Analiza svojstava sustava za upravljanje sigurnosnim informacijama i događajima

Penga, Ivan

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Ivan Penga

ANALIZA SVOJSTAVA SUSTAVA ZA UPRAVLJANJE SIGURNOSNIM INFORMACIJAMA I DOGAĐAJIMA

DIPLOMSKI RAD

Varaždin, 2019.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Ivan Penga

Matični broj: 46428/17-R

Studij: Informacijsko i programsko inženjerstvo

ANALIZA SVOJSTAVA SUSTAVA ZA UPRAVLJANJE SIGURNOSNIM INFORMACIJAMA I DOGAĐAJIMA

DIPLOMSKI RAD

Mentor:

Dr. sc. Mario Žgela

Varaždin, rujan 2019.

Ivan Penga

Izjava o izvornosti

Izjavljujem da je moj završni/diplomski rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor/Autorica potvrdio/potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

Sažetak

Koncept upravljanja sigurnosnim informacijama i događajima odnosi se na procese prikupljanja, obrade, korelacije, analize i vizualizacije događaja sigurnosnog informacijskog sustava. Automatizacijom sigurnosnih procesa mogu se postići znatni napredci u kontroli i viziji sustava kao cjeline za razliku od tradicionalnog sustava decentraliziranog prikupljanja događaja. Temeljna ideja ovoga rada je opisati važnost upravljanja sigurnosnim događajima i problematiku implementacije sigurnosnih sustava te prikazati svojstva SIEM (eng. *Security Information and Event Management*) sustava.

Ključne riječi: sigurnosni događaj, SIEM, korelacija, centralizirano prikupljanje događaja, Syslog, analiza događaja

Sadržaj

1. Uvod

U poslovnom okruženju informacije predstavljaju važan resurs te kao takve moraju biti zaštićene. Informacije se nalaze u svakom poslovnom području i na svakoj hijerarhijskoj razini, od uprave sve do operativne razine. Kako bi se zaštitio ovaj vrijedni resurs, nužno je implementirati niz sigurnosnih mehanizama kako bi se ublažili ili eliminirali potencijalni rizici te optimiziralo poslovanje.

Implementacija sigurnosnih kontrola nije nimalo lak zadatak. Golema količina informacija otežava mogućnost promptne reakcije na individualna upozorenja s različitih uređaja, platformi i aplikacija ili na čekanje sigurnosnog agenta na obavijest o promjeni stanja u sustavu. S druge strane, a s obzirom na poslovne modele koji često funkcioniraju na principu 24/7 i moraju osigurati permanentnu dostupnost usluga, vrlo često se očekuje reakcija na prijetnje u stvarnom vremenu. Prema tome, danas je više nego ikad važno prikupljati i korelirati kritične informacije cijelog informacijskog sustava kako bi se identificiralo, evaluiralo i pravovremeno reagiralo na incidente i prijetnje. Pohranjeni podaci sigurnosnih dnevnika zapisa su krucijalni za rekonstrukciju slijeda događaja prilikom istrage sigurnosnog incidenta te također mogu poslužiti za identifikaciju uzroka problema.

Velika količina sigurnosnih podataka prikupljenih iz raznih dijelova informacijskog sustava nije pogodna za manualnu obradu čime ne može izvršiti validna analiza, koja u konačnici može sugerirati na donošenje pogrešnih odluka. Sustav za upravljanje sigurnosnim informacijama i događajima (SIEM) predstavlja kompleksni skup tehnologija dizajniranih s namjerom da pruže jasnu viziju na sustav informacijske tehnologije u cijelosti. Kao takav, postaje snažan dio sigurnosne infrastrukture malim, srednjim ili velikim poduzećima. Centraliziranom pohranom svih mrežnih podataka, SIEM formira znanje o kontekstu poslovanja čime pomaže ne samo prikupljanju, nego i povezivanju informacija kako bi se sagledala kompletna slika sustava.

1.1. Važnost događaja

Korištenje softvera ne zasniva se samo na povjerenju. Organizacije koje pružaju usluge korisnicima pomoću informacijske tehnologije moraju biti svjesne kako svaka aktivnost korisnika, zaposlenika ili samog softvera bila namjerna ili ne u jednom trenutku može eskalirati i izazvati incident.

Ako nije poznato kakve radnje se odvijaju u informacijskom sustavu, nije moguće niti reagirati. Također, kod nastanka proboja, nemoguće je izvršiti forenziku i ustanoviti razlog nastanka problema ako se nije bilježila aktivnost rada sustava. To je formula koja jamči da će incident ponovno uslijediti, a kad uslijedi, neće biti moguće poduzeti pravovremene akcije.

Svaki događaj dio je velike slike koja predstavlja ponašanje sustava. Veliki broj događaja stvara jasniju sliku o sustavu te pruža informativnu analizu. Nasuprot tome, velika količina neispravno protumačenih događaja može stvoriti pogrešne predodžbe. Mnogo događaja koji se pogrešno interpretiraju mogu upozoriti na pogreške u sustavu koje ne postoje te prema tome ukazati na nepostojeću opasnost. Stoga je bitno korelirati što veći broj događaja kako bi se izbjegle zamke u donošenju odluka prilikom reakcije na moguće incidente.

2. Sigurnost informacijskog sustava

Sigurnost poslovanja postaje sve važnija karakteristika informacijskog i računalnog sustava. S razvojem tehnologije, odnosno novih oblika poslovanja i tehnoloških rješenja te porastom broja korisnika povećava se količina informacija koje se obrađuju. Informacije je potrebno zaštiti kako bi njihov integritet ostao sačuvan i kako bi bile dostupne samo ovlaštenim osobama. Iz navedenih razloga potrebno je razviti mehanizme koji sprječavaju zlonamjerne napade na informacijski sustav i ispunjavaju sigurnosne zahtjeve.

Napad na informacijski sustav može se definirati kao svaki namjerni pokušaj da se informacije neovlašteno čitaju, modificiraju, uklone ili da se ugrozi njihova raspoloživost. Prijetnje postoje otkad postoje i računalni sustavi, a računalni napadi iz dana u dan postaju sve sofisticiraniji. Napredne metode zaštite su potaknule nastanak novih, učinkovitijih i kreativnijih tehnika koje potencijalno mogu ugroziti sigurnost informacijskih sustava.

2.1. Osnovni sigurnosni zahtjevi

S ciljem zaštite informacija od mogućih napada i osiguranja nesmetanog rada korisnika, potrebno je jasno definirati osnovne sigurnosne zahtjeve:

1. Tajnost – informacije u sustavu smiju biti pristupačne samo ovlaštenim korisnicima (Budin, Golub, Jakobović i Jelenković, 2010). Kao važan sigurnosni zahtjev, tajnost ograničava pristup resursima poduzeća samo uz autoriziranu dozvolu dodijeljenu privilegiranim korisnicima.
2. Dostupnost – informacije moraju biti dostupne korisnicima u svakom trenutku. Osnovna karakteristika dostupnosti je osigurati neprekidan pristup informacijama visoke važnosti. Kontinuiran pristup informacijama, primjerice u sustavu kontrole leta iznimno je bitan kako bi se u svakom trenutku mogla ustanoviti pozicija i smjer kretanja zrakoplova, čime se postiže adekvatna signalizacija s ciljem otklanjanja opasnosti i ublažavanja rizika.
3. Integritet – informacije mogu mijenjati samo ovlašteni korisnici kako bi se osigurala konzistentnost informacija kroz njihov životni ciklus. Integritet informacija se narušava ako ih je presreo i mijenjao napadač ili su nenamjerno promijenjene (od strane korisnika ili softvera).

2.2. Osnovne vrste ugrožavanja sigurnosti

Napad na informacijski sustav predstavlja sigurnosnu prijetnju koja uključuje maliciozne akcije poput prikupljanja, mijenjanja, uništavanja informacija ili sprečavanja pružanja usluge narušavanjem raspoloživosti. Cilj napada je zaobići sigurnosne mehanizme kako bi se navedene aktivnosti mogle realizirati. Sljedećim aktivnostima narušavaju se osnovni sigurnosni zahtjevi.

1. Prisluškivanje – smatra se napadom ako napadač neovlašteno pregledava podatke korisnika u sustavu ili čita poruke koje mu nisu namijenjene. Tajnost podataka može biti narušena ako između komunikacijskog kanala više korisnika stoji napadač koji prisluškuje podatke i može ih interpretirati ako podaci nisu kriptirani ili napadač posjeduje kriptografske ključeve kojima ih može dekriptirati. Tajnost se također može narušiti ako napadač uspije pristupiti neovlaštenim podacima (primjerice datotekama) te može pročitati njihov sadržaj.
2. Prekidanje – napad koji utječe na dostupnost podataka gdje napadač prekida komunikaciju između korisnika ili narušava dostupnost računalnih resursa, primjerice datoteka. Prekidanje ne mora nužno biti izazvano napadom. Također je moguće da se dostupnost ugrozi prirodnim nepogodama poput požara i poplava ili kvarom računalne opreme.
3. Promjena sadržaja podataka – narušava integritet podataka. Napadači mogu presresti poruke ili pristupiti neovlaštenim podacima te im mijenjati sadržaj. Promjenom sadržaja napadači se mogu lažno predstavljati u informacijskom sustavu. Ugrožavanje integriteta podataka također može biti izazvano od strane neispravnog softvera ili nevještih korisnika.

3. Događaji u informacijskom sustavu

Informacije su važan resurs svakog poduzeća. Relevantnije i novije informacije imaju veći značaj za organizaciju čime stvaraju dodatnu vrijednost pri poslovanju. Vrlo je važno imati kontrolu nad cijelim informacijskim sustavom kako bi se u svakom trenutku moglo zaključiti što se događa i u kojem smjeru poslovanje ide. Uvidom u ponašanje sustava moguće je predvidjeti probleme koji se u budućnosti mogu pojaviti i na vrijeme ih spriječiti. Na ovaj način se smanjuje mogućnost potencijalnih rizika s kojima se organizacija susreće. Buduće ponašanje sustava određuje trenutno stanje te svako prethodno stanje koje potencijalno može utjecati na daljnje ishode. Proučavanjem trenutnih i prošlih događaja smanjuju se potencijalni rizici, a moguće je optimizirati poslovanje, rast organizacije i dobit.

Izvršavanje zlonamjernih aktivnosti u računalnim sustavima postaje sve složenije i sofisticiranije. Prema tome, potrebno je obratiti pozornost na moguće propuste u sustavu kako bi se na vrijeme osigurali i poboljšali. Propuste mogu uzrokovati pogreške u samoj konfiguraciji, loš i nedovoljno testiran kod. Također, propusti mogu biti iskorišteni od strane nezadovoljnih zaposlenika.

