Istraživanje mogućnosti SIEM sustava i interoperabilnosti s alatima za zaštitu informacijsko-komunikacijskog sustava

Tomas, Kristijan

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Kristijan Tomas

ISTRAŽIVANJE MOGUĆNOSTI SIEM SUSTAVA I INTEROPERABILNOSTI S ALATIMA ZA ZAŠTITU INFORMACIJSKO-KOMUNIKACIJSKOG SUSTAVA

DIPLOMSKI RAD

Zagreb, rujan 2024.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 28. svibnja 2024.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Sigurnost i zaštita informacijsko komunikacijskog sustava**

DIPLOMSKI ZADATAK br. 7690

Pristupnik: **Kristijan Tomas (0135257163)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Istraživanje mogućnosti SIEM sustava i interoperabilnosti s alatima za zaštitu informacijsko-komunikacijskog sustava**

Opis zadatka:

Istraživanje u okviru diplomskog rada treba se fokusirati na analizu Security Information and Event Management (SIEM) sustava i njihovu integraciju s drugim sigurnosnim alatima. Istraživanjem je potrebno analizirati važnost SIEM sustava za modernu sigurnosnu infrastrukturu, pružiti pregled dosadašnjih istraživanja kako bi se postavile teorijske osnove. Potom je potrebno detaljno istražiti i predstaviti različite SIEM sustave, njihove funkcije i mogućnosti. U radu je ključno identificirati i analizirati glavne izazove u integraciji SIEM sustava s ostalim sigurnosnim alatima, razmotriti različite pristupe integraciji i njihovu efikasnost. Također, rad treba istražiti buduće smjerove u razvoju i integraciji SIEM sustava. Zaključak rada treba sintetizirati nalaze istraživanja, predstaviti ključne uvide i preporuke za poboljšanje integracije SIEM sustava u sigurnosne strategije organizacija.

Mentor:

doc. dr. sc. Ivan Cvitić

Predsjednik povjerenstva za diplomski ispit:

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

ISTRAŽIVANJE MOGUĆNOSTI SIEM SUSTAVA I INTEROPERABILNOSTI S ALATIMA ZA ZAŠTITU INFORMACIJSKO-KOMUNIKACIJSKOG SUSTAVA

RESEARCH ON THE CAPABILITIES OF SIEM SYSTEMS AND INTEROPERABLITY WITH TOOLS FOR INFORMATION-COMMUNICATION SYSTEM PROTECTION

Mentor: doc. dr. sc. Ivan Cvitić

Student: Kristijan Tomas

JMBAG: 0135257163

Zagreb, rujan 2024.

ISTRAŽIVANJE MOGUĆNOSTI SIEM SUSTAVA I INTEROPERABILNOSTI S ALATIMA ZA ZAŠTITU INFORMACIJSKO-KOMUNIKACIJSKOG SUSTAVA

SAŽETAK

Sustavi za upravljanje sigurnosnim informacijama i događajima (engl. *Security Information and Event Management,* SIEM) postali su ključni dio moderne kibernetičke sigurnosne arhitekture. Omogućuju organizacijama prikupljanje, analizu i korelaciju sigurnosnih podataka iz više izvora, pružajući sveobuhvatan pregled njihove sigurnosne situacije. Međutim, učinkovitost SIEM-a često je ograničena ukoliko djeluje samostalno. Integracija SIEM sustava s drugim alatima za zaštitu informacijsko-komunikacijskog sustava, poput vatrozida (engl. *Firewall*), značajno povećava učinkovitost SIEM sustava i kibernetičku sigurnost organizacije. Iako postoje razni izazovi prilikom integracije, takva rješenja donose mnoge prednosti i dodatan sloj zaštite, što je u današnjem dobu sve sofisticiranijih napada itekako potrebno. Ovaj rad istražuje mogućnosti integracije SIEM-a s drugim sigurnosnim alatima, raspravlja o izazovima integracije različitih sigurnosnih arhitektura i pruža primjere uspješnih integracija SIEM-a u stvarnom svijetu.

Ključne riječi: SIEM, kibernetička sigurnost, integracija i interoperabilnost

SUMMARY

Security Information and Event Management (SIEM) systems have become a critical component of modern cybersecurity architecture. They enable organizations to collect, analyze, and correlate security data from multiple sources, providing a comprehensive view of their security posture. However, the effectiveness of SIEM is often limited when it operates in isolation. Integrating SIEM systems with other information and communication system protection tools, such as firewalls, significantly enhances the efficiency of SIEM systems and the cybersecurity of an organization. Although there are various challenges associated with integration, such solutions offer many advantages and an additional layer of protection, which is crucial in today's era of increasingly sophisticated attacks. This paper explores the possibilities of integrating SIEM with other security tools, discusses the challenges of integrating different security architectures, and provides examples of successful SIEM integrations in the real world.

Keywords: SIEM, cybersecurity, integration and interoperability

SADRŽAJ

1. UVOD

U današnjem digitalnom dobu, organizacije se suočavaju s neprestanim izazovima sigurnosti, uključujući napade hakera, krađu podataka, *ransomware* napade i mnoge druge prijetnje. SIEM (engl. *Security Information and Event Management*) sustavi imaju važnu ulogu u detekciji, analizi i odgovoru na ove prijetnje pružajući organizacijama potrebnu vidljivost i razumijevanje nad sigurnosnim događajima u stvarnom vremenu, ali ukoliko se integriraju s ostalim sigurnosnim alatima dolazi do stvaranja efikasnog, proaktivnog i odgovornog sigurnosnog okruženja koje može adekvatno odgovoriti na sve složenije kibernetičke prijetnje..

Tema Istraživanje mogućnosti SIEM sustava i interoperabilnosti s alatima za zaštitu informacijsko-komunikacijskog sustava istražuje važnost i metodologiju integracije SIEMsustava s drugim sigurnosnim alatima u informacijskim okruženjima.

Svrha diplomskog rada je identificirati zašto je integracija SIEM sustava s ostalim sigurnosnim alatima ključna za efikasno upravljanje sigurnošću informacijskih sustava.

Cilj ovog diplomskog rada je istražiti, analizirati i pružiti uvid u procese, izazove i najbolje prakse integracije SIEM sustava s drugim sigurnosnim alatima u informacijskim okruženjima.

Diplomski rad se sastoji od 7 poglavlja:

1. Uvod
2. Pregled dosadašnjih istraživanja
3. Pregled SIEM sustava
4. Izazovi integracije SIEM sustava
5. Analiza različitih pristupa integraciji SIEM sustava s ostalim sigurnosnim alatima
6. Budući smjerovi integracije SIEM sustava
7. Zaključak

Drugo poglavlje sažeto će prikazati pregled dosadašnjih istraživanja koja su vezana uz SIEM sustav i važnost integracije SIEM sustava s drugim sigurnosnim alatima kako bi se poboljšala kibernetička sigurnost informacijsko-komunikacijskog sustava.

Treće poglavlje pružit će detaljan uvid u funkcije, prednosti i ograničenja SIEM sustava kako bi se razumjeli osnovni koncepti SIEM sustava.

U četvrtom poglavlju identificirat će se specifične poteškoće s kojima se stručnjaci za kibernetičku sigurnost suočavaju prilikom integracije SIEM sustava s ostalim sigurnosnim alatima, poput različitih formata logova ili problema performansi sustava.

U petom poglavlje istražit će se različite strategije i tehnike koje se koriste za uspješnu integraciju SIEM sustava, kao što su API (engl. *Application Programming Interface*) integracije, upotreba zajedničkih protokola ili razvoj prilagođenih rješenja. Također pružit će se detaljan pregled konkretnog primjera integracije SIEM sustava s jednim od najvažnijih sigurnosnih alata - vatrozidom, kako bi se demonstrirala praktična primjena i koristi integracije.

U šestom poglavlju opisat će se potencijalne inovacije, trendovi i tehnološki napreci koji bi mogli utjecati na budućnost integracije SIEM sustava s ostalim sigurnosnim alatima.

2. PREGLED DOSADAŠNJIH ISTRAŽIVANJA

Danas je SIEM sustav neophodan zbog rastućih kibernetičkih prijetnji i potrebe za efikasnom zaštitom informacija i mrežne infrastrukture. Važnost SIEM sustava i integracija s ostalim sigurnosnim alatima je opisana kroz razne znanstvene literature, a u nastavku su navedena neka od znanstvenih istraživanja.

Autori rada [1] istražuju prednosti integracije SIEM sustava s drugim sigurnosnim alatima, raspravljaju o izazovima integracije različitih sigurnosnih arhitektura i pružaju primjere uspješnih integracija SIEM sustava. Učinkovitost SIEM-a često je ograničena njegovom izolacijom od drugih sigurnosnih alata. Integracija SIEM sustava s drugim sigurnosnim alatima, poput vatrozida, sistema za otkrivanje upada (engl. *Intrusion Detection System,* IDS) i rješenja za sigurnost krajnjih točaka, značajno može poboljšati sigurnosnu poziciju organizacije i povećati njenu sposobnost odgovora na prijetnje. Ova integracija omogućava besprijekornu razmjenu podataka i obavještajnih informacija o prijetnjama stvarajući ujedinjeni sigurnosni ekosustav koji može otkriti, istražiti i reagirati na prijetnje na učinkovitiji način.

Istraživački rad [2] prikazuje ključnu ulogu integracije SIEM sustava sa sustavom za otkrivanje upada temeljenim na analizi uživo pomoću strojnog učenja. Integracija ovih tehnologija omogućuje stvaranje sveobuhvatnog sigurnosnog okruženja sposobnog za detekciju i reakciju na prijetnje u stvarnom vremenu. Naglašava se važnost ovakvih integriranih sustava za industrijske okoline, pružajući alate za učinkovito nadgledanje mreža i zaštitu od napada. Buduća istraživanja trebala bi proširiti ovaj koncept na veće mreže i optimizirati konfiguraciju sustava kako bi se smanjila potrošnja resursa. Rad naglašava ključnu ulogu SIEM i IDS tehnologija u suvremenim sigurnosnim arhitekturama, ističući potrebu za integracijom i kontinuiranim unaprjeđenjem kako bi se zaštitili osjetljivi sustavi od sve složenijih kibernetičkih prijetnji.

U radu [3] istražuje se ključna uloga integracije SIEM sustava i upravljanja ranjivostima u kibernetičkoj sigurnosti, koji često djeluju izolirano. Integracija ovih disciplina može značajno poboljšati opći sigurnosni položaj organizacije pružanjem sveobuhvatnog pristupa detekciji prijetnji, prevenciji i sanaciji. Rad istražuje kako SIEM može biti iskorišten za unaprjeđenje upravljanja ranjivostima i odgovorom na njih, naglašavajući koristi te integracije. Integracija SIEM-a i upravljanja ranjivostima nudi nekoliko koristi za organizacije, uključujući smanjenje rizika eksploatacije ranjivosti, poboljšanje vremena odgovora na incidente i unaprjeđenje donošenja odluka. Kako bi se učinkovito integrirale ove dvije discipline, organizacije bi trebale definirati jasne ciljeve, uspostaviti protokole za dijeljenje podataka, razviti pravila korelacije,

definirati postupke odgovora te pružiti obuku i podršku sigurnosnim timovima. Učinkovitom integracijom SIEM-a i upravljanja ranjivostima, organizacije mogu ojačati svoj sigurnosni položaj proaktivnim identificiranjem i rješavanjem ranjivosti, minimizirajući potencijal za povrede podataka i kompromise sustava. Ovaj sveobuhvatni pristup detekciji, prevenciji i sanaciji prijetnji omogućuje sigurnosnim timovima da zaštite digitalne resurse organizacije i održe otporan sigurnosni položaj.

Rad autora [4] govori o pristupu osiguranja informacijske tehnologije SIEM za poboljšanje sigurnosti informacijskih sustava u poslovnim mrežama, posebno u malim i srednjim poduzećima. Autori ističu da su takva poduzeća često meta vanjskih napadača jer nemaju dovoljno razvijene sigurnosne strategije i komponente u svojim mrežama. Tradicionalni alati za sigurnost poput antivirusnih programa, vatrozida i sustava za otkrivanje upada često rade izolirano jedni od drugih. Autori predlažu korištenje SIEM sustava koji omogućuje integraciju i korelaciju logova i događaja iz različitih sigurnosnih komponenti.

Autori u radu [5] dolaze do zaključka da integracija SIEM sustava nije samo poželjna već i neophodna kako bi se osigurala efikasna zaštita i odgovor na incidente. Osim što omogućava centraliziranu analizu i korelaciju podataka iz različitih izvora, integracija SIEM-a s drugim sigurnosnim alatima i tehnologijama doprinosi povećanju vidljivosti, poboljšava detekciju napada i olakšava odgovor na incidente. Stoga je važno razmatrati mogućnosti integracije SIEM-a sa drugim sigurnosnim rješenjima kako bi se izgradio sveobuhvatan sigurnosni okvir koji efikasno štiti organizaciju od suvremenih *cyber* prijetnji.

Iz navedenih istraživanja jasno je koliko je važna integracija SIEM sustava s ostalim alatima za zaštitu informacijsko-komunikacijskog sustava i koje prednosti donosi. Takve integracije su nužne u današnjem dobu kada napadači koriste razne ranjivosti sustava, aplikacija ili mreže neke organizacije. Iako stručnjaci za kibernetičku sigurnost razvijaju nove metode zaštite, potrebno je uložiti resurse u povezivanje različitih sigurnosnih alata u centralizirani SIEM sustav kako bi stručnjaci gubili manje vremena na provjeru svakog alata zasebno. Također je potrebno i ulagati u znanja i daljnju edukaciju stručnjaka za kibernetičku sigurnost kako bi mogli pratiti tempo napadača i u najboljem slučaju biti i korak ispred napadača.

3. PREGLED SIEM SUSTAVA

Sustav upravljanja sigurnosnim informacijama i događajima je rješenje koje pomaže organizacijama otkriti, analizirati i odgovoriti na sigurnosne prijetnje prije nego one naštete poslovnim operacijama, kombinirajući upravljanje sigurnosnim informacijama (engl. *Security Information Management,* SIM) i upravljanje sigurnosnim događajima (engl. *Security Event Management,* SEM). Moderni SIEM sustavi također sadrže tehnologije orkestracije i automatizacije sigurnosti te odgovora na incidente (engl. *Security Orchestration, Automation and Response,* SOAR) za automatiziranje odgovora na prijetnje i otkrivanje prijetnji temeljenih na sumnjivoj aktivnosti. Zajedno, oni ubrzavaju prepoznavanje i rješavanje sigurnosnih događaja i incidenata unutar IT okruženja [6].

SIEM rješenja poboljšavaju otkrivanje prijetnji, usklađenost i upravljanje sigurnosnim incidentima kroz prikupljanje i analizu podataka o sigurnosnim događajima u stvarnom vremenu. Izvorne SIEM platforme bile su alati za upravljanje zapisnicima (logovima). Kombinirale su funkcije upravljanja sigurnosnim informacijama i upravljanja sigurnosnim događajima. Ove platforme omogućavale su praćenje i analizu sigurnosnih događaja u stvarnom vremenu. Također, omogućavale su praćenje i bilježenje sigurnosnih podataka u svrhu usklađenosti ili revizije. Tijekom godina, SIEM softver je evoluirao kako bi uključio analitiku ponašanja korisnika i entiteta (engl. *User Entity and Behavior Analytics,* UEBA) [7], kao i druge napredne sigurnosne analitike, umjetnu inteligenciju (engl. *Artificial Intelligence,* AI) i mogućnosti strojnog učenja (engl. *Machine Learning*, ML) za prepoznavanje sumnjivog ponašanja i indikatora prijetnji. Danas je SIEM postao temelj u suvremenim sigurnosnim operativnim centrima (*Security Operations Center,* SOC) za slučajeve sigurnosnog nadzora i upravljanja usklađenošću.

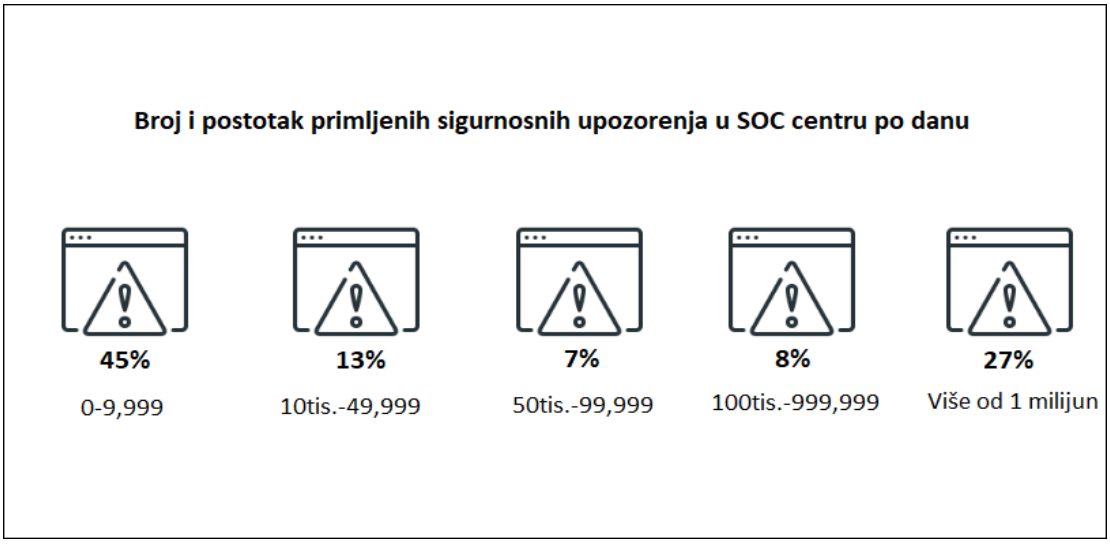
3.1. Uloga SIEM sustava

SIEM rješenja prikupljaju podatke o događajima i zapisima koje generiraju glavni sustavi, aplikacije i sigurnosna oprema, poput antivirusnih programa i vatrozida, te ih dostavljaju centraliziranoj platformi. SIEM alati otkrivaju i kategoriziraju informacije u skupine kao što su uspješne i neuspješne prijave, aktivnost zlonamjernog softvera i drugo potencijalno štetno ponašanje. Kada SIEM pronađe moguće sigurnosne probleme, stvara sigurnosna upozorenja. Organizacije mogu tim obavijestima dodijeliti visoki ili niski prioritet koristeći skup utvrđenih kriterija.

Na primjer, korisnički račun s 10 neuspješnih pokušaja povezivanja u 10 do 15 minuta može biti označen kao sumnjiv, ali mu je dodijeljen niži prioritet jer je zahtjeve za pristup

vjerojatno uputio korisnik koji je zaboravio svoje vjerodajnice za prijavu. Unatoč tome, račun koji proizvede 500 neuspješnih pokušaja prijave unutar 10 do 15 minuta bio bi označen kao povišeni incident jer je sasvim sigurno riječ o *brute-force* napadu.

SIEM sustavi su ključni za organizacije koje se suočavaju s brojnim prijetnjama. S prosječnim sigurnosnim operativnim centrom koji prima više od 10 000 upozorenja dnevno, a 27% kompanija preko milijun upozorenja (slika 1.) [8], većina organizacija nema dovoljno velike sigurnosne timove da bi pratili ogroman broj upozorenja. Međutim, rastući rizik od sve sofisticiranijih *cyber* prijetnji može dovesti do velikih posljedica. Jedno upozorenje može značiti razliku između otkrivanja i sprječavanja velikog incidenta i njegovog potpuna propuštanja. SIEM sustav pruža učinkovitiji način razvrstavanja i istraživanja upozorenja. Sa SIEM tehnologijom, sigurnosni timovi mogu držati korak s velikim brojem sigurnosnih podataka.



Slika 1. Broj i postotak primljenih sigurnosnih upozorenja u SOC centru po danu

Izvor: [8]

Rješenja SIEM sustava analiziraju zapise i sigurnosne događaje zajedno s drugim podacima kako bi ubrzala otkrivanje prijetnji i podržala upravljanje sigurnosnim incidentima i događajima, kao i usklađenost. Generalno, SIEM sustav prikuplja podatke iz više izvora, omogućujući brži odgovor na prijetnje. Ako se otkrije anomalija, može prikupiti više informacija, pokrenuti upozorenje ili staviti resurs u karantenu.

Iako su SIEM tehnologiju tradicionalno koristile velike tvrtke i javne tvrtke koje su trebale dokazati usklađenost, organizacije su shvatile da je upravljanje sigurnosnim informacijama i događajima mnogo kvalitetniji način zaštite podataka. SIEM tehnologije su se od tada razvile kao ključni alat za otkrivanje prijetnji za organizacije svih veličina. S obzirom na sofisticiranost današnjih prijetnji i nedostatak stručnjaka u području kibernetičke sigurnosti,

ključno je imati sustav za upravljanje sigurnosnim informacijama i događajima koji može brzo i automatski otkriti povrede i druge sigurnosne probleme. SIEM mogućnosti potiču sve veći broj malih i srednjih organizacija da implementiraju rješenje za upravljanje sigurnošću i događajima.

3.2. Komponente SIEM sustava

SIEM sustav sastoji se od različitih komponenti koje pomažu sigurnosnim timovima u otkrivanju zlonamjernih aktivnosti stalnim nadzorom i analizom mrežnih uređaja i događaja. SIEM sustav čini 9 komponenata: prikupljanje podataka, analitika sigurnosnih podataka, korelacija i praćenje sigurnosnih događaja, forenzička analiza, otkrivanje i odgovor na incidente, odgovor na događaj (konzola za upozorenja u stvarnom vremenu), obavještajni podaci o prijetnjama, analitika ponašanja korisnika i entiteta te upravljanje IT usklađenošću. Svaka od 9 komponenti SIEM sustava je opisana u nastavku.

3.2.1. Prikupljanje podataka

Ova komponenta SIEM rješenja odgovorna je za prikupljanje *log* podataka generiranih iz više izvora unutar korporativne mreže, kao što su serveri, baze podataka, aplikacije, vatrozidi, ruteri (usmjerivači), *cloud* sustavi i drugi. Ovi logovi, koji sadrže zapis svih događaja koji su se dogodili na određenom uređaju ili aplikaciji, prikupljaju se i pohranjuju na centralizirano mjesto. Različite tehnike prikupljanja logova u SIEM-u uključuju prikupljanje logova pomoću agenta, prikupljanje logova bez agenta i prikupljanje logova putem API-ja. U tehnici prikupljanja logova pomoću agenta agent je instaliran na svakom mrežnom uređaju koji generira logove. Agenti su odgovorni za prikupljanje logova s uređaja i prosljeđivanje tih podataka centralnom SIEM serveru. Osim ovih odgovornosti, oni također mogu filtrirati log podatke na razini uređaja na temelju unaprijed definiranih parametara i pretvoriti u odgovarajući format prije prosljeđivanja. Ova prilagođena tehnika prikupljanja i prosljeđivanja logova pomaže u optimalnom korištenju širine pojasa. Metoda prikupljanja logova pomoću agenata uglavnom se koristi u zatvorenim i sigurnim zonama gdje je komunikacija ograničena [9]. U tehnici prikupljanja logova bez agenta ne uključuje se implementacija agenata na bilo kojem mrežnom uređaju. Umjesto toga, potrebno je izvršiti promjene u konfiguraciji uređaja kako bi uređaji mogli sigurno slati generirane logove centralnom SIEM serveru. Na uređajima kao što su *switchevi* (preklopnici), ruteri, vatrozidi itd., često nije podržana instalacija alata treće strane za prikupljanje logova, pa je prikupljanje logova putem agenata otežano. U takvim slučajevima može se koristiti tehnika prikupljanja logova bez agenata. Također smanjuje opterećenje mrežnog uređaja jer nije potrebno implementirati dodatnog agenta. U zadnjoj tehnici, odnosno tehnici prikupljanja logova putem API-ja logovi se mogu prikupljati direktno

s mrežnih uređaja uz pomoć sučelja za programiranje aplikacija. Softver za virtualizaciju pruža API-je koji omogućuju SIEM sustavu da prikuplja logove s virtualnih strojeva na daljinu. Također, kada tvrtke prelaze s lokalnog softvera na *cloud-based* rješenja, postaje teško direktno slati logove SIEM-u jer usluge nisu povezane s fizičkom infrastrukturom. Kada se to dogodi, *cloud-based* SIEM rješenja koriste API-je kao posrednike za prikupljanje i upit logova mreže [9].

3.2.2. Analitika sigurnosnih podataka (izvješća i nadzorne ploče)

SIEM rješenja dolaze s komponentom za sigurnosnu analitiku, koja uglavnom uključuje *live* nadzorne ploče (engl. *dashboards*) koje intuitivno prikazuju sigurnosne podatke u obliku grafova i dijagrama. Ove nadzorne ploče se automatski ažuriraju, pomažući sigurnosnom timu da brzo identificira zlonamjerne aktivnosti i riješi sigurnosne probleme. Pomoću nadzornih ploča, sigurnosni analitičari mogu otkriti anomalije, korelacije, obrasce i trendove koji mogu biti prisutni u podacima te steći različite uvide u događaje koji se odvijaju u stvarnom vremenu. SIEM rješenja također korisnicima omogućuju stvaranje i prilagodbu vlastitih nadzornih ploča. Drugi aspekt ove sigurnosne analitičke komponente su unaprijed definirana izvješća. Često SIEM rješenja dolaze sa stotinama unaprijed definiranih izvješća koja pomažu u pružanju uvida u sigurnosne događaje, otkrivanju prijetnji i olakšavanju usklađenosti. Ova izvješća, koja su uglavnom izgrađena na temelju poznatih indikatora kompromitacije (engl. *Indicators of Compromise,* IOCs), također se mogu prilagoditi kako bi odgovarala internim sigurnosnim potrebama [10].

Većina SIEM rješenja također korisnicima pruža opcije za filtriranje, pretraživanje i detaljno istraživanje ovih izvješća, postavljanje rasporeda za generiranje izvješća prema potrebama korisnika, pregled podataka u obliku tablica i grafova te izvoz izvješća u različitim formatima.

3.2.3. Korelacija i praćenje sigurnosnih događaja

Mehanizam za korelaciju je jedan od najvažnijih komponenti SIEM sustava. Koristeći unaprijed definirana ili korisnički definirana pravila korelacije, prikupljeni podaci iz dnevnika analiziraju se kako bi se otkrili odnosi između različitih mrežnih aktivnosti, zajedničkih atributa ili uzoraka koji mogu postojati. Mehanizmi za korelaciju imaju sposobnost povezivanja različitih sigurnosnih incidenata kako bi se dobio sveobuhvatan pregled sigurnosnih napada. Oni su sposobni rano otkriti znakove sumnjivih aktivnosti, kompromitacije ili potencijalnog proboja u mreži, a SIEM sustav će generirati upozorenja za te aktivnosti.

3.2.4. Forenzička analiza

Ova komponenta SIEM rješenja koristi se za provođenje analize uzroka i generiranje izvještaja o incidentu koji pruža detaljnu analizu pokušaja napada ili tekućeg napada, što pomaže organizacijama da odmah poduzmu odgovarajuće korektivne mjere. Unatoč konstantnom razvoju obrambenih mehanizama, nije uvijek moguće da organizacije spriječe sve kibernetičke napade. Međutim, organizacija može provesti forenzičku analizu kako bi rekonstruirala mjesto zločina i utvrdila osnovni uzrok proboja. Budući da podaci iz dnevnika sadrže zapis svih događaja koji su se dogodili na određenom uređaju ili aplikaciji, mogu se analizirati za tragove koje su ostavili napadači. SIEM sustavi pomažu sigurnosnom timu pregledati dnevnike, generirati forenzičke izvještaje i otkriti vrijeme kada se određeni sigurnosni proboj dogodio, sustave i podatke koji su kompromitirani, hakere iza zlonamjerne aktivnosti, kao i točku ulaska.

Ova komponenta također pomaže organizacijama ispuniti određene zahtjeve usklađenosti kao što su pohrana i arhiviranje podataka iz dnevnika kroz duže vremensko razdoblje te mogućnost provođenja forenzičkih istraga na njima.

