povezivanjem opterećenog poslužitelja s novim poslužiteljem. To je značajno ograničilo mogućnost prikupljanja podataka u većim organizacijama.

Osim velike mane mogućnosti samo vertikalnog skaliranja, autor (Gailey S., 2020.) spominje kako su prvi SIEM alati nudili su osnovno prikupljanje podataka sa različitih vrsta hardvera, kao i osnovne tehnike analize korelacije. Još jedna velika mana SIEM alata prve generacije, je prema autoru (Gailey S., 2020.) bila oslanjanje na bazu otprije poznatih prijetnji kao jedini način zaštite od napada, bez načina prepoznavanja prijetnji koje nisu poznate. Iz

tog razloga su organizacije sa SIEM alatima prve generacije bile izložene novim vrstama napada, odnosno „zero-day“ napadima.

Još neke od mana ranih SIEM alata koje se spominju u članku bile su greške poput velikog broja javljanja lažno pozitivnih prijetnji, uzrok tome bio je loše odrađena analiza korelacije koja se radila samo određivanjem raznih pravila u domeni. Valja napomenuti i kako je veliki broj lažno javljanih pozitivnih prijetnji često dovodio i do ignoriranja pravih prijetnji koje bi korisnik krivo identificirao kao lažno pozitivne. Osim toga, autor (Gailey S., 2020.) navodi da su pravila radila i probleme u promjeni politike i određenih pravila. Kada je organizacija imala veliki broj pravila, promjena istih oduzimala je puno vremena i dovodila do gubitka produktivnosti, jer je promjena jednog pravila utjecala na drugo itd.

3.2 SIEM 2.0

Gailey navodi kako je takozvana druga generacija SIEM alata stigla početkom 2010-ih. Bitna razlika za velika poduzeća bila je dodana mogućnost horizontalnog skaliranja, pa je tako sada bilo moguće podatke skupljati na više različitih poslužitelja i svejedno ih prikazati na jednoj konzoli. Autor (Gailey S., 2020.) navodi kako je uvedeno i horizontalno skaliranje, koje je značajno povećalo mogućnosti skupljanja sve veće količine zapisa, kojih je bilo sve više i koji su eksponencijalno rasli.

Alati druge generacije su, prema Stephenu Gaileyu, donijeli značajna poboljšanja u prikazu podataka i bolja izvješća, kao i mogućnosti uspješnijeg zadržavanja i iskorištavanja starih podataka. Kod SIEM alata prijašnje generacije, podaci su postajali beskorisni već nakon nekoliko tjedana.

No, autor (Gailey S., 2020.) također navodi da je druga generacija također imala svoje poprilično velike mane. Naime, s većim brojem prikupljenih podataka, bilo je nemoguće pregledati sve zapise i odrediti koji od njih su relevantni, a koji ne. Problem je nastao jer u drugoj generaciji SIEM alata još uvijek nije postojao dobar sustav za upozoravanje korisnika o mogućim prijetnjama i incidentima. Tako su se ponavljali nedostaci prijašnje generacije,

kao što je javljanje lažnih pozitivnih prijetnji, što bi dovelo do ignoriranje stvarnih prijetnji itd.

3.3 SIEM 3.0

Autor članka (Gailey S., 2020.) također navodi kako se treća i aktualna revolucija dogodila se polovicom 2010-ih i još uvijek je u tijeku. Fokus ove revolucije je, prema autoru, bio ponajviše na poboljšavanju iskoristivosti sustava. Najveća novost ove generacije je uvođenje analitike uz pomoć strojnog učenja. Strojno učenje detaljnije je objašnjeno u kasnijim poglavljima.

Gailey navodi kako Strojno učenje donosi mogućnost obavještavanja korisnika o prijetnjama pomoću sigurnosnog praćenja koje se temelji na analitici. Izrađuju se detaljni operativni modeli za svakog korisnika i entitet u željenom okruženju. Korisnik se obavještava ukoliko dođe do drastične promjene u operativnom modelu svakog korisnika (npr. Ukoliko se neki korisnik prijavi sa nepoznate lokacije ili se prijavi van radnog vremena itd.). Osim takvog obavještavanja, i dalje je zadržano obavještavanje uz pomoć analize korelacije i pravila koje se koristilo i u prijašnjim generacijama.

S obzirom da je ova generacija SIEM alata trenutna i ovaj završni rad se bazira na njoj, detaljnija analiza svih njenih mogućnosti odvijati će se u sljedećim poglavljima.

4. Mogućnosti SIEM alata

Svaki moderni SIEM alat ima veliki broj različitih mogućnosti, no da bi se neki alat smatrao SIEM alatom, mora sadržavati osnovne značajke kao što su prikupljanje zapisa, analiza korelacija događaja, baza podataka poznatih sigurnosnih prijetnji, sposobnost obavještavanja o sigurnosnim prijetnjama itd. U ovom poglavlju će se detaljno objasniti svaka od popularnijih mogućnosti koje sadrži većina modernih SIEM alata.

4.1 Upravljanje zapisima

Ben Canner u svom članku „7 Key SIEM Capabilities to Look For in Your Solution“(Canner B., 2018.) navodi kako je osnovna mogućnost upravljanja zapisima naslijeđena iz SIM sustava. Canner (2018.) također navodi upravljanje zapisima prisutno je od samih početaka SIEM-a. Kao što se i ranije spominjalo u ovom završnom radu, upravljanje zapisima je mogućnost SIEM alata koja je naj bitnija za rad istih, s obzirom da od nje sve počinje. Pomoću ove mogućnosti, zapisi se prikupljaju sa svih hardverskih komponenti lokalne mreže i šalju se na centraliziranu lokaciju. To omogućuje lakši pristup svim zapisima pošto se nalaze na jednom mjestu.

4.2 Analiza korelacije sigurnosnih događaja

Ova mogućnost prvotno je nastala u SEM sustavima, te ju autor članka, Ben Canner (2018.) smatra naj osnovnijom mogućnošću koju jedan SIEM alat može imati. Analiza korelacije sigurnosnih događaja koristi se od nastanka prvih SIEM alata. Canner navodi i da je za izvršenje analize potrebno prikupiti sve podatke i zapise iz lokalne mreže. Nakon toga je potrebno postaviti pravila prema kojima će SIEM alat određivati nepravilnosti i sigurnosne prijetnje na mreži. Korisnik, odnosno IT odjel definira korelacijska pravila kako on to želi. Većina SIEM alata dolazi sa gotovim pravilima, koje tada korisnik može iskoristiti te izmijeniti tako da bolje odgovaraju njegovoj situaciji. Pravila rade tako da se odredi situacija koja se želi pratiti. Primjer analize korelacije može se naći u članku “What is event correlation“(ManageEngine, 2022.) na stranici proizvoda ManageEngine. U primjeru se uzima pokušaj prijave sa određene IP adrese. Zatim se dodaju pravila kojima možemo lakše

nadzirati situaciju. Na navedenom primjeru bi se prvim pravilom pratio broj pokušaja prijave sa određene IP adrese, dok bi se drugim pravilom javljala uspješno odrađena prijava sa te iste IP adrese. Pomoću određenih pravila korisnik lakše može odlučiti radi li se o normalnoj ili sumnjivoj aktivnosti, kako bi se lakše objasnila situacija, u primjeru koji je ranije objašnjavan bi se incident javio ako bi prvo pravilo javljalo sto pokušaja prijave sa IP adrese, a drugo pravilo javlja samo jednu uspješnu prijavu sa iste IP adrese. Tada je velika mogućnost da se radi o sigurnosnom incidentu i „brute force“ napadu. Normalna situacija smatrala bi se kada bi pokušaj prijava bio jednak ili približno jednak broju uspješnih prijava.

