SBNZ – Projekat za maksimalnu ocenu 7

(pojednostavljeni BSEP-SBNZ projekta iz 2019)

2. SIEM

SIEM alata predstavlja softver koji posmatra proizvoljan softverski sistem u produkciji i prikuplja, normalizuje, filtrira i korelira događaje koje posmatrani sistem generiše tokom svog rada, kako bi detektovao, alarmirao i reagovao na potencijalne napade i bezbednosne probleme. Jedan primer ovakvog alata predstavlja SPLUNK.

SIEM alat vrši svoj posao centralizovanim skupljanjem i analizom log datoteka. Upotrebom sistema zasnovanim na pravilima, ovaj alat korelira događaje koji se dešavaju u sistemu u nekom vremenskom periodu i na osnovu njih odlučuje da li će okinuti nekakav alarm. Ilustrativan primer ove funkcionalnosti je detekcija i alarmiranje kada se deset puta u minutu izvrši prijava na sistem sa istim korisničkim imenom. SIEM se sastoji iz dve celine – SIEM centra i SIEM agenta.

2.1. SIEM centar

SIEM centar predstavlja glavni deo projektnog zadatka iz predmeta SBNZ. Ova aplikacija vrši obradu logova koje prihvata od agenata. Putem veb-interfejsa, operater i admin dobijaju uvid u određene podatke i pristup funkcionalnostima. SIEM centar treba da podrži sledeće funkcionalnosti:

- Prihvatanje i skladištenje logova dobavljanih od strane SIEM agenata.
- Operater i admin mogu da koriste funkcije prikaza i pretraga logova po različitim poljima, sa mogućnošću upotrebe regularnih izraza. Omogućiti pretragu logova i u radnoj memoriji rule engine-a.
- Operater i admin mogu da pregledaju alarme.
- Operater može da dodaje nova pravila za alarme i aktivnosti opisane ispod, gde dodavanje pravila ne sme da izazove prekid u radu SIEM centra.
- Rule templates, u vidu DSL-a kako bi admin mogao da definiše nova tipična pravila bez da poznaje Drools. Format pravila je: polje vrednost broj_pojava interval

- Operater i admin mogu da generišu izveštaja bitnih aktivnosti u određenom vremenskom periodu (broj logova po sistemu, broj logova po mašinama, broj alarma po sistemu, broj alarma po mašini, itd.).

Alarmi

Dizajniranje komponente za kreiranje i okidanje alarma predstavlja najveći izazov ovog sistema, gde je neophodno omogućiti kreiranje alarma koji se okida za proizvoljan broj konkretnih događaja u nekom vremenskom periodu. Ovo uključuje:

- Neuspešni pokušaji prijave na sistem na istoj mašini. Prijava može biti na nivou operativnog sistema ili na nivou simuliranog informacionog sistema;
- Neuspešni pokušaji prijave na sistem sa istim korisničkim imenom. Prijava može biti na nivou operativnog sistema na ili nivou simuliranog informacionog sistema;
- Pojava loga čiji tip je ERROR;
- Pokušaj prijave na nalog koji nije bio aktivan 90 ili više dana;
- 15 ili više neuspešnih pokušaja prijave na različite delove informacionog sistema sa iste IP adrese u roku od 5 dana;
- Prijavljivanje na sistem od istog korisnika na dva ili više dela informacionog sistema u razmaku manjem od 10 sekundi sa različitih IP adresa;
- Pojava loga u kome antivirsu registruje pretnju, a da u roku od 1h se ne generise log o uspešnom elimisanju pretnje;
- Uspešna prijava na sistem praćena sa izmenom korisničkih podataka ukoliko je sa iste IP adrese u poslednjih 90 sekundi bilo registrovano 5 ili više neuspešnih pokušaja prijavljivanja na različite naloge;
- U periodu od 10 dana registrovano 7 ili više pretnji od strane antivirusa za isti računar;
- Prijava ili pokušaj prijave sa IP adrese koje se nalazi na spisku malicioznih IP adresa;
- Pojava loga u kojoj se nalazi IP adresa sa spiska malicioznih IP adresa.

Omogućiti detekciju suviše učestalih zahteva (više od 50 u roku od 60 sekundi):

- Zahtevi bilo kog tipa aktiviraju alarm za DoS napad;
- Zahtevi koji su povezani sa podsistemom za plaćanja aktivira alarm za payment sistem;
- Zahtev koji su povezani sa prijavom korisnika aktiviraju brute-force alarm.

Navedeni alarmi su međusobno isključivi, gde se aktivira alarm sa najvećim prioritetom. Prioritet alarma se određuje tako što se broj zahteva određenog tipa pomnoži sa modifikatorom, gde su modifikatori: 1 za DoS, 3 za payment, 5 za brute-force napad.

Aktivnosti

SIEM centar omogućuje automatske reakcije na određene tipove alarma:

- SIEM omogućava klasifikovanje korisničkih naloga po riziku i to:
    - Low
      Korisnički nalog nije asociran sa alarmima u poslednjih 90 dana;
    - Moderate
      Korisnički nalog je asociran sa alarmima antivirusa u poslednjih 6 meseci,
      Korisnički nalog je ima više od 15 neuspešnih pokušaja prijavljivanja u poslednjih 90 dana;
    - High
      Korisnički nalog je asociran sa alarmima u poslednjih 30 dana pri čemu nalog ima administratorske privilegije,
      Korisnički nalog sa administratorskim privilegijama se uspešno prijavio na nalog van radnog vremena nakon 2 neuspešna pokušaja prijavljivanja;
    - Extreme
      Korisnički nalog je asociran sa alarmima antivirusa u poslednjih 6 meseci, pri čemu je pri poslednjoj prijavi registrovana barem dva neuspešna pokušaja prijavljivanja praćeno uspešnim prijavljivanjem i promenom podataka,
      Korisnički nalog ima prijavu sa IP adrese koja se nalazi na spisku malicioznih IP adresa;

  Napomena: Administrator može da izmeni klasifikaciju korisničkog naloga po riziku.
- Ukoliko sa iste IP adrese registruje 30 ili više neuspešnih pokušaja prijave na sistem u roku od 24h, dodati tu IP adresu u spisak malicioznih IP adresa;
- Generisanje spiska korisnika koji su izazvali barem 6 alarma u poslednjih 6 meseci na barem 3 različita dela informacionog sistema;
- Generisanje spiska korisnika koji su imali neuspešne prijave sa N[1] različitih IP adresa u poslednjih 12 sati;
- Generisanje spiska korisnika koji su asocirani sa barem 10 alarma antivirusa u periodu od 10 dana;
- Ispis delova informacionog sistema koji su generisali barem 5 alarma dok su na njima radili korisnici koji pripadaju High ili Extreme kategoriji rizika.

[1] N je promenljiva (broj) koju uz pomoć globala koristite u pravilu

2.2. SIEM agent

SIEM agent predstavlja jednostavnu aplikaciju koja se postavlja na računar čiji logovi žele da se prate. SIEM Agent generiše logove i šalje ih SIEM centru, potrebno je implementirati SIEM agente koje generišu logove u realnom vremenu kao i JUnit testove koje koriste pseudo clock.

Izvršiti modelovanje činjenica tako da se pokriju sva navedena pravila. SIEM centar treba da ima veb-interfejs.