3.2.5. Otkrivanje i odgovor na incidente

Otkrivanje incidenta je komponenta SIEM rješenja koja je uključena u otkrivanje sigurnosnih incidenata. Sigurnosni incident odnosi se na pokušaj ili uspješan proboj podataka u mreži od neovlaštene strane, ili kršenje sigurnosnih politika organizacije. Neki uobičajeni primjeri sigurnosnih incidenata su napadi uskraćivanja usluge, zloupotreba podataka i resursa, virusi i *phishing* napadi. Ove incidente treba otkriti i analizirati, te poduzeti odgovarajuće radnje kako bi se riješio sigurnosni problem uz osiguranje kontinuiteta poslovanja. Dok se tijekom otkrivanja incidenata nastoji smanjiti prosječno vrijeme otkrivanja kako bi smanjila štete uzrokovane napadačima, tijekom odgovora na incidente teži se smanjenju prosječnog vremena za rješavanje. Odgovor na incidente je modul SIEM rješenja koji je odgovoran za korektivne radnje koje se poduzimaju kako bi se riješili sigurnosni incidenti nakon otkrivanja. Obzirom na to da se organizacije suočavaju s mnoštvom sigurnosnih problema svakodnevno, a napadači koriste sve sofisticiranije tehnike, odgovor na incidente postao je izazovan pothvat.

3.2.6. Odgovor na događaj (konzola za upozorenja u stvarnom vremenu)

SIEM rješenja obavljaju prikupljanje i korelaciju logova u stvarnom vremenu. Ako se otkrije bilo kakva sumnjiva aktivnost, odmah se podiže upozorenje, a tim za odgovor na incidente će odmah djelovati kako bi ublažio napad ili spriječio njegovu pojavu. Obavijesti o upozorenjima mogu se slati putem e-pošte ili SMS-a (engl. *Short Message Service*) u stvarnom vremenu, a mogu se kategorizirati na temelju prioriteta koji im se dodjeljuju: visok, srednji ili

nizak. Radni tokovi mogu se dodijeliti sigurnosnim incidentima tako da kada se podigne upozorenje, odgovarajući radni tok će se automatski izvršiti.

3.2.7. Obavještajni podaci o prijetnjama

Obavještajni podaci o prijetnjama (engl. *Threat intelligence*) pružaju informacije potrebne za identifikaciju različitih vrsta kibernetičkih prijetnji te poduzimanje odgovarajućih mjera za njihovo sprječavanje, rješavanje ili ublažavanje. Razumijevanjem izvora napada, motivacije iza njega, strategija i metoda korištenih za provođenje napada, kao i znakova kompromitacije, organizacije mogu bolje razumjeti prijetnju, procijeniti rizike i donijeti dobro informirane odluke [11].

Kako bi dodali kontekstualne informacije, kompanije mogu ili dobiti informacije o prijetnjama od trećih strana ili prikupljati i koristiti otvorene izvore informacija o prijetnjama dostupne u STIX/TAXII formatu (STIX i TAXII su standardi razvijeni u nastojanju da poboljšaju prevenciju i ublažavanje kibernetičkih napada. STIX odgovara na pitanje "što" kod obavještajnih podataka o prijetnjama, dok TAXII definira "kako" se te informacije prenose [12]). Vrsta prijetnje može se odmah identificirati, a može se pokrenuti i postupak sanacije, čime se smanjuje prosječno vrijeme otkrivanja.

Ova komponenta također pomaže sigurnosnim administratorima u provođenju potrage za prijetnjama, procesu aktivnog pretraživanja cijele mreže radi pronalaženja bilo kakvih prijetnji ili indikatora kompromitacije koji bi mogli izbjeći sigurnosni sustav.

3.2.8. Analitika ponašanja korisnika i entiteta

Ova komponenta pomaže u otkrivanju sigurnosnih incidenata. S napadačima koji neprestano razvijaju nove tehnike za hakiranje mreže, konvencionalni sigurnosni sustavi brzo postaju zastarjeli. Međutim, organizacije se mogu obraniti od kibernetičkih prijetnji uz pomoć tehnika strojnog učenja. UEBA komponente koriste tehnike strojnog učenja za razvoj modela ponašanja na temelju normalnog ponašanja korisnika i uređaja u organizaciji. Ovaj model ponašanja razvija se za svakog korisnika i entiteta obradom velikih količina podataka dobivenih iz različitih mrežnih uređaja. Svaki događaj koji odstupa od ovog modela ponašanja smatrat će se anomalijom i dalje će se procjenjivati radi potencijalnih prijetnji. Korisniku ili entitetu dodjeljuje se ocjena rizika; što je ocjena rizika viša, veća je sumnja. Na temelju ocjene rizika provodi se procjena rizika, a poduzimaju se korektivne aktivnosti [13].

3.2.9. Upravljanje IT usklađenošću

Kada je riječ o zaštiti podataka i sigurnosti, općenito se očekuje da kompanija zadovolji potrebne standarde, propise i smjernice koje nameću različita regulatorna tijela. Ovi regulatorni zahtjevi variraju za različite kompanije ovisno o vrsti industrije i regiji u kojoj

posluju. Ako organizacija ne uspije udovoljiti tim zahtjevima, bit će kažnjena. Kako bi se osiguralo da organizacija ispunjava sve zahtjeve usklađenosti koje je postavila vlada radi zaštite osjetljivih podataka, SIEM rješenja uključuju komponentu upravljanja usklađenošću. Trebaju se poduzeti i proaktivne mjere poput primjene različitih tehnika za identifikaciju anomalija, uzoraka i kibernetičkih prijetnji kako bi se zaštitili osjetljivi podaci od kompromitacije. SIEM rješenja imaju sposobnost pohranjivanja i arhiviranja podataka iz dnevnika kroz dugi vremenski period kako bi ih revizori mogli provjeriti. Također mogu generirati izvještaje usklađenosti poput HIPAA (engl. *Health Insurance Portability and Accountability Act*), PCI DSS (engl. *Payment Card Industry Data Security Standard*), GDPR (engl. *General Data Protection Regulation*), ISO 27001 (engl. *International Organization for Standardization*) putem prikupljanja i analize dnevnika, kao i izvještaje prilagođene specifičnim zahtjevima navedenim u propisima.

Svi ovi dijelovi SIEM sustava zajedno surađuju kako bi pomogli sigurnosnom timu pružajući uvide u različite vrste prijetnji, njihove obrasce napada i zlonamjerne aktivnosti koje se mogu događati u mreži, kao i nužne korake koji se moraju poduzeti kako bi se riješili problemi sigurnosti.

3.3. Funkcije SIEM sustava

SIEM sustavi pružaju sveobuhvatan pregled svih aktivnosti koje se događaju u IT infrastrukturi praćenjem mrežnih aktivnosti te primjenom obavještajnih podataka o prijetnjama i analitike ponašanja korisnika i entiteta radi otkrivanja i ublažavanja napada. Na slici 2. su prikazane funkcije SIEM sustava koje će biti opisane u nastavku.

Slika 2. Funkcije SIEM sustava

Izvor: [14]

3.3.1. Upravljanje zapisnicima

Upravljanje zapisnicima je praksa kontinuiranog prikupljanja, pohranjivanja, obrade i analize podataka iz različitih programa i aplikacija s ciljem optimizacije performansi sustava, prepoznavanja tehničkih problema, boljeg upravljanja resursima, jačanja sigurnosti i poboljšanja usklađenosti. Obično se logovi bilježe u jednom ili više *log* datoteka. Upravljanje logovima omogućuje da se podaci skupe na jednom mjestu i promatraju kao cjelina umjesto kao zasebni entiteti. Na taj način se mogu analizirati prikupljeni *log* podaci, identificirati problemi i obrasci kako bi se dobila jasna i vizualna slika o tome kako svi sustavi funkcioniraju u bilo kojem trenutku. Učinkovito rješenje za upravljanje zapisnicima pruža mnoge prednosti poput poboljšane vidljivosti događaja u cijeloj organizaciji kroz centralizirani zapisnik događaja, praćenja u stvarnom vremenu i brže i preciznije rješavanje problema [15].

3.3.2. Upravljanje incidentima

Incidenti mogu uzrokovati mnoštvo problema za organizacije, od privremenog prekida rada do gubitka podataka. Kada se dobro izvede, upravljanje incidentima (engl. *Incident management*) može pružiti učinkovit i djelotvoran način za popravljanje svih vrsta incidenata uz malo prekida i ostaviti organizacije spremnijima za buduće incidente. *Incident management* je ključni aspekt upravljanja IT uslugama. Omogućuje vraćanje usluge u normalno stanje što je brže moguće nakon incidenta, minimiziranje utjecaja na poslovne operacije te osiguravanje najbolje moguće razine usluge i dostupnosti. Obuhvaća skup praksi za identifikaciju, analizu i rješavanje operativnih problema te donosi razne koristi.

Implementacijom robusnog procesa upravljanja incidentima, organizacije mogu unaprijediti svoju sposobnost odgovora na incidente i sprječavanja budućih poremećaja. Ovaj proaktivni pristup omogućuje tvrtkama da identificiraju i riješe potencijalne probleme prije nego što eskaliraju, čime se minimizira utjecaj na poslovne operacije. Sveukupno, upravljanje incidentima igra ključnu ulogu u održavanju stabilnosti i pouzdanosti IT usluga, omogućujući organizacijama da pružaju visokokvalitetne usluge svojim korisnicima [16].

3.3.3. Revizija povlaštenog pristupa

Privilegirani korisnički računi su oni s administratorskim ovlastima. Te ovlasti mogu omogućiti korisniku instalaciju, uklanjanje ili ažuriranje softvera; izmjenu konfiguracija sustava; stvaranje, izmjenu ili promjenu korisničkih dozvola; i više. Privilegirani računi od iznimne su važnosti za osiguranje sigurnosti mreže, jer samo jedan kompromitirani privilegirani korisnički račun može omogućiti napadaču veći pristup mrežnim resursima. Važno je pratiti i revizirati radnje privilegiranih korisnika te generirati upozorenja u stvarnom

vremenu za neobične aktivnosti. Praćenje privilegiranih korisničkih računa može pomoći u praćenju i sprječavanju unutarnjih napada, jer ovi računi imaju ovlasti za promatranje aktivnosti drugih korisnika u mreži. Ako korisnici pokušaju eskalirati svoje ovlasti, to može biti potencijalna prijetnja. SIEM rješenja mogu detektirati takvo ponašanje i revizirati aktivnosti privilegiranih korisnika kako bi unaprijedila sigurnost mreže.

3.3.4. Obavještajni podaci o prijetnjama

Obavještajni podaci o prijetnjama (engl. *Threat Intelligence*) su podaci koji se prikupljaju, obrađuju i analiziraju kako bi se razumjeli motivi, ciljevi i ponašanje aktera. Obavještajni podaci o prijetnjama omogućuju donošenje bržih, informiranijih sigurnosnih odluka potkrijepljenih podacima i promjenu njihovog ponašanja iz reaktivnog u proaktivno u borbi protiv prijetnji. *Threat intelligence* kombinira znanje dobiveno iz dokaza, kontekstualnih informacija, indikatora i akcijskih odgovora prikupljenih iz različitih prijetnji te proizvodi konkretne primjere indikatora kompromitacije. Također može pružiti informacije o taktikama, tehnikama i postupcima (engl. *Tactis Techniques and Procedures*, TTP) uključenim u novonastale prijetnje te može nadzirati trenutne mrežne aktivnosti radi prepoznavanja sumnjivih uzoraka [17].

3.3.5. Sigurnost u oblaku

Sigurnost u oblaku se odnosi na zaštitu resursa koji se nalaze na platformama u oblaku. Ti resursi uključuju aplikacije, infrastrukture ili baze podataka. Organizacije mogu osigurati svoje podatke u oblaku primjenom kombinacije pravila, tehnika i tehnologija za praćenje i zaštitu podataka koji ulaze i izlaze iz oblaka. Davatelji usluga u oblaku implementiraju sigurnosne mjere poput enkripcije, detekcije upada, naprednih vatrozida, zapisivanja događaja, usklađenosti s sigurnosnim propisima te fizičke sigurnosti u podatkovnim centrima kako bi održali sigurnost u oblaku. Oni se opremaju najnovijim tehnologijama i iskusnim stručnjacima za kibernetičku sigurnost kako bi svojim korisnicima ponudili sigurnost podataka vrhunske klase. Dodatno, korisnici mogu odabrati dodatne mjere kibernetičke sigurnosti poput vatrozida za *web* aplikacije (engl. *Web Application Firewall,* WAF), upravljanja identitetom i pristupom (engl. *Identity and Access Management,* IAM) itd., kao dodatne sigurnosne mjere po potrebi [18].

3.3.6. Analitika ponašanja korisnika i entiteta

UEBA u SIEM rješenjima obično se temelji na ML-u ili AI-u te analizira normalni radni uzorak korisnika ili tipičan način na koji određeni korisnik pristupa mreži svakodnevno. Može detektirati odstupanja od normalnog ponašanja, podići upozorenje i odmah obavijestiti administratora za sigurnost. Što više informacija SIEM rješenje obradi iz različitih izvora poput

rutera, vatrozida, kontrolera domene, aplikacija, baza podataka i svakog računalnog uređaja u mreži, to preciznije može postati otkrivanje anomalija tijekom vremena. UEBA koristi ML tehnike i AI algoritme za obradu informacija, učenje uzoraka prijetnji te identifikaciju ako je određeni uzorak u mreži sličan anomaliji prijetnje koja se već dogodila. S ovim otkrivanjem, UEBA pomaže generirati upozorenja u stvarnom vremenu i koristi automatizaciju u prevenciji prijetnji kako bi bila pouzdanija [13].

3.3.7. Zaštita podataka

Jedan od glavnih ciljeva stručnjaka za kibernetičku sigurnost je spriječiti gubitak ili iznošenje osjetljivih podataka. SIEM rješenja pomažu u otkrivanju, ublažavanju i sprječavanju povreda podataka kontinuiranim praćenjem ponašanja korisnika. SIEM rješenja prate pristupe kritičnim podacima te identificiraju neovlaštene pristupe ili pokušaje pristupa. Također nadziru eskalacije privilegija u korisničkim računima i promjene podataka koje su izvršene tim računima. Kada se ove sposobnosti detekcije kombiniraju s upravljanjem radnim procesima, stručnjaci za kibernetičku sigurnost mogu konfigurirati SIEM rješenje kako bi spriječili zlonamjerne aktivnosti u mreži.

4. IZAZOVI INTEGRACIJE SIEM SUSTAVA

Integracije SIEM sustava pružaju organizacijama dodatni sloj zaštite za njihove podatke. Povezivanjem sustava kako bi se informacije dijelile između različitih aplikacija u stvarnom vremenu, postaje mnogo teže neovlaštenim osobama poput hakera ili kriminalaca da pristupe ili manipuliraju osjetljivim informacijama. Nadalje, korištenjem najnovijih tehnologija, kao što su umjetna inteligencija i strojno učenje , organizacije mogu dodatno ojačati svoje sigurnosne sustave i osigurati da su uvijek ažurirani s najnovijim prijetnjama. Još jedna prednost implementacije sveobuhvatnog sigurnosnog sustava sa SIEM integracijama su napredne mogućnosti detekcije koje pruža. Povezivanjem postojećih sustava u jednu platformu, organizacije mogu iskoristiti moćne analitičke alate za otkrivanje potencijalnih prijetnji prije nego što postanu problem. Na primjer, ako se pojavi sumnjiva aktivnost na nekom sustavu ili aplikaciji, sigurnosno operativni centar može odmah biti upozoren kako bi se poduzele potrebne mjere za sprječavanje bilo kakve štete. Time se značajno smanjuje rizik od zastoja ili gubitka podataka zbog zlonamjernih napada ili drugih nepredviđenih okolnosti.

Integracija SIEM sustava s ostalim alatima za zaštitu informacijsko-komunikacijskog sustava predstavlja ključan korak u izgradnji sveobuhvatnog i učinkovitog sigurnosnog okvira za bilo koju organizaciju. Kako bi se organizacije maksimalno zaštitile, potrebno je pažljivo planirati i upravljati procesom integracije. Pravilno planiranje uključuje provođenje temeljitih procjena potreba, odabir pravog SIEM rješenja i dodjelu adekvatnih resursa. Međutim, proces integracije SIEM-a s ostalim sigurnosnim alatima kao što su antivirusni programi, sustavi za sprječavanje upada (engl. *Intrusion Prevention System,* IPS), vatrozidi, i drugi alati za mrežnu sigurnost i upravljanje ranjivostima, može biti izazovan. Ovi izazovi proizlaze iz različitih aspekata kao što su tehnička složenost, problemi kompatibilnosti i performansi, ograničenja resursa i potreba za kontinuiranim održavanjem i ažuriranjem koja je nužna za održavanje učinkovitosti i efikasnosti SIEM sustava.

Ulaganje u sveobuhvatan sigurnosni sustav sa SIEM integracijama izvrstan je način za organizacije da zaštite svoje podatke, dok istovremeno ostvaruju i druge koristi tijekom vremena. Ova rješenja pružaju dodatni sloj zaštite od potencijalnih prijetnji, dok također olakšavaju otkrivanje sumnjivih aktivnosti prije nego što postanu problem, ali također je bitno savladati izazove integracije kako bi cjelokupan sustav radio na željeni način, odnosno pružao maksimalnu zaštitu sustava.

4.1. Formati log zapisa

SIEM sustav nadzire i osigurava mrežu organizacije nadziranjem različitih vrsta podataka iz mreže. *Log* podaci bilježe svaku aktivnost koja se događa na uređaju i aplikacijama diljem mreže. Kako bi procijenila sigurnosnu situaciju mreže, SIEM rješenja moraju prikupljati i analizirati različite vrste *log* podataka.

Log podaci su bitna komponenta svakog IT sustava i pomažu kod:

- praćenja performansi infrastrukture,
- otkrivanja pogreške u aplikaciji,
- praćenja i analize aktivnosti,
- otkrivanja i odgovora na sigurnosne incidente,
- praćenja ponašanja korisnika,
- forenzičke istrage.

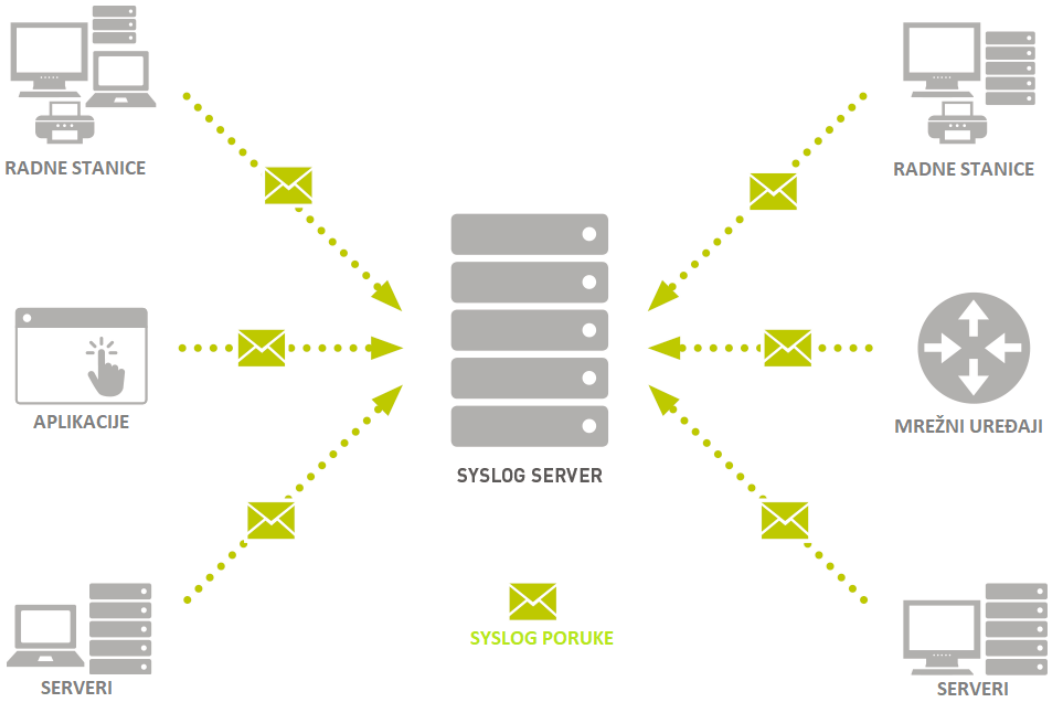
Dobro osmišljeno rješenje za upravljanje logovima će učitati, analizirati i pohraniti *log* podatke bez obzira na njihov format. To znači da se mogu pretraživati, analizirati i povezivati podaci iz različitih sustava kako bi se pronašli trendovi, izradile nadzorne ploče, pa čak i pokrenula upozorenja kako bi se poboljšali poslovni procesi organizacije.

U kontekstu SIEM sustava, rukovanje različitim formatima logova ključno je za učinkovito prikupljanje, agregiranje, normaliziranje i analizu podataka iz različitih izvora. U sljedećim poglavljima su navedeni neki od uobičajenih formata logova s kojima se SIEM sustavi mogu susresti

4.1.1. Karakteristik*e Syslog* formata logova

Syslog je kratica za *System Logging Protocol* i predstavlja standardni protokol koji se koristi za slanje sistemskih logova ili poruka o događajima na određeni server, nazvan *syslog* server. Popularni standard za zapisivanje poruka je razvijen kao dio *SendMail* projekta 1980.-ih godina [19]. Prvenstveno se koristi za prikupljanje logova s nekoliko različitih uređaja na jednom centralnom mjestu radi praćenja i pregleda. Protokol je omogućen na većini mrežne opreme kao što su ruteri, preklopnici, vatrozidi, pa čak i neki pisači i skeneri. *Syslog* server je također poznat kao *syslog* kolektor ili prijemnik. *Syslog* poruke se šalju s uređaja koji ih generira na kolektor (slika 3.). IP (engl. *Internet Protocol*) adresa odredišnog *syslog* servera mora biti konfigurirana na samom uređaju, bilo putem komandne linije ili putem *config* datoteke. Nakon što je konfiguracija postavljena, svi *syslog* podaci će se slati na taj server koji

pohranjuje podatke u */etc/syslog.conf* datoteku. Unutar *syslog* protokola ne postoji mehanizam koji bi omogućio drugom serveru da zatraži *syslog* podatke.



Slika 3. Prikupljanje *syslogova* iz različitih izvora na *Syslog* server

Izvor: [20]

Syslog poruke o događajima generiraju pojedinačne aplikacije ili drugi dijelovi sustava. Sve *syslog* poruke slijede standardni format, što je potrebno za dijeljenje poruka između aplikacija. Ovaj format uključuje sljedeće komponente:

- Zaglavlje koje uključuje specifična polja za prioritet, verziju, vremenski pečat, naziv hosta, aplikaciju, ID procesa i ID poruke.
- Strukturirane podatke s blokovima podataka u formatu ključ-vrijednost.
- Poruku koja treba biti kôdirana u UTF-8 (engl. *Unicode Transformation Format*). Uključuje oznaku koja identificira proces koji je pokrenuo poruku, zajedno sa sadržajem poruke.

Za identifikaciju izvora poruke, *syslog* koristi numerički kôd objekta, ili *facility*, koji generira izvor poruke. Ovi kôdovi potječu iz Unix sustava i nisu očiti na temelju njihovih vrijednosti. Slika 4. pokazuje kôd poruke koji se povezuje s odgovarajućim objektom.

Facility Number	Facility Description	Facility Number	Facility Description
0	kernel messages	12	NTP subsystem
1	user-level messages	13	log audit
2	mail system	14	log alert
3	system daemons	15	clock daemon
4	security/authorization messages	16	local use 0 (local0)
5	messages generated internally by syslog	17	local use 1 (local1)
6	line printer subsystem	18	local use 2 (local2)
7	network news subsystem	19	local use 3 (local3)
8	UUCP subsystem	20	local use 4 (local4)
9	clock daemon	21	local use 5 (local5)
10	security/authorization messages	22	local use 6 (local6)
11	FTP daemon	23	local use 7 (local7)

Slika 4. Kôdovi poruke i njihovo povezivanje s odgovarajućim objektom, [19]

Syslog poruka je također označena numeričkim pokazateljem ozbiljnosti (slika 5.), pri čemu 0 označava potpunu hitnost, a 7 se koristi za svrhe otklanjanja pogrešaka.

Severity Level	Severity Description
0	EMERGENCY - System unusable
1	ALERT - Action must be taken immediately
2	CRITICAL - Critical conditions
3	ERROR - Error conditions
4	WARNING - Warning conditions
5	NOTICE - Normal but significant conditions
6	INFORMATIONAL - Informational messages
7	DEBUG - Debug level messages

Slika 5. Numerički pokazatelj ozbiljnosti *syslog* poruke, [19]

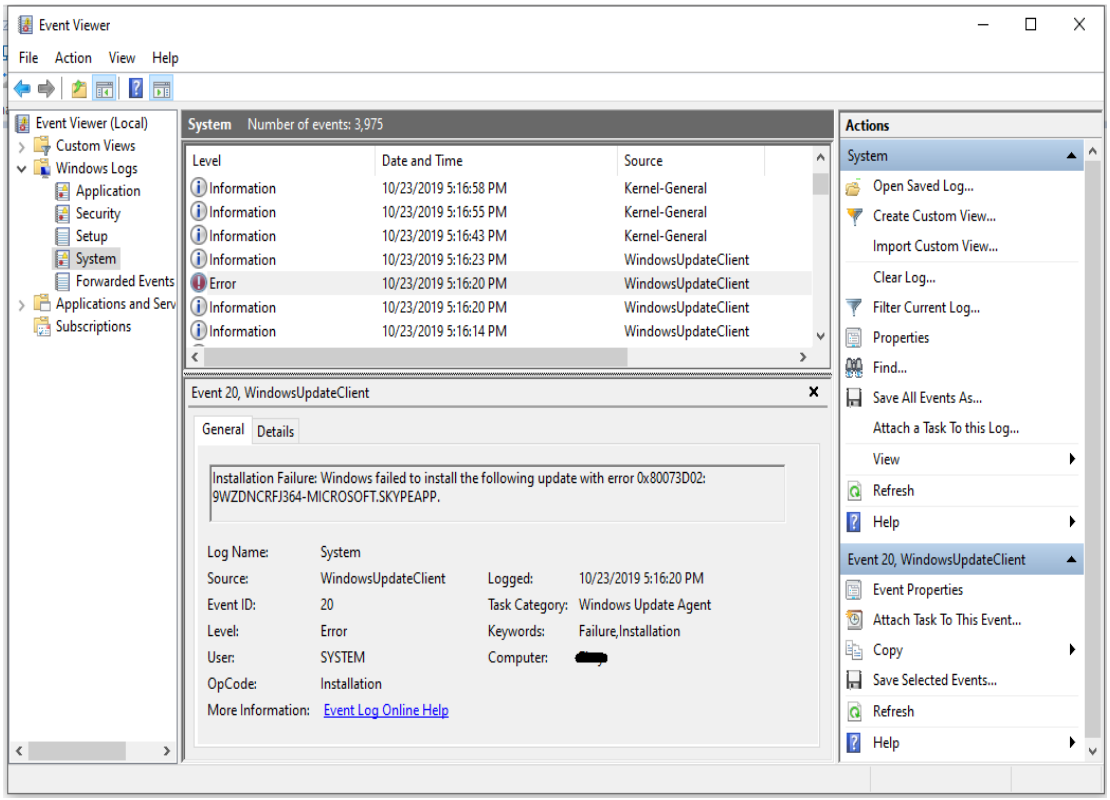
Vrijednosti oba pokazatelja nemaju stroge definicije. Stoga je na sustavu ili aplikaciji da odredi kako će zabilježiti događaj (na primjer, kao upozorenje, obavijest ili nešto drugo) i na kojem objektu. Unutar iste aplikacije ili usluge, niži brojevi trebaju odgovarati ozbiljnijim problemima u odnosu na specifični proces. Osim toga, *syslog* je dostupan na Unix i Linux sustavima te na mnogim web poslužiteljima uključujući *Apache*. *Syslog* nije instaliran na *Windows* sustavima, koji koriste vlastiti *Windows Event Log* opisan u sljedećem poglavlju. Ti događaji mogu biti proslijeđeni putem alata trećih strana ili drugih konfiguracija koristeći *syslog* protokol.