ManageEngine (2022.) na svojoj stranici u istom članku navodi da je potrebno analiziranje napada kako bi se steklo bolje razumijevanje istih. Iz tog razloga postoji statička analiza korelacije, autor članka navodi da se statička korelacija odrađuje analizom i istraživanjem već prikupljenih zapisa. Statička korelacija pomaže u otkrivanju uzoraka prema kojima su nastali prijašnji napadi. S tim znanjem organizacije mogu postaviti nova pravila kojima će se zaštiti od ponovnog napada iste vrste.

ManageEngine također navodi da se svi događaji analiziraju pomoću dinamičke korelacije kada su pravila postavljena. Ona uzima pravila koja su postavljena i traži događaje koji odgovaraju pravilima kako bi se zaustavio novi napad ili prijetnja.

4.3 Integracija Threat Intelligence-a

Svaki SIEM alat ima mogućnost integracije baze podataka poznatih sigurnosnih prijetnji (eng. Threat Intelligence). Dodavanje ove baze podataka u SIEM sustave je bitno kako bi se mreža mogla osigurati od prijetnji lakše, brže i bolje. Integracija baze može se napraviti dodavanjem platforme posebno namijenjene za tu svrhu (IBM X-Force Exchange, Anomali ThreatStream ,itd.) ili pomoću ručnog dodavanja poznatih sigurnosnih prijetnji iz različitih javno dostupnih izvora (Ransomware Tracker, URLhaus).

Ben Canner (Canner B., 2018.) navodi kako dodavanje baze podataka poznatih sigurnosnih prijetnji u SIEM sustave, te također navodi kako to donosi dodatnu razinu zaštita, te omogućuje pronalaženje sumnjivih radnji ili datoteka koje sam SIEM možda ne bi

detektirao, ovisno o postavljenim pravilima. Zato ova mogućnost može prepoznati razne događaje ili datoteke koje su unesene u njegovu bazu. Također je moguće omogućiti SIEM alatu da automatski poduzima neke radnje, poput blokiranja određenih IP adresa, s obzirom da se dodavanjem baze podataka poznatih sigurnosnih prijetnji dobiva više konteksta o pojedinim datotekama, radnjama ,itd…

4.4 Sigurnosna upozorenja

Kada SIEM alat misli da je pronašao opasnost, potrebno je obavijestiti korisnika o novim i potencijalno opasnim događanjima na mreži. To je razlog za postojanje sigurnosnih upozorenja unutar SIEM alata. Ben Canner (2018.) navodi kako ukoliko analizom korelacije SIEM sustav dođe do zaključka da je neki događaj potencijalno opasan, korisnika se odmah obavještava. Također spominje i da se obavijesti mogu slati na nekoliko načina, ovisno o alatu. Svi alati imaju mogućnost postavljanja obavijesti na svoju kontrolnu ploču, dok neki alati imaju i mogućnosti slanja obavijesti putem maila ili drugih poruka kako bi korisnik još prije dobio obavijest o prijetnji u slučaju da trenutno ne radi na kontrolnoj ploči alata.

4.5 Prezentacija izvještaja

Pošto SIEM sustavi prikupljaju puno podataka, korisniku je gotovo nemoguće pregledati sve informacije koje je sustav skupio, a još je teže odrediti relevantne informacije. Zato svi SIEM alati grupiraju podatke i prezentiraju ih putem grafikona ili tablica, te sortiraju i grupiraju razne zapise ovisno o njihovom tipu (zapisi operacijskog sustava, zapisi antivirusnog programa, itd.).

4.6 Strojno učenje

Kako bi se mogla objasniti uloga strojnog učenja u SIEM alatima, prvo je potrebno ukratko objasniti na što se odnosi taj pojam. Strojno učenje je grana umjetne inteligencije koja koristi razne algoritme kako bi naučila iz prijašnjih iskustava.

Ben Canner u svom članku „6 Questions About Machine Learning in SIEM (Answered!)“(Canner B., 2019.) navodi kako se integracija u SIEM sustave odvija tako da se pravila i podaci koriste u poboljšanju sigurnosne analize. Odnosno, proces analize, koji je do sada obavljao čovjek, sada preuzima umjetna inteligencija. Canner također navodi da je velika prednost strojnog učenja ta da ono smanjuje vrijeme i trud potreban za izvršenje analize. Autor također navodi kako je u nekim slučajevima umjetna inteligencija toliko dobro razvijena da može sama donositi odluke ovisno o prikupljenim podacima.

Još jedna mogućnost koji Canner spominje, osim obavljanja analize, je strojno učenje. Ono omogućuje i neke napredne mogućnosti kao što su predviđanje budućih napada. Autor (Canner B., 2019) spominje kako strojno učenje buduće prijetnje može predvidjeti analizom uzoraka prijašnjih napada, te kako ova mogućnost rješava jednu od mana starijih SIEM sustava, koji su djelovali samo reaktivno.

Kao što je ranije navedeno u prezentaciji izvještaja, SIEM alati mogu sortirati i grupirati zapise ovisno o njihovom tipu. Ta mogućnost dostupna je upravo zbog strojnog učenja.

Autor članka spominje još jednu bitnu stavku strojnog učenja u SIEM alatima, a to je mogućnost učenja pravilnog odgovaranja na incidente. Ova mogućnost je prema autoru (Canner B., 2019.) jako bitna jer pomaže IT odjelu u donošenju pravilne odluke u suzbijanju prijetnje. Strojno učenje daje prijedloge ovisno o prijašnjem incidentu sličnog tipa. Kako su napadi sve češći, ova mogućnost postaje jedna od najbitnijih mogućnosti cjelokupnog SIEM sustava.

5. SIEM alati otvorenog koda

U ovom poglavlju pisati će se o SIEM alatima otvorenog koda na kojima će se kasnije vršiti usporedba. Alati o kojima će se pisati su Wazuh i AlienVault OSSIM. Svaki od alata izabran je jer koristi više različitih pomoćnih alata otvorenog koda koji su se pokazali kao najrelevantniji pomoćni alati otvorenog koda za izgradnju uspješnog SIEM alata, no u isto vrijeme SIEM alati koriste gotovo potpuno različite pomoćne alate, što ih čini prikladnim za usporedbu.

Analizom literature, posebice članka Thu Nguyen: „5 Open Source SIEM Solutions“ (Nguyen C.,2019.) odabrao se alat Wazuh jer se bazira na ELK Stack alatu i nastao je kao nadogradnja na drugi alat imena OSSEC, te iz tog razloga ima više mogućnosti od ostalih alata otvorenog koda, kao i unaprijeđeno korisničko sučelje u odnosu na OSSEC, na kojem se nije vršila usporedba jer je previše sličan Wazuhu.