Praćenje događaja ne mora nužno biti orijentirano na računalnu sigurnost. Događaji mogu ukazivati na probleme u brzini sustava, smanjenoj dostupnosti, potrošnji resursa i zadovoljstvu korisnika. Ovisno o ulozi softvera, različitim funkcijama se mogu dodijeliti različiti nadzorni mehanizmi koji su specifični za određeno područje djelovanja. Nemoguće je pratiti svaki nastali događaj pa se tako administratori sustava moraju odlučiti koji procesi će imati veći, a koji manji prioritet. Primjerice, u aplikacijama za upravljanje bankovnim računom preciznost i događaji o transakcijama će imati mnogo veći prioritet nego prikupljanje podataka o iskorištenju procesorske snage u pojedinom trenutku.

Prikupljanje svih događaja unutar informacijskog sustava nikad nije u potpunosti realizirano. Velika količina podataka prisiljava administratore sustava da odrede prioritete važnosti događaja kako bi se obrađivali relevantni podaci. Također, skaliranjem sustava vjerojatnost nastanka propusta raste. S druge strane, praktički je nemoguće analizirati svaki događaj i korelirati ga s ostalim događajima s kojima je povezan. U nadi da administratori pridobiju potrebne informacije kako bi stekli kvalitetan uvid u rad sustava, zaposlenika i korisnika pritom primajući samo korisne informacije nastali su Sustavi za upravljanje sigurnosnim informacijama i događajima, poznatiji pod akronimom – SIEM (Security Information and Event Management).

Prije zadiranja u tematiku SIEM sustava bitno je definirati i protumačiti pojmove vezane za sigurnost informacijskih sustava, nadzor i bilježenje podataka o računalnim aktivnostima.

1. Log sustav (eng. *log system*) – dnevnik zapisa aktivnosti nastalih na računalnom sustavu ili na mreži. Dnevnik zapisa sadrži podatke o događajima koji su nastali kao posljedica korisničke ili softverske aktivnosti koja se aktivno nadzire.
2. Događaj (eng. *event*) – svaka relevantna aktivnost nastala na računalnom sustavu ili na mreži. CorreLog (2015) navodi kako se zapisi razlikuju od događaja po četiri karakteristike:
    - Važnost – događaj je relevantan u sustavu. Što se češće događaj bilježi to je sve manje relevantniji.
    - Kontekst – događaj mora imati dovoljno konteksta kako bi se mogao protumačiti. Izjava: „nešto se dogodilo“ ne pruža adekvatne informacije o vrsti događaja niti vremenu nastanka, odnosno ne postoji kontekst iza navedene izjave.
    - Vrijeme – informacija mora biti određena konkretnom vremenskom oznakom. Jasnije definirano vrijeme nastanka zapisa pruža vrjedniju informaciju te se zapis može više smatrati događajem.
    - Mogućnost poduzimanja akcije – na svaki događaj mora se moći reagirati. Svakom događaju mora slijediti akcija: dodatno istraživanje o nastalom događaju ili korektivna akcija.

    Ako zapis u dnevniku događaja posjeduje navedene karakteristike, može se smatrati događajem. Svaki događaj je potencijalno značajan za organizaciju.
3. Sigurnosni događaj (eng. *security event*) – svaki događaj u informacijskom sustavu koji može utjecati na sigurnost sustava. Za razliku od običnog događaja, sigurnosni događaj je potrebno pomno istražiti i čim prije izvršiti preventivne akcije kako bi se smanjio potencijalni rizik od nastanka incidenta.
4. Incident (eng. *incident*) – svaki sigurnosni događaj koji ugrožava status informacijskog sustava.
5. Prijetnja (eng. *threat*) – svaka potencijalna akcija koja može naštetiti imovini (Kim i Solomon, 2018). Prijetnje se mogu kategorizirati u tri skupine – namjerne, slučajne i prirodne. Namjerne prijetnje smatraju se potencijalnim akcijama koje zlonamjerne osobe mogu upotrijebiti protiv sustava. Slučajne prijetnje izaziva nepouzdan softver ili neiskusno osoblje s većom razinom prava nego što bi trebali imati. Prirodne prijetnje odnose se na elementarne nepogodne poput poplava, požara i potresa.

6. Ranjivost (eng. *vulnerability*) – slabost sustava koja omogućava prijetnjama da se realiziraju ili da imaju utjecaj na imovinu poduzeća (Kim i Solomon, 2018). Ranjivost predstavlja slabu točku sustava koju napadač nastoji iskoristiti kako bi mogao izvršiti ilegalne aktivnosti na računalnom sustavu. *SQL injection* je primjer ranjivosti dok je otimanje osjetljivih podataka prijetnja. Ako se radi o vrlo osjetljivim podacima, ovaj primjer može se smatrati ranjivosti visokog rizika.
7. Proboj (eng. *breach*) – unatoč pokušajima da se informacijski sustav zaštiti, moguće je da se prijetnja ostvari. U tom trenutku može se reći da je nastao proboj. Svaki događaj koji rezultira kršenjem tajnosti, integriteta ili dostupnosti smatra se sigurnosnim probojem (Kim i Solomon, 2018). Proboj može ali i ne mora biti namjerno izazvan. Aktivnosti koje mogu uzrokovati oštećenje imovine mogu biti:
    - DoS (eng. *Denial of Service*) napadi – uskraćivanje dostupnosti uzastopnim slanjem zahtjeva ili poruka prema poslužitelju
    - Prisluškivanje – čitanje podataka između dvije strane unutar komunikacijskog kanala između dvije ili više osoba
    - (Ne)namjerno brisanje podataka – uništavanje ili mijenjanje podataka koji su od važnosti organizaciji

4. Sigurnosni log

Sistemski sigurnosni log sustavi važan su dio svakog informacijskog sustava. Osim pohrane podataka o događajima poput aktivnosti korisnika ili promjeni stanja sustava, ovi sustavi pružaju vrijedne forenzičke dokaze koji služe za rekonstrukciju događaja koji su uslijedili. Uvid u povijest događaja nastalih u konkretnom vremenskom periodu sigurnosnom osoblju poduzeća pruža mogućnost kvalitetnog zaključivanja o djelovanju sustava čime se može uočiti nepravilnost u samom radu sustava. Podaci mogu na ukazati na maliciozne aktivnosti napadača tijekom ili nakon napada. Log sustavi često akumuliraju velik broj podataka koje se zapisuju u bazu podatka ili u datoteke različitih formata zapisa.

4.1. Zaštita sigurnosnog loga

Osjetljivi podaci pomoću kojih se može dokazati povijest zlonamjernih aktivnosti često su meta napadača koji nastoje prikriti tragove napada. Sigurnosni log smatra se pouzdanim izvorom informacija pa je vrlo važno omogućiti konstantan pristup kako bi se mogli pratiti svi relevantni događaji na kojima se može vjerovati. Nezaštićen sigurnosni log sustav predstavlja ranjivu točku informacijskog sustava. Log sustav često je primarna meta napadača jer sadrži niz izvršenih aktivnosti koje mogu pružiti kao dokazni materijal. Modificiranjem, brisanjem ili prekidanjem rada sustava napadač može prikriti vlastito djelovanje kako bi zadržao anonimnost. Bez dokaza je nemoguće identificirati identitet napadača te procjena štete nastale u sustavu postaje vrlo složena. Iz navedenih razloga potrebno je obratiti pažnju da su informacije zaštićene. Također je potrebno posvetiti pozornost na veličinu log datoteka. Ako ponestane prostora za zapisivanje podataka, moguće je da se podaci prestanu zapisivati ili da se zapisuju jedni preko drugih.

Jedan od načina provjere konzistentnosti podataka u log sustavu je provjera integriteta. Svakom zapisu ili datoteci se izračuna sažetak (eng. *hash*) te se spremi na sigurno mjesto. Ako nastane promjena na zapisu, odnosno datoteci, novoizračunati sažetak se neće podudarati s originalnim sažetkom te se može zaključiti kako je zapis modificiran.

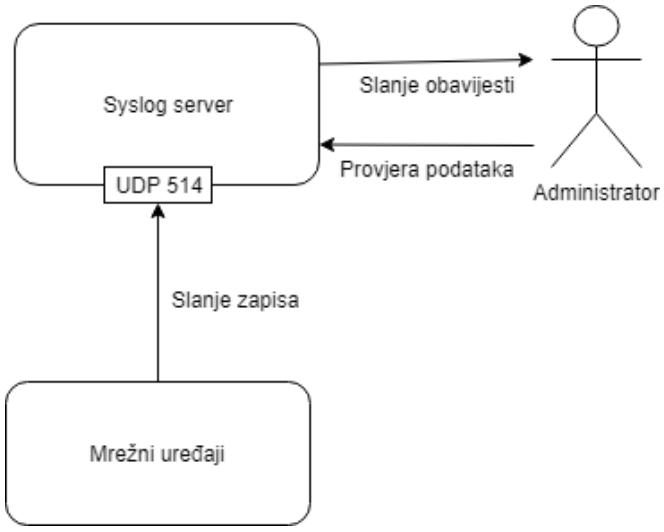
4.2. Syslog

Softver je često dizajniran da pruža informacije o vlastitom izvršavanju. Promjene stanja mogu ukazati na početak i završetak izvršavanja operacija, dostizanje određene točke izvođenja

ili na sam status aktivnosti. U svrhu izvještavanja i praćenja događaja softver posjeduje vlastito rješenje zapisa ili koristi specijaliziran sustav za prikupljanje događaja s više različitih izvora (Parker, 2016).

Syslog (System Logging Protocol) je standard generiranja, pohranjivanja i slanja log podataka i događaja iz različitih operacijskih sustava poput Linuxa i Unixa ili uređaja kao što su usmjerivači (eng. *router*) i vatrozidi (eng *firewall*) centraliziranom log sustavu. Podržan je na širokom rasponu uređaja te može rukovati različitim vrstama događaja. Primjerice usmjerivač može slati poruke o odbijenim paketima dok web poslužitelj može slati podatke o pokušajima autentikacije. Nastao je u ranim 1980 godinama kao podrška logiranju Unix sustavima nakon čega se proširio i na ostale operacijske sustave i uređaje (Cox, 2019).

Syslog server izgrađen je od više komponenti koje međusobno komuniciraju u svrhu prikupljanja i obrade podataka. Syslog „slušač“ (eng. *listener*) služi za primanje poruka koje se izmjenjuju unutar mreže. Za komunikaciju se primarno koristi UDP (User Datagram Protocol) protokol na portu 514 dok se mogu koristiti i ostali protokoli poput TCP-a (Transmission Control Protocol) i HTTP-a (Hypertext Transfer Protocol). Velika količina generiranih podataka zahtijeva i bazu podataka u svrhu brze pohrane i dohvaćanja zapisa. Syslog server također posjeduje sustav za filtriranje i menadžment podataka kako bi u velikoj količini podataka pronašao potrebne informacije te mogao generirati obavijesti i upozorenja kao odgovor na zadane događaje.