4.1.2. Karakteristike *Windows Event Logs* formata logova

Operacijski sustav *Windows* ima protokol za zapisivanje događaja koji omogućuje aplikacijama i samom sustavu bilježenje važnih hardverskih i softverskih događaja [21]. *Windows Event* logovi često se koriste od strane sistemskih administratora za otklanjanje pogrešaka sustava ili aplikacija, istraživanje sigurnosnih incidenata ili praćenje prijava

korisnika. Elementi koji čine *Windows Event Logs* su slijedeći razina, datum, vrijeme, izvor ID događaja, kategorija zadatka, korisnik i računalo. Razina predstavlja ozbiljnost događaja uključujući informacije, upozorenja i pogrešku (sve detaljno prikazano). Datum i vrijeme prikazuju točan datum i vrijeme kada se određeni događaj dogodio. Izvor predstavlja program ili komponentu koja je uzorkovala događaj. ID događaja je zapravo *Windows* identifikacijski broj koji specificira točno određenu vrstu događaja, dok kategorija zadatka prikazuje vrstu zabilježenog događaja. Elementi korisnik i računalo predstavljaju korisničko ime korisnika koji bio prijavljen na računalo i naziv računala.

Prikaz *log* datoteke podijeljen je na dva dijela smještena u središtu *Event Viewera*. Gornji dio prikazuje glavne detalje o svakom događaju u formatu popisa (slika 6.). Popis se može sortirati klikom na bilo koji od naslova na vrhu gornjeg dijela. Donji dio prikazuje detalje povezane s bilo kojim zapisom događaja koji je odabran s popisa događaja iznad.



Slika 6. Prikaz *Windows Event* logova u *Event Vieweru,* [19]

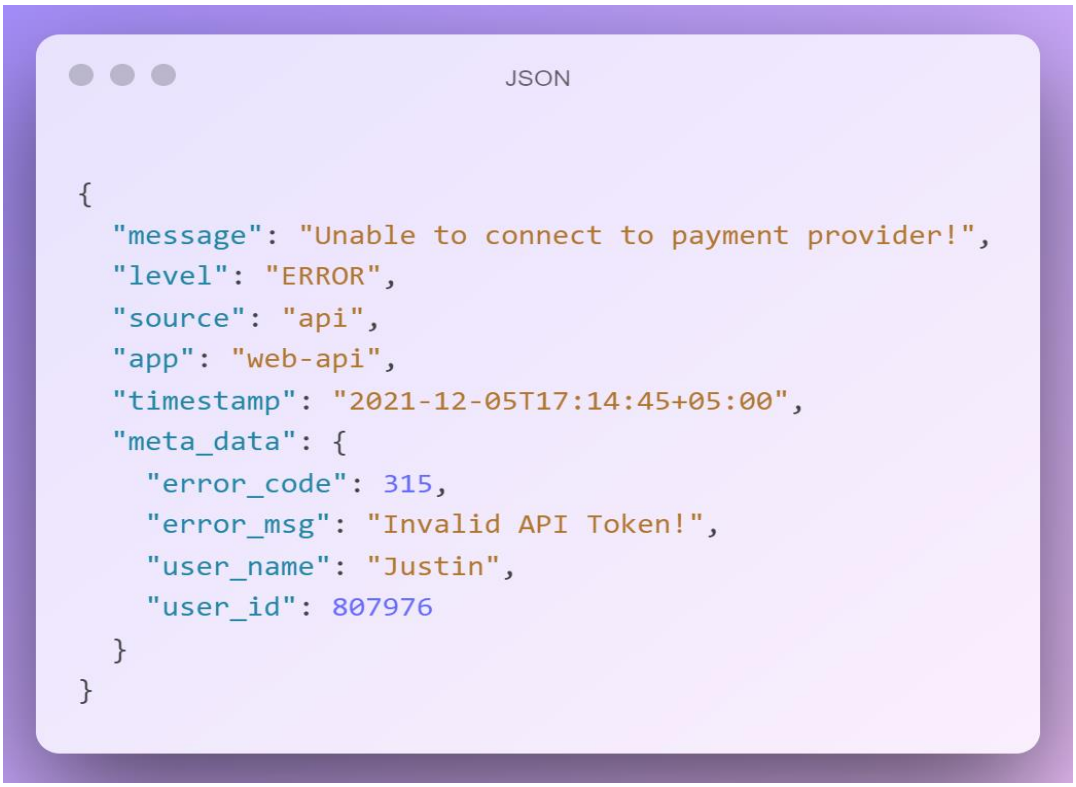
4.1.3. Krakteristike JSON formata logova

JavaScript Object Notation (JSON) jedan je od najčešće korištenih formata za zapisivanje logova. JSON logovi su polustrukturirani (engl. *semi-structured logs* su lako čitljivi za ljude, ali također imaju shemu ili uzorak, što ih čini čitljivima i za strojeve. Imaju složenije razdjelnike polja i događaja od zareza ili znaka jednakosti, ali ipak imaju uzorak. Sustavi za upravljanje logovima mogu unositi polustrukturirane logove, ali obično zahtijevaju parser za

razdvajanje događaja i izdvajanje parova ključ-vrijednost [22].), sadrže više parova ključ-vrijednost.

Jedna od prednosti JSON-a u odnosu na druge formate za razmjenu podataka, poput XML-a, je ta što ga je ljudima lako i čitati i pisati (slika 7.). Za razliku od XML-a, JSON se ne oslanja na složenu shemu i potpuno izbjegava velik broj uglatih zagrada koje nastaju zbog potrebe da sve bude unutar oznaka. To čini JSON puno lakšim za početnike. JSON dokument sastoji se od jednostavne sintakse parova ključ-vrijednost, koji su poredani i ugniježđeni unutar nizova. Na primjer, ključ nazvan "status" može imati vrijednosti "*success*" (uspjeh), "*warning*" (upozorenje) i "*error*" (pogreška). Ključevi su definirani unutar dokumenta i uvijek su navedeni u navodnicima, što znači da nema rezerviranih riječi koje treba izbjegavati, a nizovi mogu biti ugniježđeni kako bi se stvorile hijerarhije [23].

To znači da se mogu stvoriti bilo koji ključevi koji imaju smisla za kontekst organizacije i strukturirati ih kako god odgovara organizaciji. Ključeve i način na koji su ugniježđeni (specifikacija JSON-a) trebaju dogovoriti pošiljatelj i primatelj, koji tada mogu čitati datoteku i izdvajati podatke prema potrebi.

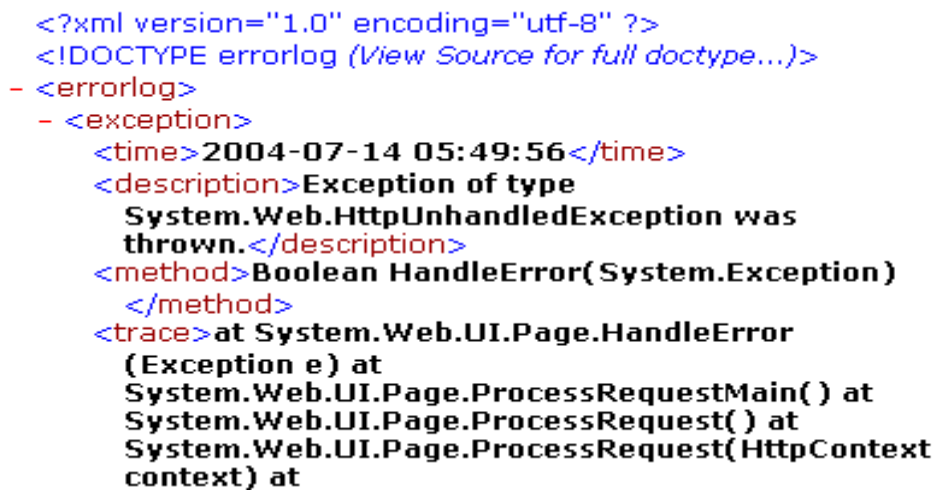


Slika 7. Prikaz JSON log zapisa, [23]

4.1.4. Karakteristike XML formata logova

XML (engl. *eXtensible Markup Language*) logovi (slika 8.) su format koji se koristi za pohranu i prijenos podataka na strukturiran način, koji mogu lako čitati i ljudi i strojevi. U

kontekstu SIEM sustava, XML logovi su jedan od mnogih formata logova koji se trebaju obrađivati za učinkovitu analizu podataka.



Slika 8. Prikaz primjera XML loga, [24]

Ključne karakteristike XML logova uključuju strukturirane podatke, čitljivost za ljude i strojeve i proširivost. Pojam strukturirani podaci znači da XML koristi strukturu stabla s ugniježđenim oznakama za prikaz podataka, što ga čini visoko organiziranim. Izuzetno je važna i čitljivost za ljude i strojeve koja je dizajnirana tako da ga ljudi i strojevi mogu čitati. Kod ljudi je to bitno ukoliko se provodi ručna provjera, a za strojeve čitljivost može biti pogodna za automatiziranu obradu i analizu. Naposljetku, proširivost XML logova kroz definiranje prilagođenih oznaka omogućuje fleksibilnost u načinu prikaza podataka.

Obrada XML logova u SIEM sustavima se obavlja kroz procese parsiranja, normalizacije, korelacije, pohrane, vizualizacije i integracije. Parsiranje je proces transformacije nestrukturiranih logova u strukturirani format koji određeni sustav ili stroj može čitati. U SIEM sustavima proces parsiranja uključuje čitanje XML strukture kako bi se izvukla relevantna polja podataka i pretvorila u format koji SIEM može razumjeti. Nakon parsiranja, XML podaci trebaju biti normalizirani čime se osigurava da se podaci iz XML logova pretvore u zajednički format koji se može analizirati uz logove iz drugih izvora. Zatim slijedi korelacija gdje SIEM sustavi koreliraju događaje iz XML logova s drugim *log* podacima kako bi otkrili obrasce i identificirali potencijalne sigurnosne incidente. Svi XML logovi se mogu pohraniti u svom izvornom formatu ili u normaliziranom obliku unutar SIEM-a za buduću analizu. Također, SIEM sustavi često pružaju mogućnost vizualizacije kako bi sigurnosnim analitičarima pomogli lakše razumjeti podatke unutar XML logova. Naposljetku, XML logovi se mogu integrirati s drugim sigurnosnim alatima i *feedovima* obavještajnih podataka kako bi se poboljšao cjelokupni sigurnosni položaj organizacije.

Nakon prikazanih procesa obrade XML logova u SIEM sustavima, u nastavku slijede primjeri upotrebe XML logova. Primjeri upotrebe XML logova mogu se prikazati kroz logove aplikacija, revizijske logove i konfiguracijske logove. Logovi aplikacija se mogu naći u mnogim poslovnim aplikacijama u XML formatu, bilježeći detaljne operativne i sigurnosne događaje. Revizijski logovi u XML formatu nastaju ukoliko razni sustavi i aplikacije bilježe revizijske tragove, što može biti ključno za usklađenost i forenzičku analizu. Naposljetku, konfiguracijski logovi u XML formatu se mogu koristiti u upravljanju konfiguracijama, gdje se bilježe i prate promjene u konfiguracijama sustava ili aplikacija koje mogu dati važne potrebne informacije za stručnjake za kibernetičku sigurnost. Efektivnim rukovanjem XML logovima, SIEM sustavi mogu pružiti sveobuhvatan pregled sigurnosnih događaja u IT okruženju organizacije, što dovodi do bolje detekcije, odgovora i ublažavanja sigurnosnih incidenata [25, 26].

4.1.5. Karakteristike CSV formata logova

CSV (engl. *Comma-Separated Values*) logovi jedan su od uobičajenih formata logova koji se koriste u SIEM sustavima. Pohranjuju *log* podatke u tabličnom formatu gdje svaki redak predstavlja zapis, a svako polje unutar zapisa odvojeno je zarezom. CSV logovi su široko korišteni jer ih je lako generirati i parsirati, te se mogu otvoriti i pregledati u raznim aplikacijama, uključujući softver za proračunske tablice poput Microsoft Excela [27].

Ključne karakteristike CSV logova su jednostavnost, struktura, fleksibilnost i kompatibilnost. Jednostavnost se očitava kroz to da su CSV datoteke obične tekstualne datoteke što ih čini lakim za generiranje i čitanje. Struktura je formirana tako da svaki redak u CSV datoteci odgovara jednom log događaju, a polja su odvojena zarezom. Fleksibilnost CSV logova je širokog raspona jer se CSV logovi mogu koristiti za bilježenje različitih tipova podataka i nisu ograničeni na određenu shemu. Kompatibilnost je još jedan razlog zašto su CSV logovi pogodni. CSV logovi mogu se uvesti u mnoge različite alate i aplikacije za daljnju analizu, uključujući SIEM sustave.

Primjer CSV logova:

```
timestamp,hostname,event_type,message
2023-10-25 14:23:01,server1,login,User 'admin' logged in successfully
2023-10-25 14:25:34,server2,logout,User 'admin' logged out
```

Budući da su CSV datoteke dizajnirane da budu relativno jednostavne, često se koriste u širokom rasponu industrija i u kibernetičkoj sigurnosti za prijenos podataka između aplikacija. Jedna od glavnih funkcija CSV datoteka je razmjena podataka. S CSV datotekama moguće je izvesti komplicirane podatke iz jedne aplikacije u CSV format, a zatim uvesti te

izvezene CSV podatke u drugu aplikaciju gdje se mogu koristiti. CSV datoteke također igraju važnu ulogu u analizi sigurnosnih logova koje generiraju različiti alati za zaštitu informacijsko-komunikacijskog sustava. Analiza sigurnosnih logova je jako važna pri identifikaciji sigurnosnih incidenata, praćenju sigurnosnih propusta kako bi se odredio njihov uzrok i asistenciji u forenzičkoj analizi napada. Zbog jednostavnog formata CSV datoteka, stručnjacima za kibernetičku sigurnost lakše je doći do željenih informacija potrebnih za procjenu sigurnosnog stanja organizacije. Još jedna svrha CSV datoteka je njihovo korištenje tijekom penetracijskih testiranja za procjenu sigurnosnog stanja neke organizacije. Tijekom penetracijskih testiranja, CSV datoteke olakšavaju dokumentiranje zbog svoje strukture i fleksibilnosti. Naposljetku, CSV datoteke imaju važnu ulogu u procesu upravljanja ranjivostima. Upravljanje ranjivostima je proces identificiranja, procjene i otklanjanja kibernetičkih ranjivosti na krajnjim točkama i sustavima, a rezultati takvog procesa često se pohranjuju u CSV formatu.

Zaključno, važno je biti upoznat s različitim formatima log zapisa kako bi SIEM sustavi mogli poboljšati sposobnost praćenja i analize sigurnosnih događaja, što u konačnici unapređuje sigurnosni položaj organizacije.

4.2. Interoperabilnost s ostalim sigurnosnim alatima

SIEM sustavi mogu raditi u kombinaciji s raznovrsnim drugim sigurnosnim alatima kako bi stvorili sveobuhvatan sigurnosni ekosustav. Ova interoperabilnost je ključna za poboljšanje ukupnog sigurnosnog položaja organizacije. Moguće su razne integracije SIEM sustava s drugim sigurnosnim alatima, a u nastavku je navedeno nekoliko ključnih integracija SIEM sustava s drugim sigurnosnim alatima te njihova interoperabilnost. Prva integracija je integracija SIEM sustava s IDS alatom. Povezujući IDS sa SIEM-om, može se iskoristiti snaga oba alata kako bi se poboljšale sposobnosti detekcije i odgovora. Na primjer, SIEM se može koristiti za filtriranje lažnih alarma, davanje prioriteta upozorenjima i generiranje izvještaja iz IDS podataka. Također, SIEM je moguće koristiti za pokretanje automatiziranih radnji, poput slanja obavijesti, blokiranja IP adresa ili izoliranja računala, na temelju IDS upozorenja.

Sljedeća moguća integracija je integracija s EDR (engl. *Endpoint Detection and Response*) alatima.EDR je najbolji za sigurnost krajnjih točaka i odgovor na prijetnje, dok je SIEM idealan za cjelokupno upravljanje sigurnošću, usklađenost i detekciju prijetnji na razini mreže. Ova integracija omogućuje bolje usklađivanje podataka s krajnjih točaka s mrežnim i sistemskim događajima. SIEM sustavi mogu se integrirati s alatima za EDR radi prikupljanja detaljnih informacija o krajnjim točkama. Ova integracija omogućuje praćenje aktivnosti krajnjih točaka u stvarnom vremenu, otkrivanje sumnjivih ponašanja i automatizirani odgovor na incidente. Na primjer, SIEM sustavi mogu prikupljati podatke iz EDR rješenja, obogaćujući

svoje sposobnosti detekcije prijetnji. Ova integracija omogućuje SIEM-u da uskladi podatke s krajnjih točaka i mrežnog prometa, pružajući sveobuhvatniji uvid u potencijalne prijetnje.

Zatim slijedi integracija SIEM-a s vatrozidima i alatima za mrežnu sigurnost. Vatrozidi i drugi uređaji za mrežnu sigurnost generiraju veliki broj logova i upozorenja. SIEM može pomoći organizacijama da izvuku više vrijednosti iz logova vatrozida. Zatim SIEM koristi tehnike poput korelacije događaja i detekcije na temelju potpisa kako bi identificirao sumnjivu aktivnost te izdaje upozorenja kako bi stručnjaci za kibernetičku sigurnost mogli brzo reagirati.

SIEM je također moguće integrirati s alatima za upravljanje ranjivostima. SIEM prikuplja i analizira sigurnosne podatke iz različitih izvora, pružajući pregled potencijalnih prijetnji, dok alati za upravljanje ranjivostima procjenjuju ranjivosti i usmjeravaju prioritizaciju za ispravljanje. Integracijom s alatima za upravljanje ranjivostima, SIEM sustavi mogu korelirati informacije o ranjivostima s podacima o stvarnim događajima u stvarnom vremenu. Integracija SIEM-a i alata za upravljanje ranjivostima nudi nekoliko prednosti za organizacije, uključujući smanjeni rizik od iskorištavanja ranjivosti, poboljšano vrijeme odgovora na incidente i pouzdanije donošenje odluka.

Integracija SIEM sustava s IAM sustavima omogućuje SIEM-ovima praćenje aktivnosti korisnika i obrazaca pristupa. Slanje informacija iz IAM sustava u SIEM sustav može pomoći stručnjacima za kibernetičku sigurnost u pronalaženju događaja i anomalija koje se možda ne bi otkrile na drugi način. Takva integracija može pomoći otkrivanje neovlaštenog pristupa napadača u sustav organizacije.

Također, SOAR platforme mogu raditi zajedno sa SIEM sustavima kako bi automatizirale odgovor na otkrivene incidente. Integracija SIEM i SOAR platformi može poboljšati sigurnosne operacije pružajući bolju vidljivost, smanjene ručnih zadataka, ubrzani odgovor i poboljšanu suradnju. Ova kombinacija podataka i obavještajnih informacija pruža uvid u okruženje, prijetnje i detalje o incidentima.

Kako organizacije sve više prelaze na okruženja u oblaku, SIEM sustavi moraju se integrirati s alatima i uslugama za sigurnost u oblaku. SIEM rješenje može pristupiti i prikupljati relevantne podatke s *cloud* usluga i aplikacija, poput logova, metrika, upozorenja i događaja. Na primjer, moguće je postaviti SIEM pravila i politike koje će obavijestiti stručnjake za kibernetičku sigurnost kada dođe do neuobičajene ili sumnjive aktivnosti u *cloud* okruženju, poput skoka u prometu, neuspjelog pokušaja prijave ili promjene konfiguracije.

Naposljetku, moguće je integrirati SIEM sustav sa sustavima za izdavanje tiketa. Integracija sustava za izdavanje tiketa sa SIEM-om može pružiti nekoliko prednosti organizacijama. Može pomoći u optimizaciji procesa odgovora na incidente, smanjenju vremena odgovora i poboljšanju ukupne učinkovitosti SOC-a. Integracija također pruža priliku

organizacijama da poboljšaju svoje sposobnosti odgovora na incidente koristeći mogućnosti oba sustava. Na primjer, sustav za izdavanje tiketa može pružiti centralizirano mjesto za praćenje i upravljanje incidentima, dok SIEM može pomoći u identifikaciji i davanju prioriteta incidentima na temelju njihove ozbiljnosti.

Interoperabilnost s drugim sigurnosnim alatima poboljšava mogućnosti SIEM sustava pružajući sveobuhvatnu vidljivost i kontrolu nad sigurnosnim okruženjem. Integracijom s raznim sigurnosnim rješenjima, SIEM sustavi mogu ponuditi učinkovitiji i kohezivniji pristup otkrivanju prijetnji, odgovoru na incidente i ukupnom upravljanju sigurnošću [28].

4.3. Problemi performansi

U današnjem digitalnom svijetu, većina problema s performansama su problemi s količinom podataka koje premašuju mogućnosti organizacija da ih obrađuju i izvlače vrijednost iz njih. U 2025. godini organizacije će upravljati s 250% više podataka nego što su upravljale 2020. godine [29]. Loše optimiziran SIEM može upotrijebiti puno više resursa nego što mu je potrebno, a to definitivno utječe na sigurnosno stanje organizacije. Izazovi upravljanja povećanjem količine poslovnih podataka izravno utječu na sposobnost organizacije da na odgovarajući način upravlja rizicima kibernetičke sigurnosti. Optimiziranje SIEM-a bolje će pozicionirati organizaciju da se nosi sa sve složenijim prijetnjama koje su danas sve češće. U okruženjima s velikim prometom javljaju se jedinstveni izazovi za performanse SIEM-a, osobito unutar velikih organizacija s velikim mrežama i protokom podataka. Osiguravanje skalabilnosti i učinkovitosti SIEM rješenja u takvim okruženjima ključno je za učinkovito otkrivanje prijetnji i odgovor. Kada se uz ogroman promet doda i integracija SIEM-a s drugim sigurnosnim alatima, može doći do potencijalnih problema s performansama kako SIEM-a tako i računala.

Jedan od primarnih izazova s kojima se SIEM susreće u okruženjima s velikim prometom je potencijal za uska grla u izvedbi koja proizlaze iz ogromne količine generiranih podataka. Ovaj priljev podataka može nadvladati konvencionalne SIEM sustave, što rezultira kašnjenjem obrade i analize. Nadalje, dinamička priroda mrežnih okruženja može zakomplicirati napore u otkrivanju prijetnji jer se rizici brzo razvijaju, što zahtijeva praćenje u stvarnom vremenu. Učinkovito upravljanje sigurnošću zahtijeva sofisticirane alate koji mogu držati korak s brzinama prijenosa podataka i brzo identificirati anomalije usred kontinuiranog protoka informacija.

Također, održavanje i ažuriranja ključni su za učinkovitost bilo kojeg SIEM-a. Implementacija SIEM-a nije jednokratni projekt, već stalan proces pregleda, praćenja i poboljšanja. Prijetnje se brzo mijenjaju, a stalno se pojavljuju nove metode napada. Kako bi se osiguralo da SIEM može otkriti nove prijetnje i obraniti se od novih napada, pravila korelacije

i mehanizmi otkrivanja moraju se redovito ažurirati. Ako se SIEM ne održava pravilno i redovito ne ažurira, neće biti učinkovit u prepoznavanju i odgovoru na nove prijetnje, ostavljajući organizaciju ranjivom.

SIEM sustavi su ključni za održavanje sigurnosti mreže, ali jedan od najčešćih izazova s kojima se suočavaju je preopterećenost upozorenjima. Ovaj problem proizlazi iz preosjetljivosti sustava na potencijalne prijetnje, što dovodi do niza upozorenja, od kojih mnoga mogu biti lažno pozitivna. Ova situacija opterećuje IT resurse. Organizacije bi se trebale usredotočiti na usklađivanje konfiguracija upozorenja i korištenje napredne analitike za rješavanje ovog izazova. To uključuje postavljanje preciznijih kriterija za upozorenja i integraciju algoritama strojnog učenja za analizu uzoraka i smanjenje lažno pozitivnih rezultata. Redovito ažuriranje i podešavanje pravila i parametara SIEM-a neophodno je za držanje koraka s rastućim prijetnjama i promjenjivim mrežnim okruženjima [30] .

Prikupljanje, pohrana i analiza sigurnosnih događaja zadaci su koji se na prvi pogled čine relativno jednostavnima. Međutim, njihovo prikupljanje, pohranjivanje, izvršavanje izvještaja o usklađenosti, primjena zakrpa i analiza svih sigurnosnih događaja koji se odvijaju na mreži tvrtke mogu predstavljati potencijalan problem. Veličina medija za pohranu, računalna snaga za obradu informacija, vrijeme integracije sigurnosne opreme, postavljanje upozorenja i još mnogo toga na što stručnjaci za kibernetičku sigurnost moraju računati ukoliko žele probleme s performansama svesti na minimum. Početna investicija može doseći stotine tisuća dolara, a tome treba dodati i godišnju podršku. Osim toga, hardverske i softverske licence čine jednu trećinu troškova SIEM-a. Na taj način, troškovi su često veći od očekivanih, što predstavlja jedan od glavnih problema SIEM-a. Analiza, konfiguracija i integracija izvještaja zahtijevaju stručnost profesionalaca [31].

Stručnjaci za kibernetičku sigurnost definitivno moraju računati na moguće probleme s performansama sustava prilikom uvođenja SIEM rješenja i njegove integracije s ostalim alatima za zaštitu informacijsko-komunikacijskog sustava. Ukoliko se pojave, takvi problemi mogu ozbiljno naštetiti organizaciji kako sigurnosno tako i financijski. Zbog toga je potrebno uložiti u optimizaciju resursa i SIEM sustava kako bi organizacija mogla imati što bolju sigurnosnu poziciju.

5. ANALIZA RAZLIČITIH PRISTUPA INTEGRACIJE SIEM SUSTAVA S OSTALIM SIGURNOSNIM ALATIMA

U današnje vrijeme postoje različite posredničke platforme koje olakšavaju integraciju između SIEM sustava i drugih sigurnosnih alata. Ove posredničke platforme mogu pružiti standardizirane načine komunikacije, pretvoriti formate logova i olakšati razmjenu podataka između različitih sustava. Također važno je spomenuti i API-je te različite vrste API-ja koji omogućavaju programski pristup funkcijama i podacima u SIEM sustavu, što olakšava integraciju s drugim alatima te ETL (engl. *Extract, Transform, Load*) alat koji se koristi za izvlačenje podataka iz različitih izvora i transformaciju podataka u format koji podržava SIEM te učitavanje u SIEM sustav.

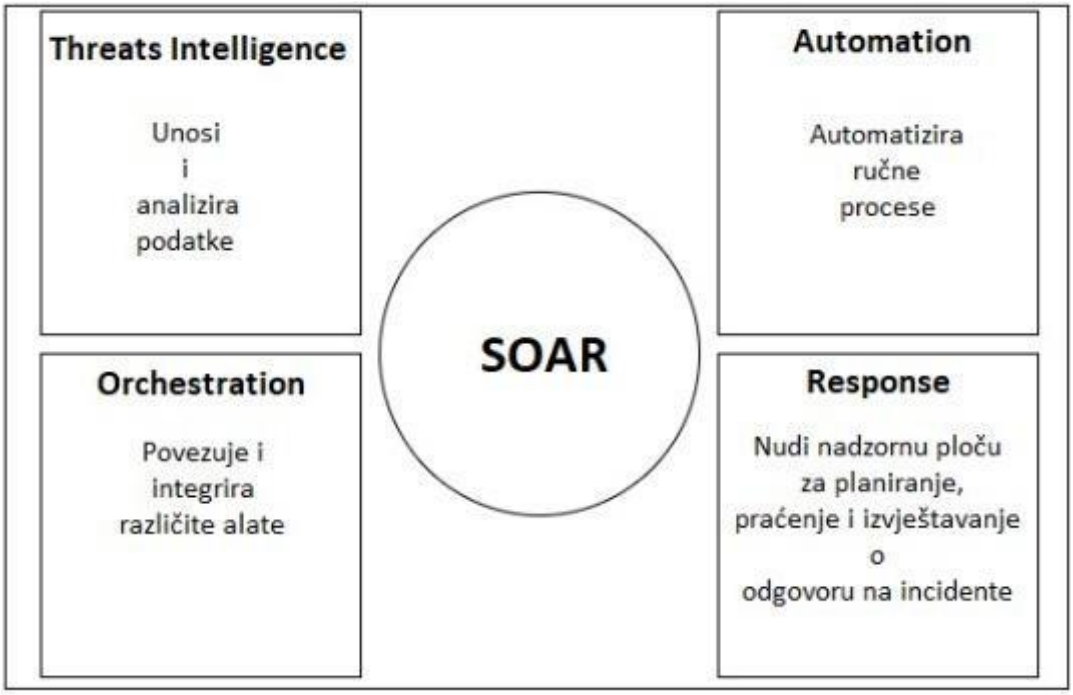
U ovom poglavlju slijedi i prikaz integracije SIEM sustava s vatrozidom koji pruža detaljan pregled konkretnog primjera integracije Microsoft Sentinel SIEM sustava s FortiGate vatrozidom, kako bi se demonstrirala praktična primjena i koristi takve integracije.