Osim Wazuha, odabran je i alat OSSIM, kao suprotnost Wazuhu. OSSIM se bazira na drugoj bazi alata otvorenog koda kako bi obavljao svoju funkciju SIEM alata. Također, OSSIM se predstavlja kao alat koji bi trebao biti pristupačniji korisniku, te je to jedan od bitnih razloga zbog kojih je odabran upravo taj alat.

Kako bi se testirala učinkovitost SIEM alata u prepoznavanju prijetnji, korištene su razne metode, kao brute force pokušaji prijavljivanja na uređaje, simuliranje ransomware napada i instaliranje poznatog malwarea na virtualnu mašinu. Ove metode koristile su se radi lakše implementacije, s obzirom da je završni rad opsežan i implementacija SIEM alata je složena. Također, dokumentacija za testiranje ove tri metode bila je lako dostupna i može se pronaći na stranicama Wazuha,

Testovi su rađeni kako bi se pronašla prikladna primjena za oba alata, kao i kako bi se otkrile potencijalne mane, kao i prednosti određenog SIEM alata u usporedbi s drugim alatima.

5.1 SIEM alat Wazuh

Wazuh je alat otvorenog koda te se osim za SIEM, može koristiti i kao sustav za otkrivanje neovlaštenog updata (Host-based intrusion detection system (HIDS)). Alat se može

koristiti na više različitih platformi i operacijskih sustava odjednom, te tako može efikasno nadgledati lokalne mreže na svim vrstama operacijskih sustava (MacOS, Windows, Linux…), kao i ostalim mrežnim uređajima.

Wazuh je osnovan 2015. u Californiji, te se u kratkom vremenu proširio i sadržava preko 100 timova koji su pozicionirani u SAD-u, Španjolskoj i Južnoj Americi. Alat je nadogradnja na stariji SIEM alat, OSSEC. Kako bi omogućio najbolje iskustvo, alat se sastoji od 3 komponente. Servera, agenata i Elasticsearcha. Wazuh je modificirana verzija ELK stack-a te je Wazuh zapravo plugin koji se instalira skupa sa ELK stackom.

5.1.1 ELK Stack

ELK Stack je kratica za 3 različita projekta otvorenog koda (Elasticsearch, Logstash i Kibana) koja su kasnije spojena u jedan projekt kojim se rješavaju problemi prikupljanja, prikaza i indeksiranja podataka. S obizorm da sva tri alata najbolje rade kada su skupa, nije potrebno zasebno objašnjavati njihov rad. Prikupljanje podataka obavlja alat Logstash. Njegova funkcija je najjednostavnija za objasniti, Logstash prikuplja podatke s agenata i prosljeđuje ih Elastisearchu. Ovaj alat je tražilica bazirana na JSON-u. Alat je iznimno popularan zbog svoje mogućnosti prikupljanja i indeksiranja podataka iz raznih izvora (zapisa, web aplikacija, resursi sustava…). Kada su podaci indeksirani u elasticsearchu, korisnik može pretraživati svoje podatke prema raznim filterima i tako se znatno povećava preglednost podataka. Nakon što su podaci indeksirani, potrebno ih je i prikazati, te tu dolazi sljedeći dio ELK stacka, a to je Kibana. Kibana je alat za prikazivanje podataka. Podatke je moguće prikazati pomoću histograma, linijskih i tortnih grafikona itd. Osim ova tri alata, ELK stack se može koristiti i dodatnim pluginovima kao što je Canvas, koji omogućava izradu vlastitih grafikona. Jedan od dodatnih pluginova je i Wazuh, koji donosi ostale SIEM elemente, kao što su sigurnosna pravila, sigurnosna upozorenja itd.

5.1.2 Wazuh Agent

Agent alata Wazuh instalira se na korisnička računala s kojih se želi prikupljati podatke. Agent zahtjeva iznimno malo resursa, te radi u pozadini, tako da korisnik niti ne primjećuje da se njegovi podaci prikupljaju. Ova komponenta alata može se instalirati na više različitih operacijskih sustava. Podržani operacijski sustavi su Windows (7 nadalje), Linux (Red Hat/CentOS, Debian / Ubuntu) i MacOS. Instalacija je vrlo jednostavna, te će biti objašnjena u poglavlju instalacije Wazuh agenta.

5.1.3 Wazuh Server

Wazuh server jedna je od 3 komponente koje čine potpuni alat. Server je, kao i svaki drugi server zadužen za prikupljanje podataka sa agenta, te njihovo dekodiranje i analiziranje podataka kroz set pravila. Server može analizirati podatke sa nekoliko tisuća agenata odjednom, te se može skalirati horizontalno, odnosno može se postaviti više fizičkih servera koji će obavljati istu funkciju na istoj adresi, što je značajno bolje od vertikalnog skaliranja, gdje je jedina opcija za poboljšavanje performansi dodavanje novih resursa novim komponentama na jedini postavljeni server.