Slika 1. Jednostavna shema toka podataka (autorski rad)

Svaka sistemska poruka koja se bilježi mora proći kroz konfiguraciju Sysloga kako bi se ustanovio koja akcija će se izvršiti. Konfiguracija sadrži nazive objekata (eng. *facility*) i prioritete (eng. *priority*), u kombinaciji zvanim selektorima. Naziv objekta specificira koji

sistemski program će generirati poruku dok se prioritetom određuje razina važnosti. Tablica 1 prikazuje popis nekoliko standardnih objekata korištenih u konfiguraciji Sysloga dok tablica 2 prikazuje prioritete sortirane prema važnosti koji im se mogu dodijeliti.

Tablica 1. Standardni objekti Syslog-a

Vrijednost	Objekt	Opis
0	kern	Poruke jezgre operacijskog sustava
1	user	Generične poruke korisnika
2	mail	Poruke podsustava e-pošte
3	daemon	Poruke pozadinskih procesa
4	auth/authpriv	Sigurnosne i autorizacijske poruke
5	syslog	Poruke sysloga
16 - 23	local0 - local7	Rezervirano za lokalnu upotrebu

Tablica 2. Prioriteti Syslog-a sortirani prema važnosti

Vrijednost	Prioritet	Opis
0	emerg	Opasnost
1	alert	Uzbuna
2	crit	Kritično
3	err	Pogreška
4	warning	Upozorenje
5	notice	Obavijest
6	info	Informacija
7	debug	Poruke kod uklanjanja pogrešaka

Uz svaki selektor nalazi se akcija koja će se izvršiti kad sustav primi poruku. Svakom selektoru može se dodijeliti samo jedna akcija. Na primjeru se nalazi nekoliko akcija koje se mogu dodijeliti selektorima.

Tablica 3. Syslog akcije

Akcija	Opis
/dev/console	Ispis poruka na konzolu
/var/log/messages.log	Pohrana poruke u messages.log datoteku
@adresa:port	Slanje poruke putem UDP protokola
@@adresa:port	Slanje poruke putem TCP protokola
|program	Slanje poruka zadanom programu

Dodjelom akcija selektoru postavlja se pravilo unutar Syslog konfiguracije. Kombinacijom objekata i prioriteta administratori sustava mogu organizirati događaje prema vrsti i važnosti te ih pohraniti ili poslati centralnom kolektoru događaja. Na slijedećem primjeru nalaze se primjeri pravila Syslog konfiguracije.

Tablica 4. Primjeri pravila Syslog konfiguracije

Selektor	Akcija
mail.info	/var/log/mail.info
mail.err	/var/log/mail.err
mail.warn	/var/log/mail.warn
kern.*	@192.168.1.50:514
.	:omusrmsg:*
*.emerg	@@192.168.1.51:1234

U nastavku slijedi pojašnjenje akcija s pripadajućim selektorima iz tablice 4:

- *mail.info* */var/log/mail.info*
  Informativne obavijesti podsustava e-pošte pohrani u datoteku s putanjom /var/log/mail.info
- *mail.err* */var/log/mail.err*
  Obavijesti o pogreškama podsustava e-pošte pohrani u datoteku s putanjom /var/log/mail.err
- *mail.warn* */var/log/mail.warn*
  Upozorenja podsustava e-pošte pohrani u datoteku s putanjom /var/log/mail.warn
- *kern.** *@192.168.1.50:514*
  Poruke jezgre operacijskog sustava svih prioriteta pošalji UDP protokolom na IP adresu 192.168.1.50:514
- **.** *:omusrmsg:**
  Poruke svih programa i prioriteta pošalji na zaslon prijavljenih korisnika
- **.emerg* *@@192.168.1.51:1234*
  Poruke svih programa s prioritetom opasnosti pošalji TCP protokolom na IP adresu 192.168.1.51:1234

U notaciji Sysloga simbol zvjezdice (*) kao objekata ili prioriteta obilježava sve elemente. Prema tome, selektor *kern.** obilježiti će sve prioritete jezgrinih poruka. Selektor *mail.warn* definira sve poruke mail podsustava sa prioritetom *warn* i sve poruke višeg prioriteta.

Tehnikom rotacije datoteka postiže se promjena mjesta zapisivanja kako datoteke ne bi zauzimale previše memorijskog prostora te kako bi se lakše obrađivale. Ako se uspostavi dnevna rotacija, svaka 24 sata će se kreirati nova datoteka sa zapisima za taj dan.

Zapis obavijesti na sučelje korisnika pruža mogućnost izvještavanja u stvarnom vremenu. Ova vrsta izvještavanja može biti od značaja porukama visokog prioriteta koje ukazuju na hitno poduzimanje akcija. Velika količina poruka na sučelju može ometati rad

administratora te dovesti do propusta bitnih događaja pa je potrebno uzeti u obzir da se samo rijetka i hitna upozorenja pojave na korisničkim sučeljima.

Pohrana događaja u datoteku pruža trajan zapis događaja koji se jednostavno mogu pregledati i raščlaniti. Ovaj pristup uklanja mogućnost obavještavanja u stvarnom vremenu. Iako konfiguracija sustava dopušta pregled datoteka u kratkim intervalima, uvijek će postojati određeno kašnjenje.

Imenovani cjevovodi (eng. *named pipes*) dopuštaju prijenos podataka s jednog programa na drugi. Syslog može predati podatke jednom od postojećih programa koji ih zatim može pravilno raščlaniti, reducirati ili obogatiti. Veći broj korištenih aplikacija može doprinijeti većoj fleksibilnosti log sustava.

Slanje podataka udaljenom računalu idealan je pristup za rad s centraliziranim poslužiteljem. Kod odabira UDP protokola za prijenos zapisa prema poslužitelju bitno je napomenuti kako protokol nije pouzdan te može izazvati gubitak podataka. Ako su podaci osjetljivog karaktera može se upotrijebiti konekcijski protokol s provjerom ispravnosti primljenih podataka poput TCP-a. Syslog mrežni paket sastoji se od tri dijela – zaglavlja, tijela te važnosti događaja (Parker, 2016). Vrijednost prioriteta računa se prema formuli:

$$važnost\ događaja = vrijednost\ objekta * 8 + prioritet$$

Formula 1. Važnost Syslog događaja (Lonvick, 2001)

Vrijednost važnosti događaja smješten je unutar šiljastih zagrada te se nalazi na samom početku poruke. Primjerice, prioritet selektora *user.alert* imati će važnost 1 * 8 + 2 = 10. Manja vrijednost važnosti događaja ukazuje na veću razinu opasnosti. Zaglavlje poruke sadrži vremensku oznaku generiranja događaja. Vrijeme se može razlikovati od uređaja do uređaja pa je potrebno obratiti pozornost na vremensku sinkronizaciju svih uređaja. Osim vremenske oznake zaglavlje sadrži i ime ili IP adresu poslužitelja (Parker, 2016). Tijelo poruke sastavljeno je od dva polja – oznake i sadržaja. Oznaka predstavlja proces ili program koji je generirao događaj dok se u sadržaju nalaze svi dodatni podaci koji se smatraju relevantnima. Primjer prikazuje UDP poruku generiranu putem Syslog-a na platformi Raspberry Pi.

<2>Aug 25 12:29:43 localhost kernel: [128.953206] Under-voltage detected! (0x00050005)

Poslužitelj *localhost* generirao je događaj jezgre operacijskog sustava u 12 sati i 29 minuta. Važnost događaja označena je brojem 2 čime se upozorava na značajan događaj. Sadržaj poruke

upućuje kako je na platformi uslijedio pad napona. Na slijedećem primjeru su prikazani događaji SSH (Secure Shell) pozadinskog procesa generirani na Raspberry Pi platformi.

<158>Aug 25 12:28:52 localhost sshd[1260]: Failed password for pi from 192.168.1.100 port 18319 ssh2
<158>Aug 25 12:29:04 localhost sshd[1260]: Accepted password for pi from 192.168.1.100 port 18319 ssh2

Syslog je generirao događaj pozadinskog procesa *sshd* – zabilježena je neuspješna prijava s IP adrese 192.168.1.100 s korisničkim imenom „*pi*“. Nekoliko sekundi nakon događaja zabilježena je uspješna prijava u sustav. Syslog je ovu vrstu događaja postavio važnost vrijednosti 158. Prema formuli za izračun važnosti događaja, može se zaključiti kako objekt događaja postavljen na *local3*, vrijednosti 19, dok je prioritet informativan (*info*) s vrijednosti 6.

4.3. Problematika prikupljanja podataka

Prikupljanje relevantnih događaja u organizaciji se odvija putem više različitih platformi. Specifične funkcije karakteristične su za svaku zasebnu platformu te prema tome generiraju različite vrste događaja. Velik raspon različitih događaja organizaciju suočava sa slijedećim problemima (Kent i Souppaya, 2006):

1. Mnogo različitih izvora podataka

   Informacijski sustav posjeduje podsustave zadužene za prikupljanje podataka o izvođenju određenih procesa. Velik broj podsustava može uzrokovati probleme prilikom usklađivanja i pronalaska svih dijelova sustava.

2. Nekonzistentnost podataka

   Log sustavi prikupljaju podatke specifične za platformu na kojoj se nalaze. Tako se primjerice u sustavima gdje se odvija mrežna aktivnost mogu pronaći podaci o IP adresama, protokolima i vremenu prijave u sustav, dok se u operacijskom sustavu mogu pronaći podaci o aktivnostima vezane za rad procesora, upravljanje datotekama i raspoloživosti radne memorije. Nekonzistentnost podataka različitih log sustava može izazvati poteškoće prilikom povezivanja događa zbog manjka zajedničkih atributa. Problem reprezentacije podataka također može uzrokovati nekonzistentnost prilikom navođenja korištene tehnologije. Primjerice, protokol SSH (eng. *Secure Shell*) u jednom log sustavu može biti zabilježen kao „SSH“ dok se u drugom može označiti brojem porta (22).

3. Različite vremenske oznake

   Vrlo važna stavka log sustava je zapisati vrijeme kad je nastala određena aktivnost. Sustavi mogu biti raspodijeljeni po različitim državama pa je potrebno obratiti dodatnu pozornost na vremenske zone te format zapisa vremena.

4. Različiti formati zapisa događaja

   Podaci o izvršenim aktivnostima zapisuju se u različitim formatima poput XML-a, JSON-a, baza podataka, binarnih datoteka i sličnih. Pojedini log sustavi zapisuju podatke u čitljivom obliku, dok drugi koriste specijalne oblike zapisa poput binarnih datoteka, različito kodiranih ili kompresiranih datoteka.