5.1. Posredničke platforme

Posredničke platforme su od velike važnosti kad je u pitanju integracija SIEM sustava s ostalim sigurnosnim alatima. Takve platforme poboljšavaju sigurnost kroz automatizaciju, pretvorbu *log* formata, koordinaciju odgovora na incidente i olakšavanje razmjene podataka između različitih sustava. Također, takvi sustavi olakšavaju proces integracije stručnjacima za kibernetičku sigurnost. Jedan od takvih sustava je i ranije spomenut SOAR sustav.

SOAR je skup kompatibilnih softverskih programa koji omogućuju organizaciji prikupljanje podataka o prijetnjama kibernetičkoj sigurnosti i odgovor na sigurnosne događaje uz malo ili nimalo ljudske pomoći. SOAR je osmišljen kako bi organizacijama omogućio prikupljanje podataka o sigurnosnim prijetnjama i upozorenjima iz više izvora. Može automatski identificirati i prioritizirati kibernetičke rizike te odgovoriti na sigurnosne događaje niže razine. Cilj korištenja SOAR platforme je poboljšati učinkovitost fizičkih i digitalnih sigurnosnih operacija. Mnoge organizacije koriste SOAR rješenja unutar sigurnosnog operacijskog centra. Sigurnosni operativni centri mogu imati koristi od korištenja SOAR automatiziranih funkcija za brže i učinkovitije rješavanje prijetnji, istovremeno smanjujući opterećenje i trajanje procesa odgovora na sigurnosne incidente. U kontekstu kibernetičke sigurnosti, SOAR se odnosi na sveobuhvatan pristup i tehnološki skup (slika 9.) koji kombinira orkestraciju, automatizaciju, odgovor na incidente i upravljanje obavještajnim podacima o

prijetnjama kako bi se poboljšala učinkovitost i djelotvornost sigurnosnih operacija organizacije [32].



Slika 9. Elementi SOAR sustava

Izvor: [32]

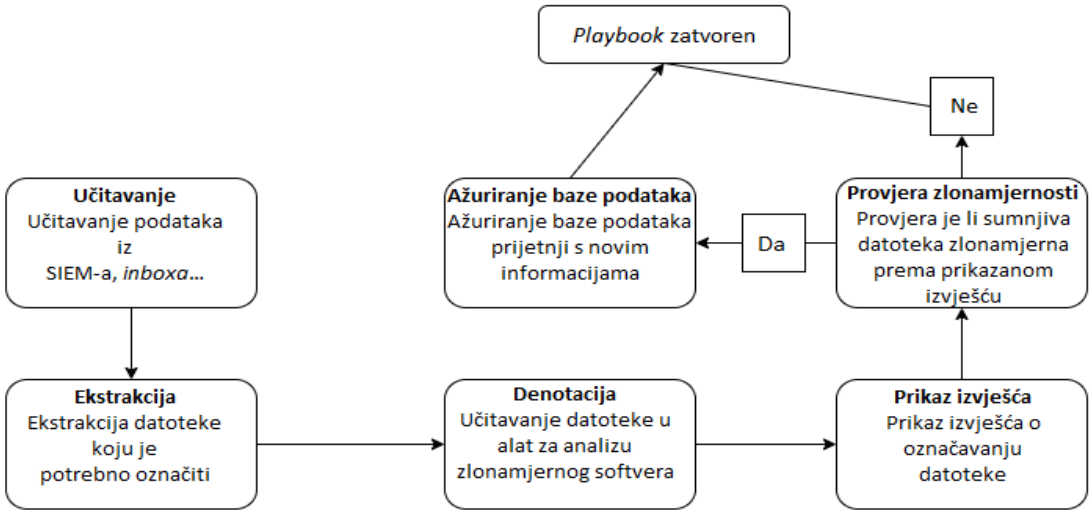
5.1.1. Orkestracija sigurnosti

Orkestracija sigurnosti povezuje i integrira različite unutarnje i vanjske alate putem ugrađenih ili prilagođenih integracija i aplikacijskih programskih sučelja. Povezani sustavi mogu uključivati skenere ranjivosti, proizvode za zaštitu krajnjih točaka, analitiku ponašanja korisnika i entiteta, vatrozide, sustave za detekciju i prevenciju upada, platforme za upravljanje sigurnosnim informacijama i događajima, softver za sigurnost krajnjih točaka, vanjske izvore obavještajnih prijetnji i druge izvore trećih strana. Što je više podataka prikupljeno putem ovih izvora, veća je šansa za otkrivanje prijetnji.

5.1.2. Automatizacija sigurnosti

Automatizacija sigurnosti, hranjena podacima i upozorenjima prikupljenima iz orkestracije sigurnosti, unosi i analizira podatke te stvara ponovljive, automatizirane procese kako bi zamijenila ručne procese. Zadaci koje su prethodno obavljali analitičari, kao što su skeniranje ranjivosti, analiza logova, provjera tiketa i mogućnosti revizije, mogu biti standardizirani i automatski izvršeni putem SOAR platformi. Koristeći umjetnu inteligenciju i strojno učenje za dešifriranje i prilagodbu uvida od analitičara, SOAR automatizacija može poslożiti prijetnje po prioritetima, davati preporuke i automatizirati buduće odgovore.

Playbookovi (niz automatiziranih koraka) su ključni za uspjeh SOAR-a. Unaprijed izgrađeni ili prilagođeni *playbookovi* su unaprijed definirane automatizirane radnje (slika 10.).



Slika 10. Primjer SOAR *playbooka* za analizu *malwarea*

Izvor: [33]

Više SOAR *playbookova* može se povezati kako bi se dovršile složene radnje. Na primjer, ako se zlonamjerni URL pronađe u e-mailu zaposlenika i identificira tijekom skeniranja, može se pokrenuti *playbook* koji blokira e-mail, upozorava zaposlenika na mogući pokušaj *phishinga* i stavlja IP adresu pošiljatelja na crnu listu. SOAR alati također mogu pokrenuti naknadne istražne radnje sigurnosnih timova, ako je potrebno. U kontekstu primjera *phishinga*, naknadne radnje mogu uključivati pretraživanje drugih *inboxa* zaposlenika za slične e-mailove i blokiranje njih i njihovih IP adresa, ako se pronađu.

5.1.3. Odgovor na sigurnosne prijetnje

Odgovor na sigurnosne prijetnje nudi jedinstven pregled za analitičare za planiranje, upravljanje, praćenje i izvještavanje o radnjama koje se provode nakon što je prijetnja otkrivena. Ovaj jedinstveni pregled omogućuje suradnju i dijeljenje informacija o prijetnjama među sigurnosnim, mrežnim i sustavnim timovima. Također uključuje aktivnosti nakon incidenta, poput upravljanja slučajevima i izvještavanja [34].

SOAR omogućuje razne procese, a neki od njih su detaljnije opisani u nastavku [35]. SOAR omogućuje integraciju sigurnosnih alata za IT operacije i alata za analizu prijetnji što znači da omogućuje povezivanje različitih sigurnosnih rješenja - čak i alate različitih proizvođača - kako bi se postigla sveobuhvatnija razina prikupljanja i analize podataka. Sigurnosni timovi mogu prestati koristiti razne konzole i alate. Sljedeće što SOAR nudi jest pregled svega na jednom mjestu. Sigurnosni tim dobiva pristup jednoj konzoli koja pruža sve

informacije potrebne za istraživanje i rješavanje incidenata. Sigurnosni timovi mogu na jednom mjestu pristupiti svim potrebnim informacijama. Uz pregled svega na jednom mjestu dolazi i do ubrzavanja odgovora na incidente. SOAR sustavi dokazano smanjuju prosječno vrijeme otkrivanja i prosječno vrijeme odgovora. Budući da su mnoge radnje automatizirane, veliki postotak incidenata može se odmah i automatski riješiti. Time dolazi do sprječavanja radnji koje troše vrijeme. SOAR drastično smanjuje broj lažno pozitivnih rezultata, ponavljajućih zadataka i ručnih procesa koji oduzimaju vrijeme sigurnosnim analitičarima. SOAR također pruža pristup boljoj inteligenciji. SOAR rješenja prikupljaju i provjeravaju podatke iz platformi za analizu prijetnji, vatrozida, sustava za otkrivanje upada, SIEM-a i drugih tehnologija, nudeći sigurnosnom timu veći uvid i kontekst. To olakšava rješavanje problema i poboljšava prakse. Analitičari su bolje opremljeni za dublje i šire istrage kada se pojave problemi. Još jedna mogućnost SOAR-a je poboljšanje izvještavanja i komunikacije. Sa svim aktivnostima sigurnosnih operacija prikupljenima na jednom mjestu i prikazanim u intuitivnim nadzornim pločama, timovi mogu dobiti sve potrebne informacije, uključujući jasne metrike koje pomažu identificirati kako poboljšati radne procese i smanjiti vrijeme odgovora. SOAR također omogućuje poboljšanje sposobnosti donošenja odluka. SOAR platforme su dizajnirane da budu jednostavne za korisnike, čak i za manje iskusne sigurnosne analitičare, nudeći značajke kao što su unaprijed izgrađeni *playbookovi*, funkcije povuci-i-pusti (*drag&drop*) za izradu *playbookova* od nule i automatsko prioritiziranje upozorenja. Osim toga, SOAR alat može prikupljati podatke i nuditi uvide koji analitičarima olakšavaju procjenu incidenata i poduzimanje ispravnih radnji za njihovo rješavanje.

Iako SOAR i SIEM platforme obje prikupljaju podatke iz više izvora, ovi pojmovi nisu jednaki. SIEM sustavi prikupljaju podatke, identificiraju odstupanja, rangiraju prijetnje i generiraju sigurnosna upozorenja. SOAR sustavi također obavljaju ove zadatke, ali imaju dodatne sposobnosti. Prvo, SOAR platforme integriraju se s većim brojem unutarnjih i vanjskih aplikacija, kako sigurnosnih, tako i nesigurnosnih. Drugo, dok SIEM sustavi samo upozoravaju sigurnosne analitičare na potencijalni događaj, SOAR platforme koriste automatizaciju, umjetnu inteligenciju i strojno učenje za pružanje većeg konteksta i automatiziranih odgovora na te prijetnje. Mnoge tvrtke koriste SOAR za dopunu internih SIEM softvera. U budućnosti se očekuje da će SIEM dobavljači dodati SOAR sposobnosti svojim uslugama, što znači da će se tržište za ove dvije linije proizvoda spojiti. Mnogi SIEM dobavljači nude SOAR mogućnosti - prvenstveno automatizaciju - u svojim SIEM proizvodima, često ih nazivajući SIEM-ovima nove generacije.

Integracija SIEM-a i SOAR-a jača sigurnost organizacije. Na ovaj način se kombiniraju mogućnosti praćenja događaja u stvarnom vremenu i korelacije s automatiziranim i orkestriranim radnjama odgovora na incidente. Ova kombinacija omogućava sigurnosnim

timovima da brzo reagiraju na nove prijetnje, poboljšavajući ukupnu učinkovitost. Da bi se učinkovito integrirali SIEM i SOAR, potrebna je analiza postojeće sigurnosne infrastrukture. Ključno je razumijevanje koje su sustavi i procesi već u upotrebi kako bi se identificirale praznine ili neefikasnosti. Potrebno je postaviti jasne ciljeve za integraciju. To može biti brža detekcija i odgovor na prijetnje, poboljšana vidljivost ili efikasnije operacije [35].

Jedna od ključnih koristi integriranja SIEM i SOAR u jedinstvenu platformu leži u omogućavanju besprijekorne suradnje između detekcije i odgovora. SIEM pruža centraliziranu vidljivost i sposobnosti detekcije, označavajući potencijalne sigurnosne incidente. S druge strane, SOAR orkestrira odgovor na incidente automatiziranjem zadataka, optimiziranjem radnih tokova i osiguravanjem koordiniranog rada. Sinergija između sveobuhvatne detekcije prijetnji SIEM-a i automatiziranog odgovora na incidente SOAR-a stvara holistički pristup upravljanju prijetnjama. Također, jedinstvena platforma optimizira korištenje resursa kombiniranjem prednosti SIEM-a i SOAR-a. Dok SIEM zahtijeva stručnost za konfiguraciju, podešavanje i kontinuirano održavanje, SOAR automatizira rutinske zadatke, smanjujući teret na timovima za kibernetičku sigurnost. Ovaj optimizirani način korištenja resursa omogućava organizacijama s ograničenim resursima učinkovitije upravljanje njihovim operacijama kibernetičke sigurnosti. SIEM-SOAR platforma također rješava izazov lažno pozitivnih upozorenja. SIEM može generirati visok broj lažno pozitivnih upozorenja ako nije pravilno konfiguriran, no SOAR poboljšava odgovor na incidente automatiziranjem akcija temeljenih na provjerenoj prijetnji. Integrirajući točnost detekcije SIEM-a s automatiziranim odgovorom SOAR-a, jedinstvena platforma minimizira lažno pozitivna upozorenja, osiguravajući da se automatizirane akcije odgovora pokreću na temelju provjerene prijetnje [36].

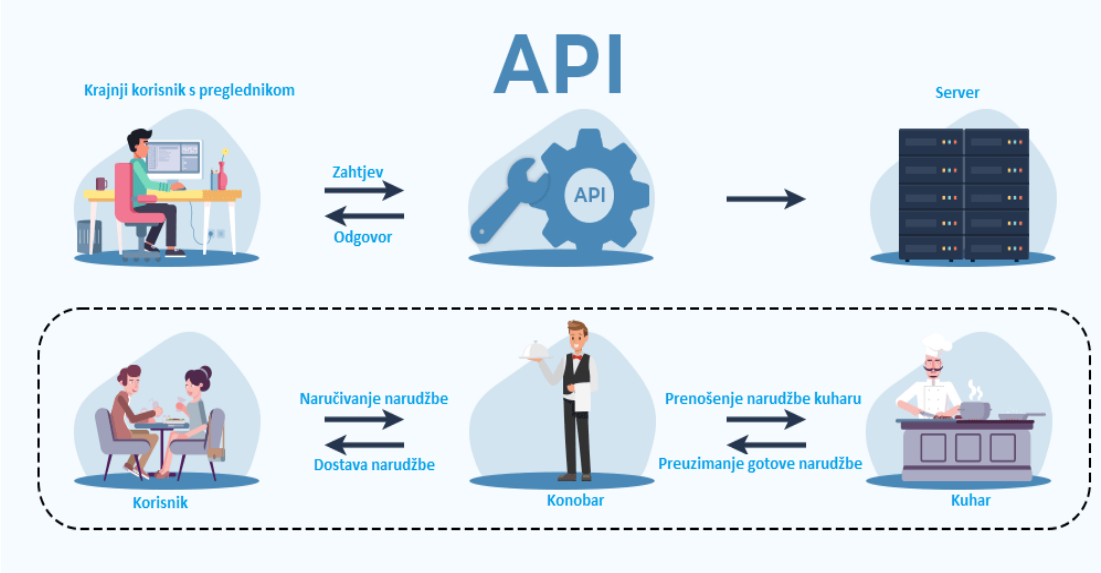
Zaključno, usvajanje jedinstvene SIEM-SOAR platforme predstavlja značajnu priliku za organizacije da ojačaju svoju kibernetičku sigurnost kako bi se suprotstavile stalno evoluirajućim prijetnjama. Iako prednosti poput besprijekorne suradnje između detekcije prijetnji i automatiziranog odgovora, optimiziranog korištenja resursa i holističkog pristupa upravljanju prijetnjama nude značajne koristi, važno je prepoznati i riješiti izazove.

5.2. Pregled aplikacijskog programskog sučelja

API ili aplikacijsko programsko sučelje je skup pravila ili protokola koji omogućuju softverskim aplikacijama međusobnu komunikaciju radi razmjene podataka, značajki i funkcionalnosti. API-ji pojednostavljuju i ubrzavaju razvoj aplikacija i softvera omogućujući programerima integraciju podataka, usluga i mogućnosti iz drugih aplikacija, umjesto da ih razvijaju od nule. API-ji također daju vlasnicima aplikacija jednostavan i siguran način da učine podatke i funkcije svojih aplikacija dostupnim odjelima unutar njihove organizacije. Vlasnici aplikacija također mogu dijeliti ili plasirati podatke i funkcije poslovnim partnerima ili trećim

stranama. API-ji omogućuju dijeljenje samo potrebnih informacija, skrivajući druge interne detalje sustava, što pomaže u sigurnosti sustava. Serveri ili uređaji ne moraju u potpunosti otkrivati podatke. API-ji omogućuju dijeljenje malih paketa podataka, relevantnih za specifičan zahtjev.

API-ji omogućuju proizvodu ili usluzi komunikaciju s drugim proizvodima i uslugama bez potrebe za poznavanjem kako su oni implementirani. To može pojednostaviti razvoj aplikacija, štedeći vrijeme i novac. Kada se dizajniraju novi alati i proizvodi, ili kada se upravlja postojećima, API-ji pružaju fleksibilnost, pojednostavljuju dizajn, administraciju i korištenje te pružaju prilike za inovacije. API-ji se ponekad smatraju ugovorima, s dokumentacijom koja predstavlja sporazum između strana. Kako bi bilo jasnije što je API, na slici 11. prikazana je sličnost API-ja i konobara u procesu obrađivanja zahtjeva: API se zamisli kao konobar u restoranu koji prima narudžbu, odlazi kod kuhara, uzima naručena jela i vraća se s narudžbom [37].



Slika 11. Usporedba API-ja i konobara u procesu obrađivanja zahtjeva

Izvor: [37]

API-ji su okosnica modernog razvoja softvera i omogućuju širok raspon funkcionalnosti i usluga. U nastavku su navedeni neki od ključnih razloga zašto su API-ji nezamjenjivi. Prvi razlog je integracija. API-ji omogućuju različitim softverskim sustavima da se integriraju i komuniciraju jedni s drugima bez ikakvih problema. Ova sposobnost integracije ključna je za izgradnju složenih aplikacija. Nakon toga, slijedi učinkovitost. API-ji omogućuju programerima da koriste postojeće usluge i podatke. To rezultira učinkovitijim procesima razvoja i bržim izlaskom novih proizvoda i usluga na tržište. Zatim slijedi još jedan razlog a to je skalabilnost. API-ji olakšavaju skaliranje aplikacija i usluga prebacivanjem određenih funkcionalnosti na

specijalizirane pružatelje usluga. To osigurava da aplikacije mogu podnijeti povećano opterećenje i promet. Još jedan razlog koji pokazuje važnost API-ja je pristup vanjskim podacima što znači da mnoge aplikacije ovise o vanjskim izvorima podataka, kao što su karte, vremenske prognoze ili financijske informacije. API-ji pružaju strukturirani način pristupa i integracije tih podataka u aplikacije. Naposljetku, API-ji potiču rast razvojnih ekosustava omogućujući vanjskim programerima stvaranje proširenja, dodataka ili integracija za postojeće platforme i usluge.

Razne prednosti i mogućnosti API-ja čini ih ključnima ne samo za tradicionalni razvoj softvera već i za nove tehnologije poput Interneta stvari (engl. *Internet of Things* – IoT), računalstva u oblaku i umjetne inteligencije.

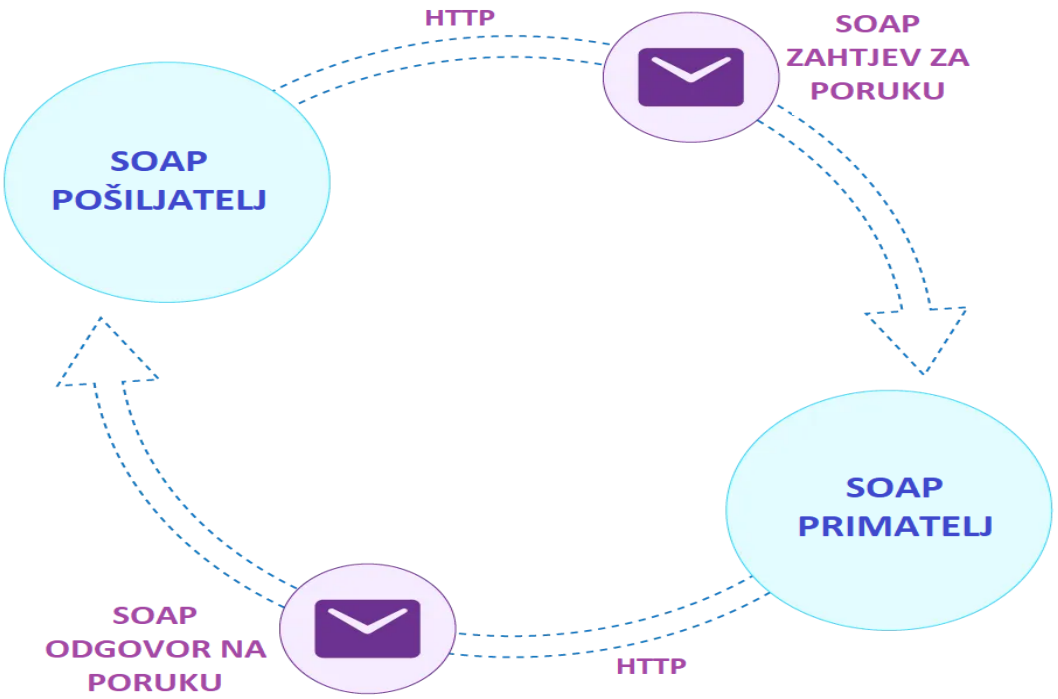
Također, bitno je znati da postoje 4 vrste API-ja, a to su otvoreni, partnerski, interni i kombinirani API-ji. Otvoreni API-j (engl. *Open APIs*) javno su dostupni za korištenje, kao što su OAuth API-ji od Googlea. Nemaju ograničenja za korištenje pa su poznati i kao javni API-ji. Partnerski API-ji (engl. *Partner APIs*) nisu dostupni javnosti i potrebna su specifična prava ili licence za pristup ovoj vrsti API-ja. Interni (engl. *Internal APIs*) ili privatni API-ji nisu dostupni za vanjske korisnike, nego samo za korištenje unutar organizacije. Takve API-je razvijaju organizacije kako bi poboljšale produktivnost i komunikaciju među timovima unutar organizacije. I naposljetku, kombinirani API-ji (engl. *Composite APIs*) su vrsta API-ja koja kombinira različite podatkovne i uslužne API-je [38]. Različiti tipovi API arhitekture postoje kako bi zadovoljili različite funkcionalnosti i zahtjeve performansi. Neki stilovi su se pojavili kako bi bolje podržali promjene u komunikacijskim protokolima zbog napretka tehnologije. Neki stilovi se fokusiraju na brzinu i učinkovitost, poput gRPC, dok drugi daju prednost integritetu podataka nad performansama. U nastavku su objašnjeni različiti stilovi arhitekture API-ja.

5.2.1. Pregled SOAP aplikacijskog programskog sučelja

Simple object access protocol (SOAP), koji održava *World Wide Web Consortium* (W3C), jedna je od najranijih API arhitektura (slika 12.). Koristi XML za formatiranje poruka, osiguravajući standardiziran pristup komunikaciji između aplikacija. U SOAP terminologiji, klijent je tražitelj usluge, a poslužitelj je pružatelj usluge. Razmjena XML poruka je u standardiziranoj strukturi s elementom "*Envelope*", koji obično sadrži odjeljke "*Header*" i "*Body*". Jezik za opisivanje web usluga (engl. *Web Services Description Language,* WSDL) definira SOAP API-je, nudeći sveobuhvatan nacrt njihove strukture [39].

Dok se REST fokusira na lagane interakcije, SOAP daje prioritet strukturiranoj razmjeni podataka i robusnoj sigurnosti. SOAP API-ji briljiraju u scenarijima gdje su sigurnost,

konzistentnost i trajnost od najveće važnosti. Međutim, kao starija tehnologija, SOAP API-ji su manje popularni u modernoj mikroservisnoj arhitekturi.



Slika 12. SOAP API arhitektura

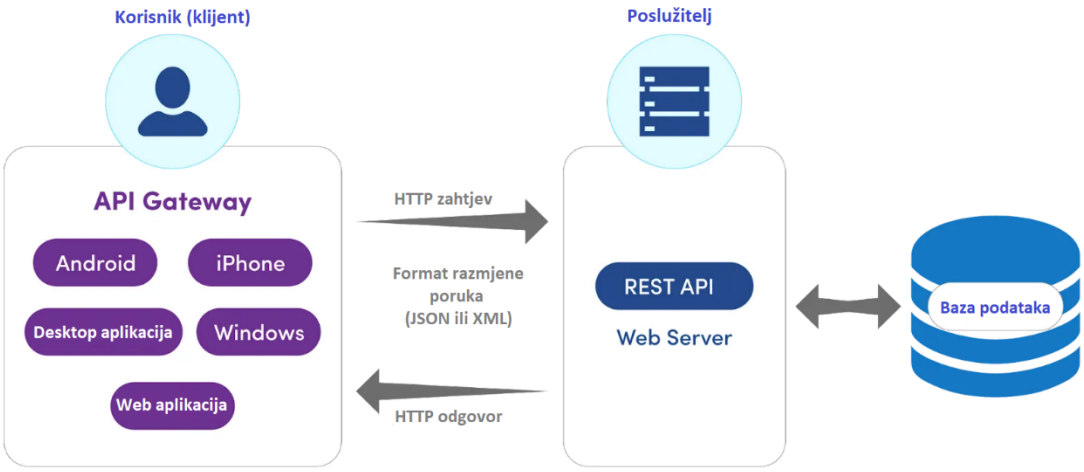
Izvor: [40]

5.2.2. Pregled REST aplikacijskog programskog sučelja

API-ji izgrađeni na arhitekturi (slika 13.) za prijenos reprezentativnog stanja (engl. *Representational State Transfer*, REST) popularni su među programerima zbog svoje jednostavnosti. REST API-ji pridržavaju se šest ključnih principa koji usmjeravaju njihov dizajn i funkcionalnost [39]. Odvajanje klijenta i servera (poslužitelja) je prvi princip REST API-ja. Odgovornosti na strani poslužitelja i klijenta su odvojene tako da se svaka strana može implementirati neovisno o drugoj. Kôd na strani poslužitelja (API) i kôd na strani klijenta mogu se mijenjati bez utjecaja jedno na drugo, sve dok oboje nastave komunicirati u istom formatu. U REST arhitekturi, različiti klijenti šalju zahtjeve na iste krajnje točke, izvršavaju iste radnje i dobivaju iste odgovore. Zatim slijedi princip bezstanje (engl. *Stateless)* koji predstavlja komunikaciju između klijenta i poslužitelja koja ne prati stanje sesija od jednog zahtjeva do drugog. Stanje sesije uključeno je u svaki zahtjev, tako da ni klijent ni poslužitelj ne moraju znati stanje onog drugog kako bi komunicirali. Nema potrebe za održavanjem stalne veze između klijenta i poslužitelja, što podrazumijeva veću otpornost na kvarove. Osim toga, to omogućava REST API-jima da odgovaraju na zahtjeve više klijenata bez zasićenja portova poslužitelja. Iznimka ovom pravilu je autentifikacija, kako klijent ne bi morao navoditi svoje

podatke za autentifikaciju u svakom zahtjevu. Nakon toga slijedi princip jedinstvenost sučelja koja predstavlja pravila za interakciju klijenata s resursima poslužitelja. Različite akcije i/ili resursi dostupni s njihovim specifičnim krajnjim točkama i parametrima moraju biti pažljivo definirani i dosljedno poštovani od strane klijenta i poslužitelja. Svaki odgovor treba sadržavati dovoljno informacija kako bi ga klijent mogao interpretirati bez potrebe za dodatnim podacima unaprijed. Odgovori ne bi trebali biti predugački i trebali bi sadržavati poveznice na druge krajnje točke. Zatim slijedi princip *cache*-iranja. Odgovori se mogu *cache*-irati kako bi se izbjeglo nepotrebno preopterećenje poslužitelja. *Cache*-iranje mora biti dobro upravljano: REST API mora specificirati hoće li i koliko dugo odgovor može biti *cache*-iran kako bi se izbjeglo da klijent primi zastarjele informacije. Nakon *cache*-iranja, slijedi princip slojeviti sustav. Stil slojevite arhitekture omogućuje da arhitektura bude sastavljena od hijerarhijskih slojeva ograničavanjem ponašanja komponenata. Klijent povezan s REST API-jem obično ne može razlikovati komunicira li s krajnjim poslužiteljem ili s posredničkim poslužiteljem. REST arhitektura omogućuje API-ju, na primjer, da prima zahtjeve na poslužitelju A, pohranjuje svoje podatke na poslužitelju B i upravlja autentifikacijama na poslužitelju C. Naposljetku, slijedi princip kôd na zahtjev. Iako je ova funkcionalnost opcionalna, REST također omogućuje proširenje funkcionalnosti klijenta preuzimanjem i izvršavanjem kôda u obliku skripti. Preuzeti kôd pojednostavljuje klijente smanjenjem broja značajki koje je potrebno unaprijed implementirati. Poslužitelji mogu pružiti dio značajki isporučenih klijentu u obliku kôda, a klijent samo treba izvršiti taj kôd.