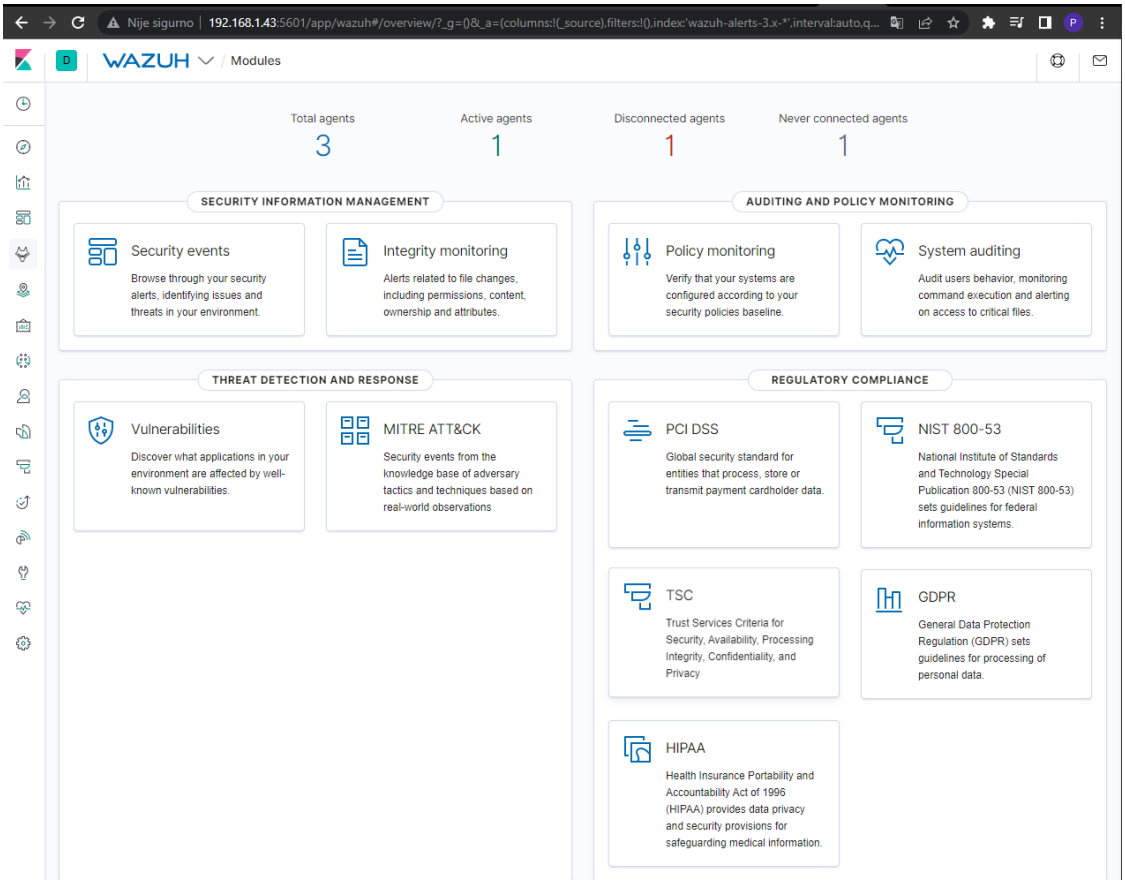
5.1.4 Instalacija Wazuha

Kako bi uspješno instalirali Wazuh potrebno je instalirati i ostale sustave koji mu omogućavaju rad. Ti sustavi su Filebeat, Elasticsearch i Kibana. Tek nakon instalacije sva tri sustava može se instalirati Wazuh plugin. Sva potrebna dokumentacija za instalaciju Wazuha nalazi se na internetskoj stranici alata

(https://documentation.wazuh.com/3.12/installation-guide/installing-wazuh-manager/linux/centos/wazuh_server_packages_centos.html#wazuh-server-packages-centos).

Server se može instalirati jedino preko Linux operacijskih sustava (Debian, Red Hat, CentOS, Ubuntu…). U ovom primjeru korišten je CentOS 7. Dok se server instalira na Linux operacijskim sustavima, agenti se mogu instalirati na više različitih operacijskih sustava (Windows, MacOS i operacijski sustavi bazirani na Linux kernelu). Nakon uspješne instalacije, serveru se pristupa unošenjem IP adrese servera u internetski preglednik.

Slika 1 Kontrolna ploča Wazuh servera



Izvor: Autor

5.1.5 Mogućnosti Wazuha

Wazuh nudi razne opcije, od opcija vezanih za SIM, pa sve do upozorenja vezanih za zaštitu osobnih podataka (GDPR). Osnovne opcije tiču se prikaza prikupljenih sigurnosnih upozorenja i prijetnji koji su pronađeni kod pojedinih agenata. Taj prikaz može se vidjeti pod opcijom Security events.

Security events kontrolna ploča prikazuje mnoštvo informacija. Prikaz podataka može se filtrirati periodično. Upozorenja se dijele na razine od 1 do 12 ovisno o razini ozbiljnosti (1-niska razina rizika, 12-jako rizično). Na kontrolnoj ploči se prikazuje broj upozorenja, te broj kritičnih upozorenja. Kao i broj neuspješnih prijava na agentima. Kontrolna ploča se može filtrirati prema pravilima koja su postavljena u sekciji rules.

Odabiranjem opcije Events, prikazuju se sva upozorenja koja je server prikupio. Ta se upozorenja također mogu filtrirati po raznim pravilima koja se mogu postaviti.

Ostale opcije koje Wazuh čine SIEM-om su Vulnerabilities i MITRE ATT&CK opcije. Vulnerabilities opcija detektira ranjivosti agenata. Wazuh detektira ranjivosti koje su zabilježene u njegovoj bazi podataka poznatih ranjivosti. MITRE ATT&CK opcija služi kako bi dala savjete za obranu od ranjivosti pronađenih na računalu. Savjeti za obranu također su sadržani u bazi podataka Wazuha. Obje opcije također imaju kontrolnu ploču, kao i sve ostale opcije u Wazuh aplikaciji.

Još jedna bitna opcija Wazuha je Policy monitoring, koja provjerava ponašaju li se sustavi u skladu sa sigurnosnim politikama postavljenim u domeni. Opcija također sadrži grafički prikaz.

System auditing je opcija koja nadzire korisničko ponašanje, te obavještava administratora ako korisnici pristupe vrlo bitnim datotekama ili ako se na računalima izvršavaju potencijalno opasne naredbe.

Preostale opcije spadaju u skupinu „Regulatory Compliance“, to su opcije koje administratoru pomažu da se pridržava svih sigurnosnih standarda zaštite podataka. Svaka

od ovih opcija ukazuje na nedostatke koje bi administrator trebao ispraviti da sustav bude sukladan standardima.

5.2 SIEM alat AlienVault OSSIM

Sljedeći alat koji će se uspoređivati je AlienVault OSSIM. S razvijanjem alata krenulo se 2003. godine. Projekt je započet pod imenom OSSIM, cilj projekta bio je razviti sustav koji će pomoći sistemskim administratorima u pronalaženju i sprječavanju napada i podizanju opće razine sigurnosti. Nekoliko godina nakon razvoja OSSIM-a, autori alata osnivaju kompaniju AlienVault, čime se i službeno ime OSSIM-a mijenja u AlienVault OSSIM. Iste godine pojavljuje se i plaćena verzija OSSIM-a, pod imenom AlienVault USM. Cijelu tvrtku je 2019. kupila američka telekomunikacijska tvrtka AT&T, te se od tada OSSIM nalazi u vlasništvu te tvrtke. Od svog osnutka do danas, AlienVault OSSIM ostaje alat otvorenog koda, te je izvorni kod alata dostupan na internetu. OSSIM je baziran na Debianu, operacijskom sustavu baziranom na Linux kernelu, te je dodatno promijenjen kako bi se korisniku ponudila što lakša implementacija i instalacija alata na lokalnu mrežu. OSSIM može nadgledati različite vrste uređaja na lokalnoj mreži, moguće je primati podatke iz računala različitih operacijskih sustava (svi operacijski sustavi bazirani na Linuxu, Windows, MacOS), također je moguće prikupljati podatke sa mrežnih uređaja kao što su usmjernici i preklopnici.

No, osim alata razvijenih samostalno, tvorci OSSIM-a koristili su i ostale komponente otvorenog koda kako bi razvili svoj alat u potpunosti. Tako se primjerice za sustav detekcije upada u početku koristio Snort, koji je kasnije zamijenjen Suricatom. Munin je korišten za analiziranje prometa na mreži, Nagios se koristi za nadziranje hostova i portova, kao i za potpuno nadziranje lokalnih uređaja. Valja napomenuti kako su tvorci OSSIM-a samostalno razvili sustav korelacije u sustav integracije zapisa.