4.4. Vrste događaja

Bitna odrednica zapisanog događaja je u tome da je zapis pravilno generiran te da se može protumačiti kako bi se mogao analizirati. Također je važno da se log jednostavno može

prenijeti na drugu platformu, odnosno da zauzima što manje memorije kako bi sačuvao što više diskovnog prostora ili što manje opteretio mrežni promet. Pretvaranje loga u ljudima čitljiv oblik bitan je tek u onom trenu kad za to dođe vrijeme. No, zapisi u log sustavima također često mogu biti bar donekle čitljivi, ali im često fali kontekst i povezanost s ostalim događajima koje ih čine razumljivima.

Vrste događaja razlikuju se s platformom na kojoj se nalaze no mogu se kategorizirati i u određene skupine. Prijave i odjave u sustav su događaji koji upućuju na aktivnost korisnika u zadanom vremenskom periodu. Prijava korisnika u sustav povećava rizik od nastanka incidenta, iako incident ne mora nužno uslijediti. Svakom prijavom korisniku se dodjeljuje određen stupanj pristupa računalnim resursima koji mu stoje na raspolaganju. Od trenutka prijave može se očekivati izvršavanje akcija u sustavu. Premda se velik broj prijava smatra bezazlenim, to ne mora biti slučaj. Prijave s računala koje ne odgovaraju standardnom uzorku podižu razinu sumnje prema navedenom korisniku. Ako se vrijeme prijave ili IP adresa računala ne poklapaju s uobičajenim, potrebno je obratiti dodatnu pozornost na nastali događaj.

Operacije rada nad objektima sustava, poznatije pod akronimom CRUD (eng. *Create-Read-Update-Delete*) su standardne operacije koje mogu posjedovati razne platforme poput baze podataka ili operacijskog sustava. U primjeru baze podataka navedene operacije odnositi će se nad rad s upitima, odnosno s podacima koji su zapisani u tabličnom ili nekom drugom formatu specifičnom za bazu podataka. CRUD operacije mogu biti iznimno opasne ako se radi o osjetljivim podacima. Pravilno definirana razina prava korisnika prilikom izvršavanja CRUD operacija ključ su uspjeha smanjenja rizika nastanka potencijalnih sigurnosnih događaja.

Mrežni zahtjevi obuhvaćaju širok pojam i mogu djelovati kroz razne komponente informacijskog sustava. Usprkos njihovoj rasprostranjenosti, svaki mrežni zahtjev mora proći kroz bar jedan od mrežnih uređaja koji služi kao posrednik u komunikaciji. Posrednici pri komunikaciji, primjerice usmjerivači, konstantno obrađuju vrlo velik broj zahtjeva koji moraju biti ispitani prije nego što se predaju slijedećoj sigurnosnoj razini. U svrhu obrane od neželjenog mrežnog prometa koriste se vatrozidi. Vatrozid je sustav mrežne sigurnosti koji nadgleda ulazni i izlazni mrežni promet prema zadanim sigurnosnim pravilima. Postavljanjem dobro osmišljenih pravila pridodaje se veća kontrola sustavu čime se smanjuje rizik nastanka incidenta i proboja. Na slijedećem primjeru prikazan je zapis generiran na ZTE usmjerniku.

0000-00-07T08:22:17 [Alert] firewall security alert! Remote (source) address:192.168.1.3,scan dest address:176.31.180.214,and source port:8621,dest port:53000

Zapis sadrži podatke o sigurnosnom upozorenju vatrozida. Osim navedene poruke, IP adresa i vremena nastanka zapisa ne postoje dodatni podaci koji bi točnije definirali upozorenje te administrator sustava ne može dijagnosticirati problem bez daljnje analize.

5. SIEM

Sigurnosna politika i poslovna pravila mnogih organizacija nalaže kako se sigurnosni događaji moraju nadzirati i analizirati kako bi se identificirali mogući problemi. Takvi podaci su često kritični za rekonstrukciju slijeda događaja koji su uslijedili prilikom ugrožavanja sigurnosti informacijskog sustava. Manualna analiza podataka nije praktična jer se često radi o enormno velikim količinama podataka koje treba provjeriti i korelirati s ostalim događajima. Ovu problematiku rješavaju SIEM sustavi pomoću automatske analize pritom generirajući smislene izvještaje i obavijesti o akcijama koje se mogu poduzeti.

Sigurnosna politika stvara doprinos administratorima sustava kako bi se definirale odgovornosti, potrebna razina, korištenje, prikupljanje i održavanje sistemskih zapisa. Tijekom incidenta administratori mogu koristiti sigurnosnu politiku kako bi identificirali kako i kome zapisi moraju biti dostavljeni (Eaton, 2003). U formalnom dokumentu RFC 3227, naslovljenom „Smjernice za prikupljanje i arhiviranje dokaza“ navodi se kakvi trebaju biti računalni dokazi (Brezinski i Killalea, 2002):

- Dopustivi – moraju biti usklađeni s određenim pravnim pravilima prije nego što se iznese pred sud
- Autentični – mora biti moguće pozitivno vezati dokazni materijal s incidentom
- Potpuni – mora biti moguće ispričati cijelu priču, a ne samo određenu perspektivu
- Pouzdani – ne smije postojati ništa što ukazuje na sumnju autentičnosti i istinitosti prikupljenog dokaznog materijala
- Vjerodostojni – moraju biti vjerodostojni i razumljivi od strane suda

Termin Sustava za upravljanje sigurnosnim informacijama i događajima poznatijeg pod akronimom SIEM nastao je 2005. godine kao odgovor na probleme u praćenju i izvještavanju o nastalim događajima (Exabeam, 2019). Prethodnici SIEM-a su SIM (Security Information Management) i SEM (Security Event Management) sustavi koji su djelovali na sličnim, ali opet različitim područjima. SIM sustavi su prva generacija složenih sustava izgrađenih na postojećim log sustavima koji su prikupljali događaje, kreirali izvještaje i analizu te pohranjivali podatke. S druge strane, SEM sustavi više pozornosti posvetili su sigurnosnim događajima, korelaciji i obavijestima generiranih na različitim platformama poput vatrozida, sustava za detekciju upada, raznim poslužiteljima i bazama podataka (Exabeam, 2019). Tada se pojavila potreba za kvalitetnom analizom i procesiranjem događaja pošto su razne platforme često

generirale prevelik broj obavijesti koje bi zagušile sustav i raspoloživo vrijeme administratora. Potreba za novim rješenjem koje će biti pouzdanije i koje će posjedovati sve funkcionalnosti postojećih rješenja bila je sve izraženija. U godinama koje su slijedile, proizvođači su ponudili novo rješenje koje će ujediniti SIM i SEM sustave. Takvi sustavi sposobni su agregirati različite vrste podataka i uspostaviti vezu između događaja što će smanjiti broj lažno pozitivnih rezultata.

Sigurnosni log SIEM sustava je izrađen s namjerom prikupljanja događaja s određene platforme, aplikacije ili sustava na centraliziranu lokaciju. Svaki zapis unutar loga sadrži informacije o događaju koji se dogodio u informacijskom sustavu. Rani log sustavi izrađeni su s namjerom kako bi se uočile i otklonile greške nastale u sustavu. Moderni log sustavi imaju mnogo veću ulogu – optimizirati sustav, pratiti aktivnosti korisnika i zlоćudne aktivnosti s namjerom ugrožavanja sustava.

Različite platforme generiraju različite događaje, prema tome, svaki log sustav se može znatno razlikovati. Primjerice logovi od mrežnih uređaja sadrže podatke o prometu i komunikaciji među korisnicima poput IP adresa, MAC adresa i poruka dok logovi sustava za upravljanje bazom podataka sadrže podatke o upitima, vremenu izvršavanja i korisnicima koji su ih izvršili.

Log sustavi pružaju dokaze o aktivnostima na računalnom sustavu ili među njima. U stanju su zapisati razne događaje stvorene na određenoj platformi – podatke o prijavama u sustav, brisanju podataka, izvršavanju upita, izvješća o pogreškama i tako dalje. Uvidom u zapisane podatke moguće je procijeniti kvalitetu rada sustava te potencijalne neželjene aktivnosti.

SIEM sustavi mogu pomoći organizaciji kod nadzora podataka u stvarnom vremenu kako bi se na vrijeme uočili sigurnosni incidenti. Jedinstven pogled na događaje stječe se korelacijom događaja iz različitih izvora podataka. Primjerice, SIEM sustav može analizirati podatke s vatrozida i baze podataka i uočiti smjer kretanja napada preko više različitih platformi, dok ostali sustavi često nadziru samo vlastito područje djelovanja. Exabeam navodi kako SIEM sustav može pomoći organizaciji koristeći navedene komponente i sposobnosti:

- Prikupljanje podataka – odnosi se na prikupljanje podataka s različitih platformi poput mrežne aktivnosti, sigurnosti, poslužitelja, baza podataka, aplikacija, anti-virusnih programa…
- Korelacija – povezuje događaje u složene i razumljive strukture koje zajedno predstavljaju značajan sigurnosni događaj, prijetnju ili ranjivost.

- Analiza i vizualizacija – SIEM sustav koristi statističke modele kako bi prezentirao podatke i povezao ih u smislenu cjelinu. Također se mogu uočiti anomalije u postojećim podacima i prikazati složeni podaci u obliku grafova ili različitih uzoraka kako bi zaposlenici mogli razmotriti stanje sustava.
- Obavijesti – nakon analize događaja i korelacije SIEM sustav može generirati obavijesti koje šalje sigurnosnom osoblju kako bi mogli u pravo vrijeme reagirati ili detaljnije proučiti poruku. Obavijesti se mogu slati putem e-pošte, SMS-a, instant poruka ili prikazom na zaslonu.
- Pohrana podataka – podaci se mogu dugotrajno pohraniti na različite medije kako bi se omogućila analiza, praćenje i korelacija zbog pravnih ili sigurnosnih razloga u budućnosti. Dugotrajna pohrana je iznimno važna ako se mora vršiti forenzika nad sustavom u kojem je nastao proboj.
- Traženje prijetnji – zaposlenici mogu izvršavati upite i pregledavati podatke da na vrijeme uoče moguće propuste u sustavu i na vrijeme ih ažuriraju.
- Integracija – SIEM se integrira s postojećim sigurnosnim rješenjima kako bi omogućio kvalitetniju analizu i pružio potrebne informacije ostalim dijelovima sustava.