Za pristup i manipulaciju resursima, moguće je koristiti standardne HTTP (engl. *Hypertext Transfer Protocol*) metode kao što su *GET, POST, PUT i DELETE*. Svaki resurs ima jedinstveni identifikator radi učinkovitosti. Korištenje zaglavlja i parametara u zahtjevima povećava fleksibilnost za programere. REST API-ji su preferirani jer su jednostavni za skaliranje zbog jednostavnog održavanja i nadogradnje.

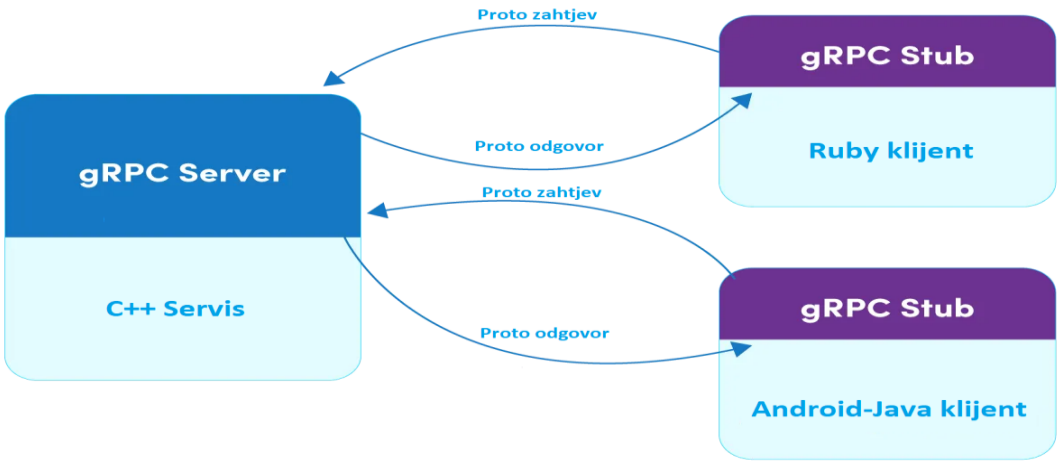


Slika 13. REST API arhitektura

Izvor: [40]

5.2.3. Pregled gRPC aplikacijskog programskog sučelja

gRPC, koji je razvio Google, je stil arhitekture API-ja (slika 14.) koji koristi udaljene pozive procedura za interakciju s API-jem. Usluge izlažu funkcionalnosti kao metode; klijenti ih mogu pozivati na način sličan lokalnim pozivima funkcija. gRPC koristi *Protocol Buffers*, jezikom neovisni format za definiranje podataka i poruka. Omogućuje učinkovitu komunikaciju između različitih programskih jezika. Kao i REST, podržava komunikaciju s jednim zahtjevom i jednim odgovorom, no, kao moderniji stil API-ja, također ima ugrađenu podršku za *server-streaming* (kontinuirana ažuriranja poslužitelja), *client-streaming* (slanje toka podataka) i dvosmjerni *streaming* (komunikacija u stvarnom vremenu). gRPC daje prioritet brzom i učinkovitom prijenosu podataka, što ga čini idealnim za aplikacije osjetljive na kašnjenje. Programeri cijene njegovu proširivost i brzinu, čineći ga pogodnim za scenarije koji zahtijevaju brzu i učinkovitu razmjenu podataka [39].



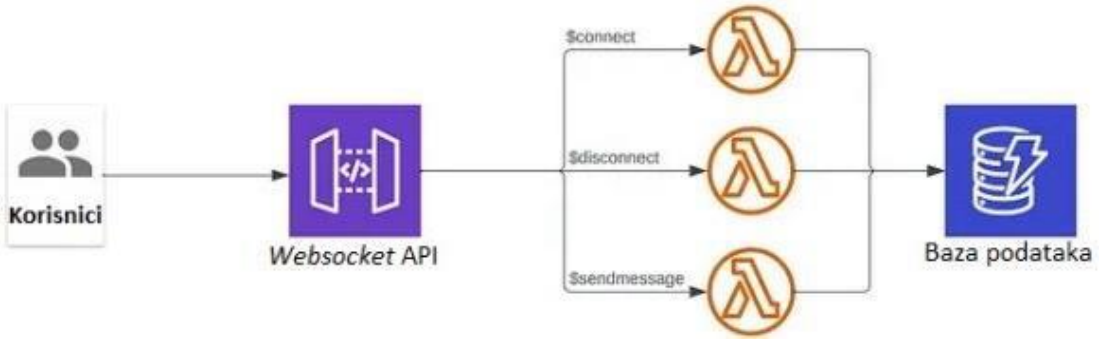
Slika 14. gRPC API arhitektura

Izvor: [40]

5.2.4. Pregled *WebSocket* aplikacijskog programskog sučelja

WebSocket je komunikacijski protokol koji omogućava dvosmjernu, komunikaciju u stvarnom vremenu između klijenta i poslužitelja. Za razliku od tradicionalnih HTTP zahtjeva, *WebSocket* omogućuje dvosmjernu komunikaciju, što znači da i klijent i poslužitelj mogu inicirati i primati poruke prema potrebi. To omogućava razmjenu podataka u stvarnom vremenu i interaktivna iskustva. Umjesto otvaranja i zatvaranja veza za svaku poruku, *WebSocket* API-ji uspostavljaju jednu trajnu vezu preko koje podaci neprekidno teku. Podaci se obično razmjenjuju u JSON-u ili *Protocol Buffers* formatu kako bi se optimizirala brzina prijenosa. Ovo smanjuje mrežno opterećenje poboljšava učinkovitost komunikacije.

WebSocket API-ji omogućavaju vrlo brzi prijenos podataka između klijenata i poslužitelja. To ih čini odličnim izborom za aplikacije koje zahtijevaju ažuriranja s niskim kašnjenjem, kao što su *chat*, *online* igre ili financijske platforme. Na slici 15. prikazana je jednostavna arhitektura *WebSocket* API-ja [39].

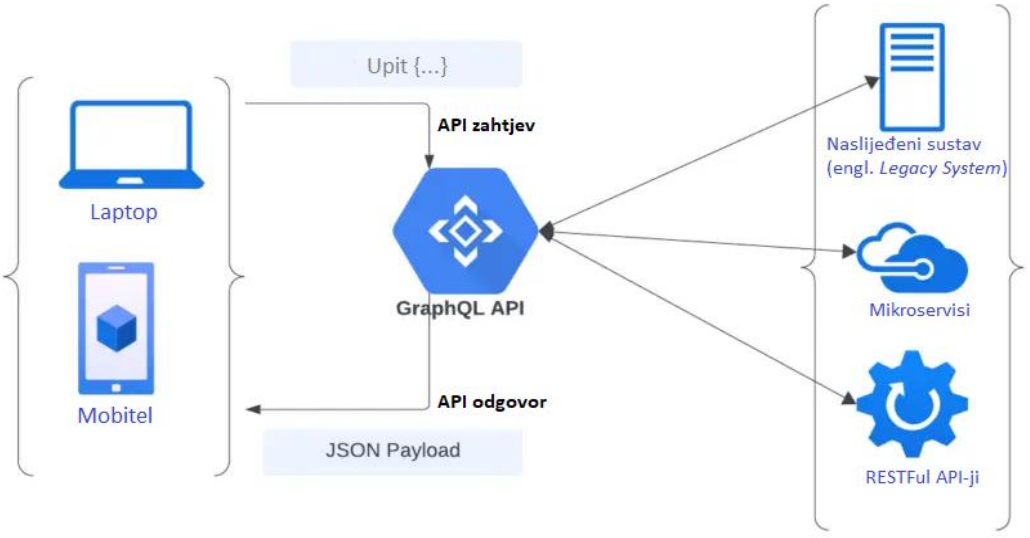


Slika 15. *WebSocket* API arhitektura

Izvor: [41]

5.2.5. Pregled GraphQL aplikacijskog programskog sučelja

REST API-ji podržavaju ograničenu granularnost u razmjeni podataka između API-ja. Na primjer, ako se zatraže podaci o kupcima, REST API-ji vraćaju cijeli zapis s poslužitelja, a klijent filtrira podatke koji mu trebaju s poslužitelja. To ponekad dovodi do preuzimanja previše ili premalo podataka, što može uzrokovati neučinkovitu komunikaciju. Nasuprot tome, GraphQL arhitektura (slika 16.) omogućava klijentima da specificiraju točne podatke koje trebaju. To se postiže upitima napisanim u fleksibilnom jeziku poput *GraphQL Schema Language* (SDL).



Slika 16. GraphQL API arhitektura

Izvor: [42]

Funkcionalnost API-ja definira se shemom koja opisuje dostupne tipove podataka, polja i njihove odnose. Klijenti koriste shemu za generiranje upita. Klijenti mogu zatražiti ugniježdene podatkovne strukture u jednom upitu, dohvaćajući povezane podatke u jednom potezu. Ovo pojednostavljuje dohvaćanje podataka i eliminira potrebu za višestrukim pozivima poslužitelju. GraphQL upiti su deklarativni, specificirajući potrebne podatke, ali ne i način na koji se oni dohvaćaju. To omogućava poslužitelju da optimizira izvršenje i učinkovito koristi različite izvore podataka. GraphQL također pruža strukturirani mehanizam za rukovanje pogreškama koji vraća detaljne informacije o pogreškama koje su se pojavile tijekom izvršenja upita. GraphQL-a se koristi kada su potrebe klijenta raznolike i dinamične, kada postoje složene podatkovne strukture i odnosi među podacima, te kad su mrežni resursi ograničeni [43].

5.3. Alat za ekstrakciju, transformaciju i učitavanje podataka (ETL)

ETL se odnosi na proces ekstrakcije, transformacije i učitavanja podataka prikupljenih iz više izvora u jedinstvenu bazu podataka. Ovaj jedinstveni izvor podataka je skladište podataka s formatiranim podacima pogodnim za obradu radi dobivanja analitičkih uvida. ETL je temeljna praksa upravljanja podacima. Primarno se koristio za izračun i analizu podataka, a sada mnoge organizacije koriste ETL za razne procese strojnog učenja i analitike velike količine podataka kako bi olakšale poslovnu inteligenciju [44].

Osim što pojednostavljuje pristup podacima za analizu i dodatnu obradu, ETL osigurava dosljednost i čistoću podataka u organizacijama. Organizacije također koriste ETL za:

- poboljšanje kvalitete podataka,
- pohranu zastarjelih podataka,
- dobivanje konsolidiranog pogleda na sve podatke unutar poslovanja.

Danas se ETL koristi u svim industrijama, uključujući zdravstvenu skrb, proizvodnju i financije, kako bi se donosile bolje odluke i pružila bolja usluga krajnjim korisnicima.

U ETL procesu, podaci se prvo izvlače iz izvora, transformiraju, a zatim učitavaju u ciljanu podatkovnu platformu. U nastavku su detaljnije objašnjeni procesi koji čine ETL [45].

5.3.1. Izvlačenje podataka

Izvlačenje podataka uključuje tri koraka, a to su identificiranje podataka za izvlačenje, procjena veličine izvlačenja podataka i odabir metode izvlačenja. Identificiranje podataka za izvlačenje je prvi korak u izvlačenju podataka. Identificiraju se izvori podataka. Ti izvori mogu biti iz relacijskih SQL baza podataka kao što su *MySQL* ili nerelacijske *NoSQL* baze podataka kao što su *MongoDB* ili *Cassandra*. Nakon identificiranja izvora podataka, potrebno je odrediti

specifična polja podataka koja se izvlače. Zatim slijedi procjena veličine izvlačenja podataka. Veća količina podataka zahtijeva drugačiju ETL strategiju. Na primjer, veći skup podataka može biti lakše upravljiv na mjesečnoj razini umjesto dnevne, čime se smanjuje veličina izvlačenja. Alternativno, može se nadograditi hardver kako bi se upravljalo većim skupom podataka. Na kraju, slijedi odabir metode izvlačenja. Postoje tri glavne metode za izvlačenje informacija. Prva metoda je odabir o ažuriranju. Preferirana metoda izvlačenja uključuje obavijesti o ažuriranju. Izvorni sustav će poslati obavijest kada se jedan od njegovih zapisa promijeni, a zatim se baza podataka ažurira samo s novim informacijama. Druga metoda, koja se može koristiti kada obavijesti o ažuriranju nisu moguće, je inkrementalno izvlačenje. Ovo uključuje identificiranje koji su se zapisi promijenili i izvođenje izvlačenja samo tih zapisa. Potencijalni problem je da inkrementalno izvlačenje ne može uvijek identificirati obrisane zapise. Kada prve dvije metode ne funkcioniraju, potrebno je potpuno ažuriranje svih podataka putem potpunog izvlačenja. Ova metoda većinom je izvediva samo za manje skupove podataka.

5.3.2. Transformacija podataka

Sljedeći proces je transformacija podataka. Ovo je proces u kojem se svi prikupljeni podaci prikladno formatiraju prije nego što se pohrane u skladište podataka. Obično se slijedi određeni skup pravila ili kôdova za transformaciju podataka u jedan čitljiv format. Neki od koraka za provedbu transformacije podataka objašnjeni su u nastavku. Prvi korak je osnovni proces transformacije koji se provodi. Ovdje se podaci izvode, transformiraju i zatim učitavaju u skladište za daljnju upotrebu. Zatim slijedi korak transformacije u skladištu. Ovdje se podaci izvode i pohranjuju u privremeno područje iz kojeg se izravno učitavaju u skladište. Nakon toga, transformacija podataka se provodi u skladištu.

Oba ova procesa imaju svoje prednosti i nedostatke. Mnogi sustavi ili organizacije koriste tradicionalnu metodu, dok neki traže ELT metodu za transformaciju podataka. Postoji nekoliko podprocesa uključenih u transformaciju podataka, a to su čišćenje, filtriranje, normalizacija, derivacija, revizija formata, spajanje, integracija i verifikacija. Čišćenje predstavlja mapiranje NULL vrijednosti na 0 ili "Muški" (engl. "*Male*") na "M" i "Ženski" (engl. "*Female*") na "F", dosljednost formata datuma, itd. Zatim slijedi filtriranje u kojem se biraju samo određeni redci i stupci potrebni za daljnju analizu. Nakon filtriranja slijedi normalizacija odnosno identifikacija i uklanjanje dupliranih zapisa. Kod derivacije koriste se podaci za dobivanje novih vrijednosti iz postojećih podataka. Zatim slijedi revizija formata odnosno pretvorba formata datuma/vremena, skupa znakova, itd. Kod spajanja, povezuju se podaci pomoću skupa unaprijed definiranih pravila. Nakon spajanja slijedi integracija kod koje se usuglašavaju različita imena i vrijednosti podataka za isti element podataka. I naposljetku, verifikacija predstavlja uklanjanje neiskorištenih podatak odnosno višak podataka [45].

Svi ovi procesi pripremaju podatke za bolju i lakšu daljnju analizu. Transformacija podataka, zauzvrat, čini integraciju lakšom i potpuno kompatibilnom s sljedećim procesom.

5.3.3. Učitavanje podataka

Učitavanje podataka je proces učitavanja izvučenih informacija u ciljanu pohranu. Učitavanje je kontinuirani proces koji može uključivati potpuno učitavanje (prvi put kada se učitavaju podaci u skladište podataka) ili inkrementalno učitavanje (kako se ažurira skladište podataka s novim informacijama).

Inkrementalna učitavanja izvlače i učitavaju informacije koje su se pojavile od posljednjeg inkrementalnog učitavanja. To se može dogoditi na dva načina: serijska inkrementalna učitavanja i *streaming* inkrementalna učitavanja. Kod serijskih inkrementalnih učitavanja skladište podataka unosi informacije u paketima ili serijama. Ako je riječ o velikom paketu, najbolje je izvršiti serijsko učitavanje tijekom izvan radnog vremena - na dnevnoj, tjednoj ili mjesečnoj osnovi - kako bi se spriječilo usporavanje sustava. Međutim, moderna skladišta podataka također mogu unositi male serije informacija na minutnoj osnovi pomoću ETL platforme poput *Integrate.io*. To im omogućava postizanje približnih ažuriranja u stvarnom vremenu za krajnjeg korisnika. A kod *streaming* inkrementalnih učitavanja, skladište podataka unosi nove podatke kako se pojavljuju u stvarnom vremenu. Ova metoda je osobito vrijedna kada krajnji korisnik zahtijeva ažuriranja u stvarnom vremenu (npr. za donošenje odluka u trenutku). Ipak, *streaming* inkrementalna učitavanja su moguća samo kada ažuriranja uključuju vrlo malu količinu podataka. U većini slučajeva, minutna serijska ažuriranja nude robusnije rješenje od streaming učitavanja u stvarnom vremenu.

Nakon općenitog objašnjenja ETL procesa, slijedi prikaz kako se ETL može primijeniti u kontekstu integracije SIEM-a s ostalim sigurnosnim alatima

5.3.4. Izvlačenje podataka u kontekstu SIEM-a

Faza izvlačenja podataka opisuje prikupljanje podataka iz različitih sigurnosnih alata i izvora. Ti podaci uključuju logove, upozorenja, podatke o prijetnjama i izvještaje o incidentima iz EDR sustava, vatrozida i drugih relevantnih izvora. Faza izvlačenja sadrži izvore podataka te API-je i konektore. Izvori podataka podrazumijevaju identificiranje i povezivanje s izvorima podataka kao što su EDR logovi, logovi vatrozida, izvori podataka o prijetnjama i sustavi za upravljanje incidentima. API-ji i konektori podrazumijevaju korištenje API-ja i konektora koje nude ovi alati za ekstrakciju podataka. To će osigurati prikupljanje podataka u stvarnom vremenu ili u redovitim intervalima.

5.3.5. Transformacija podataka u kontekstu SIEM-a

U fazi transformacije, prethodno izvučeni podaci preoblikuju se u format kompatibilan sa SIEM sustavom. Ovo može uključivati normalizaciju formata logova kao što su XML, CSV, JSON i drugi. Većina ovih logova je formirana prema nekim standardnim formatima kako bi ih SIEM mogao razumjeti i obraditi. Faza transformacije podataka uključuje normalizaciju, obogaćivanje te filtriranje i agregaciju. Normalizacija predstavlja standardizaciju svih polja i formata radi dosljednosti. Na primjer, svi vremenski žigovi mogu se pretvoriti u jedan format ili se različita terminologija korištena od strane različitih alata može mapirati u jedan standardizirani okvir. Obogaćivanje predstavlja dodavanje dodatnog konteksta podacima. Primjeri uključuju geolokacijske podatke IP adresa i povezivanje logova s podacima o prijetnjama radi dobivanja konteksta prijetnje. Filtriranje i agregacija predstavljaju filtriranje nepotrebnih podataka kako bi se smanjila razina šuma, a zatim agregaciju različitih događaja u jasan i sažet skup podataka koji SIEM može obraditi.

5.3.6. Učitavanje podataka u kontekstu SIEM-a

U ovoj fazi učitavanja, transformirani podaci se uvoze u SIEM sustav za analizu, korelaciju i pohranu. Koriste se mogućnosti unosa podataka SIEM-a za uvoz normaliziranih/obogaćenih podataka. To može uključivati korištenje API-ja, uvoz datoteka ili izravne veze s bazama podataka. SIEM može u potpunosti iskoristiti ETL procese za integraciju s drugim sigurnosnim alatima kako bi osigurao korisne i kvalitetne podatke za analizu i detekciju incidenata. Važno je i spomenuti da s druge strane postoji ELT (engl. *Extract, Load, Transform*) alat koji izvodi transformacije podataka izravno unutar samog skladišta podataka. Za razliku od ETL-a, ELT omogućuje slanje neobrađenih podataka izravno u skladište podataka, čime se eliminira potreba za procesima u međuspremniku. Glavna razlika između ETL-a i ELT-a je u tome što ETL transformira podatke prije njihovog učitavanja na poslužitelj, dok ih ELT transformira nakon učitavanja.

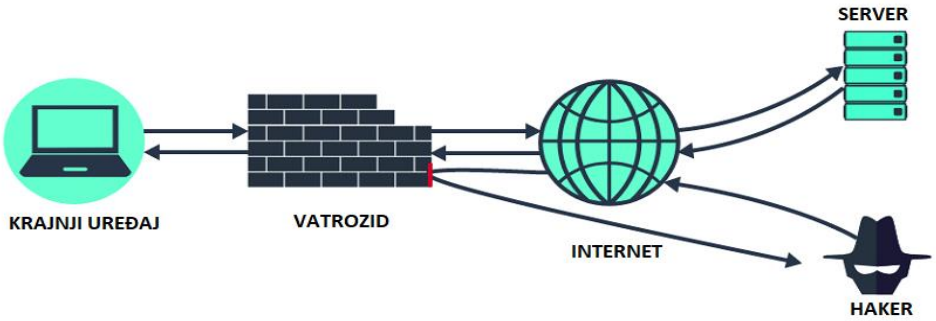
5.4. Integracija SIEM sustava s vatrozidom

U području kibernetičke sigurnosti postoji više alata i tehnologija osmišljenih za zaštitu organizacija od sve većih prijetnji. Svaki alat ima svoje prednosti i mane, ali integriranjem različitih alata dolazi do bolje sveukupne zaštite informacijsko-komunikacijskog sustava neke organizacije. Dva često pogrešno shvaćena pojma su ranije objašnjen SIEM sustav, i vatrozid. Integracija SIEM sustava i vatrozida organizacijama donosi mnoge prednosti, a stručnjacima za kibernetičku sigurnost olakšava posao zbog preglednosti. Iako su i SIEM i vatrozid ključni dijelovi snažne sigurnosne infrastrukture, oni služe različitim svrhama. U nastavku slijede

karakteristike vatrozida, pregled Microsoft Sentinel SIEM sustava i prikaz integracije Microsoft Sentinel SIEM sustava s Fortigate vatrozidom.

5.4.1. Karakteristike vatrozida

Vatrozid je uređaj za sigurnost mreže koji djeluje kao prva linija obrane u zaštiti organizacije od neovlaštenog pristupa (slika 17.)



Slika 17. Slikovit prikaz vatrozida

Izvor: [46]

Vatrozid odlučuje koji mrežni promet može proći mrežom, a koji ne te se smatra opasnim. U suštini, on radi tako da filtrira dobro od lošeg, ili pouzdano od nepouzdanog. Vatrozidi su namijenjeni zaštiti privatnih mreža i krajnjih uređaja unutar njih, poznatih kao mrežni *hostovi*. Mrežni *hostovi* su uređaji koji komuniciraju s drugim *hostovima* na mreži. Oni šalju i primaju podatke unutar internih mreža, kao i izlazno i ulazno između vanjskih mreža. Jednostavno rečeno, vatrozid štiti internu mrežu organizacije od nesigurnih vanjskih izvora, djelujući kao barijera između njih. Smatra se prvom linijom obrane jer, bez vatrozida, neovlaštene osobe izvan mreže organizacije mogle bi pristupiti mreži organizacije bez ikakve prepreke. Ako bi se to dogodilo, napadač bi mogao lako kompromitirati druge uređaje kako bi eskalirao privilegije ili iznio osjetljive podatke. Međutim, s postavljenim vatrozidom, svaki zahtjev za povezivanje s mreže bit će nadziran i filtriran prema pravilima koje organizacija postavi. Stoga će neželjeni zahtjevi biti blokirani, a samo stvarni zahtjevi će proći, što pomaže spriječiti pokušaje krađe identiteta i druge opasne napade. Kada se politika vatrozida konfigurira da blokira zahtjeve iz bilo kojeg sumnjivog ili zlonamjernog izvora, podaci i privatnost bit će zaštićeni, a rizik da napadači zaraze mrežne uređaje zlonamjernim softverom će se znatno smanjiti. Vatrozid može biti hardverski ili softverski. Prvi je fizički uređaj koji omogućava centralizirano upravljanje mrežom; drugi je aplikacija koja dolazi uz operativni sustav uređaja i nadzire promet između aplikacija i interneta. Usmjerivač s ugrađenim vatrozidom primjer je hardverskog vatrozida, dok je *Windows Defender Firewall* primjer

softverskog vatrozida. Oba imaju svoje prednosti i nedostatke, pa je uvijek bolje imati oba kako bi se što kvalitetnije osigurala mreža i uređaji [47].

Vatrozid je učinkovit samo ako je njegova politika pravilno konfigurirana, a tu dolazi do izražaja SIEM rješenje. Moderna SIEM rješenja dolaze sa SOAR mogućnostima koje mogu pomoći u stvaranju novih pravila za vatrozid iz centralne konzole na temelju automatiziranih tijekova rada. Ovi tijekovi rada mogu se aktivirati kad god se dogodi događaj koji zahtijeva promjenu u pravilima vatrozida. Iako će ukupna konfiguracija SIEM rješenja varirati od dobavljača do dobavljača, svako dobro SIEM rješenje omogućit će analitičarima da kreiraju vlastiti tijek rada. Za vatrozide, tijek rada bi se temeljio na pravilima *"Inbound"* i *"Outbound".* SIEM rješenje će dati opciju da se odabere sučelje kao globalno ili drugačije, te želi li administrator da se pravila primjenjuju na određeni odredišni uređaj ili na sve uređaje u mreži. Na taj način, SIEM rješenje automatski će izvršiti željenu akciju prema postavljenoj konfiguraciji. Tako, ako obavijest iz SIEM rješenja upozori na zahtjev za povezivanjem iz zlonamjernog izvora, umjesto da se ručno mijenjaju postavke vatrozida kako bi se blokirala ta IP adresa, moguće je automatski blokirati IP adresu ako je pravilno konfiguriran tijek rada povezan s tim upozorenjem. U nastavku su navedene neke od prednosti integracije SIEM sustava s vatrozidom [48]:

- Vatrozidi generiraju zapise i događaje povezane s mrežnim prometom, koje SIEM rješenje može prikupljati i analizirati.
- Integracijom zapisa vatrozida u SIEM, sigurnosni timovi dobivaju vrijedne kontekstualne informacije, omogućujući bolju korelaciju i analizu sigurnosnih događaja.
- SIEM može pružiti uvid u obrasce mrežnog prometa, identificirati sumnjive aktivnosti i otkriti potencijalne sigurnosne incidente koji su možda prošli kroz početne filtere vatrozida.