Alat također posjeduje bazu podataka poznatih prijetnji i ranjivosti, pod imenom OTX. Podaci se u bazu prikupljaju kada korisnici reagiraju i otkriju probleme. Za aktivaciju ove usluge potrebno je kreirati korisnički račun na stranici OTX-a, kako bi se

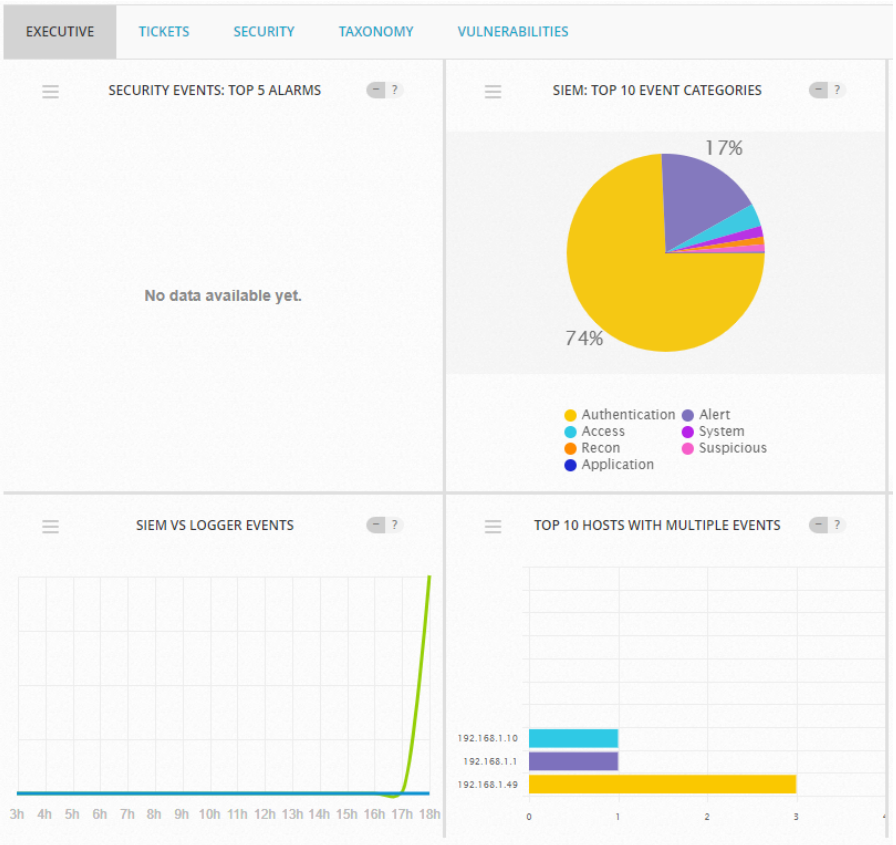
omogućilo pridonošenje što većeg broja korisnika dopunjavanju baze novim prijetnjama. Ovaj alat naravno nije savršen, jer uvijek postoji mogućnost nedostatka najnovijih prijetnji.

5.2.1 Pregled mogućnosti AlienVault OSSIM-a

Kada su postavljene osnovne postavke servera, prikazuje se početni prikaz. Moguće je odabrati prikaz nekoliko različitih kontrolnih ploča, no najbitnije za ovaj primjer su kontrolne ploče „Executive“ i „Security“.

Na „Executive“ kontrolnoj ploči mogu se vidjeti podaci o računalima sa najviše upozorenja i sigurnosnim problema, te tipovi događaja koji se najčešće prikupljaju na server.

Slika **2**: Executive Kontrolna ploča AlienVault OSSIM



Izvor: Autor

Kada se otvori „Security“ kontrolna ploča, mogu se vidjeti hostovi sa najviše promjena na svom sustavu i hostovi koji imaju najviše prikupljenih događaja, kao i liste 5 najčešćih upozorenja i događaja.

Osim ove dvije kontrolne ploče, valja spomenuti i kontrolnu ploču „Taxonomy“ na kojoj se prikazuju hostovi kod kojih je zabilježeno postojanje malwarea, dozlove i blokirana pravila na vatrozidu, te uspješne i neuspješne prijave korisnika.

Sljedeća opcija u izborniku nosi naziv „Analysis“, te se ovdje mogu vidjeti događaji, upozorenja i čisti logovi, kao i korisnički ticketi (ako se omogući ticketing

sustav). Prikazi se mogu filtrirati sa opcijama poput izvora podataka, razine rizika, postavljenim grupama itd.

Opcija Enviroment omogućuje dodavanje grupa, te daje prikaz svih uređaja na lokalnoj mreži i omogućava obavljanje skeniranja. Skeniranje se može obaviti u bilo kojem trenutku, te se može zakazati za određeni termin. Također je moguće napraviti mrežne grupe, ako postoji više različitih subneta.

Posljednja opcija „Reports“, omogućava preuzimanje raznih izvješća. Izvješća koja AlienVault OSSIM nudi su izvješće o uzbunama, izvješće o uređajima na određenom subnetu, izvješće o usklađenosti, izvješće o geografskim lokacijama pristupanja na mrežu, izvješće o SIEM događajima, Baza podataka prijetnji i ranjivosti i izvješća o ticketing sustavu. Neka se izvješća mogu preuzeti u PDF formatu, dok se ostala mogu samo pregledati na samom serveru.

6. Usporedba alata

U završnom radu su obrađena dva SIEM alata, te je potrebno usporediti prednosti i mane svakog sustava kako bi se donijela odluka, kada i kome više odgovara koji sustav. Kako su se u prethodnom poglavlju opisale mogućnosti i funkcionalnosti navedenih alata, u ovom poglavlju napravit će se njihova usporedba. Kriteriji koji su se koristili za usporedbu alata su sljedeći: potrebni računalni resursi, lakoća instalacije/implementacije, mogućnost dodavanja uređaja, funkcionalnosti, prezentacija izvještaja, zaštita i sigurnost, primjerena primjena svakog alata.

6.1 Resursi

Kako bi se instalirao i implementirao softver, potrebno je serversko računalo na koje će se instalirati željeni SIEM alat. Za instalaciju oba alata potrebno je imati procesor sa minimalno dvije jezgre i minimalno 4GB RAM memorije, što u današnje doba nije pretjerano veliki zahtjev za poduzeća s puno servera. Iako u teoriji zahtijevaju jednako resursa, u praksi se pokazalo da je Wazuh ipak „lakši“ alat. U praktičnom dijelu ovog završnog rada, oba servera pokretala su se na virutalnim mašinama koje zadovoljavaju minimalne zahtjeve za rad servera, ali se pokazalo da AlienVault-ov alat radi primjetno sporije od Wazuha. Performanse su se izjednačile tek kada su na virtualnoj mašini OSSIM servera resursi povećani sa 4 na 6 GB RAM memorije.

6.2 Implementacija

Prvi korak s kojim se susretne svaki administrator kada je u pitanju novi softver je instalacija i implementacija istog. OSSIM je u ovom slučaju puno bolji izbor. Instalacija OSSIM-a je u usporedbi s Wazuhom jako jednostavna, te ga svatko sa osnovnim poznavanjem mreža i rada na računalu može uspješno instalirati i implementirati. Sve što je potrebno za instalaciju servera je pokrenuti instalacijski disk i pratiti upute programa.

Ovaj dio Wazuha jednostavno nije dobro izveden, te iako na internetskim stranicama alata postoji odlična dokumentacija koja korisnika navodi kroz sve korake, što je veliki napredak u usporedbi sa OSSEC-om, na kojem je Wazuh baziran, dokumentacija pružena s instalacijom

ne može se usporediti s jednostavnošću instalacije OSSIM-a. Kako bi Wazuh uspješno radio, potrebno je ručno mijenjati konfiguraciju raznih servisa u Linux terminalu, što može biti zastrašujuće korisniku koji nema previše iskustva s Linux operacijskim sustavima, te je potrebno samostalno pokretati servise koji se instaliraju, dok kod OSSIM-a ništa od toga nije potrebno, već instalacija obavlja sve na osnovu parametara unesenih u potrebna polja.