5.1. Implementacija SIEM sustava

Planiranje i implementacija SIEM sustava zahtjeva detaljnu analizu čimbenika koje treba uzeti u obzir kako bi se projekt ostvario. Sustavi i uređaji na kojima će se bilježiti događaji uobičajeno spadaju u tri kategorije (Cater, 2009):

1. Sigurnosni sustavi obuhvaćaju sve sustave koji obavljaju zaštitne funkcije, primjerice anti-virusni softver, virtualna privatna mreža, vatrozidi, sustavi za detekciju i prevenciju upada, sustavi za autentikaciju i tako dalje.
2. Sustavi kritični za poslovanje sastoje se od svih sustava koji su bitni kako bi informacijski sustav funkcionirao. To su primjerice mrežni uređaji, DNS i web poslužitelji.
3. Sustavi kritični za infrastrukturu sustava također se odnose na sustave i uređaje ključne za ispravno funkcioniranje informacijskog sustava. Pri određivanju najkritičnijih dijelova sustava potrebno je sagledati kvalitetu funkcioniranja sustava dok je odabrana komponenta pod visokim opterećenjem ili je nedostupna.

Poduzeće koje uvodi SIEM sustav ima ograničene resurse te vrijeme s kojim raspolaže. S toga je bitno odrediti koji sustavi će imati viši, a koji manji prioritet prilikom nadziranja. Dodjela

prioriteta kritičnim sustavima zahtjeva utvrđivanje dijelova informacijskog sustava na kojima se nalaze kritične informacije od visoke važnosti. Javno dostupni sustavi, odnosno sustavi dostupni putem Interneta, smatraju se manje sigurnima te će imati viši prioritet od zatvorenih, privatnih sustava.

Pri odabiru komercijalnog sustava za upravljanje sigurnosnim informacijama i događajima važno je sagledati i usporediti više rješenja kako bi se odabrao proizvod koji najbolje odgovara potrebama poduzeća. Cater (2009) navodi kako osim cijene u obzir treba uzeti različite faktore prilikom evaluacije:

- SIEM mora podržavati sve vrste uređaja, softvera i operacijskih sustava koji se koriste u poslovanju organizacije
- Metode prikupljanja podataka moraju pravilno funkcionirati unutar poslovnog okruženja
- Korištenje ugrađenih i vlastitih napisanih korelacijskih pravila mora biti razumljivo i strukturirano
- Sustav za pohranu podataka mora biti dovoljno fleksibilan kako bi se svi podaci mogli pohraniti
- Performanse sustava moraju zadovoljavati zahtjeve kako bi SIEM mogao obraditi maksimalan broj podataka
- Skalabilnost sustava mora biti ostvarena kako bi se sustav mogao prilagoditi budućim zahtjevima
- Sigurnost sustava se mora prilagoditi sigurnosnoj politici
- Korisničko sučelje mora biti upotrebljivo, funkcionalno te programabilno
- Sustav mora posjedovati mogućnost integriranja s eksternim bazama podataka i sustavima

5.1.1. Utvrđivanje značajnih sigurnosnih događaja

Važnost pojedinih događaja ispituje se revizijom svih sustava koji će dostavljati podatke u centralni SIEM sustav. Ovim postupkom pridodaje se prioritet različitim uređajima ili softveru, odnosno dodjeljuje se viši ili niži značaj specifičnim događajima. Događaji koji se kontinuirano ponavljaju smatraju se manje značajnima za poduzeće. Primjerice, događaj koji se ponavlja nekoliko puta dnevno, ne može posjedovati kritične informacije za sustav. Vatrozid obrađuje velike količine mrežnih paketa te prema zadanim pravilima određuje koje pakete

propušta, a koje blokira. Definiranjem preciznih pravila vatrozida, osjetljivi sustavi se mogu međusobno izolirati prilikom čega se postiže generiranje manjeg broja sigurnosnih događaja. Kod forenzike sustava paketi koje su dospjeli u sustav imaju znatno veću važnost od blokiranih jer direktno utječu na sustav.

5.2. Prikupljanje događaja s različitih platformi

Informacijski sustav sastavljen je od mnogo različitih softverskih i hardverskih komponenti koje zajedno djeluju stvarajući vrijednost za korisnika. Svaka komponenta ima svoje odgovornosti te prema tome izvršava specifične zadatke i generira podatke o karakterističnim akcijama platforme. Baza podataka primjerice može generirati podatke o izvršenim upitima, dok operacijski sustav može generirati podatke o prijavi u sustav ili o radu nad datotečnim sustavom (brisanje, stvaranje ili modificiranje datoteka).

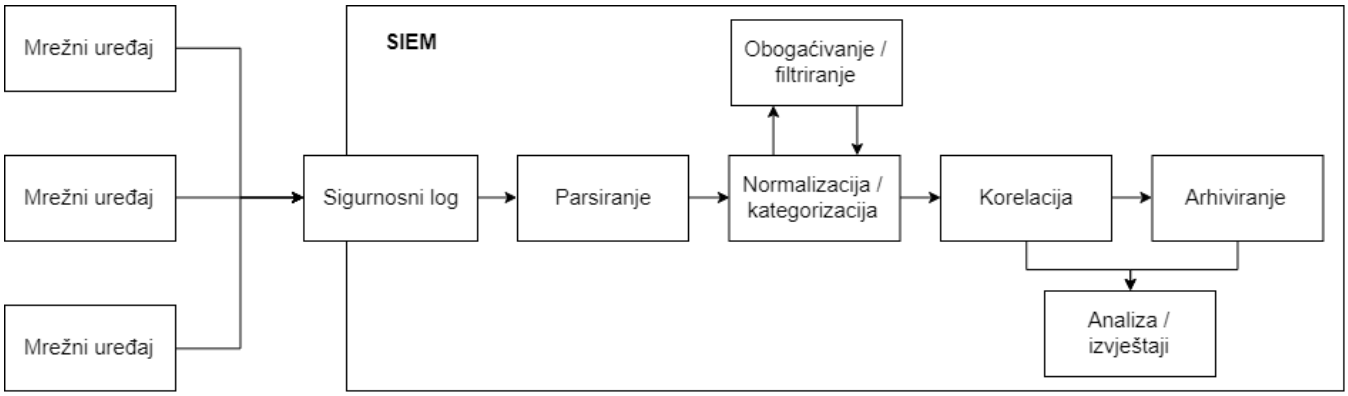
5.2.1. Metode prikupljanja podataka

U svrhu jednostavnije obrade podataka, podaci generirani od strane različitih platformi pohranjuju se u centraliziran sustav. SIEM sustavi najčešće koriste slijedeće metode kako bi obavile navedeni zadatak:

- Metodu slanja podataka (eng. *Push*) koriste platforme koje generiraju događaje te ih izravno šalju centraliziranom sustavu. Pristup je jednostavan za konfiguraciju te se podaci prenose u realnom vremenu. U trenutku nastanka događaja, platforma ga šalje centraliziranom SIEM sustavu. Ovaj pristup slanja podataka, naime dolazi s određenim manama. Kako se često koristi UDP protokol, podaci se mogu izgubiti pri prijenosu. Također, ako se izgubi veza između pošiljatelja i primatelja, podaci se nikad neće moći poslati. U slučaju napada na sustav, napadač može slati lažne podatke, te pritom generirati vrlo velike količine lažnih podatka koje mogu preopteretiti poslužitelja.
- Metodu dohvaćanja podataka (eng. *Pull*) koriste sustavi kako bi prikupili podatke s raznih platformi. Kako se podaci ne šalju izravno nego se moraju prikupljati u određenim vremenskim intervalima, ova metoda ne omogućava rad s podacima u stvarnom vremenu. Konfiguracijom intervala između prikupljanja podataka mogu se prioritizirati platforme koje generiraju manje ili više bitne događaje.

5.3. Obrada događaja

Log sustavi izvršavaju specifične akcije kako bi ubrzale i unaprijedile rad sustava, spremanje i analizu podataka. Procesiranje zapisa je proces prikupljanja neobrađenih podataka s mnogo različitih izvora te pretvaranje dotičnih u smislene i standardizirane strukture. Svaki log sustav posjeduje podatke strukturirane u karakterističnom obliku koji posjeduju razne atribute i vrijednosti specifične za platformu na kojoj se nalazi. Slika 2 prikazuje dijagram standardnih operacija SIEM sustava. Mrežni uređaji šalju podatke prema centraliziranom sigurnosnom logu SIEM-a nakon čega se parsiraju, normaliziraju i kategoriziraju te prema potrebi obogaćuju i filtriraju. Korelacija događaja tumači podatke i shvaća kontekst poslovanja organizacije te događaje prenosi na daljnju analizu, odnosno predaje ih prezentacijskom sloju te podatke arhivira.



Slika 2. Dijagram toka obrade događaja (autorski rad)

5.3.1. Parsiranje

Kako se formati mogu znatno razlikovati, potrebno ih je parsirati da se izgrade smislene podatkovne strukture. Svaki SIEM sustav posjeduje velik broj parsera zaduženih za prevođenje raznih formata zapisa. Prema tome, može se reći kako je parsiranje proces izvlačenja podataka iz određenog zapisa kako bi se navedeni podaci mogli pregledavati ili prenijeti drugom procesu. Ovaj postupak zadužen je za izvlačenje potrebnih podataka iz manje čitljivog oblika zapisa u određeni oblik. Na primjer, Syslog zapis zabilježen od jezgre operacijskog sustava:

Aug 31 18:43:13 localhost kernel: [315.979954] IN=wlan0 OUT= MAC=b8:27:eb:28:e3:82:7c:67:a2:9b:ef:b5:08:00 SRC=192.168.1.100 DST=192.168.1.200 LEN=60 TOS=0x00 PREC=0x00 TTL=128 ID=20806 PROTO=ICMP TYPE=8 CODE=0 ID=1 SEQ=247

Iz navedenog zapisa može se uočiti datum i vrijeme nastanka zapisa te podaci o mrežnoj aktivnosti. Također, može se zaključiti kako je ICMP (Internet Control Message Protocol) paket pristigao s IP adrese 192.168.1.100 na IP adresu 192.168.1.200 mrežnog sučelja *wlan0*. Zapis je moguće parsirati u slijedeći format zapisa:

Datum: Aug 31

Vrijeme: 18:43:13

Mrežno sučelje: wlan0

Izvorišna IP adresa: 192.168.1.100

Odredišna IP adresa: 192.168.1.200

Protokol: ICMP

Duljina: 60

5.3.2. Normalizacija

Normalizacija je proces standardiziranja zapisa podataka u određeni dogovoreni format, često kompaktnog oblika s uobičajenim atributima. Ovaj proces je vrlo bitan ako se radi o sustavu koji prikuplja podatke s više različitih izvora. Svaki sustav može imati različitu notaciju zapisa podataka, pa je potrebno uskladiti podatke u svrhu jednostavnijeg pretraživanja i analize. Jedan od najčešćih primjera normalizacije je usklađivanje formata zapisa datuma. Primjerice, jedan log sustav može generirati datume dan/mjesec/godina, dok drugi može generirati godina/mjesec/dan. Zadatak procesa normalizacije je uskladiti načine zapisa te zapisati podatke u dogovorenom obliku. Na primjeru koji slijedi nalaze se dva događaja zabilježena na različitim platformama (tablica 5 i 6) te normalizirani podaci u centralnom sustavu (tablica 7).