Kako se kibernetičke prijetnje nastavljaju razvijati, organizacijama su potrebna snažna sigurnosna rješenja za otkrivanje, odgovaranje na incidente i njihovo sprječavanje. Microsoft Sentinel SIEM pruža inteligentnu sigurnosnu analitiku i informacije o prijetnjama. S druge strane, *Fortigate Firewalls* (NGFWs) je pouzdano rješenje za sigurnost mreže koje štiti mrežu od vanjskih prijetnji. Integracija ova dva proizvoda može značajno unaprijediti kibernetičku sigurnost organizacije. Prije obrade integracije ova dva alata, u nastavku slijedi opis Microsoft Sentinel SIEM sustava.

5.4.2. Pregled Microsoft Sentinel SIEM sustava

Microsoft Sentinel je *cloud-native* (izraz *cloud-native* odnosi se na aplikaciju koja je dizajnirana da boravi u oblaku od samog početka [49]) SIEM rješenje te SOAR rješenje koje

radi u Azure oblaku. Cilj mu je omogućiti cjelovite sigurnosne operacije pružanjem mogućnosti prikupljanja, otkrivanja, odgovora i istraživanja.

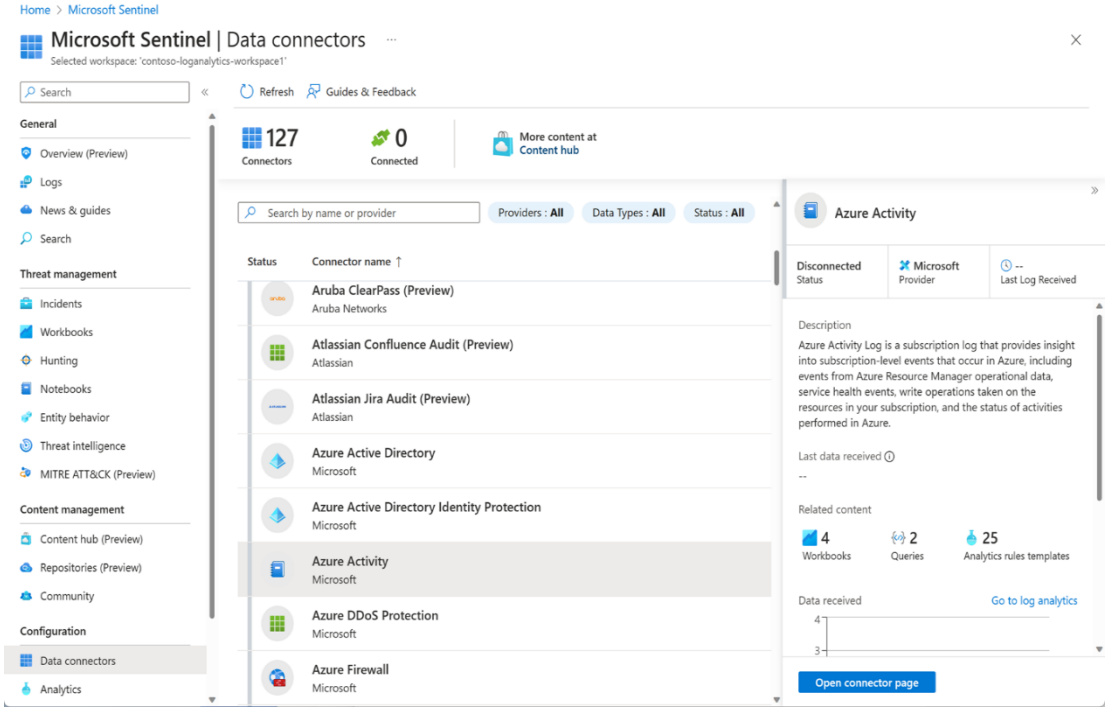
Microsoft Sentinel može se koristiti za analizu sigurnosnih događaja u *cloud* i o*n-premises* (lokalno) okruženjima. Uobičajeni slučajevi upotrebe uključuju:

- vizualizaciju podataka iz zapisa,
- otkrivanje anomalija i slanje upozorenja,
- istraživanje sigurnosnih incidenata,
- proaktivno lovljenje prijetnji,
- automatizirani odgovor na sigurnosne događaje.

Microsoft Sentinel pruža informacije o prijetnjama i inteligentne sigurnosne analitičke mogućnosti koje olakšavaju vidljivost prijetnji, otkrivanje upozorenja, odgovor na prijetnje i proaktivno lovljenje prijetnji. Microsoft Sentinel radi prema ciklusu koji započinje upravljanjem zapisima, nastavlja se normalizacijom sheme, provjerom podataka, otkrivanjem i istraživanjem te uključuje automatizirane odgovore na upozorenja. Sentinel to omogućuje kroz prikupljanje, otkrivanje, istraživanje i odgovor. Sentinel prikuplja podatke sa svih uređaja, korisnika, aplikacija i infrastrukture, uključujući komponente smještene lokalno i u više oblaka. Način prikupljanja podataka određuje koje se detekcije mogu pokrenuti na temelju tih podataka. Otkrivanje predstavlja analitičke mogućnosti i informacije o prijetnjama kako bi pomogao u otkrivanju prethodno neotkrivenih prijetnji i smanjio broj lažnih pozitivnih rezultata. Detekcije su napisane u KQL-u (engl. *Kusto Query Language*) i mogu se pohraniti kao kôd. Istraživanje znači da Sentinel koristi tehnologiju umjetne inteligencije kako bi pomogao stručnjacima za kibernetičku sigurnost u lovu na sumnjive aktivnosti u velikom opsegu. Automatizacija obogaćivanja i automatizacija zadržavanja doprinose uspješnim operacijama sigurnosnog operativnog centra. Odgovor u Sentinelu omogućuje prilagođenu orkestraciju i automatizaciju za uobičajene sigurnosne zadatke i zadatke integracije poslovanja kako bi se olakšao brz odgovor na incidente između timova koji koriste Microsoftove tehnologije.

U nastavku su navedene ključne komponente Microsoft Sentinela. Prva komponenta su konektori (engl. *Data Connectors).* Konektori omogućuju Microsoft Sentinelu da unosi podatke iz različitih izvora. Mogu se dodati usluge jednostavnim odabirom. Druge usluge, poput *sysloga*, mogu zahtijevati konfiguraciju. Sentinel pruža konektore podataka koji pokrivaju uobičajene izvore i scenarije, uključujući *syslog*, oblake poput *Amazon Web Services* (AWS) i Microsoft Azure, CEF i TAXII. Prilagođene aplikacije, jedinstveni ne-sigurnosni zapisnici

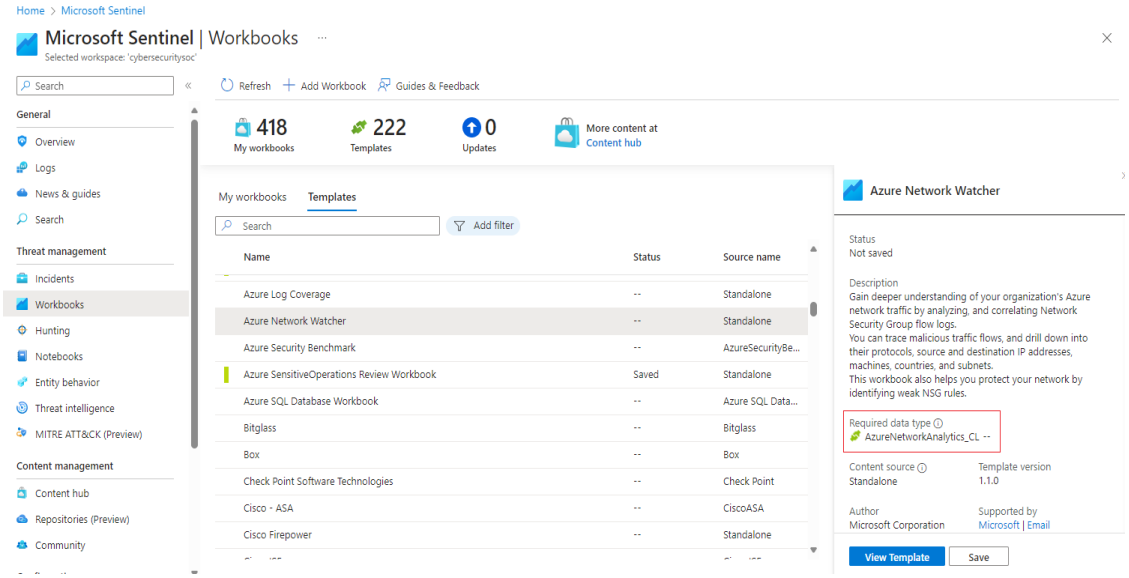
i fizički sigurnosni zapisnici također se mogu integrirati u Microsoft Sentinel [51]. Na slici 18. prikazan je izbornik konektora u Microsoft Sentinelu.



Slika 18. Prikaz izbornika konektora, [51]

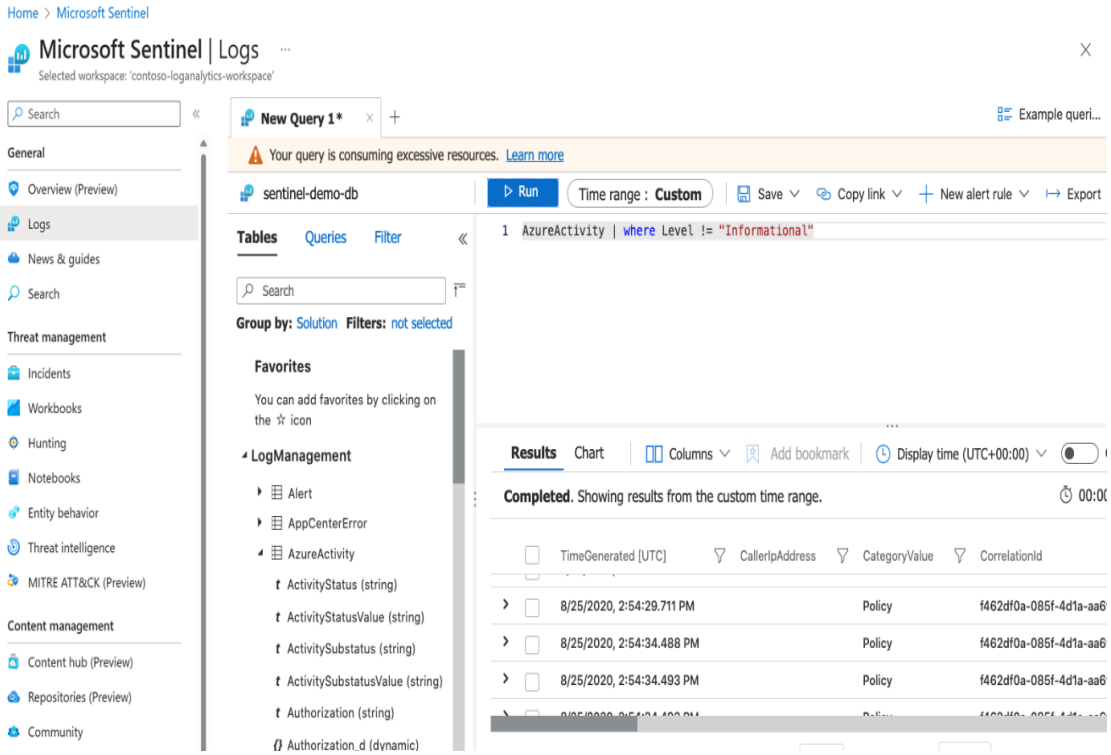
Zatim slijede radne knjige (engl. *Workbooks*). Radne knjige su prilagodljivi, interaktivni izvještaji koji omogućavaju fleksibilan prostor za analizu podataka. Microsoft Sentinel radne knjige omogućavaju sigurnosnim analitičarima i administratorima da pregledaju podatke o sigurnosti u svom okruženju koristeći grafičke prikaze. Ovo je moćan alat jer svi podaci koji se mogu pretraživati sada mogu biti prikazani i u lako razumljivom grafičkom formatu. Sentinel omogućuje integraciju radnih knjiga kako bi se mogli nadzirati, mjeriti i kontrolirati podaci. Radne knjige mogu kombinirati tekst, analitičke upite, metrike, parametre i sve to povezati u interaktivni izvještaj s više izvora podataka, koji mogu vidjeti i uređivati svi članovi tima koji imaju pristup istim resursima. Izrada prilagođenih i interaktivnih radnih knjiga može započeti s raznim predlošcima koji se mogu pregledati u Sentinelu. Mogu se koristiti ugrađeni predlošci radnih knjiga u Sentinelu kako bi se odmah dobio uvid nakon povezivanja izvora podataka. Prilagođene radne knjige mogu se izraditi kako bi pomogle u tijeku istraživanja, izvješćivanju

za izvršne funkcije ili za nadzor specifičnih anomalija, poput onih s WAF-om [52]. Na slici 19. prikazan je izbornik *Workbooks* u Microsoft Sentinelu.



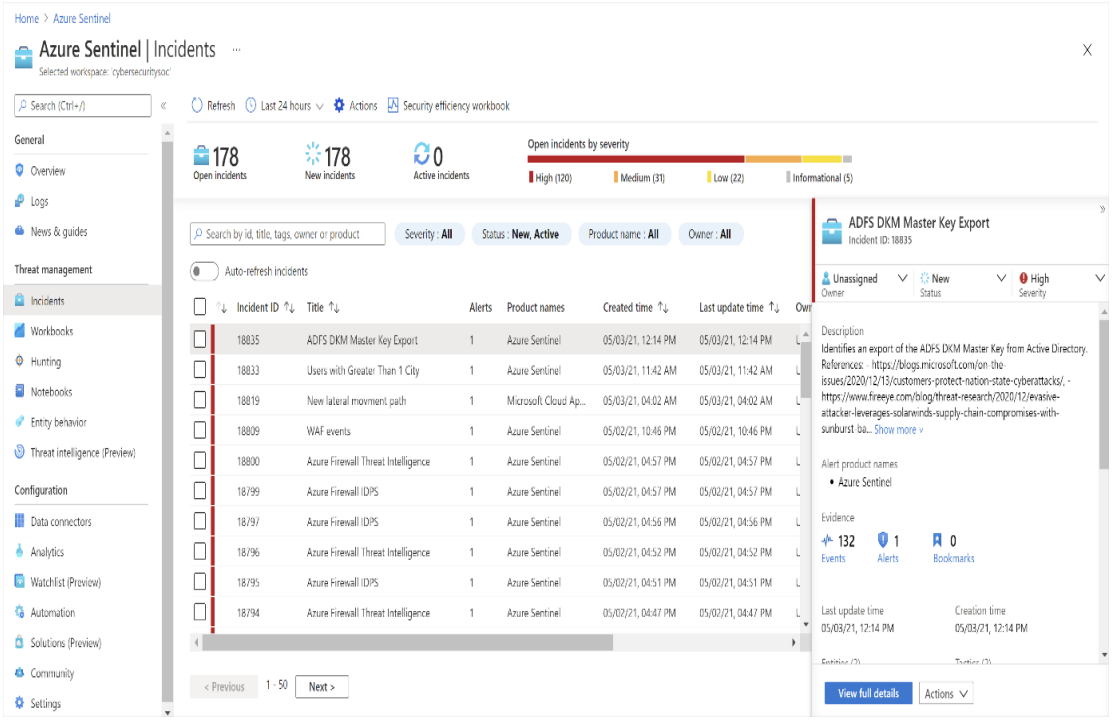
Slika 19. Izbornik *Workboks* u Microsoft Sentinelu, [52]

Sljedeća ključna komponenta je zadržavanje zapisnika. Sentinel pohranjuje unesene podatke korištenjem *Log Workspaces*. Zapisnici se također mogu proslijediti za dugotrajnu pohranu u ADX (engl. *Azure Data Explorer*). Za upite u Microsoft Sentinelu potrebno je poznavanje upitnog jezika KQL [53]. Na slici 20. prikazan je *Logs* izbornik u Microsoft Sentinelu.



Slika 20. *Logs* izbornik u Microsoft Sentinelu, [55]

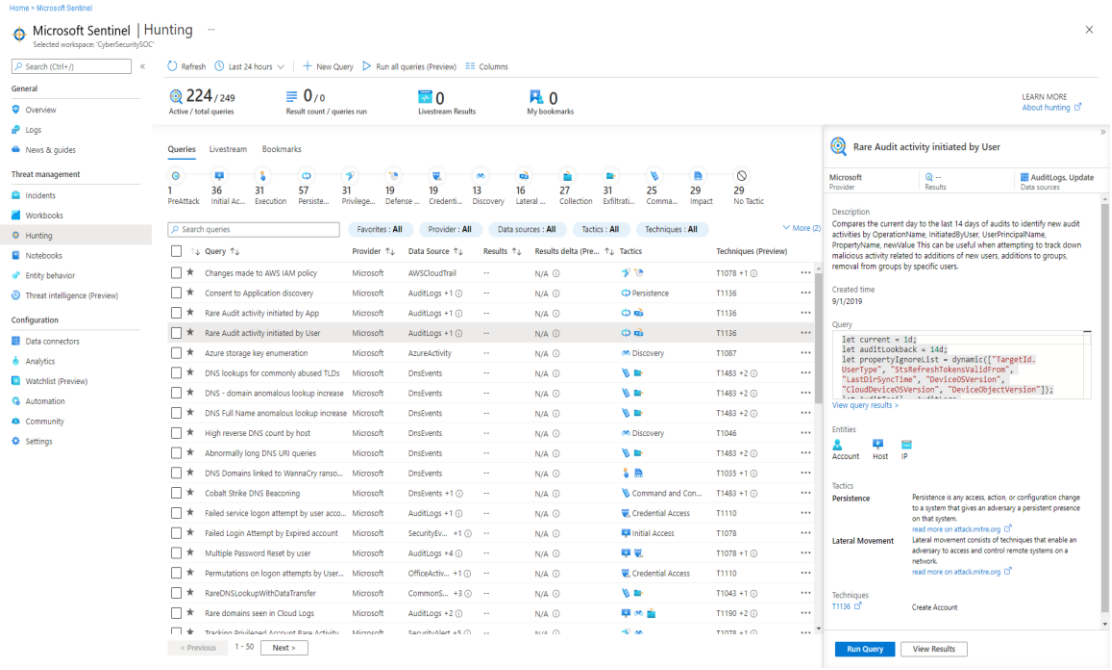
Analitika je iznimno važna komponenta Microsoft Sentinela. Postoje analitička pravila koja se koriste za povezivanje upozorenja i incidenata. Analitička pravila mogu biti zakazani upiti ili upiti koji se pokreću na zahtjev. Incident (slika 21.) uključuje grupu povezanih upozorenja koja zajedno predstavljaju potencijalnu prijetnju. Grupiranje upozorenja omogućuje istraživanje i rješavanje nekoliko upozorenja istovremeno. Sentinel pruža ugrađena pravila za korelaciju i pravila strojnog učenja kako bi pomogao u mapiranju ponašanja mreže i otkrivanju anomalija, ali će biti potrebno prilagođavanje unutar okruženja organizacije kako bi se postigla maksimalna vrijednost. Prilagođavanje pravila, iako zahtijeva početno ulaganje, može uštedjeti sate istraživanja i provjere lažno pozitivnih rezultata [55].



Slika 21. Prikaz incidenata u Microsoft Sentinelu, [55]

Zadnja komponenta je lov na prijetnje koji uključuje identificiranje prijetnji koje su zaobišle druge kontrolne mehanizme otkrivanja u okruženju. To uključuje analizu zapisa i drugih izvora podataka kako bi se identificirale prijetnje. Sigurnosni analitičari koji provode lov na prijetnje slijede *zero trust* (sigurnosni model koji se temelji na načelu održavanja strogih kontrola pristupa i nevjerovanja nikome prema zadanim postavkama, čak ni onima koji su već unutar mrežnog perimetra) princip i sposobni su identificirati sofisticirane prijetnje koje već

postoje u okruženju i time teže stvaranju sigurnog okruženja [56]. Na slici 22. prikazan je *Hunting* izbornik u Microsoft Sentinelu.



Slika 22. *Hunting* izbornik u Microsoft Sentinelu, [55]

Lov na prijetnje se koristi kroz:

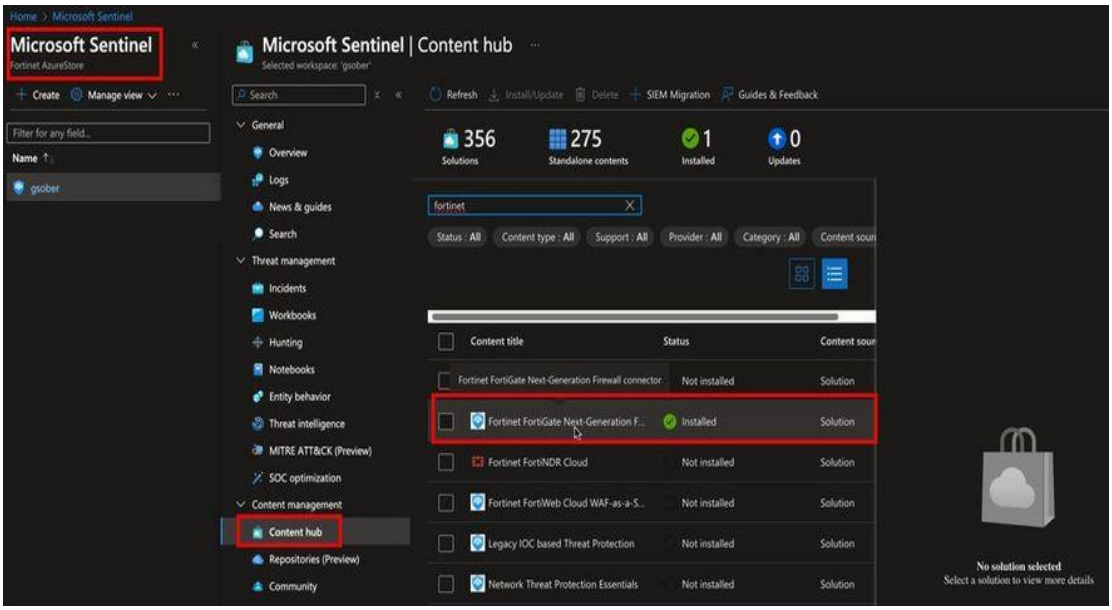
- **Upit:** lov na prijetnje u Sentinelu može pomoći otkriti upit koji pruža vrijedne uvide u potencijalne napade. Uvide dobivene iz upita mogu se koristiti za kreiranje vlastitih prilagođenih pravila za otkrivanje. Također, ove uvide moguće je prikazati kao upozorenja za odgovorne za incidente.
- **Lov:** Sentinel omogućuje stvaranje oznaka za zanimljive događaje tijekom lova. Moguće je vratiti se na te događaje kasnije ili podijeliti informacije s drugim suradnicima. Dodatno, Sentinel omogućuje grupiranje događaja u jedan incident kako bi ga se istražilo kao cjelinu.

Sigurnost je stalna ravnoteža između proaktivnih i reaktivnih obrambenih mjera. Obje su jednako važne i nijedna se ne smije zanemariti. Učinkovita zaštita organizacije znači stalno optimiziranje te prevenciju i otkrivanje prijetnji. Kombiniranje prevencije i otkrivanja omogućuje sprječavanje sofisticiranih prijetnji kada je to moguće, dok se istovremeno otkrivaju *cyber* napadi te se brzo reagira na njih.

5.4.3. Prikaz integracije Microsoft Sentinel SIEM sustava s Fortigate vatrozidom

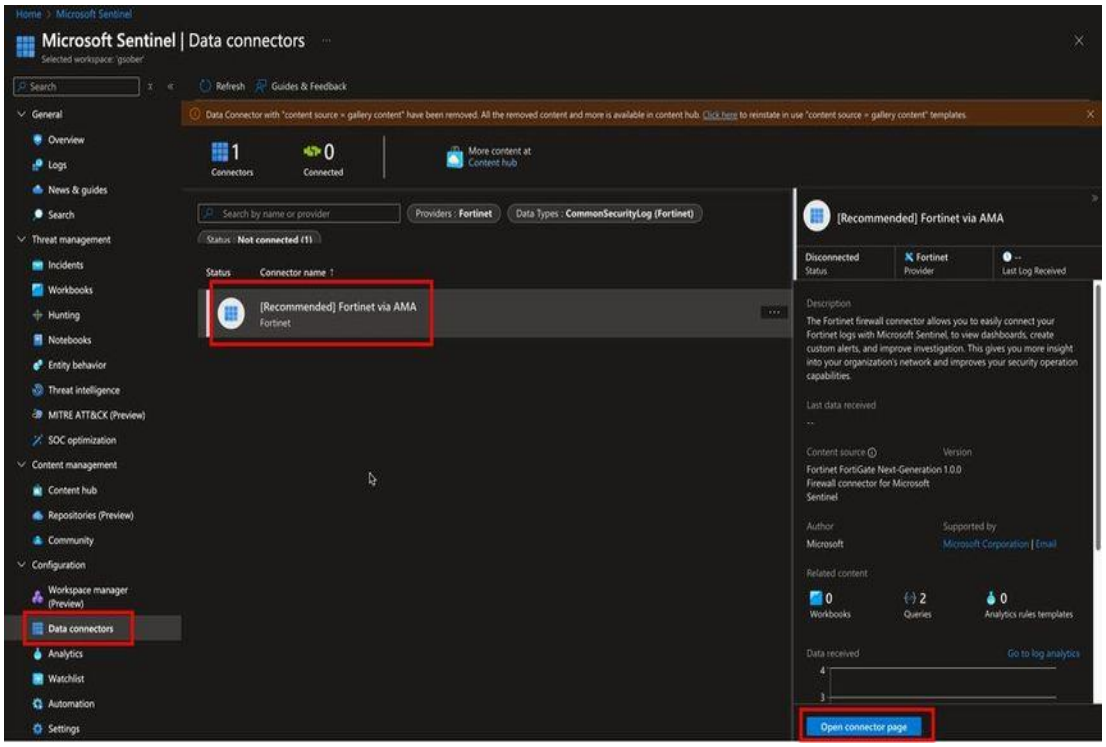
Integracija FortiGate vatrozida s Microsoft Sentinelom će poboljšati sigurnosni položaj svake organizacije kroz nadzor, detekciju incidenata i odgovore na incidente. Integriranjem FortiGate vatrozida s Microsoft Sentinel SIEM-om omogućuje prikupljanje i analizu podataka

o sigurnosti s vatrozida unutar Sentinel okruženja, što poboljšava sposobnost otkrivanja prijetnji i odgovora na incidente. Za integraciju FortiGate vatrozida na Azure za slanje zapisa (logova) u Microsoft Sentinel s Linux VM-om (engl. *Virtual Machine* – virtualna mašina) koji radi kao *log forwarder*, potrebno je slijediti sljedeće korake [57, 58, 59]. Prvi korak je iz *Content huba* u Microsoft Sentinel-u, instalirati *Fortinet FortiGate Next-Generation Firewall* konektor prikazan na slici 23.