6.3 Dodavanje uređaja

Kako bi uspješno mogli nadzirati računala u lokalnoj mreži, potrebno ih je dodati na serveru, kako bi alat mogao prikupljati logove sa različitih uređaja.

OSSIM je u ovoj situaciji ponovno jednostavniji od Wazuha. Oba sustava mogu dodavati i različite uređaje s mreže, kao računala, printere i mrežne uređaje. Postupak dodavanja uređaja na OSSIM-u je jednostavan. Uređaje je moguće dodati tako da se skenira subnet mreže koju želimo dodati, te alat skeniranjem prepozna dostupne uređaje, koje zatim dodaje na server. Uređaji se također mogu dodati ručno, unošenjem IP adrese uređaja.

Wazuh koristi sustav „agenata“ koji se dodaju tako da se odabere operacijski sustav računala na koje se želi instalirati „agent“, te se unese IP adresa servera. Zatim Wazuh generira naredbu koju je potrebno unijeti na željeno računalo. Problem s ovakvim načinom instalacije je takav da je instalaciju agenta nemoguće obaviti bez spajanja ili pristupanja računalu. Problem nije toliko izražen u malim ili srednjim poduzećima, ali ako se radi o velikom poduzeću problem se mora rješavati drugim načinima, kao provođenjem skripte na svim željenim računalima, što samo stvara dodatne korake, kojih OSSIM nema. Još jedan nedostatak Wazuha u usporedbi s OSSIM-om je taj da se mrežni uređaji moraju dodavati putem Linux terminala servera, što dodatno komplicira stvari.

U ovom segmentu, OSSIM se pokazao kao bolje rješenje.

6.4 Mogućnosti

U ovom segmentu usporedbe, sagledati će se mogućnosti koje posjeduju oba alata, kao i mogućnosti koje nedostaju kod oba alata. Nedostatak nekih mogućnosti kod AlienVault OSSIM-a značajno smanjuju funkcionalnost samog alata.

Oba alata imaju mogućnosti pregleda događaja, prikaz ranjivosti, iako koriste različite baze podataka, oba alata uspješno detektiraju iste poznate prijetnje na mreži, također u oba sustava je moguće kreirati vlastita pravila, kao i definirati koja već kreirana pravila se žele koristiti,

Wazuh posjeduje neke opcije koje OSSIM nema i obrnuto. Jedna od bitnijih stavki koje nedostaju OSSIM-u su nadziranje kršenja sigurnosne politike, kao i sve opcije vezane za usklađenost s propisima. Wazuh ima raznovrsnije dodatne mogućnosti, pa tako posjeduje i opciju nadgledanja integriteta datoteka, koja mu omogućava prepoznavanje ranjivosti koje OSSIM ne može prepoznati. Wazuh može nadzirati promjene odrađene na ključnim datotekama kako bi spriječio napade poput ransomware napada. Valja napomenuti kako se ova opcija može nadodati u OSSIM instalacijom HIDS agenata na korisnička računala, ali ako gledamo oba alata u osnovnoj verziji, ovo se smatra nedostatak OSSIM-a. Također, u Wazuhu je moguće provjeriti krše li se ikakva zakonska pravila u obradi podataka (primjer: krše li se pravila GDPR-a). Ti sustavi jednostavno nedostaju u OSSIM-u.

No, opcije koje OSSIM posjeduje također su korisne. Jedan od veliki nedostataka Wazuha je taj što je kompliciranо rasporediti računala po različitim grupama. Tu opciju u Wazuhu nije moguće odraditi kroz web sučelje, već je ponovno potrebno unositi naredbe u Linux terminal.. OSSIM ovu funkciju ima ugrađenu u svoje web sučelje i jednostavno se koristi. Iako nije funkcija koja nedostaje, njena nedostupnost čini rad sa samim alatom kompliciranijim.

Oba alata imaju sve mogućnosti koje ih čine SIEM alatima, jedine razlike nalaze se u mogućnostima koje nisu nužne za SIEM alate. Iako se ovdje mora napomenuti kako Wazuhove dodatne mogućnosti imaju više smisla u SIEM alatu. Jedina velika razlika između

oba alata je OSSIM-ov nedostatak opcije provjeravanja integriteta datoteka, što je jedna od bitnijih opcija u Wazuhu.

6.5 Prezentacija

Prezentacija alata uspoređivati će se s obzirom na preglednost sustava, dostupnost svih opcija u svakom trenutku, prikazu podataka i mogućnostima filtriranja podataka.

Oba alata nude mnoštvo različitih prikaza zahvaljujući raznim grafikonima i tablicama. Snalaženje u oba alata je relativno jednostavno i pregledno. Oba sustava imaju dobre mogućnosti filtriranja zapisa. Podaci se mogu filtrirati po klijentima, vremenu prikupljanja podataka, tipu prikupljenog zapisa, razini prijetnje itd. Oba alata imaju kvalitetno odrađenu prezentaciju, te su gotovo pa izjednačeni na području prezentacije. Ipak, iako Wazuh ima dojmljiviju prezentaciju sa više boja i različitih vrsta grafikona, OSSIM ipak ima sveukupno bolji UX, uglavnom zbog uvijek prisutnog izbornika, što kod Wazuha nije slučaj.

Jedna velika zamjerka Wazuhu je ta da sve opcije nisu dostupne na samom web sučelju, već im je potrebno pristupiti kroz terminal servera, nešto što kod OSSIM-a nije slučaj. S ovim nedostatkom Wazuhovo web sučelje ponekad može davati osjećaj kao da nije dovršeno, te da nedostaju neke opcije, koje zapravo postoje, ali im je nemoguće pristupiti putem izbornika na web sučelju.

6.6 Zaštita

Posljednja stavka usporedbe biti će zaštita, SIEM alati koriste se kako bi cijela okolina ostala sigurna, stoga je zaštita vrlo bitan dio istih alata. Zaštita je uspoređivana pregledom svih sigurnosnih mogućnosti koje određeni alat posjeduje, kao i rezultatima provedenih simuliranja napada. Napadi koji su se simulirali na lokalnoj mreži su ransomware napadi, brute force napadi i instalacija otprije poznatih malwarea. Ransomware napadi testiraju rad opcije provjeravanja integriteta datoteka, brute force napadi testiraju mogu li alati uspješno prepoznati neuspješne prijave, te koliko neuspješnih prijava je potrebno kako bi alat upozorio korisnika o sumnjivom ponašanju. Instaliranjem otprije poznatog malwarea testira se baza

podataka poznatih prijetnji kojom se alati koriste, također se testira koliko je vremena potrebno da alat prepozna prijetnju.

Wazuh nudi mogućnosti detektiranja skrivenih datoteka i procesora, kao i prepoznavanje neregistriranih network listenera. Od aktivnih načina zaštite nudi postavljanje automatskog odgovora na akciju ukoliko su zadovoljeni svi postavljeni parametri. Pa je tako moguće blokirati pristup mreži ukoliko su primijećene sumnjive radnje s te IP adrese i još mnogo primjera. Također Wazuh može detektirati napade poput „SQL Injection“ napada. Nakon testiranja ranije navedenih metodi, Wazuh je uspješno detektirao sve tri prijetnje. Ransomware napad je prepoznat prilikom prvog skeniranja, isti je slučaj bio i sa otprije poznatim malwareom. Detekcija brute force napada odrađena je tako da su javljani svi pokušaji neuspješne prijave, ali bi se svakim neuspješnim pokušajem prijave razina ozbiljnosti prijetnje podizala. Nakon određenog broja neuspješnih prijava u kratkom roku, alat je poslao upozorenje administratoru.