Tablica 5. Primjer zapisa

Vrijeme	IP Adresa Izvor	IP Adresa Destinacija	Događaj
11:23 AM	192.168.1.100	192.168.1.200	Failure

Tablica 6. Primjer zapisa

Vrijeme	IP Adresa Izvor	IP Adresa Destinacija	Događaj
17:39	192.168.1.100	192.168.1.200	Pogreška

Tablica 7. Primjer normaliziranog zapisa

Vrijeme	IP Adresa Izvor	IP Adresa Destinacija	Događaj
17:39	192.168.1.100	192.168.1.200	EVENT ID: 9
23:23	192.168.1.100	192.168.1.200	EVENT ID: 9

Normalizacija podataka također obuhvaća i kategorizaciju. Kategorizacija smješta događaje u pripadajuće skupine kako bi se u budućnosti jednostavnije pretraživale i korelirale.

5.3.3. Obogaćivanje i filtriranje zapisa

Zapisi mogu sadržavati mnogo podataka, no vrlo često im nedostaje kontekst. Ove informacije ponekad ne mogu biti generirane u log sustavima ili bi ih nepotrebno opterećivale. Iz navedenog razloga prilikom ili nakon normalizacije koristi se tehnika obogaćivanja podataka (eng. *data enrichment*). Ovom tehnikom već strukturiranim zapisima dodaju se novi informativni atributi koji ih čine vrjednijima. Primjerice, originalni zapis ne mora sadržavati podatke o IP adresi računala koje ih odašilje ali se može nadodati, kao i recimo geolokaciju iz koje IP adresa potječe.

Filtriranje (eng. *filtering*) je proces izostavljanja podataka koji se ne smatraju relevantnima. Ovaj proces može doprinijeti manjoj količini podataka koje je potrebno obraditi te prema tome i ubrzati rad sustava. Primjer podataka koji mogu biti filtrirani su duplikati ili standardne operacije sustava te manje relevantni podaci koji se u pojedinim analizama ne smatraju relevantnima. Filtriranje prema atributima može pomoći sigurnosnom osoblju kod generiranja izvještaja kako bi se prikazale samo najvažnije informacije.

5.3.4. Agregacija

Agregacija (eng. *aggregation*) je proces koji grupira slične zapise te na temelju njih generira samo jedan zapis. Nedostatak agregacije je u tome da se prilikom sumiranja zapisa gube podaci, tako da će samo atributi uključeni u proces biti dostupni slijedećoj razini obrade. Na primjer, detekcija skeniranjem sustava odnosi se na skeniranje portova, raspona IP adresa i uzastopnog traženja ranjivosti. Navedene akcije često prethode stvarnim napadima na sustav jer nastoje locirati ranjivu točku sustava. Kako se radi o velikom broju akcija, tako se generira

velik broj događaja koji ukazuju na potencijalnu opasnost. Prilikom napada uzastopnim pokušajem (eng. *brute force*) na sustav za autentikaciju, umjesto zapisivanja svakog pokušaja zasebno, log sustav može agregirati jedan zapis koji sadrži podatke o broju pokušaja autenticiranja u određenom vremenskom razdoblju. Tablica 8 prikazuje uzastopne pokušaje prijave bez agregacije dok tablica 9 prikazuje agregiran zapis uzastopnih neuspješnih pokušaja prijave.

Tablica 8. Primjer uzastopnih zapisa o autentikaciji

Vrijeme	IP Adresa Izvor	IP Adresa Destinacija	Događaj
2.6.2019 20:05	192.168.1.100	192.168.1.200	Failure
2.6.2019 20:05	192.168.1.100	192.168.1.200	Failure
2.6.2019 20:05	192.168.1.100	192.168.1.200	Failure
2.6.2019 20:05	192.168.1.100	192.168.1.200	Failure
2.6.2019 20:05	192.168.1.100	192.168.1.200	Failure
2.6.2019 20:05	192.168.1.100	192.168.1.200	Failure
2.6.2019 20:05	192.168.1.100	192.168.1.200	Failure
2.6.2019 20:05	192.168.1.100	192.168.1.200	Failure
2.6.2019 20:05	192.168.1.100	192.168.1.200	Failure
2.6.2019 20:05	192.168.1.100	192.168.1.200	Failure
2.6.2019 20:06	192.168.1.100	192.168.1.200	Failure
2.6.2019 20:06	192.168.1.100	192.168.1.200	Failure
2.6.2019 20:07	192.168.1.100	192.168.1.200	Failure
2.6.2019 20:07	192.168.1.100	192.168.1.200	Failure

Tablica 9. Primjer agregiranog zapisa autentikacije

Vrijeme	IP Adresa Izvor	IP Adresa Destinacija	Događaj
2.6.2019 20:05 - 2.6.2019 20:07	192.168.1.100	192.168.1.200	Failure (14)

5.3.5. Arhiviranje

SIEM prikupljene sigurnosne događaje pohranjuje na određen vremenski period ovisan o budžetu, veličini loga te sigurnosnim i poslovnim zahtjevima. Uobičajena je praksa pohraniti događaje na disk računala prvih nekoliko tjedana do nekoliko mjeseci, ovisno o raspoloživoj količini memorije. Navedenim kratkoročnim pristupom pohrane omogućava se prikladan pristup te izvršavanje svih operacija nad podacima čime se postiže visoka brzina pretraživanja.

S vremenom, zapisanim događajima smanjuje se vrijednost te postaju sve manje aktualni dok se više pozornosti pridodaje svježim, novonastalim događajima. Dugoročna pohrana podataka koristi tehnike kompresije kako bi se kvalitetnije iskoristio raspoloživi memorijski prostor dok kratkoročni, novonastali podaci ostaju nekomprimirani kako bi analiza bila efikasna. Dugoročni zapisi u komprimiranom obliku često se arhiviraju na magnetske vrpce, sustave za pohranu podataka poput NAS-a (Network Attached Storage) i SAN-a (Storage Area Network) gdje mogu biti pohranjeni i do nekoliko godina, sve ovisno o poslovnoj i sigurnosnoj politici.

5.3.6. Korelacija događaja

Korelacijom događaja stvara se visoka razina pogleda na informacije koje protječu sustavom. Umjesto proučavanja pojedinačnog događaja, razmatra se niz događaja prema kojima se može pronaći konkretan uzorak. Primjerice, povećana količina uporabe diskovnog prostora web poslužitelja ne mora nužno upućivati na opasnost već može biti izazvana izvršavanjem legitimnih aktivnosti. Iako je moguće da se nad poslužiteljem izvršava DoS napad također je moguće kako se radi o trenutnom i prirodnom ponašanju. Korelacija događaja povezuje različite događaje čijom se analizom može utvrditi kompleksno ponašanje sustava. Procesom se pruža kompletna slika stanja sustava kako bi se uklonile određene sumnje.

Korelacijska pravila odnose se na niz instrukcija koje SIEM izvršava kako bi ustanovio postoji li povezanost između događaja prikupljenih s različitih izvora. Pravilima se definiraju veze između događaja kako bi se aktivirale obavijesti SIEM sustava koje zadovoljavaju unaprijed definirane zahtjeve. Prema pravilima, korelacija povezuje više standardnih događaja te prema njima generira jedan korelirani događaj.

Analiza događaja promatrana iz perspektive samo jedne platforme može dovesti do krivih zaključaka zbog nedostatka informacija o široj slici sustava. Prema tome, korelacija događaja zahtjeva razumijevanje konteksta kako bi se uočile nepravilnosti u cjelokupnom sustavu i smanjio broj pogrešnih upozorenja.

5.3.7. Automatizirani odgovori

Konfiguracija sigurnosnih sustava dopušta automatsko prilagođavanje razine sigurnosti kod detekcije prijetnje. Automatizirani odgovori spadaju u kategorije sustava za prevenciju upada (eng. *Intrusion Prevention System*) temeljenih na znanju ili na ponašanju. Sustavi za prevenciju upada temeljenih na znanju oslanjaju se na poznate uzorke napada dok sustavi za prevenciju upada temeljenih na ponašanju nadziru sustav kako bi ustanovili kretanje napada koje trenutno nije poznato (Miller, Harris, Harper, VanDyke i Blask, 2010). Takvi sustavi

prema zadanim pravilima nastoje ustanoviti „normalno“ ponašanje sustava te mogu automatski izvršiti protumjere ako se uoči odstupanje od normalnog ponašanja.

Automatizirani odgovori konstantno nadziru sustav, pritom analizirajući veliku količinu događaja i različitih parametara. Ispravnim konfiguracijama postiže se visoka brzina odgovora te se rijetko propušta pozitivni rezultat čime se uvelike doprinosi organizacijskoj sigurnosnoj strukturi.

Automatizirani odgovori također posjeduju negativne aspekte vlastitog djelovanja. Navedeni odgovori skloni su „lažno-pozitivnim“ obavijestima, odnosno legitimno djelovanje mrežne ili sistemske aktivnosti sustavima za prevenciju upada može djelovati kao maliciozno. S druge strane, napadači mogu iskoristiti funkcije automatiziranih odgovora protiv samog sustava. Otkrivanje načina djelovanja sustava za detekciju upada napadačima može dati priliku da izvrše protumjere slanjem određenog mrežnog prometa. Nedovoljno testiran sustav može ograničiti legitimni promet kako bi zaustavio potencijalni proboj te na isti način uskratiti korisnicima usluge.

5.3.8. Analiza

Posljednja faza obuhvaća interakciju korisnika sa zapisima pohranjenim u SIEM sustavu. Nakon što su podaci prikupljeni i postupno obrađeni, moraju se prezentirati kako bi se mogli iskoristiti. SIEM sustavi imaju grafičko sučelje pomoću kojeg korisnici nadgledaju rad, definiraju pravila, upravljaju pohranjenim zapisima te kreiraju informativne izvještaje. Za razliku od klasičnog pristupa, gdje se zapisi nalaze raspršeni po različitim platformama u originalnom formatu, administratori sustava pomoću SIEM-a mogu analizirati zapise svih platformi informacijskog sustava koje sudjeluju u prikupljanju podataka te ih pregledati u normaliziranom obliku.