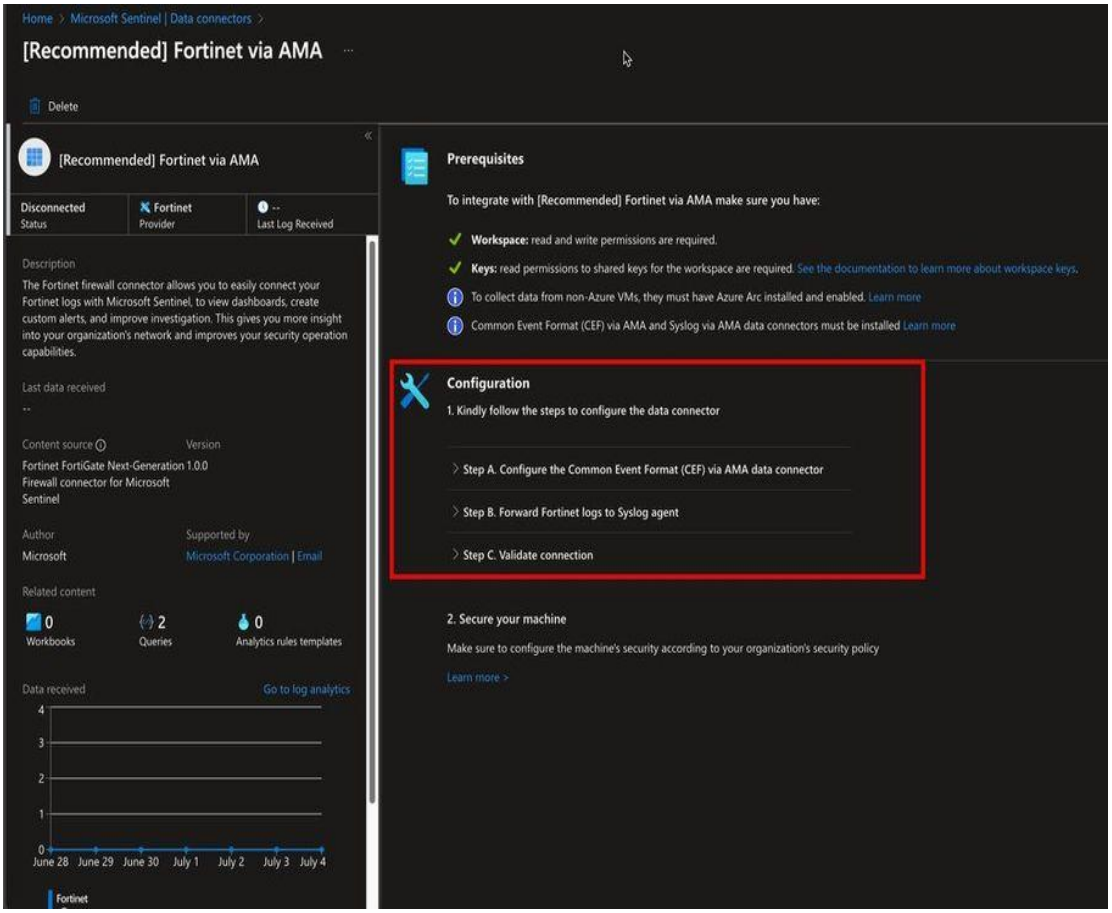
Slika 23. Prikaz *Fortinet FortiGate Next-Generation Firewall* konektora u Microsoft Sentinelu, [57]

Konektor *Fortinet via AMA* je vidljiv na slici 24.



Slika 24. Konektor *Fortinet via AMA,* [57]

Nakon otvaranja konektora, za uspješnu konfiguraciju potrebno je slijediti tri koraka (korak A, korak B, korak C) prikazana na slici 25.



Slika 25. Tri koraka potrebna za uspješnu konfiguraciju, [57]

Korak A: da bi se konfigurirao CEF (engl. *Common Event Format*) s AMA (engl. *Azure Monitor Agent*) konektorom podataka, potreban je *syslog* server ili *proxy* server, kao *log forwarder* za prikupljanje logova. *Syslog* server je potreban kako bi FortiGate vatrozid mogao proslijediti logove na *syslog* server, koji će zatim proslijediti te logove u *Log Analytics* radni prostor u *Azure Cloudu*. *Syslog* server može biti konfiguriran lokalno, kao virtualni stroj u Azure Cloudu ili EC2 u AWS Cloudu. *Syslog* server je svojevrsni *proxy* između *Log Analytics* radnog prostora i lokalnog FortiGate *firewalla*. Međutim, važno je napomenuti da se koristi virtualni stroj u Azureu ili EC2 u AWS-u koji se konfigurira kao *syslog* server, potrebno je osigurati da *Network Security Group* (NSG) dopušta promet na portu 514. To znači da se moraju provjeriti pravila koja omogućuju promet na tom portu.

Kao primjer, koristi se Ubuntu 20.04 s instaliranim *Syslog-NG*. Moguće je koristiti i bilo koju drugu verziju koju AMA podržava, bilo sa *Syslog-NG* ili *Rsyslog-om*.

Instaliranje *Syslog-NG* na Ubuntu:

Koraci instalacije u nastavku su za Ubuntu 20.04, ali je moguće koristiti ih s minimalnim izmjenama na bilo kojoj drugoj podržanoj distribuciji.

Preuzme se i instalira ključ pomoću naredbe ispod.

```
wget -qO - https://ose-repo.syslog-ng.com/apt/syslog-ng-ose-pub.asc | sudo apt-key add -
```

Dodaje se repozitorij koji sadrži najnoviju stabilnu verziju *Syslog-NG* u APT (engl. *Advanced Package Tool*) izvore. Na primjer, na Ubuntu 20.04.

```
echo 'deb https://ose-repo.syslog-ng.com/apt/ stable ubuntu-focal' | sudo tee -a /etc/apt/sources.list.d/syslog-ng-ose.list
```

Pokreće se sljedeća naredba.

```
apt-get update
```

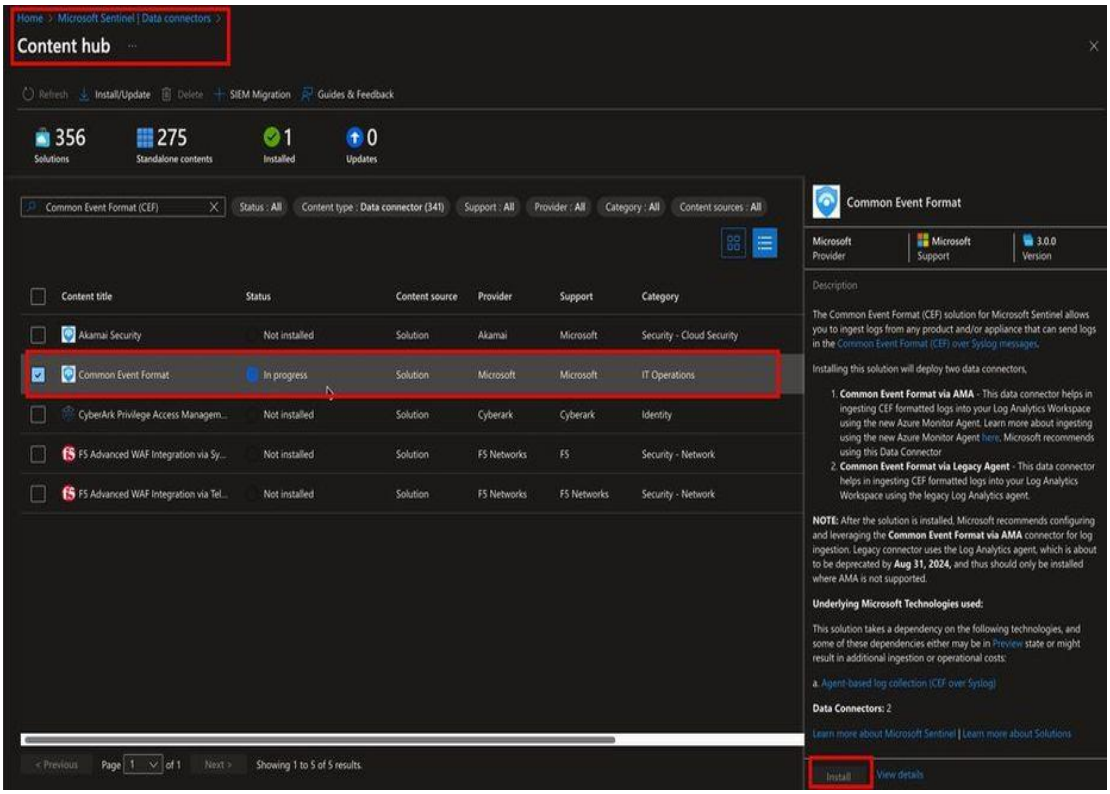
Instalira se *Syslog-NG* i svi njegovi pod-paketi pomoću sljedeće naredbe.

```
apt-get install syslog-ng-core syslog-ng-scl
```

Nakon toga potrebno je omogućiti portove 514 za TCP (engl. *Transmission Control Protocol*) i UDP (engl. *User Datagram Protocol*) promet naredbom.

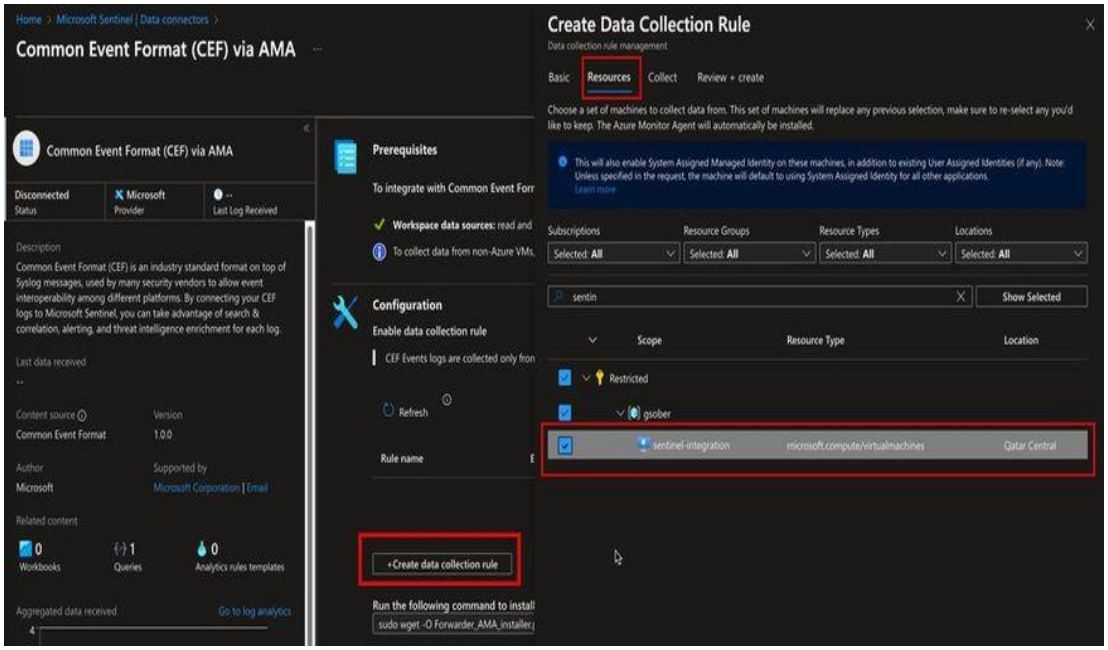
```
firewall-cmd --permanent --add-port=514/tcp i firewall-cmd --permanent --add-port=514/udp.
```

Konfiguracija konektora (slika 26.) se obavlja sljedećim koracima: Microsoft Sentinel radni prostor (engl. *Content hub*) -> Konfiguracija -> Kartica Konektor podataka. Odabrati konektor *Common Event Format (CEF) via AMA* i instalirati ga.



Slika 26. Prikaz konektora *CEF via AMA* u Microsoft Sentinelu, [57]

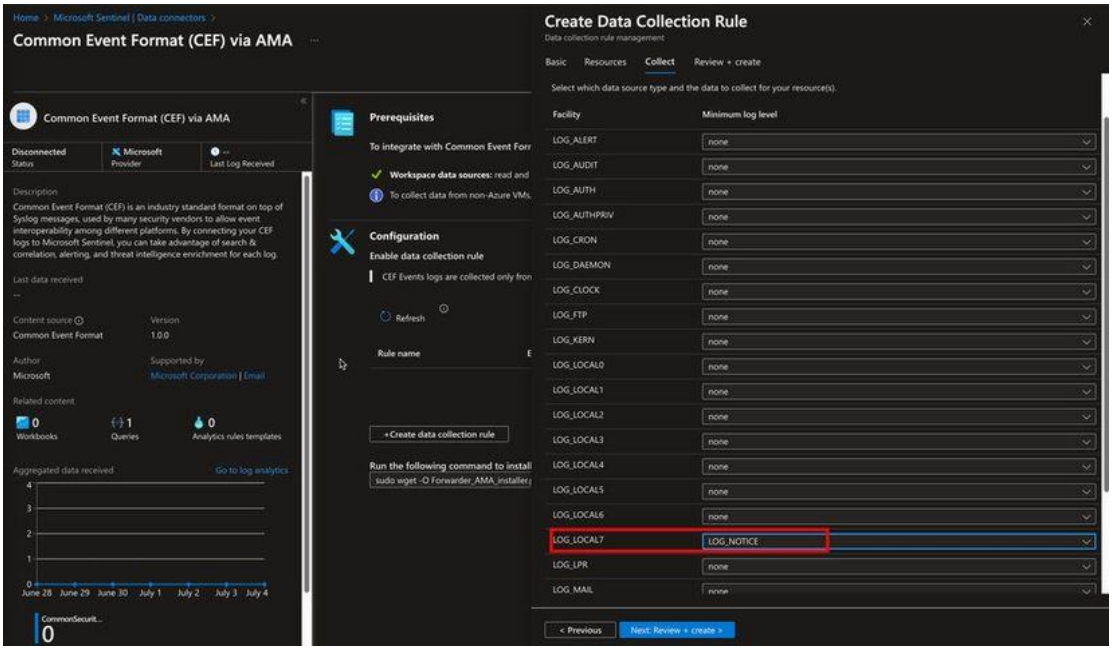
Potrebno je provjeriti je li već konfiguriran DCR (engl. *Data Collection Rule* – pravilo prikupljanja podataka) za prikupljanje potrebne vrste logova. Ako nije, kreira se novi DCR. U dijelu Resursi odabere se Linux VM koji je kreiran za prosljeđivanje logova (slika 27.).



Slika 27. Kreiranje novog DCR pravila, [57]

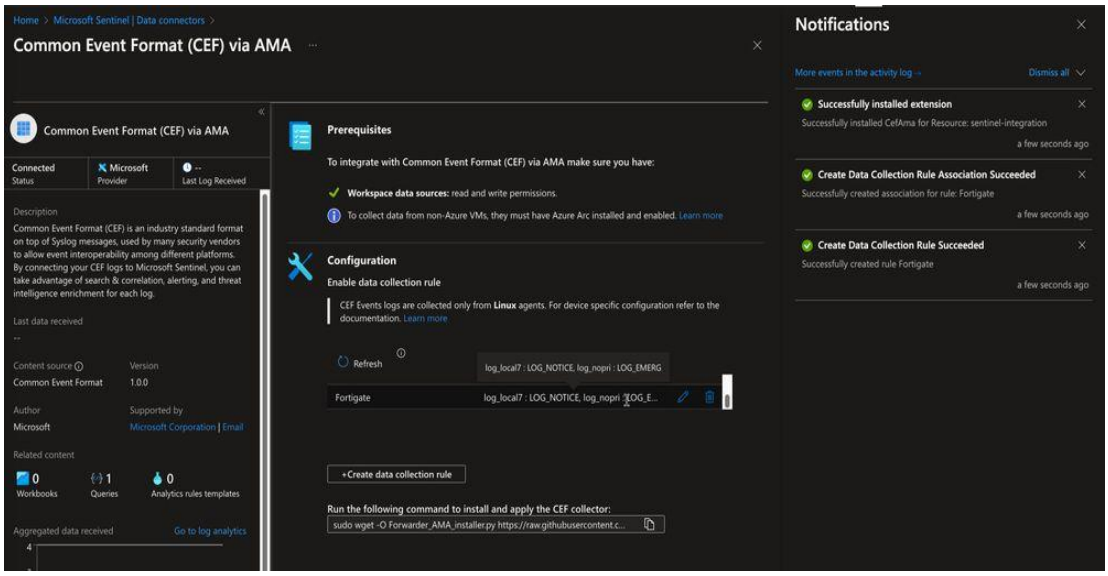
Nakon toga, odabere se tip izvora podataka i podaci koji se prikupljaju za resurse. Što god se ovdje konfigurira, treba odgovarati konfiguraciji na FortiGate vatrozidu za slanje podataka na Linux *log forwarder*.

Odabrani su *Local7* i *LOG_NOTICE* nivo (slika 28.), što će odgovarati FortiGate uređaju.



Slika 28. Odabir Local7 i LOG_NOTICE, [57]

Konačni rezultat prikazan je na slici 29.



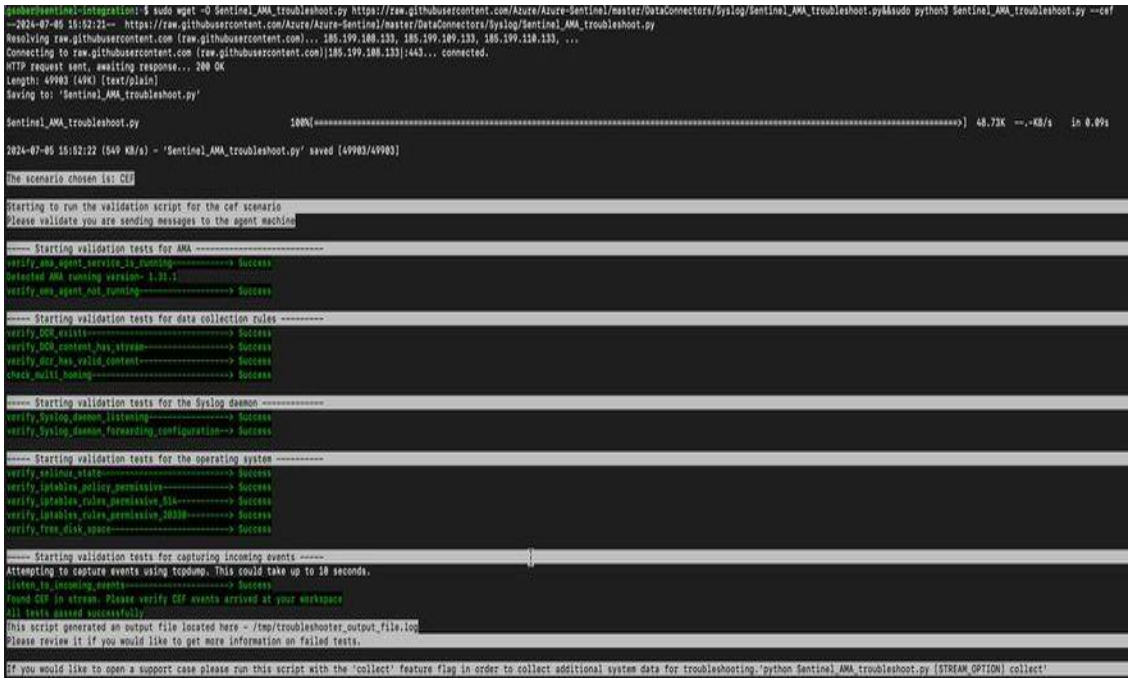
Slika 29. Prikaz *CEF via AMA* konektora nakon postavljenih postavki, [57]

Pokreće se naredba navedena na stranici CEF putem AMA podatkovnog konektora za konfiguraciju CEF-a (slika 30.).

```
sudo wget -O Forwarder_AMA_installer.py
```

```
https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/DataConnectors/Syslog/Forwarder_AMA_installer.py

python3 Forwarder_AMA_installer.py
```



Slika 30. Pokretanje naredbe u Linux VM-u, [57]

Korak B: konfigurira se FortiGate da šalje logove na Linux VM. Zatim se poveže se putem SSH (*Secure Shell*) na FortiGate instancu ili putem CLI (engl. *Command Line Interface*) konzole:

```
config log syslogd setting
    set status enable
    set server <----- IP adresa log forwardera
    set mode udp
    set port 514
    set facility local7
    set format cef
end
```

Napomena: *facility* je postavljen na *local7*, što odgovara pravilu za prikupljanje podataka na Azureu, a format je konfiguriran kao CEF.

Korak C: da bi se provjerilo je li konektor ispravno instaliran, pokreće se skripta za provjeru i otklanjanje problema (slika 31.).

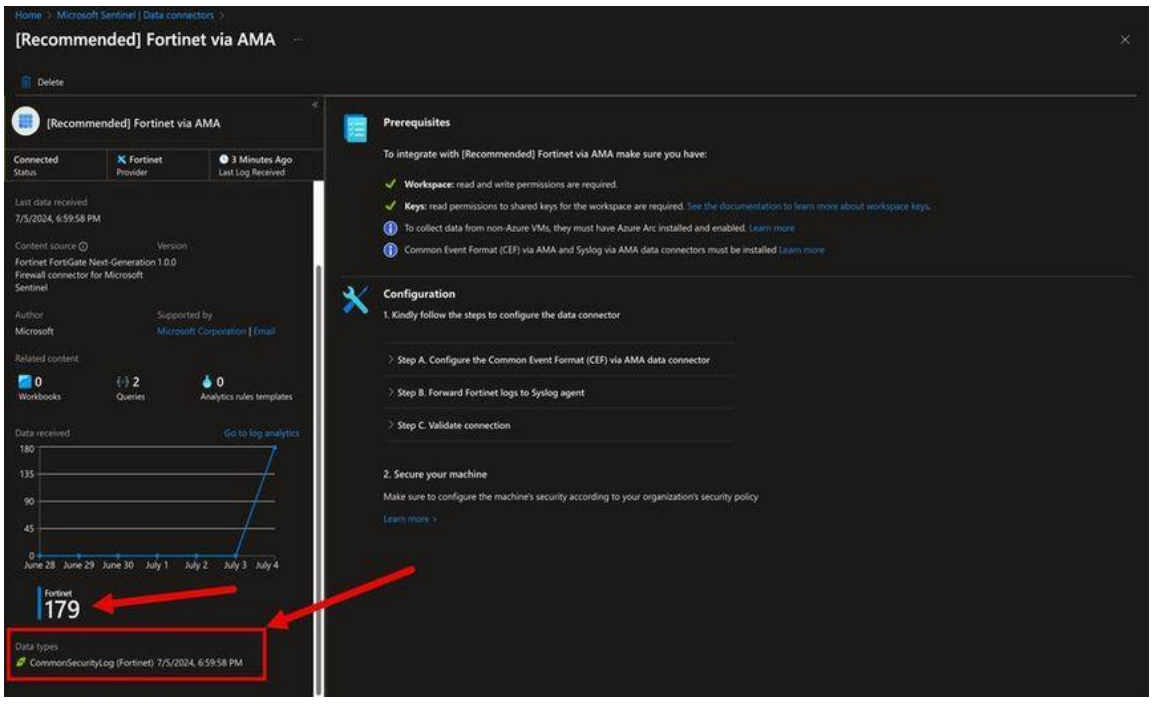
sudo wget -O Sentinel_AMA_troubleshoot.py

`https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/DataConnectors/Syslog/Sentinel_AMA_troubleshoot.py`

`python3 Sentinel_AMA_troubleshoot.py –cef`

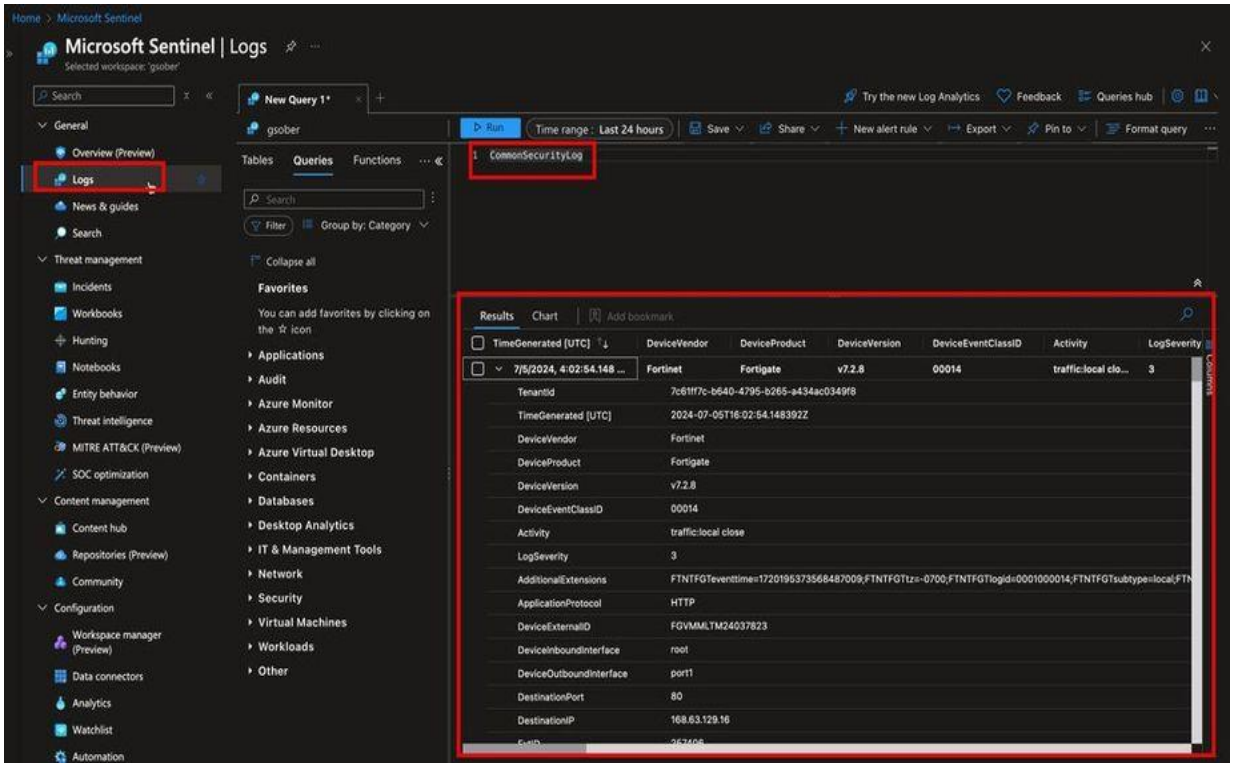
Slika 31. Skripta za provjeru i otklanjanje problema, [57]

Nakon svih prethodnih koraka, FortiGate vatrozid je integriran s Microsoft Sentinel SIEM sustavom (slika 32.).



Slika 32. Uspješna integracija FortiGate vatrozida s Microsoft Sentinel SIEM-om, [57]

Kako bi se vidjeli logovi FortiGate vatrozida u Sentinelu, u izborniku se odabere *Logs* i *New Query* te se u *New Query*-ju pokrene naredba *CommonSecurityLog.* Rezultat je vidljiv na slici 33.



Slika 33. FortiGate logovi vidljivi u Sentinelu, [57]

Zaključno, važno je razumjeti da SIEM nije vatrozid. Vatrozidi i SIEM rješenja imaju različite uloge u osiguravanju mreža organizacija. Dok se vatrozidi fokusiraju na kontrolu mrežnog prometa i upravljanje pristupom, SIEM rješenja pružaju sveobuhvatno upravljanje zapisima i događajima, otkrivanje sigurnosnih incidenata i mogućnosti odgovora. Kombinacijom snaga obje tehnologije, organizacije mogu postići snažnu i višeslojnu sigurnosnu infrastrukturu koja brani od širokog spektra prijetnji. Ključno je implementirati i vatrozid i SIEM kao dio sveobuhvatne strategije kibernetičke sigurnosti kako bi se osigurala snažna obrambena pozicija i zaštitili ključni resursi od potencijalnih sigurnosnih proboja.

6. BUDUĆI SMJEROVI INTEGRACIJE SIEM SUSTAVA

Ono što je počelo kao alat za upravljanje logovima evoluiralo je u sofisticiranu mrežu procesa i alata za kibernetičku sigurnost koji pomažu tvrtkama da otkriju i odgovore na prijetnje prije nego što one poremete poslovne operacije. Kako prijetnje evoluiraju, SIEM se također mora poboljšavati i držati korak. Posebno se očekuje da će algoritmi strojnog učenja i umjetne inteligencije biti na čelu evolucije SIEM-a. To ne bi trebalo biti iznenađenje – AI je već donio velike promjene u mnogim industrijama zbog svoje jedinstvene sposobnosti analize ogromnih količina podataka i generiranja prediktivnih uvida u kratkom vremenskom razdoblju. Glavna integracija umjetne inteligencije i strojnog učenja u SIEM tehnologiju stoga će pomoći sigurnosnim timovima da značajno unaprijede svoje sposobnosti za otkrivanje prijetnji. Nadalje, kako organizacije sve više premještaju svoje IT operacije u oblak, *cloud-native Next-Gen* SIEM modeli dobivaju na popularnosti, posebno jer pružaju organizacijama skalabilnost i fleksibilnost potrebnu za proširenje njihovih sigurnosnih kapaciteta kako se razvijaju. Još jedna stvar koju se očekuje u budućnosti je integracija i automatizacija dijeljenja obavještajnih podataka o prijetnjama iz trećih strana u SIEM tehnologiju. Uključivanjem podataka o prijetnjama u stvarnom vremenu iz vanjskih izvora, SIEM rješenja mogu biti u toku s najnovijim trendovima prijetnji i pokazateljima kompromitacije. To će poboljšati njegove kapacitete za otkrivanje prijetnji, smanjujući vrijeme potrebno za identificiranje i rješavanje potencijalnih sigurnosnih incidenata.