S druge strane imamo OSSIM, koji je kako smo ranije spominjali, verzija otvorenog koda alata AlienVault USM, stoga mu nedostaje mnogo mogućnosti koje Wazuh posjeduje. Pa tako primjerice OSSIM ne može pronaći neregistrirane network listenere, također ne postoji mogućnost aktivnog načina zaštite, što je svakako veliki minus. Još veći nedostatak je nemogućnost prepoznavanja napada. Iako ni Wazuh ne može prepoznati sve napade (primjer: DOS), barem postoji mogućnost solidne zaštite samo sa jednim alatom, dok je s OSSIM-om potrebno posjedovati dodatne alate za zaštitu. Na provedenim testovima, OSSIM nije bio uspješan kao Wazuh. Uspješno je detektirao prethodno poznati malware, zahvaljujući OTX bazi podataka, koju popunjavaju korisnici. Iako je u ovom slučaju detekcija malwarea bila uspješna, s obzirom da bazu podataka prijetnji ispunjavaju korisnici, može se dogoditi da baza podataka nije uvijek potpuno ažurna, što može dovesti do sigurnosnih prijetnji. Test detekcije brute force napada AlienVault OSSIM je uspješno odradio, te se po tom pitanju ponašao isto kao i Wazuh. Logovi neuspješnih prijava su se pojavljivali, ali svaki puta sa većom razinom sigurnosne prijetnje. Jedina razlika kod ova dva alata prilikom ovog testa bila je u načinu obavještavanja korisnika. OSSIM korisnika o prijetnji može obavijestiti samo putem web sučelja, dok Wazuh obavijest može poslati putem maila uz obavještavanje

korisnika u web sučelju. Posljednji test je test prepoznavanja ransomwarea, koji OSSIM nije uspješno odradio. OSSIM-u nedostaje mogućnost prepoznavanja integriteta datoteka bez instaliranja HIDS agenata na korisnička računala, te iz tog razloga nije uspješno prepoznao sigurnosnu prijetnju ransomware napada.

Iako OSSIM-u nedostaje nekoliko ključnih mogućnosti zaštite, oba sustava mogu spriječiti veliki broj sigurnosnih prijetnji, uz oba alata se svakako preporučuju dodatne mjere zaštite, jer ne posjeduju nikakve aktivne načine zaštite, već se oslanjaju na upozorenja korisnicima, koji dalje moraju otklanjati probleme.

6.7 Primjena

Iako oba alata imaju istu svrhu, njihova primjena znatno će se razlikovati. Alat se smatra boljim rješenjem za veća poduzeća ako posjeduje mogućnosti poput vertikalnog skaliranja, ako posjeduje sve bitne sigurnosne mogućnosti, također, alat mora biti fleksibilan i mora imati sposobnost aktivne zaštite uz pomoć postavljanja određenih pravila itd.

Wazuh je kompleksniji alat, čija je primjena najbolja za velika poduzeća, te je za uspješnu implementaciju Wazuha potrebno imati puno iskustva s radom na Linuxu. Bolja primjena u većim poduzećima je zbog omogućene vertikalne skalabilnosti, kao i zbog boljih načina zaštite nego kod OSSIM-a.

AlienVault OSSIM jako je dobar alat za početnike, koji se prvi puta susreću s Linuxom i sa SIEM alatima općenito. Njegova primjena nije primjerena za poduzeća, jer mu nedostaje nekoliko funkcija koje su poželjne u SIEM alatima, te ne nudi veliku razinu zaštite. OSSIM je jako dobar alat za početnike i mala poduzeća, te je odličan alat za testirati AlienVaultove proizvode, prije unapređenja na AlienVault USM, komercijalnu verziju AlienVaultovog SIEM-a. Jedina svrha OSSIM-a u poduzećima mogla bi biti kao alat koji služi za nadgledanje događaja na lokalnoj mreži, s obzirom da mogućnosti koje posjeduje više odgovaraju SIM alatu.

Tablica 1: Usporedba SIEM alata

	Wazuh	AlienVault OSSIM
Resursi	Minimalno: procesor sa 2 jezgre i 4GB RAM memorije	Minimalno: procesor sa 2 jezgre i 4GB RAM memorije
Implementacija	Instalacija unošenjem naredbi u Linux terminal	Jednostavna instalacija uz pomoć instalacijskog programa
Dodavanje uređaja	Potrebna instalacija agenta na korisnička računala	Uređaji se dodaju skeniranjem subneta lokalne mreže
Mogućnosti	Pregled događaja, prikaz ranjivosti, kreiranje pravila, detekcija „brute force“ napada, analiza korelacije događaja, nadziranje kršenja sigurnosne politike, nadgledanje integriteta datoteka, upravljanje zapisima	Pregled događaja, prikaz ranjivosti, kreiranje pravila, detekcija „brute force“ napada, analiza korelacije događaja
Prezentacija	Prikaz podataka uz pomoć raznih grafova i tablica, razne mogućnosti filtriranja, nedostatak nekih opcija u samom web sučelju	Prikaz podataka uz pomoć raznih grafova i tablica, razne mogućnosti filtriranja, Sve opcije dostupne u web sučelju
Zaštita	Uspješna detekcija svih napada koji su testirani u završnom radu	Neuspješna detekcija jednog od tri napada testiranih u završnom radu, zbog nedostatka HIDS agenata
Primjena	Prigodan za srednja i velika poduzeća zbog mogućnosti vertikalnog skaliranja i svih sigurnosnih mogućnosti	Prigodan za početnike i za korisnike koji razmatraju plaćeni softver AlienVault USM

Izvor: Autor

7. Zaključak

SIEM alati u današnjem svijetu informatike su prijeko potrebni, s obzirom na ogromnu količinu podataka koja se prikuplja. Ovi alati omogućuju bolju preglednost podataka, kao i pronalaženje prijetnji koje bi mogle naštetiti lokalnoj mreži. SIEM alati nude analizu sigurnosnih upozorenja svih uređaja i aplikacija koje se nalaze u lokalnoj mreži. SIEM je nastao spajanjem dva različita sustava, SIM i SEM. SIM alati koristili su se za prikupljanje zapisa sa računala lokalne mreže u centralno spremište, kako bi se mogla vršiti daljnja analiza trendova. SEM alati kao primarni fokus imaju nadziranje u stvarnom vremenu, analiza korelacije različitih događaja, te slanje obavijesti.

SIEM alati napredovali su kroz povijest. Najveći napredci su bili mogućnost horizontalnog skaliranja i dodavanje strojnog učenja.