5.4. Komercijalni SIEM sustavi

5.4.1. AlienVault

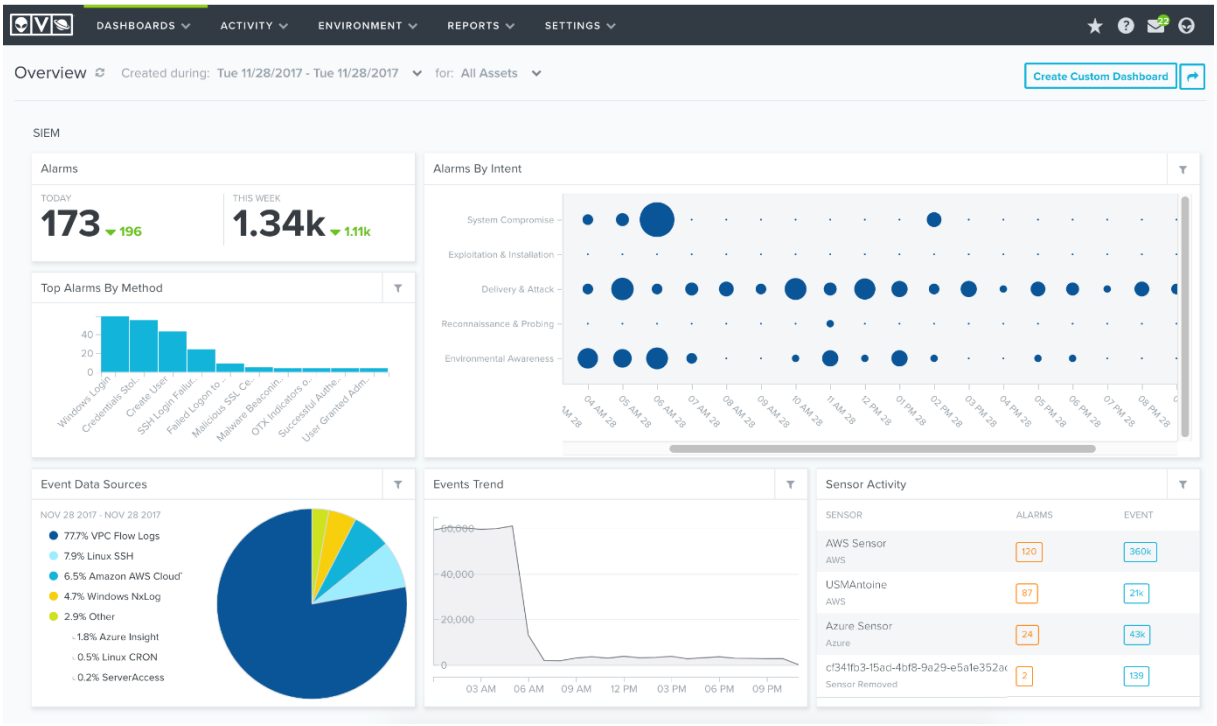
AlienVault OSSIM, Sustav otvorenog koda za upravljanje sigurnosnim informacijama (Open Source Security Information Management) nudi atraktivan pristup SIEM-u. Sam naziv indicira kako se radi o otvorenom kodu, prema tome ovaj sustav je besplatan za preuzimanje, modificiranje i korištenje. Radi nedostatka dostupnih SIEM sustava otvorenog koda,

AlienVault OSSIM izrađen je kako bi pružio esencijalne sigurnosne zahtjeve putem ujedinjene platforme (AlienVault, 2019):

- Pronalaska imovine
- Procjene ranjivosti
- Otkrivanja upada
- Bihevioralnog praćenja
- Korelacije događaja

AlientValut OSSIM koristi sustav za razmjenu prijetnji – AlienVault Open Threat Exchange (OTX) kako bi korisnicima pružio pristup informacijama u stvarnom vremenu o malicioznim poslužiteljima ali i mogućnost vlastitog doprinosa zajednici. Poduzeće navodi kako pruža neprestani razvoj sustava jer vjeruju kako bi svi trebali imali pristup sofisticiranim sigurnosnim tehnologijama kako bi unaprijedili svačiju sigurnost (AlienVault, 2019).

Iako besplatna verzija SIEM rješenja posjeduje određene nedostatke, poput performansi, pohrane, podrške i integracije s ostalim platformama, otvoreni kod sustava pruža dodatnu fleksibilnost i omogućuje organizacijama smanjenje troškova te kvalitetno iskorištenje potencijala zaposlenika. U trenutku rasta organizacije i težnje za prelaskom na sofisticiraniju i robusniju platformu AlienVault nudi profesionalnu verziju SIEM sustava. Na slijedećoj slici prikazan je kontrolni zaslon AlienVault USM-a.



Slika 3. Kontrolni zaslon AlienVault USM-a

AlienVault USM (eng. *Unified Security Management*) Anywhere je SIEM sustav koji pruža prepoznavanje prijetnji, odgovor na incidente te upravljanje usklađenošću putem „oblaka“, lokalnog i hibridnog okruženja (AlienVault, 2019). Za razliku od OSSIM platforme, USM posjeduje napredne karakteristike poput kontinuiranih ažuriranja o prijetnjama, integracije sa sustavima za projektni menadžment te praćenja prijetnji u oblaku. „SaaS“ (Software as a Service) pristup pojednostavljuje postavljanje, smanjuje vrijeme implementacije i kompleksnost integracije te prema tome smanjuje ukupne troškove rješenja. Tablica prikazuje usporedbu osnovnih karakteristika besplatnog i profesionalnog rješenja AlienVaulta.

Tablica 10. Usporedba karakteristika OSSIM i USM Anywhere AlienVault SIEM rješenja

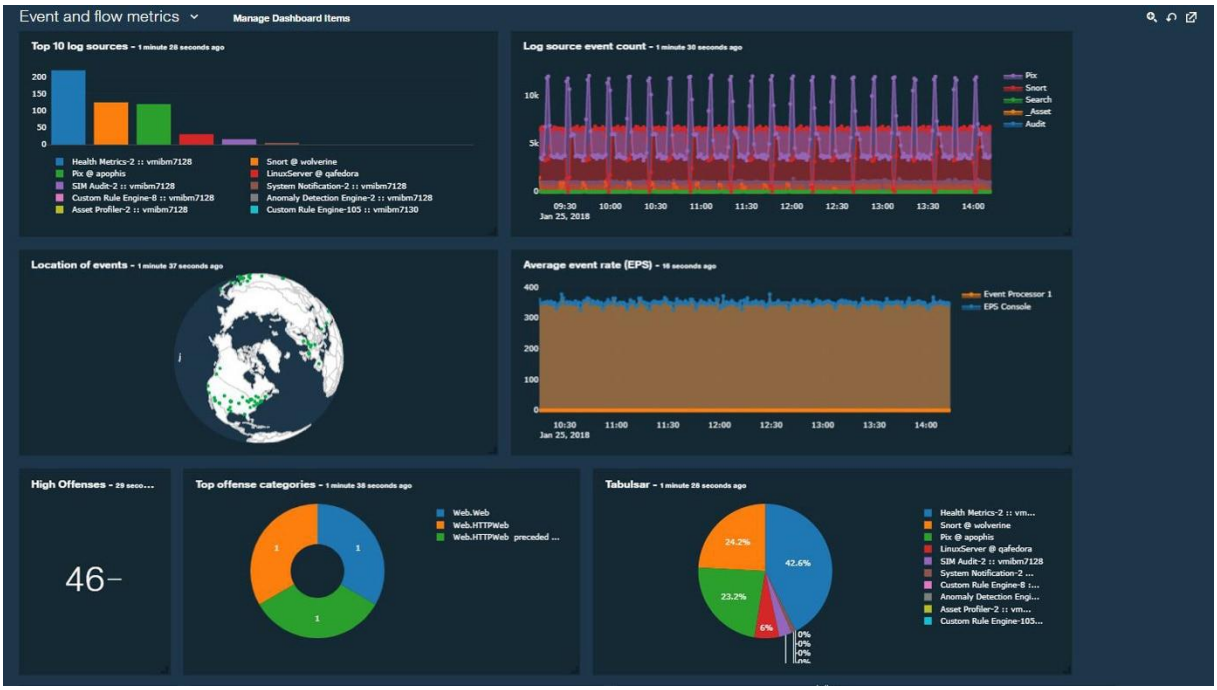
	AlienVault OSSIM	**USM Anywhere**
Dostupnost	Softver otvorenog koda	Usluga u oblaku
Cijena	Otvoren kod	Godišnja pretplata
Sigurnosni nadzor	Lokalna fizička i virtualna okruženja	AWS i Azure okruženja u oblaku Aplikacije u oblaku Lokalna, fizička i virtualna okuženja
Arhitektura razvoja	Jedan poslužitelj	SaaS isporuka sa senzorima u svakom okuženju koje se nadzire
Pronalazak imovine	Da	Da
Detekcija upada	Da	Da
Korelacija događaja	Da	Da
Upravljanje zapisima	Ne	Da
AWS & Azure nadzor	Ne	Da
Vizualizacija podataka	Ne	Da
Integracija	Ne	Da
Dokumentacija i baza znanja	Ne	Da

5.4.2. IBM QRadar

IBM QRadar Sustav za upravljanje sigurnosnim informacijama i događajima pomaže sigurnosnim timovima precizno otkrivanje prijetnji te pruža inteligentne uvide u događaje kako bi odgovori bili efikasni i s time se smanjio utjecaj incidenata. Kao i USM Anywhere, QRadar također podržava lokalno okruženje kao i okruženje u oblaku, no ne nudi besplatnu verziju sustava.

Uz ostale standardne sposobnosti SIEM sustava, QRadar nudi mogućnost integracije s sustavom obavještavanja o izvorima prijetnji koristeći STIX/TAXII (eng. *Structured Threat*

Information Expression/Trusted Automated eXchange of Indicator Information) tehnologije (IBM, 2019). QRadar se može implementirati kao harvder, softver ili virtualni uređaj (Scarfone, 2015). Sustav je vrlo skalabilan i robustan čime postaje idealan kandidat za nadzor događaja u većim poduzećima. Platforma donosi i kompleksnost što krivulju učenja čini strmijom nego kod AlienVault USM-a. Slika prikazuje kontrolni zaslon QRadar-a.



Slika 4. Kontrolni zaslon IBM QRadar-a

AlienVault USM je prigodan odabir SIEM sustava za organizacije srednje veličine ili one u razvoju koje traže pristupačno i povoljno rješenje dok posjeduju kompetentnu sigurnosnu platformu dok cijena i strma krivulja učenja QRadara ograničavaju korištenje SIEM sustava na organizacije s veći budžetom i profesionalnim resursima.