Kao što je već spomenuto, umjetna inteligencija i napredna analitika preuzimaju središnju ulogu u pronalaženju rješenja. Pojava velike količine podataka i jeftinih opcija pohrane pomogli su učiniti SIEM učinkovitijim. Na primjer, Amazon S3 i drugi pružatelji usluga riješili su problem dugoročne pohrane arhiviranih podataka. 2015. godine AI i strojno učenje uvedeni su kako bi se dodatno poboljšao SIEM. Analiza velikih podataka i strojno učenje integrirani su u SIEM alate kako bi se brzo obradili puno veći volumeni podataka bez ručne evaluacije. Otkrivanje *zero-day* prijetnji i novih te poznatih obrazaca napada značajno se poboljšalo. Osim toga, ove su tehnologije otvorile vrata za implementaciju SIEM alata u *cloud* okruženjima. AI i napredna analitika nude stručnjacima za kibernetičku sigurnost bržu obradu, učinkovitije otkrivanje prijetnji i vještinu prepoznavanja obrazaca napada. Budući da ti AI alati mogu obraditi više podataka brže nego čovjek, oni također drastično poboljšavaju točnost i produktivnost [60].

Jedno područje u kojem AI ostvaruje veliki napredak u sigurnosnim aplikacijama je automatizirano otkrivanje prijetnji. Automatizacija vođena umjetnom inteligencijom poboljšava proces otkrivanja složenih i novih prijetnji. Dobro dizajniran SIEM sustav obogaćen AI-om može identificirati i upozoriti osoblje na prijetnje mnogo brže nego što to može

stručnjak za kibernetičku sigurnost koji istražuje prijetnje. Primjer može biti SIEM sustav dizajniran za otkrivanje sofisticiranih taktika socijalnog inženjeringa u *phishing* e-mailovima. Kako napadači evoluiraju, e-mailovi postaju sve legitimniji, bez uobičajenih grešaka u gramatici i lošeg engleskog (ili hrvatskog). Pravilno usmjeren AI alat mogao bi otkriti manje anomalije, označiti ih kao neželjenu poštu i blokirati ih prije nego uđu u mrežu. Čovjek bi mogao biti prevaren, ali automatizirani sustav može primijetiti sitne nijanse koje ukazuju na prijetnju.

Što se tiče *ransomware* napada, AI pomaže na nekoliko različitih načina. Na primjer, tvrtke koriste algoritme strojnog učenja ugrađene u AI kako bi automatski otkrili obrasce i anomalije puno brže nego što to mogu stručnjaci za sigurnost. Uz nadzor i otkrivanje, stručnjaci za kibernetičku sigurnost također koriste AI za automatski odgovor na prijetnje bez ikakve ljudske intervencije.

Osim širokog spektra SIEM rješenja, neki pružatelji sigurnosti nude i specijalizirana rješenja poput EDR-a. Ako AI otkrije bilo kakve sigurnosne probleme, automatski pokreće odgovor na temelju skupa unaprijed definiranih pravila. Kako AI uči, dodaje više pravila. AI se također koristi za prediktivnu analitiku kako bi predvidio i ublažio potencijalne sigurnosne proboje. Automatiziranjem praćenja aktivnosti korisnika i ponašanja, sustav bi mogao spriječiti upad nadgledajući tisuće korisnika istovremeno, tražeći specifične obrasce napada. Na primjer, ako sustav primijeti da se određeni korisnik prijavljuje u neobično vrijeme i pokušava pristupiti specifičnim dijelovima mreže, AI alat bi mogao blokirati prijavu tog korisnika dok stručnjak za kibernetičku sigurnost ne istraži dalje [61].

Poboljšano upravljanje podacima još je jedno područje u kojem AI unapređuje napore u kibernetičkoj sigurnosti. Podaci se povećavaju nevjerojatnom brzinom, a AI može učinkovitije pregledati ogromne količine informacija i identificirati prijetnje. AI koristi računalnu snagu za obradu velike količine podataka i može ih očistiti kako bi ispravio loše oblikovane podatke i uklonio duplikate, čime se pomaže u izbjegavanju lažno pozitivnih rezultata. Umjetna inteligencija također ima sposobnost odvajanja bitnih podataka od nebitnih, čineći praćenje podataka učinkovitijim. Kako količina podataka raste, AI će se također morati razvijati i koristiti veću računalnu snagu i evolucijske metode kako bi obradio više informacija i izdvojio samo ono što je korisno.

Iako umjetna inteligencija nije novost, najnoviji i najveći proboj ima ChatGPT (engl. *Chat Generative PreTrained Transformer*). U svim sektorima, uključujući sigurnost, vlada uzbuđenje oko pronalaženja načina za korištenje velikih jezičnih modela kako bi se povećala učinkovitost. Trenutno, ChatGPT ima sposobnost analiziranja dokumenta ili informacija i proizvodnje sažetka te informacije na razini kvalitete koju bi napravio čovjek. Ljudi također mogu voditi razgovore s ChatGPT-om, postavljati pitanja i dobivati uvjerljive odgovore.

Međutim, postoji jedna napomena: ChatGPT je još u početnoj fazi i može pružiti netočne odgovore, iako vjeruje da su ispravni [62]. Dakle, bitno je informacije provjeriti kada se koristi ChatGPT. Također, ChatGPT može skratiti krivulju učenja i automatizirati složene zadatke. Na primjer, stručnjaci za prijetnje moraju biti SQL programeri i razumjeti kako iskoristiti razne jezike upita da bi učinkovito obavljali svoj posao. ChatGPT može olakšati i ubrzati proces postavljanja pitanja i dobivanja odgovora za početnike, bez potrebe za učenjem programskih jezika. Općenito, AI i jezični modeli transformiraju funkcionalnost i dostupnost SIEM sustava, uglavnom utječući na brzinu, učinkovitost i uspjeh.

Drugi fokus je integracija s novim tehnologijama. Povijesno gledano, SIEM i SOAR bili su odvojeni entiteti. SIEM se bavi nadzorom i otkrivanjem, a SOAR se bavi odgovorom na prijetnje. Dobavljači su počeli preuzimati SIEM ili SOAR tvrtke kako bi ponudili obje strane medalje, ali tehnologije su još uvijek podijeljene u odvojena rješenja, što ih čini manje učinkovitim. Budućnost je u izgradnji proizvoda od temelja s kombiniranim SIEM i SOAR rješenjima koja koriste AI i prediktivnu analitiku od samog početka. Sada postoje potpuno integrirana rješenja koja rade sve: nadzor, otkrivanje i reagiranje, a sve funkcionira besprijekorno zajedno.

SIEM će se integrirati sa strojnim učenjem, *blockchainom* i IoT-om za sveobuhvatnu sigurnost. Novi programi, uređaji i rješenja neprestano se pojavljuju. Stoga će SIEM rješenja morati biti dovoljno fleksibilna da uključe tehnologije koje danas ne postoje, ali će postojati sutra. Dodavanje tih resursa mora biti jednostavno i učinkovito. Najveća promjena u budućim SIEM rješenjima je pomak fokusa s reaktivnog na proaktivan pristup. Cilj modernih SIEM sustava je automatski identificirati i ublažiti kibernetičke prijetnje prije nego što se dogode, uz minimiziranje potrebe za transakcijskim nadzorom od strane analitičara prijetnji. Iako postoje pretjerane zabrinutosti da će AI zamijeniti ljude, najvjerojatniji scenarij je kombinacija AI-a i ljudi, gdje AI upravlja niskim razinama procesa, a obučeni analitičari fokusiraju se na strateške izazove višeg nivoa. AI također utječe na SIEM rješenja mijenjajući korisničko sučelje i povećavajući dostupnost. Generativni alati poput ChatGPT-a u kombinaciji s NLP-om (engl. *Natural Language Processing* – obrada prirodnog jezika) olakšavaju analitičarima da postave sigurnosno pitanje na jednostavnom jeziku i odmah dobiju odgovor bez obzira na složenost pitanja. Najnapredniji AI alati mogu pretražiti milijarde podataka (sada mjerene u petabajtima) kako bi došli do odgovora u roku od nekoliko sekundi, umjesto dana. Tako AI ima potencijal smanjiti krivulju učenja s jezicima upita, čineći SIEM sustave dostupnijim širem krugu korisnika [63].

Automatizirani odgovor na prijetnje jedno je od najvažnijih područja budućih unapređenja očekivanih u SIEM alatima. AI unutar sustava za otkrivanje prijetnji može pojednostaviti pristup odgovoru na incidente i upravljanju prijetnjama, eliminirajući potrebu

za odvojenim sustavima, opsežnim programiranjem i, u mnogim slučajevima, čak i ljudskom intervencijom. Iako AI uvijek može brže reagirati od sigurnosnog stručnjaka, ljudi (kako je ranije spomenuto) moraju biti uključeni u proces. Strojno učenje, temeljeno na *big data*, širi svoj doseg. AI-pokretani SIEM sustavi brzo napreduju, povećavajući svoje sposobnosti profiliranja prijetnji, otkrivanja anomalija i stvaranja pravila o tome što izgleda kao normalno ponašanje i što se smatra prijetnjom.

Zaštita privatnosti podataka i poštivanje zakonskih propisa još su jedno područje u kojem će se u budućnosti dogoditi poboljšanja. Nije tajna da vlade, posebno u Europi, daju prioritet privatnosti i sigurnosti, a zakoni koji se odnose na to stalno se mijenjaju. SIEM rješenja se prilagođavaju kako bi zadovoljila sve veći naglasak na privatnosti podataka i pravilima o usklađenosti diljem svijeta. Izazov nastaje kada zakon kaže da se ne može pregledavati nešto, iako je to potrebno iz sigurnosnih razloga. Na primjer, u nekim zemljama, e-mailovi zaposlenika su privatni, iako su to e-mailovi tvrtke i prijenosna računala tvrtke. Dakle, sigurnosni stručnjak, iako ne može čitati e-mailove korisnika dok ih primaju kako bi tražio *phishing* napade, može tu ulogu premjestiti na poslužitelj, pregledati ih čim stignu prije nego što budu isporučeni i staviti u karantenu sve sumnjive e-mailove.

Zaključno, kako prijetnje postaju sve sofisticiranije i nepredvidljivije, SIEM sustavi se prilagođavaju kako bi odgovorili na nove trendove i izazove – prvenstveno kroz uvođenje AI tehnologije i algoritama strojnog učenja. Oslanjanje na AI i automatizaciju je dobrodošlo, jer omogućuje tvrtkama da se usmjere na ono što je zaista važno, umjesto da troše dragocjeno vrijeme na rutinske zadatke. AI tehnologija također pruža uvide koji tvrtkama omogućuju bolji pregled njihovog digitalnog okruženja. Kao što je naglašeno, AI tehnologija će igrati ključnu ulogu u budućnosti SIEM sustava i industrije kibernetičke sigurnosti. Nevjerojatna sposobnost AI-a da obrađuje informacije i generira korisne uvide u impresivnom vremenskom roku daleko nadmašuje sposobnosti sigurnosnih timova, čineći ga neophodnim za moderne tvrtke.

7. ZAKLJUČAK

U ovom diplomskom radu istražena je integracija SIEM sustava s ostalim sigurnosnim alatima u informacijskim okruženjima, s naglaskom na važnost takve integracije za učinkovito upravljanje kibernetičkom sigurnošću. Kroz pregled funkcionalnosti SIEM sustava, izazova s kojima se suočavaju stručnjaci prilikom integracije, te različitih strategija i pristupa koji omogućuju uspješnu implementaciju, dobiveni su uvidi koji doprinose razumijevanju ove teme.

Kroz istraživanje je potvrđena važnost SIEM sustava kao centralnog elementa u sustavu kibernetičke sigurnosti, no također je naglašena potreba za integracijom s drugim alatima za zaštitu informacijsko-komunikacijskog sustava, poput vatrozida. Takva integracija omogućuje stvaranje jedinstvenog sigurnosnog ekosustava koji značajno poboljšava sposobnost organizacije da detektira, analizira i odgovori na složene kibernetičke prijetnje u stvarnom vremenu.

Također, istraživanje naglašava kako budućnost leži u daljnjoj integraciji SIEM sustava s naprednim tehnologijama poput umjetne inteligencije i strojnog učenja, što će omogućiti proaktivno prepoznavanje prijetnji i automatiziranu reakciju na incidente. Očekuje se da će ove inovacije dodatno smanjiti potrebu za ručnom intervencijom, omogućujući sigurnosnim timovima da se usmjere na stvaranje što bolje sigurnosne pozicije organizacije.

Zaključno, integracija SIEM sustava s ostalim alatima za zaštitu informacijsko-komunikacijskog sustava nije samo tehnička potreba, već i strateška prednost koja organizacijama pruža sveobuhvatnu zaštitu od suvremenih kibernetičkih prijetnji. Uspješna implementacija ove integracije ključna je za održavanje visoke razine sigurnosti i otpornosti informacijskih sustava u sve složenijem digitalnom okruženju.

LITERATURA

1. D., Avinash Gupta, P., Srinivas Reddy, J., Vinay Dutt., 2019. Integrating SIEM with Other Security Tools: Enhancing Cybersecurity Posture and Threat Response. Turkish Journal of Computer and Mathematics Education (TURCOMAT). 10. pp. 1140-1144. Preuzeto s: https://www.researchgate.net/publication/376811244_Integrating_SIEM_with_Other_Security_Tools_Enhancing_Cybersecurity_Posture_and_Threat_Response [Pristupljeno: travanj 2024.]
2. A. R., Muhammad, P., Sukarno, A. A., Wardana, 2023. Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning. Procedia Computer Science, Volume 217, pp. 1406-1415 Preuzeto s: https://www.sciencedirect.com/science/article/pii/S1877050922024243 [Pristupljeno: travanj 2024.]
3. J. V., Dutt, P., S., Reddy, D. A., Gupta, 2021. Utilizing SIEM to Enhance Vulnerability Management and Response. Preuzeto s: https://www.researchgate.net/publication/376645921_Utilizing_SIEM_to_Enhance_Vulnerability_Management_and_Response [Pristupljeno: travanj 2024.]
4. K. -O., Detken, T., Rix, C., Kleiner, B., Hellmann, and L., Renners, 2015. SIEM approach for a higher level of IT security in enterprise networks. IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Warsaw, Poland, 2015, pp. 322-327. Preuzeto s: https://ieeexplore.ieee.org/abstract/document/7340752 [Pristupljeno: travanj 2024.]
5. G.G., Gustavo, G. Z., Susana, D., Rodrigo, 2021. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Preuzeto s: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8309804/ [Pristupljeno: travanj 2024.]
6. IBM. *What is security information and event management (SIEM)?* Preuzeto s: https://www.ibm.com/topics/siem [Pristupljeno: kolovoz 2024.]
7. Logsign. *SIEM and UEBA: A Match Made in Cybersecurity Heaven.* Preuzeto s: https://www.logsign.com/blog/siem-and-ueba-how-they-work-together/ [Pristupljeno: kolovoz 2024.]

8. Imperva. *Survey: 27 Percent of IT professionals receive more than 1 million security alerts daily.* Preuzeto s: https://www.imperva.com/blog/archive/27-percent-of-it-professionals-receive-more-than-1-million-security-alerts-daily/ [Pristupljeno: kolovoz 2024.]
9. ManageEngine. *What is logging?* Preuzeto s: https://www.manageengine.com/products/eventlog/logging-guide/log-collection-and-techniques.html [Pristupljeno: kolovoz 2024.]
10. Logsign. *What are The Types of Dashboards in a SIEM Solution?* Preuzeto s: https://www.logsign.com/blog/what-are-the-types-of-dashboards-in-a-siem-solution/ [Pristupljeno: kolovoz 2024.]
11. IBM. *What is threat intelligence?* Preuzeto s: https://www.ibm.com/topics/threat-intelligence [Pristupljeno: kolovoz 2024.]
12. Anomali. *What are STIX/TAXII?* Preuzeto s: https://www.anomali.com/resources/what-are-stix-taxii [Pristupljeno: kolovoz 2024.]
13. Fortinet. *What Is UEBA?* Preuzeto s: https://www.fortinet.com/resources/cyberglossary/what-is-ueba [Pristupljeno: kolovoz 2024.]
14. ManageEngine. *Functions of SIEM.* Preuzeto s: https://www.manageengine.com/log-management/siem/siem-functions.html [Pristupljeno: kolovoz 2024.]
15. Crowdstrike. *What is Log Management? The Importance of logging and best practices.* Preuzeto s: https://www.crowdstrike.com/cybersecurity-101/observability/log-management/ [Pristupljeno: kolovoz 2024.]
16. TechTarget. *IT incident management.* Preuzeto s: https://www.techtarget.com/searchitoperations/definition/IT-incident-management [Pristupljeno: kolovoz 2024.]
17. Crowdstrike. *What is Cyber Threat Intelligence?* Preuzeto s: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/ [Pristupljeno: kolovoz 2024.]
18. Zscaler. *What Is Cloud Security?* Preuzeto s: https://www.zscaler.com/resources/security-terms-glossary/what-is-cloud-security [Pristupljeno: kolovoz 2024.]
19. Crowdstrike. *Syslog Logging Guide: The Basics.* Preuzeto s: https://www.crowdstrike.com/guides/syslog-logging/ [Pristupljeno: kolovoz 2024.]

20. Paessler. *IT Explained: Syslog.* Preuzeto s: https://www.paessler.com/it-explained/syslog [Pristupljeno: kolovoz 2024.]
21. Sumo logic. *The Ultimate Guide to Windows Event Logging.* Preuzeto s: https://www.sumologic.com/blog/windows-event-logging/ [Pristupljeno: kolovoz 2024.]
22. Sematext. *Structured Logging.* Preuzeto s: https://sematext.com/glossary/structured-logging/ [Pristupljeno: kolovoz 2024.]
23. Atatus. *JSON Logging: 7 Must-Know Tips.* Preuzeto s: https://www.atatus.com/blog/json-logging-tips/ [Pristupljeno: kolovoz 2024.]
24. Code Project. *Simple XML based Error Log.* Preuzeto s: https://www.codeproject.com/Articles/7711/Simple-XML-based-Error-Log [Pristupljeno: kolovoz 2024.]
25. Slavomíra D., Yehor S. Dynamic security log processing using deep learning techniques. *Proceedings II of the 28st Conference STUDENT EEICT 2022*. 2022, 184-187. Preuzeto s: https://dspace.vut.cz/items/6a8444ed-9df1-40ff-a4f2-ea6cf93da79f [Pristupljeno: kolovoz 2024.]
26. IEEE. *Lazy XML Parsing/Serialization Based on Literal and DOM Hybrid Representation.* Preuzeto s: https://www.computer.org/csdl/proceedings-article/icws/2008/3310a295/12OmNx5GUb9 [Pristupljeno: kolovoz 2024.]
27. Flatfile. *What is a CSV file: A comprehensive guide.* Preuzeto s: https://flatfile.com/blog/what-is-a-csv-file-guide-to-uses-and-benefits/ [Pristupljeno: kolovoz 2024.]
28. Rantos, K.; Spyros, A.; Papanikolaou, A.; Kritsas, A.; Ilioudis, C.; Katos, V. Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem. *Computers*. 2020, 9, 18. Preuzeto s: https://www.mdpi.com/2073-431X/9/1/18 [Pristupljeno: kolovoz 2024.]
29. Cribl. *Why Cyber Resilience Is Foundational to Your SIEM Success*. Preuzeto s: https://cribl.io/blog/why-cyber-resilience-is-foundational-to-your-siem-success/ Pristupljeno: kolovoz 2024.]
30. Riversafe. *Is your SIEM up to scratch? Unveiling the security risks of a poorly implemented SIEM*. Preuzeto s: https://riversafe.co.uk/resources/tech-blog/the-security-risks-of-an-unoptimised-siem/ Pristupljeno: kolovoz 2024.]
31. Sheeraz, Muhammad & Paracha, Muhammad & Ulhaq, Mansoor & Durad, Hanif & Mohsin, Syed Muhammad & S. Band, Shahab & Mosavi, Amir. Effective Security Monitoring Using Efficient SIEM Architecture. *Human-centric Computing and Information Sciences*. 2023. Preuzeto s:

https://www.researchgate.net/publication/371173436_Effective_Security_Monitoring_Using_Efficient_SIEM_Architecture [Pristupljeno: kolovoz 2024.]

32. Cyvatar. *What is SOAR security orchestration and why is it important?* Preuzeto s: https://cyvatar.ai/soar-security-orchestration-automation-response/ [Pristupljeno: kolovoz 2024.]
33. PaloAltoNetworks. *What Is SOAR?* Preuzeto s: https://www.paloaltonetworks.com/cyberpedia/what-is-soar [Pristupljeno: kolovoz 2024.]
34. IBM. *What is SOAR (security orchestration, automation and response)?* Preuzeto s: https://www.ibm.com/topics/security-orchestration-automation-response [Pristupljeno: kolovoz 2024.]
35. Jackhenry. *Next-gen SIEM and SOAR: a powerful duo against cyber threats.* Preuzeto s: https://www.jackhenry.com/hubfs/resources/white-papers/next-gen-siem-and-soar.pdf [Pristupljeno: kolovoz 2024.]
36. IEEE Xplore. *SIEM integration with SOAR.* Preuzeto s: https://ieeexplore.ieee.org/document/10094537 [Pristupljeno: kolovoz 2024.]
37. Geeksforgeeks. *What is an API (Application Programming Interface)?* Preuzeto s: https://www.geeksforgeeks.org/what-is-an-api/ [Pristupljeno: kolovoz 2024.]
38. IBM. *What is an API (application programming interface)?* Preuzeto s: https://www.ibm.com/topics/api [Pristupljeno: kolovoz 2024.]
39. Medium. *The six Guiding Principles of RESTful Architecture*. Preuzeto s: https://medium.com/@Ian_carson/the-six-guiding-principles-of-restful-architecture-852d707b9036 [Pristupljeno: kolovoz 2024.]
40. Catchpoint. *API Architecture Patterns and Best Practices.* Preuzeto s: https://www.catchpoint.com/api-monitoring-tools/api-architecture [Pristupljeno: kolovoz 2024.]
41. Medium. *Understanding WebSocket API in Amazon API Gateway.* Preuzeto s: https://kvs-vishnu23.medium.com/understanding-websocket-api-in-amazon-api-gateway-60dc930307c6 [Pristupljeno: kolovoz 2024.]
42. MyCPlus. *What is the right API for your Project, GraphQL or REST?* Preuzeto s: https://www.mycplus.com/featured-articles/what-is-the-right-api-for-your-project-graphql-or-rest/?utm_content=cmp-true#google_vignette [Pristupljeno: kolovoz 2024.]
43. AWS. *What's the Difference Between GraphQL and REST?* Preuzeto s: https://aws.amazon.com/compare/the-difference-between-graphql-and-rest/ [Pristupljeno: kolovoz 2024.]

44. IBM. *What is ETL (extract, transform, load)?* Preuzeto s: https://www.ibm.com/topics/etl [Pristupljeno: kolovoz 2024.]
45. DataChannel. *What Is ETL And How the ETL process works?* Preuzeto s: https://www.datachannel.co/blogs/what-is-etl-and-how-the-etl-process-works [Pristupljeno: kolovoz 2024.]
46. Secureops. *Why Organizations Are Moving to Managed Firewall and SIEM Solutions?* Preuzeto s: https://secureops.com/blog/siem-and-firewall-management/ [Pristupljeno: kolovoz 2024.]
47. Cisco. *What is a firewall?* Preuzeto s: https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-firewall.html#~types-of-firewalls [Pristupljeno: kolovoz 2024.]
48. Fortinet. *What Is SIEM?* Preuzeto s: https://www.fortinet.com/resources/cyberglossary/what-is-siem [Pristupljeno: kolovoz 2024.]
49. AWS. *What is Cloud Native?* Preuzeto s: https://aws.amazon.com/what-is/cloud-native/ [Pristupljeno: kolovoz 2024.]
50. Security Investigation. *Azure Sentinel for IT Security and its SIEM Architecture.* Preuzeto s: https://www.socinvestigation.com/azure-sentinel-for-it-security-and-its-siem-architecture/ [Pristupljeno: kolovoz 2024.]
51. Microsoft. *Microsoft Sentinel data connectors.* Preuzeto s: https://learn.microsoft.com/en-us/azure/sentinel/connect-data-sources?tabs=azure-portal [Pristupljeno: kolovoz 2024.]
52. Microsoft. *Visualize and monitor your data by using workbooks in Microsoft Sentinel.* Preuzeto s: https://learn.microsoft.com/en-us/azure/sentinel/monitor-your-data?tabs=azure-portal [Pristupljeno: kolovoz 2024.]
53. Microsoft. *Custom data ingestion and transformation in Microsoft Sentinel.* Preuzeto s: https://learn.microsoft.com/en-us/azure/sentinel/data-transformation
54. Microsoft. *Log analytics.* Preuzeto s: https://docs.microsoft.com/en-us/training/modules/intro-to-azure-sentinel/media/03-log-analytics.png [Pristupljeno: kolovoz 2024.]
55. Microsoft. *Create a scheduled analytics rule from scratch*. Preuzeto s: https://learn.microsoft.com/en-us/azure/sentinel/create-analytics-rules?tabs=azure-portal [Pristupljeno: kolovoz 2024.]

56. Microsoft. *Threat hunting in Microsoft Sentinel*. Preuzeto s: https://learn.microsoft.com/en-us/azure/sentinel/hunting?tabs=azure-portal [Pristupljeno: kolovoz 2024.]
57. Fortinet. *Technical Tip: FortiGate Integration with Microsoft Sentinel via AMA*. Preuzeto s: https://community..fortinet.com/t5/FortiGate/Technical-Tip-FortiGate-Integration-with-Microsoft-Sentinel-via/ta-p/324681 [Pristupljeno: kolovoz 2024.]
58. Microsoft. *Fortinet via Legacy Agent connector for Microsoft Sentinel*. Preuzeto s: https://learn.microsoft.com/en-us/azure/sentinel/data-connectors/deprecated-fortinet-via-legacy-agent [Pristupljeno: kolovoz 2024.]
59. Fortinet. *FortiNDR Cloud for Microsoft Sentinel*. Preuzeto s: https://docs.fortinet.com/document/fortindr-cloud/2024.6.0/fortindr-cloud-for-microsoft-sentinel/527351/overview [Pristupljeno: kolovoz 2024.]
60. TechTarget. *The history, evolution and current state of SIEM*. Preuzeto s: https://www.techtarget.com/searchsecurity/tip/The-history-evolution-and-current-state-of-SIEM [Pristupljeno: kolovoz 2024.]
61. SecurityIntelligence. *The future of SIEM: Embracing predictive analytics*. Preuzeto s: https://securityintelligence.com/posts/the-future-of-siem-embracing-predictive-analytics/ [Pristupljeno: kolovoz 2024.]
62. Clictadigital. *ChatGPT Capabilities and Limitations.* Preuzeto s: https://clictadigital.com/chatgpt-capabilities-and-limitations/ [Pristupljeno: kolovoz 2024.]
63. Exabeam. *AI SIEM: How SIEM with AI/ML is Revolutionizing the SOC*. Preuzeto s: https://www.exabeam.com/explainers/siem/ai-siem-how-siem-with-ai-ml-is-revolutionizing-the-soc/ [Pristupljeno: kolovoz 2024.]

POPIS SLIKA

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je Diplomski rad (*vrsta rada*) isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.
Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom

Istraživanje mogućnosti SIEM sustava i interoperabilnosti s alatima za zaštitu informacijsko-komunikacijskog sustava, u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, 19.09.2024.

Kristijan Tomas Tomas

(ime i prezime, *potpis*)