Naj bitnije mogućnosti SIEM alata su upravljanje zapisima, što omogućuje prikupljanje i organizaciju podataka prikupljenih sa lokalne mreže, zatim je tu analiza korelacije, koja donosi prepoznavanje potencijalne prijetnje ukoliko su zadovoljeni parametri koji su u prijašnjim situacijama dovodili do prijetnji. Integracijom baze podataka sigurnosnih prijetnji u SIEM alatu se dobiva povećana mogućnost zaštite od otprije poznatih prijetnji. Kako bi korisnik znao da je alat našao prijetnju, SIEM alati imaju i mogućnost sigurnosnih upozorenja, odnosno poruka koje može slati putem web sučelja, na mail adresu, itd. Kako bi korisnik imao dobar uvid u hrpu nepreglednih podataka, SIEM alati su razvili i prezentaciju izvještaja, odnosno oku ugodan prikaz svih relevantnih podataka, kroz grafove i tablice. Donedavno najveća mana SIEM alata bila je nemogućnost prepoznavanja prijetnji izvan baze podataka poznatih prijetnji, stoga je implementirano i strojno učenje, koje bi trebalo smanjiti broj nepoznatih prijetnji.

U ovom završnom radu radila se usporedba između dva SIEM alata, Wazuha i AlienVault OSSIM-a. Wazuh je alat otvorenog koda te se osim za SIEM, može koristiti i kao HIDS sustav. Za pokretanje ovog alata, potrebno je instalirati sve komponente Elasticstacka .Wazuh je modificirana verzija drugog SIEM alata, OSSEC-a. AlienVault OSSIM je alat otvorenog koda. OSSIM je baziran na Debianu, operacijskom sustavu baziranom na Linux kernelu, te je dodatno

promijenjen kako bi se korisniku ponudila što lakša implementacija i instalacija alata na lokalnu mrežu. Ovaj alat koristi dodatne alate za uspješno obavljanje zadataka poput Snorta, kasnije zamijenjenog Suricatom, Munina, Nagiosa itd.

Odrađena je instalacija oba alata, te njihovo konfiguriranje, kao i testiranje rada samih alata. Oba alata uspješno su instalirana, te je bilo moguće prikupiti podatke sa lokalne mreže.

Usporedbom alata zaključeno je kako su oba alata sposobna obavljati dužnosti SIEM alata, uz neke nedostatke.

Wazuh posjeduje više i bolje mogućnosti, ali je njegova mana ta što je iznimno kompliciran za korištenje, te je njegova instalacija poprilično zahtjevna za odraditi. Preporučuje se za korištenje u većim poduzećima, zbog mogućnosti horizontalne skalabilnosti i zbog odličnih mjera zaštite koje posjeduje, Kako bi se iskoristio maksimalni potencijal Wazuha, potrebno je imati puno prijašnjeg iskustva sa radom na SIEM alatima i Linux serverima.

AlienVault OSSIM ne posjeduje sve mogućnosti koje posjeduje Wazuh, ali je vrlo jednostavan za korištenje i implementaciju. Ne preporučuje se njegovo korištenje u većim poduzećima jer ga nije moguće skalirati horizontalno, te je njegov rad ograničen na samo jedan server. Ne postoji mogućnost aktivne zaštite. Također, baza podataka prijašnjih prijetnji koju koristi se popunjava od strane korisnika, što može dovesti do određenih propusta. Ovo je sve napravljeno jer je OSSIM zapravo verzija otvorenog koda drugog softvera, USM-a, koji se mora licencirati kako bi se upotrebljavao.

POPIS LITERATURE

1. AlienVault OTX: https://otx.alienvault.com/?provider=google#socialSignup
2. AlienVault OSSIM: https://cybersecurity.att.com/products/ossim
3. Amritw: The Future of SIEM – The market will begin to diverge: https://techbuddha.wordpress.com/2007/01/01/the-future-of-siem-%E2%80%93-the-market-will-begin-to-diverge/
4. Awati Rahul: Security Information Management (SIM): https://www.techtarget.com/searchsecurity/definition/security-information-management-SIM
5. Barmak Meftah: AT&T Cybersecurity Is Born: https://cybersecurity.att.com/blogs/security-essentials/att-cybersecurity-is-born
6. Bassett Santiago, Pauette Mike: Improve Security Analytics with the Elastic Stack, Wazuh, and IDS: https://www.elastic.co/blog/improve-security-analytics-with-the-elastic-stack-wazuh-and-ids
7. Canner Ben: 7 Key SIEM Capabilities to Look For in Your Solution: https://solutionsreview.com/security-information-event-management/7-key-siem-capabilities-look-solution/
8. Canner Ben: 6 Questions About Machine Learning in SIEM (Answered!) : https://solutionsreview.com/security-information-event-management/6-questions-about-machine-learning-in-siem-answered/
9. Elasticstack: What is the ELK Stack? Why, it's the Elastic Stack: https://www.elastic.co/what-is/elk-stack
10. Gailey Stephen: A Brief History of SIEM : https://cybersecurity-magazine.com/a-brief-history-of-siem/
11. Jamil Amir: The difference between SEM, SIM and SIEM: https://www.gmdit.com/NewsView.aspx?ID=9IfB2Axzeew=
    (Datum pristupa: 10.5.2022.)

12. Johnson Arnold, Dempsey Kelley, Ross Ron, Gupta Sabari, Bailey Dennis: Guide for Seucirty-Focused Configuration Management of Inromation Systems: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf
13. Kent Karen, Souppaya Murugiah : Guide to Computer Security Log Management: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf
14. Linares Jesus; Preventing and detecting ransomware with Wazuh: https://wazuh.com/blog/preventing-and-detecting-ransomware-with-wazuh/
15. Logisign Team: Evolution of SIEM Over the Years : https://www.logsign.com/blog/evolution-of-siem-over-the-years/
16. ManageEngine: What is event correlation?: https://www.manageengine.com/log-management/siem/static-dynamic-event-correlation.html
17. Nguyen Tho: 5 Open Source SIEM Solutions: https://www.mezmo.com/blog/open-source-siem-tools
18. Peikari Cyrus, Chuvakin Anton: Security Warrior: Know Your Enemy: https://books.google.hr/books?id=LILroPpCP0cC&q=Security+Warrior&redir_esc=y#v=onepage&q&f=false6.
19. Priyanka R: Wazuh – Open Source Host and Endpoint Security: https://cybersafe.news/wazuh-open-source-host-and-endpoint-security/
20. Wazuh Installation guide: https://documentation.wazuh.com/current/installation-guide/index.html

POPIS POKRATA

SIEM - Security Information and Event Management

SIM - Security Information Management

SEM – Security Event Management

RMF - Risk management framework

IP – Internet protocol

IT – Information technology

IBM – International Buisness Machines

HIDS – Host-based intrusion detection system

SAD – Sjedinjene Američke Države

ELK – Elasticsearch, Logstash, Kibana

JSON – JavaScript Object Notation

GDPR – General Data Protection Regulation

MITRE ATT&CK - MITRE Adversarial Tactics, Techniques, and Common Knowledge

OSSIM – Open source Security Information Management

USM – Unified Security Management

AT&T - American Telephone and Telegraph Company

OTX - Open Threat Exchange

ISO - International Organization for Standardization

USB – Universal Serial Bus

RAM – Random Access Memory

OSSEC – Open Source HIDS SECurity

SQL – Structured Query Language

GB - Gigabajt

UX – User experience

POPIS SLIKA

POPIS TABLICA