6. „Lažno-pozitivne“ obavijesti

SIEM sustav neprestano obrađuje brojne podatke koji će kroz određeno vrijeme ukazati na maliciozne ili sumnjive događaje. Ukoliko sigurnosni događaj nastane SIEM sustav će obavijestiti nadležne zaposleniku o sumnjivim događajima. Ove događaje je potrebno provjeriti kako bi se ustanovilo da li se uistinu radi u mogućem incidentu. Upozorenja u sustavu ne moraju nužno ukazivati na značajni sigurnosni događaj, no u slučaju obavijesti visokog prioriteta sigurnosno osoblje je prisiljeno detaljnije istražiti nastali događaj. Ako se ustanovi da sustav ipak nije kompromitiran, tada se može zaključiti kako je SIEM kreirao „lažno-pozitivnu“ obavijest (eng. *false positive*).

Velika količina navedenih obavijesti postavlja sigurnosno osoblje organizacije u neprestano stanje pripravnosti i potencijalno suočavanje s procesom dodatnog istraživanja događaja bili oni maliciozni ili ne. Konstantnim ispitivanjem takvih događaja zaposlenicima se skreće pažnja na čime se njihovo vrijeme troši na proučavanje benignih događaja. Povećanjem broja ovakvih rezultata također se povećava vjerojatnost neopaženog pravog sigurnosnog događaja.

Lažno-pozitivni događaji mogu biti generirani u SIEM sustavu radi neispravnog i ne dovoljno testiranog koda te pri definiranju nejasnih i nevaljanih korelacijskih pravila. Nedovoljno specifična pravila mogu obuhvatiti širok spektar događaja, prema tome i onih koji nisu relevantni.

Sustavi za detekciju i prevenciju upada podložni su visokoj razini lažno-pozitivnih upozorenja (Miller et al., 2010). Često se legitimni mrežni promet može protumačiti kao maliciozna aktivnost napadača. Na primjeru lažno-pozitivnih rezultata može se razmatrati FTP (eng. *File Transfer Protocol*) web poslužitelj koji po satu izvrši prosječno 30 preuzimanja datoteka. Prag je postavljen između 10 i 50 preuzimanja kako bi se moglo uočiti odstupanje od uobičajenog rada te u slučaju prelaska gornje granice onemogućiti preuzimanje kako bi se izbjeglo previsoko opterećenje sustava. Nakon ažuriranja proizvoda, klijenti poduzeća započinju preuzimanje prilikom čega izazovu povećanje opterećenosti FTP web poslužitelja prilikom čega se aktivira sigurnosni automatizirani odgovor sustava te se rad poslužitelja obustavi. Stvarni primjer uslijedio je u studenom 2008. godine kad je AVG Anti-virusni softver pogrešno je označio kritičnu datoteku Windows operacijskog sustava kao zloćudnu čime te preporučio korisnicima da ju uklone (Protalinski, 2008). Velika količina korisnika je uklonila datoteku što je prouzrokovalo neprestano ponovno podizanje sustava ili ne podizanje sustava

uopće. Tehnička podrška AVG-a je priznala pogrešku, javno se ispričala korisnicima te izdala novu verziju softvera kojom su ispravili pogrešno protumačeni sadržaj datoteke. Korištenjem sofisticiranih SIEM sustava, smanjenje lažno-pozitivnih obavijesti postiže se pažljivim kreiranjem filtera i korelacijskih pravila čime se postiže visoka razina identifikacije i pouzdanosti upozorenja na samo visoko prioritetne sigurnosne događaje dok se s druge strane izostavlja golem dio lažno-pozitivnih rezultata.

Lažni negativni rezultati (eng. *false negatives*) su događaji koji su maliciozne naravi ali ostaju ne zamijećeni u sigurnosnom sustavu. Kevin Timm (2001) navodi kako postoje brojni potencijalni razlozi za navedene propuste u sustavu za praćenje upada u mrežni sustav:
Problemi u dizajnu mreže: nemogućnost praćenja svih ulaznih točaka u mreži ili prevelika količina podataka koja se ne može obraditi

- Kriptirani podaci – problemi mogu nastati ako se kriptirani podaci prenose mrežom
- Nejavni napad – napad koji još nije javno poznat, te proizvođači ovakvih sustava nemaju znanje o mogućim propustima
- Loša konfiguracija sustava – loše postavljena pravila, sustav ne može obraditi sve podatke, alarmiranje nije dobro konfigurirano, administrator sustava posjeduje malu količinu znanja o mogućim prijetnjama.

7. Zaključak

Informatizacijom poslovnih procesa potreba za zaštitom informacijskog sustava, odnosno resursa organizacije, postaje sve izraženija. Centralizirana arhitektura prikupljanja, obrade, korelacije i analize događaja pruža sveobuhvatni pogled na prošlo i trenutno stanje sustava dok pritom prepoznaje potencijalne prijetnje. Pravilnom implementacijom SIEM sustava sjedinjuje se rad udaljenih, odvojenih platformi čime se postiže razumijevanje konteksta iz naizgled nepovezanih događaja te se također podiže razina efikasnosti sigurnosnog nadzora i odgovora na prijetnje i incidente. Administratorima se pruža visoka razina kontrole događaja informacijskog sustava te pravovremeni izvještaji koji se pravilnim tumačenjem mogu iskoristiti kako bi se na vrijeme reagiralo na moguće incidente. Automatizirane operacije i inteligentno zaključivanje SIEM-a omogućiti će analitičarima i administratorima sustava provođenje manje vremena uz sigurnosne konzole i reviziju sigurnosnih događaja dok će se minimizirati broj lažno pozitivnih upozorenja. Najvažniji faktor implementacije SIEM sustava je osiguranje pouzdanog izvora informacija te pohrane istih u centraliziranu bazu podataka. Manjak ili nedostupnost smanjuje vrijednost analize, što u krajnosti dovodi od pogrešnih rezultata. Prema tome, svaki SIEM je vrijedan proporcionalno kvaliteti podataka koje posjeduje.

8. Literatura

1. AlienVault (2019). *Products*. Preuzeto 1.9.2019. s https://www.alienvault.com/products/

2. AlienVault USM kontrolna ploča [Slika] (bez dat.) Preuzeto 9.9.2019. s https://www.cybersecurity-insiders.com/wp-content/uploads/2017/12/USMAnywhere-Overview_Dashboard.png

3. Brezinski D., Killalea T. (2002). *Guidelines for Evidence Collection and Archiving.* Preuzeto 1.6.2019. s https://tools.ietf.org/html/rfc3227#section-2.4

4. Budin L., Golub M., Jakobović D., Jelenković L. (2010). *Operacijski sustavi.*

5. Cater G. (2009). *Security Event Management.* Preuzeto 17.7.2019. s http://www.infosectoday.com/Articles/Security_Event_Management/Security_Event_Management.htm

6. Cisco (2017). *2017 Annual Cybarsecurity Report.* Preuzeto 1.9.2019. s http://www.grouppbs.com/wp-content/uploads/2017/02/Cisco_2017_ACR_PDF.pdf

7. CorreLog (2015). *Event Data versus Log Data, and the Difference between IT Security and Breach.* Preuzeto 13.7.2019. s http://correlog.com/Images/White_papers_biz-cases/Correlog_wp_Event_vs_log-15_4web.pdf

8. [8] Cox J. (2019). *What is Syslog?* Preuzeto 10.7.2019. s https://www.ittsystems.com/what-is-syslog/

9. Eaton I. (2003). *The Ins and Outs of System Logging Using Syslog.* Preuzeto 12.7.2019. s https://www.sans.org/reading-room/whitepapers/logging/ins-outs-system-logging-syslog-1168

10. El-Taj, H., Abouabdalla, O., Manasrah, A. (2010). *False Positive Reduction by Correlating the Intrusion Detection System Alerts: investigation Study. Journal of Communication and Computer.* Preuzeto 21.7.2019. s https://www.researchgate.net/publication/210195144_False_Positive_Reduction_by_Correlating_the_Intrusion_Detection_System_Alerts_investigation_Study

11. Exabeam (2019). *The Essential Guide to SIEM.* Preuzeto 1.6.2019. s https://www.exabeam.com/siem-guide/what-is-siem/

12. Ho, C., Lin, Y.R., Lai, Y, Chen, I., Wang, F., Tai, W. (2012*). False Positives and False Negatives from Real Traffic with Intrusion Detection/Prevention Systems*. Preuzeto 21.7.2019 s https://www.researchgate.net/publication/260986371_False_Positives_and_False_Negatives_from_Real_Traffic_with_Intrusion_DetectionPrevention_Systems/link/0a85e532f0a8d09f09000000/download

13. IBM (2019). *IBM QRadar SIEM.* Preuzeto 1.9.2019. s https://www.ibm.com/us-en/marketplace/ibm-qradar-siem

14. IBM QRadar Kontrolna ploča [Slika] (bez dat.) Preuzeto 9.9.2019. s https://mp.s81c.com/pwb-production/36bc5fb21dea628dd3f04814233fdd77/additionalOfferingImg__0_2d4a7df4-7b32-4878-9e66-b8efe1061a94.jpg

15. Kent K., Souppaya M. (2006). *Guide to Computer Security Log Management.* Preuzeto 27.6.2019. s https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

16. Kim, D., Solomon M. (2018). *Fundamentals of Information Systems Security*

17. Lonvick, C. (2001). *The BSD syslog Protocol.* Preuzeto 13.7.2019. s http://www.ietf.org/rfc/rfc3164.txt

18. Ma D., Tsudik G. (2008). *A New Approach to Secure Logging.* Preuzeto 12.7.2019. s https://eprint.iacr.org/2008/185.pdf

19. Miller D.R., Harris S., Harper A. A., VanDyke S., Blask C. (2010). *Security Information and Event Management (SIEM) Implementation.*

20. Protalinski E. (2008). *AVG incorrectly flags user32.dll in Windows XP SP2/SP3.* Preuzeto 28.8.2019. s https://arstechnica.com/information-technology/2008/11/avg-incorrectly-flags-user32-dll-in-windows-xp-sp2sp3/

21. Pantola V. A., Yatco F. R., Pineda J. D. (2010). *Normalization of Logs for Networked Devices in a Security Information Event Management System*. Preuzeto 15.8.2019. s https://www.researchgate.net/publication/286937242_Normalization_of_Logs_for_Networked_Devices_in_a_Security_Information_Event_Management_System/link/56717c4208ae2b1f87af0387/download

22. Parker J. (2016). *What is Syslog, including Linux and Windows Servers, Ports and more*. Preuzeto 10.7.2019. s https://www.pcwdld.com/what-is-syslog-including-servers-and-ports

23. Scarfone K. (2015). *IBM Security QRadar: SIEM product overview.* Preuzeto 2.9.2019. s https://searchsecurity.techtarget.com/feature/IBM-Security-QRadar-SIEM-product-overview

24. Timm K. (2001). *Strategies to Reduce False Positives and False Negatives in NIDS.* Preuzeto 25.7.2019. s https://www.symantec.com/connect/articles/strategies-reduce-false-positives-and-false-negatives-nids

9. Popis slika

10. Popis tablica